

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

DOLBY LABORATORIES, INC.,
Petitioner,

v.

INTERTRUST TECHNOLOGIES CORPORATION,
Patent Owner.

IPR2020-00662
Patent 6,640,304 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 24 of U.S. Patent No. 6,640,304 B2 (Ex. 1001, “the ’304 patent”). Paper 13 (“Institution Decision”). 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”).

With our authorization (Paper 25), the parties submitted additional briefing regarding Exhibits 2037 and 2038, which Intertrust submitted with its Sur-reply and which relate to a claim construction issue.¹ Papers 26, 27.

We held an oral hearing on July 13, 2021, and the transcript is entered on the record. Paper 31 (“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 24 of the ’304 patent is unpatentable.

¹ Dolby asked for this briefing in lieu of moving to strike Exhibits 2037 and 2038 and associated text in the Sur-reply. *See* Paper 25 (citing Ex. 3002). In our decision, we have considered Exhibits 2037 and 2038, the associated passages in the Sur-reply, and the briefs (Papers 26 and 27) by both parties. *See infra* part III.B.1(b).

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.

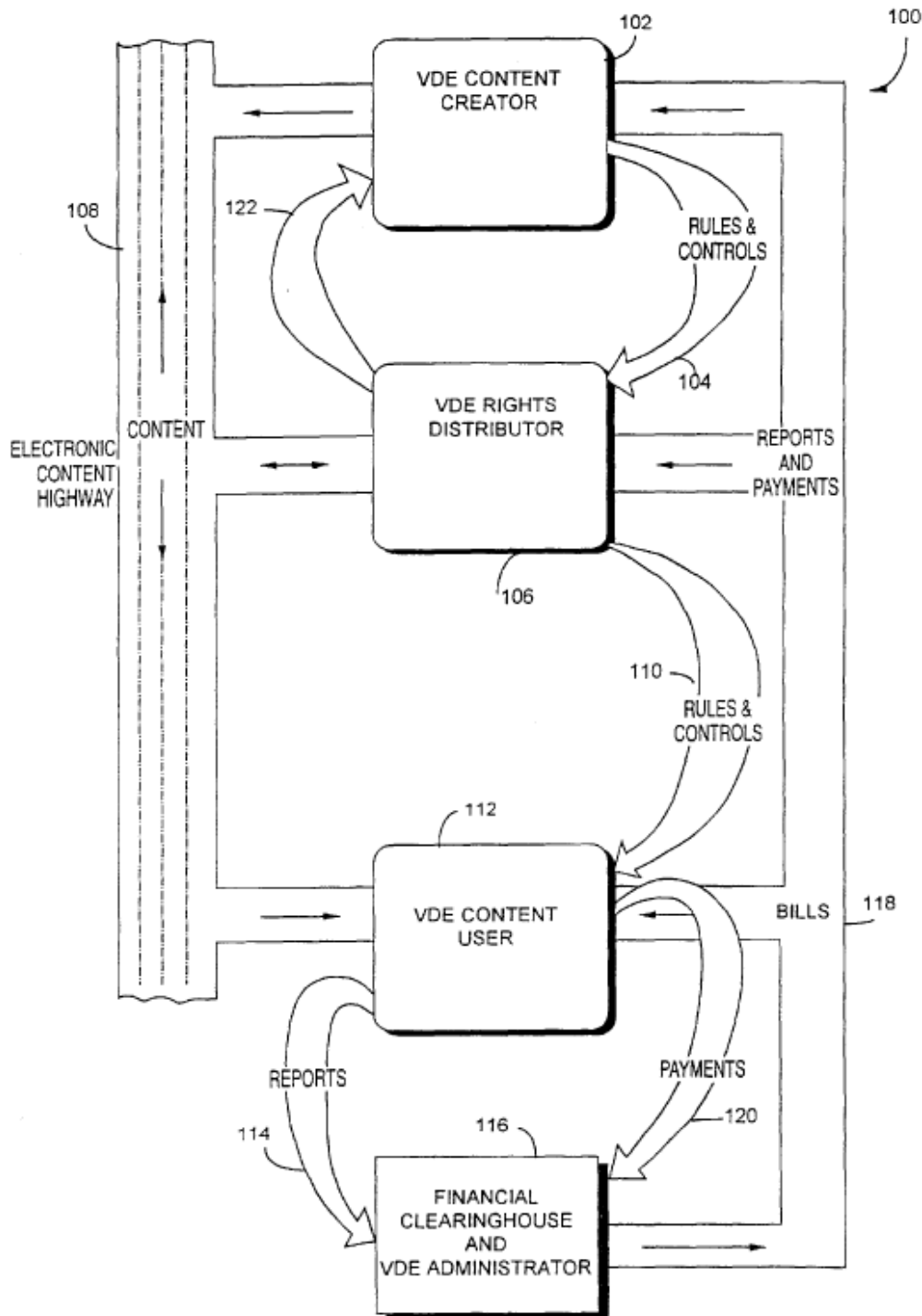
The parties also refer to a claim construction order in *Intertrust Technologies Corp. v. Microsoft Corp.*, 4:01-cv-01640 (N.D. Cal. terminated May 7, 2004) (“Microsoft Action”). PO Resp. 21–22 n.2; Exs. 2021–2022.

B. THE ’304 PATENT (EX. 1001)

According to the ’304 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, 2:44–47. The ’304 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 2:31–34.

Figure 2, below, illustrates how a VDE “may be used to provide a ‘chain of handling and control’ for distributing content.” Ex. 1001, 55:57–59.

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, 55:63–67. Arrow 104 illustrates how VDE content creator 102 may send these rules and controls to VDE rights distributor box 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 56:7–11. 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 56:14–18.

Figure 2 also illustrates financial clearinghouse 116 which receives content usage reports (arrow 114) and content usage payments (arrow 120) from VDE content user 112. *See* Ex. 1001, 56:19-25. Via “reports and payments” network 118, financial clearinghouse 116 may also send bills to VDE content user 112, and reports and payments to VDE rights distributor 106 and VDE content creator 102. *Id.* at 56:25–35.

The VDE “prevents use of protected information except as permitted by the ‘rules and controls’ (control information)” established for the VDE. Ex. 1001, 56:57–59; *see also id.* at Fig. 2. Such rules and controls may, for example, “grant specific individuals or classes of content users . . . ‘permission’ to use certain content. They may specify what kinds of content usage are permitted, and what kinds are not. They may specify how content usage is to be paid for and how much it costs.” *Id.* at 56:60–64. They may also “require content usage information to be reported back to the distributor . . . or content creator.” *Id.* at 56:65–67. In one embodiment, rules and controls can include (a) “[p]ermission record[s]” (PERCs), which contain security information; (b) “budgets,” which are methods that “specify, among other things, limitations on usage of information content . . . and how usage

will be paid for,” and (c) “other methods,” which may include, for example, “how usage is to be ‘metered,’ if and how content . . . and other information is to be scrambled and descrambled, and other processes associated with handling and controlling information content.” *Id.* at 59:34–65.

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, 57:60–63; *see id.* at 56:1–5 (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 57:63–65. 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, 60:7–10. One portion of this electronic appliance is a secure processing unit (“SPU”), which “stores important information securely.” *Id.* at 60:10–14. 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 64:6–9. The SPU “may also perform secure data management processes including governing usage of, auditing of, and where appropriate, payment for VDE objects.” *Id.* at 64:9–12.

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

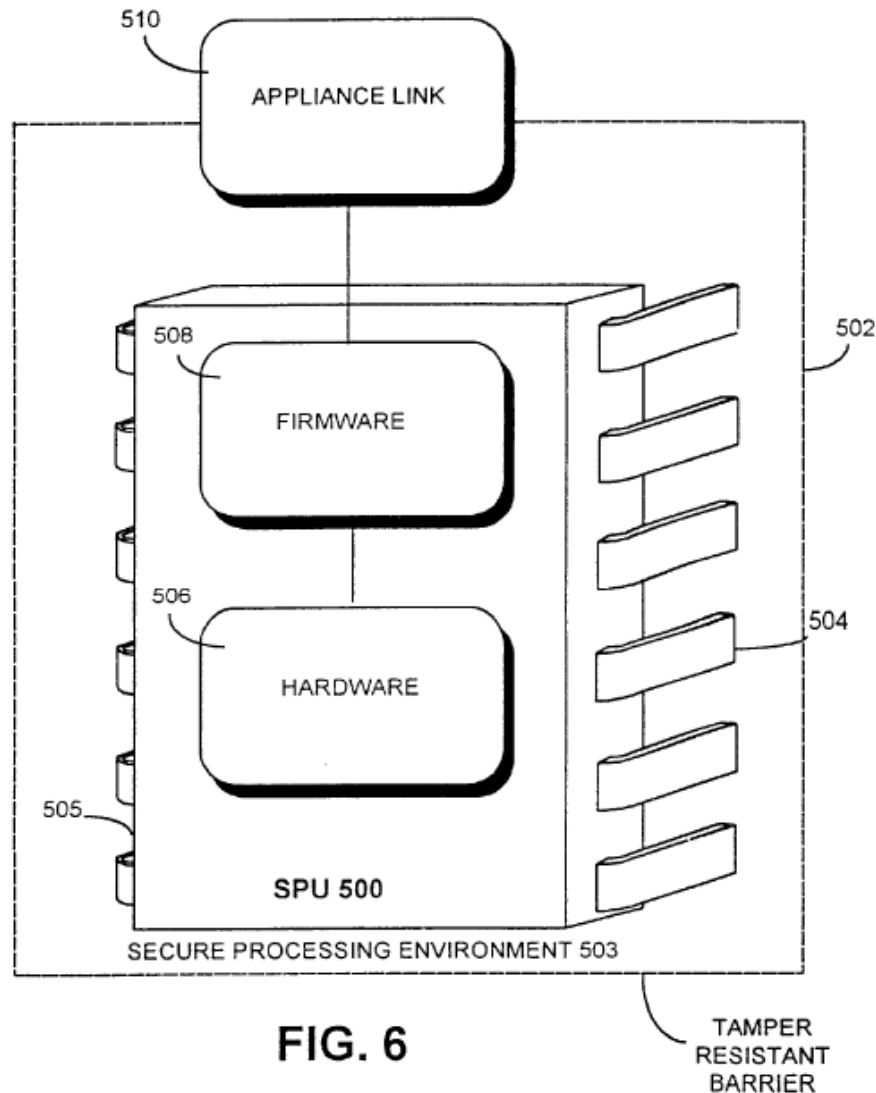


Figure 6, above, depicts SPU 500, which “is enclosed within and protected by a ‘tamper resistant security barrier’ 502” that “separates the secure environment 503 from the rest of the world.” Ex. 1001, 60:16–18. For example, tamper resistant barrier 502 can be “formed by security features such as ‘encryption,’ and hardware that detects tampering and/or destroys sensitive information within secure environment 503 when tampering is detected.” *Id.* at 60:24–28. “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 64:33–40. The SPU can also have other protections to deter tampering, such as obscuring the visual appearance of the conductors to deter visual inspection, a self-destruct mechanism, additional physical enclosures or metal layers, “security protections such as requiring password or other authentication to operate,” or shuffling data to varying memory locations. *See id.* at 64:53–65:19.

The ’304 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), 1:8–9.

C. CHALLENGED CLAIM AND ASSERTED GROUNDS OF
UNPATENTABILITY

Claim 24, the sole challenged claim, is as follows:

24. A method for monitoring use of a digital file at a computing system, the method comprising:

- [a] receiving the digital file;
- [b] receiving a first entity’s control information separately from the digital file;
- [c] using the first entity’s control information to govern, at least in part, a use of the digital file at the computing system; and
- [d] reporting information relating to the use of the digital file to the first entity;
- [e] wherein at least one aspect of the computing system is designed to impede the ability of a user of the computing system to tamper with at least one aspect of the computing system’s

performance of one or more of said using and reporting steps.

Ex. 1001, 327:42–328:15 (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
24	102(a) ²	Hornbuckle ³
24	103(a)	Katznelson, ⁴ Narasimhalu ⁵

Pet. 7.

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, 1019–1022, and 1024, and a declaration by

² 35 U.S.C. §§ 102(a), 103(a) (2006), *amended by* Leahy–Smith America Invents Act, Pub. L. No. 112-29 §§ 102, 103, sec. (n)(1), 125 Stat. 284, 286–87, 293 (2011) (effective Mar. 16, 2013). The 2006 versions of §§ 102 and 103 apply because the effective priority date of the ’304 patent is before the effective date of the AIA amendments. *See supra* part II.B.

³ Hornbuckle, US 5,388,211 (issued Feb. 7, 1995) (Ex. 1007).

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

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

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 24 of the '304 patent is unpatentable. 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 Prof. Black's testimony, Dolby argues that a person of ordinary skill in the art “would have been a person who has had 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. 13 (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. 13. 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 ’304 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 following three terms of claim 24: “control information,” “receiving . . . control information separately from the digital file,” and “impede the ability . . . to tamper with at least one aspect of . . . said using and reporting steps.” Pet. 15–18. Intertrust contends that we should also construe the terms “first entity’s control information” and “govern.” *See* PO Resp. 14–26. We address each of these terms below.

1. “control information”

Dolby argues that we should construe “control information” to include “information, such as executable code or associated data, related to controlling use of a digital file.” Pet. 15 (citing Ex. 1002 ¶¶ 57–58). To support its proposed construction, Dolby points to a passage in the ’304 patent stating that “VDEF load modules, associated data, and methods form a body of information that for the purposes of the present invention are called ‘control information.’” Pet. 16 (footnote omitted) (quoting Ex. 1001, 18:56–62). Dolby also points to four examples of control information listed in the patent:

Control information can determine, for example:

- (1) How and/or to whom electronic content can be provided, for example, how an electronic property can be distributed;
- (2) How one or more objects and/or properties, or portions of an object or property, can be directly used, such as decrypted, displayed, printed, etc[.];
- (3) How payment for usage of such content and/or content portions may or must be handled; and
- (4) How audit information about usage information related to at least a portion of a property should be collected, reported, and/or used.

Id. (quoting Ex. 1001, 46:42–55).

As Intertrust points out, the Texas defendants proposed the same construction in the Texas Actions, and made similar arguments, but the district court rejected that construction. *See* PO Resp. 14 (citing Ex. 2007, 33–40). The court held that “the patents do not suggest that information simply ‘related’ to control is ‘control information,’ as [the Texas] Defendants propose. Rather, ‘control information’ is something that can be enacted, information that is for controlling.” Ex. 2007, 38. As examples of control

information, the court noted that the '304 patent included permission records, budgets (including “how much of the total information content . . . can be used and/or copied”), and “security related information such as scrambling and descrambling ‘keys.’” *Id.* at 38–39 (quoting Ex. 1001, 59:35–65). According to the court, “[a]ll these examples of control information appear more than merely related to control, but actually are for control.” *Id.* at 39.

On the other hand, the court held that a plain reading of claim 24 indicates that “control information” is “broader than simply specifying permitted or prohibited uses.” Ex. 2007, 36. According to the court, the passage in the '304 patent stating that “VDEF load modules, associated data, and methods form a body of information that for the purposes of the present invention are called ‘control information’” is “definitional, not exemplary.” *Id.* at 38 (quoting Ex. 1001, 18:56–62). Thus, control information includes “load modules,” “associated data,” and “methods.” *Id.*

Based on this analysis, the court in the Texas Actions construed “control information” as follows: “information and/or programming controlling operations on or use of resources.” Ex. 2007, 40. The parties to that action, including Intertrust, agreed to this construction at the hearing without argument. *Id.* at 36.

We agree with the Texas court that the Texas Action defendants’ proposed construction of “control information,” now proposed by Dolby, is untenable for the reasons given by the court. In its Reply, Dolby does not explicitly contest the Texas court’s construction, but notes that after Intertrust filed its Response, the court in the California Action adopted a similar construction: “information and/or programming controlling

operations on or use of a digital file or electronic item.” Pet. Reply 1 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. Neither Dolby nor Intertrust contest that the controlled “resources” are specifically a digital file or electronic item. *See, e.g.*, Pet. Reply 1–2; PO Sur-reply 2–6, 15–24.⁶

In its Response (filed before the construction in the California Action), Intertrust argues “that ‘control information’ should be construed consistent with the Texas court’s construction.” PO Resp. 14. Particularly, Intertrust agrees with the Texas court’s reasoning that the scope of the term “control information” is narrower than merely information “related to” control. *See id.* at 17–19 (citing Ex. 2007, 28–39; Ex. 1001, 46:51–52, 56:63–64, 57:10–11, 58:46–57; Ex. 2026, 39:13–42:1, 89:12–15, 91:14–93:5; Ex. 2024 ¶¶ 63–66). Intertrust also agrees with the Texas court that control information must be “something that can be enacted, information that is for controlling.” *Id.* at 19–20 (emphasis omitted) (quoting Ex. 2007, 38) (citing Ex. 2007, 38–39; Ex. 2024 ¶ 67).

⁶ The court in the Microsoft Action also issued a third construction of “control information.” *See Intertrust Technologies Corp. v. Microsoft Corp.*, 275 F. Supp. 2d 1031, 1060 (N.D. Cal. 2003) (Ex. 2021). There, the California court construed the term as “[i]nformation and/or programming controlling operations on or use of resources (e.g., content) including (a) permitted, required, or prevented operations, (b) the nature or extent of such operations, or (c) the consequences of such operations.” 275 F. Supp. 2d at 1060. We regard this as essentially the same as the Texas court’s construction, except that it provides a list of specific, non-limiting examples.

However, in its Response, Intertrust proposes that we narrow the Texas court’s construction by specifying that control information (1) conveys some “permission, restriction, and/or condition”; (2) excludes simple cryptographic keys; and (3) if in the form of data, must have a tight association with its related programming. We address these issues in turn.

(a) “Permission, Restriction, and/or Condition”

Intertrust contends that the we should construe “control information” to “convey[] some permission, restriction, and/or condition that—in the form of information and/or programming—controls operations on or use of the protected content.” PO Resp. 15 (citing Ex. 2024 ¶ 61). According to Intertrust, the ’304 patent “provides numerous examples of control information that all prevent the use of protected information except as provided by the permissions, restrictions, and/or conditions that control operations on or use of the protected information.” *Id.* at 14–15 (citing Ex. 1001, 32:18–32, 32:56–61, 48:46–61, 56:35–65). And Intertrust contends that “[c]ontrol information does not include software or hardware that simply carries out instructions and processes necessary for the enforcement of such permissions, restrictions, and/or conditions.” *Id.* at 28 (citing Ex. 2024 ¶ 83); *see also id.* at 43–44 (citing Ex. 1001, 46:44–51, 55:6–10, 56:8–11, 56:14–16, 56:59–64, 58:60–67, 59:53–59; Ex. 2024 ¶ 106) (arguing that control information should, for example, dictate who is authorized, what can be done, how content is to be paid for, or how many times the content can be accessed).

Intertrust contends that its proposal is consistent with the Texas court’s holdings in the following ways: (1) it allows control information to “do[] more than simply specify permitted or prohibited uses,” PO Resp. 15–

16 (quoting Ex. 2007, 39) (citing Ex. 2026, 56:13–57:5; Ex. 2024 ¶ 62); (2) it is more specific than information that is merely “related to” controlling operations on or use of resources, such as “an input that is received and used by control information to determine whether to grant or deny a use of protected content,” *id.* at 17–19 (citing Ex. 2024 ¶ 66);⁷ and (3) it is consistent with the Texas court’s determination that control information must be “something that can be enacted, information that is for controlling,” because “the Texas court clearly did not rule that control information includes *any* enactable information that plays *some* part in determining whether to grant access to a file (such as an input),” *id.* at 19–20 (quoting Ex. 2007, 38) (citing Ex. 2024 ¶ 67).

We do not agree with Intertrust that the Texas (or California) court’s construction is consistent with further limiting the term to information or programming that conveys some permission, restriction, or condition. The Texas court held, and we agree, that the ’304 patent includes a definitional passage indicating that control information includes not just a “load module,” but “data associated with the load modules” and “the control methods formed from [aggregating] the load modules.” Ex. 2007, 38 (quoting Ex. 1001, 18:56–62). At least some of the data and methods

⁷ Intertrust argues that the language “using the first entity’s control information to govern, at least in part, a use of the digital file” found in claim 24, “does not broaden the scope of the preceding ‘control information’ to include information that is merely *related to* control information.” PO Resp. 20–21 (citing Ex. 2024 ¶ 68); Ex. 1001, 328:5–6. We agree that “at least in part” does not broaden the scope of “control information,” because it reflects an independent limitation.

associated with the load modules might happen to convey a permission, restriction, or condition, as reflected in many of the examples in the '304 patent. But the definitional passage in the '304 patent does not limit the type of data and control methods that may constitute control information, so long as these control elements can be enacted *for* controlling operations on, or use of, digital content items. *See* Ex. 1053, 39; *see also* Ex. 1001, 18:63–65 (“VDEF transaction control elements reflect and enact content specific and/or more generalized administrative . . . control information.”).

(b) Cryptographic Keys

Intertrust also contends that we should construe the term “control information” to exclude a simple cryptographic key. *See* PO Resp. 21–23. However, according to Dolby, Intertrust admitted during the Microsoft Action “that a key is an example of control information.” Pet. 27 (citing Ex. 1003, 1369–70).

As background, the '304 patent and related patents disclose a tamper resistance scheme for the SPU that “disables a portion or all of SPU 500 or *associated critical key and/or other control information* in the event of tampering.” Ex. 1001, 172:4–14 (emphasis added); *accord* Ex. 2022, 24 ¶ 85, item 8(F) (quoting related US 6,253,193, 169:5–13). In the Microsoft Action, Intertrust referred to this passage in its opening claim construction brief, stating that “[c]ontrol information can consist of either programming (e.g., load modules) or data. *See, e.g.,* 8(D) (load modules, data and methods), 8(F) (*a key is control information*),” Ex. 1003, 1369 (emphasis added). During prosecution of the '304 patent, the applicant submitted these contentions “to inform the Examiner of the status of the litigation case between InterTrust and Microsoft.” Ex. 1003, 885. So a person of ordinary

skill in the art would have been aware of this admission by examining the prosecution history of the '304 patent.

Addressing this admission in the Texas Actions, the court declined to “rule as a matter of claim construction that all keys are control information.” Ex. 2007, 40. The court found that Intertrust’s admission “did not represent that any key is control information, rather it represented that ‘a key’ is control information, referring back to the ‘associated critical key’ described in the [patent disclosure].” PO Resp. 23 (quoting Ex. 2007, 39–40).

Intertrust urges us to reevaluate its admission, because it “was an error.” PO Resp. 22. Intertrust asserts that, instead of “a key is control information,” the statement should have read “key information is control information.” *Id.* Thus, Intertrust makes a distinction between a “key” and “key information.” According to Intertrust, “while ‘control information’ includes at least some types of key information, it does not include a simple cryptographic key.” *Id.* (citing Ex. 1001, 172:6–14, 210:40–62; Ex. 1003, 1369; Ex. 2022, 25 ¶ 8(F); Ex. 2024 ¶ 70). Instead, Intertrust contends that only “key information” can be control information. *See* PO Resp. 41 (citing Ex. 2024 ¶ 101) (arguing that the phrase “associated critical key and/or other control information” should be read as “associated critical key . . . information”).

We disagree. Based on the most straightforward reading of the phrase “associated critical key and/or other control information,” we agree with the Texas court that a person of ordinary skill in the art would have understood this phrase to indicate that an SPU’s associated critical key is an example of control information. *See* Ex. 2007, 39–40. We also find persuasive Dolby’s argument that what the '304 patent calls “key information” includes the

encryption key itself: “[k]ey information may be the actual decryption key to be used to decrypt the content, or it may be information from which the decryption key may be at least in part derived or calculated.” Pet. Reply 10–11 (alteration in original) (emphasis omitted) (quoting Ex. 1001, 196:24–27) (citing Ex. 1001, 196:1–34). Thus, even if we were to read the phrase “associated critical key and/or other control information” as “associated critical key . . . information,” a person of ordinary skill in the art would have understood this key information to include the key itself.

In our Institution Decision, we mentioned that, in addition to the “associated critical key,” the ’304 patent also describes “scrambling and descrambling ‘keys’” as part of the control information. Paper 13, 31 (quoting Ex. 1001, 59:50–52) (citing Ex. 1001, 59:34–35, 67:55–68:35, 121:60–123:16). These scrambling and descrambling keys are part of a permissions record (“PERC”), which the ’304 patent identifies as an example of “rules and controls.” Ex. 1001, 59:35–52.

Intertrust addressed this issue in its Response. *See* PO Resp. 38–40 (citing Paper 13, 31). Although Intertrust does not dispute that a PERC contains control information, Intertrust disagrees that encryption keys are part of that control information. *See* PO Resp. 40 n.8. According to Intertrust, the Texas court declined to hold that all keys—which would include the PERC keys—are control information. *See* PO Sur-reply 12–13 & n.6. Intertrust also argues that the ’304 patent does not actually disclose that scrambling and descrambling keys are part of the PERC, only that the PERC *identifies* the scrambling and descrambling keys, and the PERC includes methods that “are *not* rules and controls at all”; rather, according to

Intertrust, they “define basic operations *used by* ‘rules and controls.’” PO Resp. 38 (citing Ex. 2024 ¶ 97).

Intertrust also contends that, when describing the structure of a PERC, the ’304 patent refers to scrambling and descrambling keys, but “does not mean that the actual scrambling/descrambling keys constitute rules and controls.” PO Resp. 38–39 (citing Ex. 1001, 59:40–52; Ex. 2024 ¶ 98). And according to Intertrust, the scrambling or descrambling keys are stored in “key blocks” within the PERC structure, and not in the same location as other parts of the PERC containing methods that defines “rights” or controls how an object exercises a right. *See id.* at 39–40 (citing Ex. 1001, 129:35–44, 130:41–49, 130:61–64, 151:26–39, 151:61–64, 153:9–14, 154:47–54; Ex. 2024 ¶ 99). Intertrust characterizes the PERC keys as merely “related to” the control information (the code), rather than being part of the control information itself. *See id.* at 40 & n.8 (citing Ex. 2024 ¶ 100; Ex. 2025, 8–9; Ex. 2026, 43:2–45, 45:13–10); *see also* PO Sur-reply 13–14 (citing Ex. 1001, 28:5–7, 59:41–48, 59:60–64, 151:26–39, 153:9–14, 327:42–328:41 (claim 31, requiring that a decryption key is stored on the computing system); Ex. 2024 ¶ 99).

Responding to Intertrust’s arguments in its Reply, Dolby argues that the scrambling and descrambling keys are part of the “rules and controls” and are described as part of the “rights” and “important key information” that the system uses for control of the digital content. Pet. Reply 10–12 (citing Ex. 1001, 56:57–59, 59:5–9, 59:50–52, 130:61–64, 135:8–12, 156:4–7, 156:18–21).

In its Sur-reply and in subsequent briefing, Intertrust contends that Dolby’s argument in its Reply is untimely. PO Sur-reply 11–12; Paper 27, 1–

2. We disagree, because as Dolby correctly notes in the additional briefing, the Petition did identify the PERC as part of the control information, and specifically listed the scrambling and descrambling keys as part of the PERC’s “rights and usage information.” Paper 26, 1 (citing Pet. 8–9). We also agree with Dolby that its argument in the Reply is not a departure from its general position in the Petition that control information may include encryption keys. *See* Paper 26, 1–2.

Having considered the parties’ contentions, we find Dolby’s arguments persuasive that a person of ordinary skill in the art would have understood a PERC’s scrambling and descrambling keys to be control information. *See* Pet. Reply 10–12 (citing Ex. 1001, 56:57–59, 59:5–9, 59:35–37, 59:50–52, 130:57–64, 135:8–12, 156:4–7, 156:18–21, 196:1–34; Ex. 2007, 38–39). First, the ’304 patent specifically describes a PERC as being (not just containing) control information. *See* Ex. 1001, 59:35–37 (“[C]ontainer 302 may . . . contain ‘rules and controls’ *in the form of*: (a) a ‘Permissions record’ 808” (emphasis added)). The Texas court held, and we agree, that a PERC is an “example[] of control information” that is “more than merely related to control,” but actually is for control. Ex. 2007, 39 (citing Ex. 1001, 59:35–65).

Second, we disagree with Intertrust that the ’304 patent’s disclosure suggests that the scrambling or descrambling keys are excluded from what the ’304 patent considers to be control information. Although the keys, themselves, are not control methods, they are no less crucial than the control methods in controlling access to the electronic content. *See* Ex. 1001, 196:24–25; Pet. Reply 11 n.4.

Alternatively, Intertrust argues that only a “critical key” (which Intertrust defines as a “private key”) can be control information. *See* PO Resp. 41 (citing Ex. 2024 ¶ 102). This is based on Dr. Jakobbbson’s opinion that a person of ordinary skill in the art would have understood that the SPU’s “associated critical key” is a private key, which is “distinctly different than content decryption keys that are received at the SPU from external sources, such as other devices.” Ex. 2024 ¶ 102.

Dr. Jakobbbson does not explain the basis for his opinion or cite to any other evidence. *See* Ex. 2024 ¶ 102. But even if we accept his statement as true, Dr. Jakobbbson’s distinction between the two types of keys has to do with how they are received: he does not testify that, once received, a private key is anything other than a simple cryptographic key. Also, Intertrust has not identified anything in the ’304 patent that makes such a distinction between types of keys. The ’304 patent appears to encompass using a broad range of encryption or decryption technologies and key types. *See* Ex. 1001, 67:55–68:35, 121:60–123:16.

Thus, having considered all the evidence of record concerning this issue, we determine that a person of ordinary skill in the art would have regarded a simple cryptographic key as control information, provided the key is part of the information that is actually enacted for controlling operations on or use of a digital file or electronic item.

(c) Associated Data

Intertrust also argues that, if control information is in the form of data, it must have a tight association with its related programming. *See* PO Resp. 23–24. Intertrust points out that the Texas court excluded information that was merely “related” to control. PO Resp. 24 (citing Ex. 2027, 38).

Consistent with this, Intertrust contends that “the [’304] patent discloses a tight ‘association’ between load modules and data wherein execution of the load module/program and its associated data together ‘run as control methods’ that might specify, for example, ‘how usage will be paid for.’” PO Resp. 23.

We agree with Intertrust that data does not become control information simply because it is associated with or related to programming, such as a load module. But we disagree that a person of ordinary skill in the art would have understood that it is the “tightness” of its association with the load modules that makes such data control information. Rather, the data is control information because the load module uses or manipulates it for controlling operations or use of the digital content. *See, e.g.*, Ex. 1001, 142:38–41 (data structures associated with a load module may be stored either within the load module or in a separate database), 146:44–147:18 (table listing “some of the more commonly occurring data structures for METER and BUDGET methods,” and stating that “load modules . . . create and manipulate the data structure” in this table⁸); *see also* Ex. 1003, 1369–70 (Intertrust arguing, in the Microsoft Action, that control information may include “mediating data” or “parameter data”). The ’304 patent defines

⁸ The data items in this table appear to enact the function of a “budget” or “metering” control, which can specify things like “limitations on usage of information content,” “how much of the total information content . . . can be used and/or copied,” limitations that “prevent use of more than the amount specified by a specific budget,” or limitations that “control how information content is to be charged based on ‘metering.’” Ex. 1001, 59:53–60:1; *see also id.* at 20:50–53 (“[R]equired load modules and data . . . might specify that sufficient credit from an authorized source must be confirmed as available.”).

control information by its function, rather than by its structure. *See* Ex. 1001, 141:45–46 (the static data associated with a load module is “functionally the equivalent” of the load module’s code).

Intertrust also argues that associated “information that is merely *used* by . . . control information [i.e., something that conveys a permission, restriction, or condition] in order to determine an outcome (*e.g.*, whether to grant access or not) is not itself control information, and is instead, at best *related* to the control information.” PO Resp. 43–44 (citing Ex. 1001, 46:44–51, 55:6–10, 56:8–11, 56:14–16, 56:59–64, 58:60–67, 59:53–59; Ex. 2024 ¶¶ 105–106) (arguing that control information should, for example, dictate who is authorized, what can be done, how content is to be paid for, or how many times the content can be accessed). For example, according to Intertrust, something in the nature of an input or operand to a permission, restriction, or condition would not be control information. *See id.* at 44–46 (citing Ex. 2024 ¶ 107).

Intertrust contends that, during cross-examination, Dr. Black “admit[ted] that while program code, for example, could be control information that controls operations on or use of a resource, *inputs* to such program code that the program code takes and processes to take a certain action are merely *related* to the control information.” PO Resp. 44 (citing Ex. 2026, 39:13–42:1). We do not agree that this fairly reflects his testimony,⁹ because immediately after the quoted portion of his transcript, he

⁹ In the cited passage, Dr. Black appears to be responding to a question asking him to compare his proposed construction (“information, such as executable code or associated data, related to controlling use of a digital file,” *see* Ex. 1002 ¶ 57) with a construction similar to that of the California Action: “information that controls use of a digital file.” *See* Ex. 2026, 39:2–

clarified it by distinguishing between an “input to the code [that] controls use of a digital file [by] influenc[ing] the controlling of the file,” and “an input that’s completely disregarded or inconsequential.” Ex. 2026, 42:11–15. It was the *latter* to which he said “maybe I wouldn’t consider such an input to be control information under this construction.” *Id.* at 42:15–17.¹⁰

Intertrust also points to a passage in which Dr. Black appears to have agreed that there is a distinction between a rule that “a user has to be over 21 years or older to use the content,” and a birthdate that someone inputs into an access device. Ex. 2026, 89:13–14, 92:20–22. When asked whether the date of birth is a “rule,” he replied, “Probably not unless we’re construing rule in the same way that we construed control information before to be related to control information, but colloquially if you said my date of birth is X, Y, Z, I wouldn’t say that that in and of itself is a rule.” *Id.* at 93:25–93:5; *see also* PO Sur-reply 21.

It appears, from his answer and the context, that Dr. Black is answering the question based on the colloquial sense of the word “rule.” But the ’304 patent does not use the term “rule” in its colloquial sense when it defines “rules and controls” to be synonymous with “control information.” *See* Ex. 1001, 56:57–59. Likewise, the Texas court construed the term “rule”

16. We find reasonable Dolby’s characterization that Dr. Black’s response “suggest[ed] a difference in the manner of control (i.e., that the information in the latter case perhaps would be executable program code, because it took action, and the latter included data helpful in controlling use of the digital file.” Pet. Reply 14 n.6.

¹⁰ Dr. Black’s reference to “this construction” relates to the construction that Intertrust’s counsel posed as part of the question: “information that controls use of a digital file.” *Id.* at 39:15–16.

the same as “control information,” which does not reflect the colloquial meaning of the word “rule.” *See* Ex. 2007, 33. So we do not agree that Dr. Black’s opinion as to whether an input is a “rule,” in the colloquial sense, undermines his other testimony that an input such as an “amount of credit extended to [a] user” would be control information, in the context of the ’304 patent, if that input were used in a comparison with the cost of a file in order to determine whether the user should have access to the file. Ex. 1002 ¶ 134.

Having considered the parties’ arguments above, we agree with the construction of “control information” in the California Action, and we determine that the evidence does not support narrowing that construction as Intertrust proposes. Thus, we construe the term “control information” to mean “information and/or programming controlling operations on or use of a digital file or electronic item.” Ex. 1053, 8–11.

2. *“receiving . . . control information separately from the digital file”*

In the Texas Actions, the court adopted the parties’ agreed construction of “receiving . . . separately”¹¹ as meaning “receiving over different paths, or from different sources, or at different times.” PO Resp. 24 (citing Ex. 2001, 1; Ex. 2007, 12). But in this proceeding and in the California action, Dolby (who was not a party to the Texas actions) proposed a slightly different construction of “receiving . . . control information separately from the digital file” to include “receiving a first entity’s control

¹¹ The term “receiving . . . separately” was an abbreviated form of the term proposed here and in the California Action.

information in a different package and/or via delivery at a different time, over a different path, or from a different source, from the digital file.”

Pet. 17 (citing Ex. 1002 ¶¶ 22–24, 59–61); Pet. Reply 2 n.2 (citing Ex. 1053, 11–16).

In the California Action, Intertrust proposed the same agreed construction from the Texas Actions: “receiving over different paths, or from different sources, or at different times.” PO Resp. 24; Ex. 1053, 11.

According to the California court, the parties agreed that the term “should be construed to include receiving delivery at a ‘different time,’ over a ‘different path,’ or from a ‘different source,” and “[t]he dispute centers on whether the term also covers receiving ‘in a different package.’” Ex. 1053, 12 (quoting Intertrust’s opening brief) (citing Dolby’s responsive brief). The California court agreed with Dolby and construed the term as “receiving in a different package and/or via delivery at a different time, over a different path, or from a different source.” *Id.* at 11, 15–16.

Because the question of whether control information is received “in a different package” is not material to the issues presented in this case, and the parties are otherwise in substantial agreement as to the meaning of this term, we agree with Intertrust that we do not need to construe the term for this decision. *See* PO Resp. 24 (citing Ex. 2024 ¶ 73; *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.’”)).

3. *“impede the ability . . . to tamper with the at least one aspect of . . . said using and reporting steps”*

Dolby proposes that we should construe the term “impede the ability . . . to tamper with the at least one aspect of . . . said using and reporting steps” such that (1) “tampering applies to any ‘aspect’ of” either the using or reporting steps; (2) “[t]he ‘using’ step recites ‘using the first entity’s control information to govern, at least in part, a use of the digital file at the computing system’”; and (3) “the ‘reporting’ step recites ‘reporting information relating to the use of the digital file to the first entity.’” Pet. 18 (citing Ex. 1002 ¶¶ 22–24, 62–63).

Intertrust argues that “construction of this phrase is not necessary to resolve the parties’ controversy.” PO Resp. 24–25. We agree, because these issues are not dispositive in this case. *See Nidec*, 868 F.3d at 1017.

4. *“first entity’s control information”*

In the Texas Actions, Intertrust argued that the term “first entity’s control information” has its plain and ordinary meaning. Ex. 2007, 53. The court stated that the term “plainly denotes that the control information belongs to the first entity,” and that “the parties and their experts agree that ‘first entity’s’ indicates that control information is possessed by the first entity,” although “there may be a variety of ways in which the information might belong to the first entity.” *Id.* at 55–56. Nevertheless, the court held that “the term has its plain and ordinary meaning without the need for further construction.” *Id.* at 56.

In this proceeding, Intertrust argues that we should construe “first entity’s control information” to mean “control information that belongs to a first entity.” PO Resp. 25. According to Intertrust, this construction “is

consistent with the teachings of the '304 patent that one or more entities may supply control information to control the use of the same content,” and that they may do so independently. *Id.* (quoting Ex. 1001, 10:60–63) (citing Ex. 1001, 10:65–67). Intertrust also notes that the term “first entity’s” is possessive. *Id.* (citing Ex. 2024 ¶¶ 74–79).

Dolby agrees that the plain and ordinary meaning of the term “first entity’s control information” may indicate that the control information belongs to the first entity. Pet. Reply 2. But Dolby disagrees with how Intertrust applies the term to the elements of Hornbuckle, as we will discuss in more detail below. *See id.* According to Dolby, because the full limitation is “receiving a first entity’s control information separately from the digital file,” this “only requires that the control information belong to the first entity at the time it is transmitted/received.” Pet. Reply 7–8 (citing Ex. 1001, 10:60–63, 10:65–67). Dolby argues that “[i]n no way does the '304 patent explicitly require that the control information must forever ‘belong’ to the first entity.” *Id.* at 8 (footnote omitted).

Because the parties are in agreement, and agree with the Texas court that the term “first entity’s control information” indicates that the control information “belongs” to the first entity, we do not need to adopt Intertrust’s proposed explicit construction for this decision. *See Nidec*, 868 F.3d at 1017. Intertrust’s proposed construction says nothing about the parties’ disputed issue, which is *when* and *how* the control information belongs to the first entity.

On that point, however, we find persuasive Dolby’s argument that nothing in claim 24 or the '304 patent requires that control information must belong to the first entity after the first entity delivers the control information

to other entities in the VDE. *See* Pet. Reply 8. As Intertrust acknowledges, the '304 patent teaches “that one or more entities may supply control information to control the use of the same content.” PO Resp. 25. The information “belongs” to them when they supply it, and after that point, the control information still reflects the interests of the entity who submitted the control information. *See* Ex. 1001, 57:2–4 (“‘Rules and controls’ define the respective rights and obligations of each of the various VDE participants.”). But it is the computing system recited in claim 24, not the first entity, that ultimately applies the submitting (“first”) entity’s control information to govern the digital content’s usage. *See* Ex. 1001, 328:2–7; *see also id.* at 57:24–26 (“‘Rules and controls’ may ‘persist’ as they pass through a ‘chain of handling and control,’ and may be ‘inherited’ as they are passed down from one VDE participant to the next.”).

5. “govern”

Intertrust argues that the term “govern” has its plain and ordinary meaning as it appears in claim 24, which according to Intertrust means “control.” PO Resp. 26 (citing Ex. 1001, 15:66–16:3, 130:57–61, 153:42–52, 328:5–7; Ex. 2024 ¶ 80). In response, Dolby agrees with Intertrust that the term “should be given its plain and ordinary meaning,” but argues that this meaning “does not require explicit construction.” Pet. Reply 2.

We agree with the parties that the term “govern” has its ordinary and customary meaning in claim 24. But we do not consider the word “control” to be any more enlightening as to that meaning than the word “govern” itself. Also, construing the term “govern” in that way would not resolve any contested issues that either party has identified in this proceeding. Therefore,

we do not need to construe the term “govern” explicitly for this decision. *See Nidec*, 868 F.3d at 1017.

C. GROUND BASED ON HORNBUCKLE

Dolby alleges that claim 24 is unpatentable under 35 U.S.C. § 102(a) as anticipated by Hornbuckle. Pet. 7, 19–35.

To establish anticipation, a petitioner must find each and every element in a claim, arranged as recited in the claim, in a single prior art reference. *See Net MoneyIN, Inc. v. VeriSign, Inc.*, 545 F.3d 1359, 1369 (Fed. Cir. 2008). The limitations may be present in the reference “either explicitly or inherently.” *In re Schreiber*, 128 F.3d 1473, 1477 (Fed. Cir. 1997). Further, an anticipating prior art reference must be enabling and must describe the “claimed invention sufficiently to have placed it in possession of a person of ordinary skill in the field of the invention.” *See Helifix Ltd. v. Blok-Lok, Ltd.*, 208 F.3d 1339, 1346 (Fed. Cir. 2000).

When evaluating a single prior art reference in the context of anticipation, we consider the reference “together with the knowledge of one of ordinary skill in the pertinent art.” *In re Paulsen*, 30 F.3d 1475, 1480 (Fed. Cir. 1994) (citing *In re Samour*, 571 F.2d 559, 562 (CCPA 1978)).

Based on these considerations, Dolby has shown that Hornbuckle anticipates claim 24 under 35 U.S.C. § 102(a). We present our findings below.

1. *Overview of Hornbuckle*

Hornbuckle describes “a system for renting computer software which derives use and billing information, prevents unauthorized use, maintains integrity of the software and controls related intercomputer

communications.” Ex. 1007, code (57). Hornbuckle’s Figure 1, reproduced below, shows an example of this system:

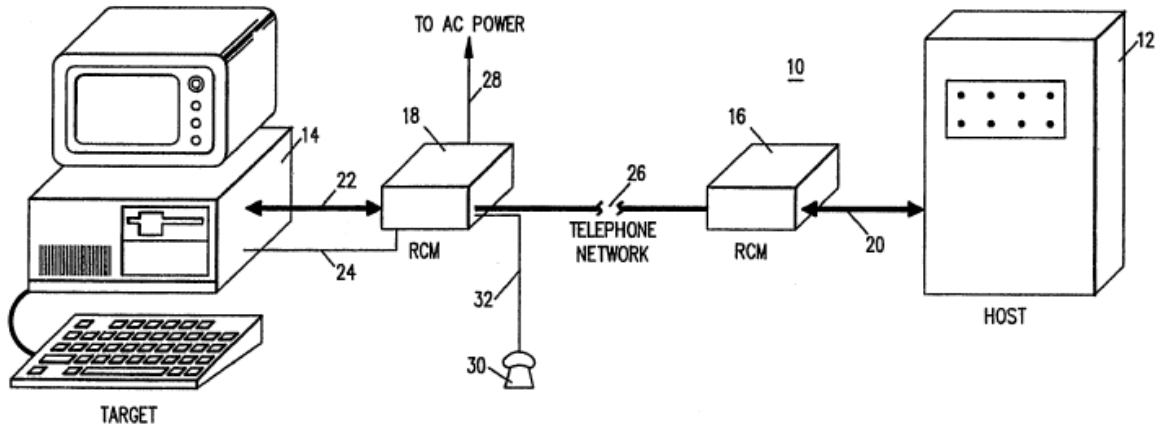


FIG. 1

Figure 1, above, depicts software rental system 10 comprising host computer 12, target computer 14, and remote control modules (“RCMs”) 16 and 18, each connected to host computer 12 and target computer 14, respectively, via serial lines 20 and 22. *Id.* at 4:45–52. RCMs 16 and 18 communicate with each other over public switched telephone network 26. *Id.* at 4:57–58.

Host computer 12 can transmit software to target computer 14, can receive customer usage data from the target computer’s RCM 18, and can perform “various accounting and software rental business functions.” Ex. 1007, 5:5–10. When host computer 12 transmits the software, it also sends an encrypted “key module” and an operating system patch (“OSP”) module. *Id.* at 11:57–61. Alternatively, the key module, the OSP module, and the remaining unencrypted rental software “may be sent to the customer on floppy disks or magnetic tape by mail or other delivery service.” *Id.* at 11:61–64.

The OSP module modifies the operating system of target computer 14 to ensure the rental software’s security. Ex. 1007, 11:35–38. When a user of

target computer 14 runs the rented software, the OSP module “initiates decryption of the encrypted key module of the rental software package by . . . RCM 18, then loads the decrypted key module into the internal memory . . . of the target computer 14 for execution.” *Id.* at 11:45–48. The OSP module also periodically “communicates with the RCM 18 to provide verification that it is still connected to the target computer 14 for security and accounting purposes.” *Id.* at 11:49–53. At the end of the rental period, or if RCM 18 becomes disconnected from target computer 14, the OSP module erases the rental software package, including the key module, from the RAM of target computer 14. Ex. 1007, 13:14–20, 13:38–44.

2. *Claim 24*

Below, we address Dolby’s evidence for why Hornbuckle discloses the preamble and each limitation of claim 24, and Intertrust’s responsive arguments.

(a) Preamble

The preamble recites “[a] method for monitoring use of a digital file at a computing system.” Ex. 1001, 327:42–43. Dolby does not assert that the preamble is limiting, but to the extent that it is, Dolby argues that Hornbuckle’s system performs such a method, and monitors use of digital files through target computer 14’s RCM 18. Pet. 25–26 & n.5 (citing Ex. 1007, code (57), 1:15–16, 1:24–28, 3:31–36; Ex. 1002 ¶¶ 79–80, 97).

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*, 868 F.3d at 1017.

(b) Limitation 24a

Limitation 24a recites “receiving the digital file.” Ex. 1001, 328:1. Dolby points to passages in Hornbuckle describing how Hornbuckle’s host computer 12 transmits software to target computer 14 as disclosing this limitation. Pet. 26–27 (citing Ex. 1007, 5:5–10, 10:27–42, 11:38–45, 11:64–12:2; Ex. 1002 ¶¶ 81–82, 97).

Intertrust does not contest Dolby’s contentions regarding limitation 24b. We find Dolby’s arguments and supporting testimonial evidence persuasive.

(c) Limitations 24b and 24c

Limitation 24b recites “receiving a first entity’s control information separately from the digital file.” Ex. 1001, 328:2–3. Limitation 24c recites “using the first entity’s control information to govern, at least in part, a use of the digital file at the computing system.” Ex. 1001, 328:5–7.

Dolby contends that Hornbuckle’s OSP module and associated encryption key are each “control information” as recited in limitations 24b and 24c. Pet. 27, 30.

As to limitation 24b, Dolby contends (1) that any of the components of the rental package (including the OSP and the encryption key) may be sent to the customer by mail on electronic media; (2) that target computer 14 may download the OSP module before (and thus “separately from”) downloading the rental software; and (3) that the encryption key may be transmitted separately. Pet. 28, 30 (citing Ex. 1007, 11:57–12:2, 13:35–40, 13:53–58, 13:62–64). Putting aside the issue of whether the OSP and

encryption key are control information, Intertrust does not contest these aspects of Dolby's argument, and we find them persuasive.

As to limitation 24c, Dolby contends that target computer 14 uses the OSP module and encryption key "to govern use of the digital file (e.g., the digital file cannot be accessed without a corresponding encryption key and if the OSP module does not initiate decryption)." Pet. 24; *see also id.* at 30–32 (claim chart). Intertrust does not contest Dolby's assertion in this respect, and we find it persuasive.

However, Intertrust disputes that either the OSP module or the encryption key are "control information" as recited in claim 24, and alternatively, to the extent that Hornbuckle's OSP is control information, Intertrust argues that it no longer continues to be "the first entity's control information" after the OSP is applied to target computer 14's operating system. *See* PO Response 27–42. We address these issues below.

(1) Whether the OSP Module is Control Information

Dolby contends that "[t]he OSP module is control information that, when activated, initiates decryption by fetching the encrypted key module and sending it to data encryption/decryption module 70 of RCM 18, where the key module is decrypted by the encryption key." Pet. 22 (citing Ex. 1007, 12:64–13:3). Then Dolby argues that "the OSP module loads the decrypted key module into the internal memory of the target computer 14 for execution." *Id.* (citing Ex. 1007, 11:45–48, 13:4–6). According to Dolby, "when execution of the rental program is complete, the OSP module erases the rental program including the key module from the [random access memory] of target computer 14, and notifies RCM 18 that the period of use

or rental period has stopped.” Pet. 23 (citing Ex. 1007, 13:6–20; Ex. 1002 ¶¶ 71–74).

Intertrust disagrees that Hornbuckle’s OSP module is control information because none of the functions of the operating system, as modified by the OSP “(e.g., initiating decryption, initiating a timer, verifying a connection with the RCM) convey a *permission, restriction, and/or condition*—in the form of information and/or programming—that controls operations on or use of the protected software application.” PO Resp. 27. By contrast, Intertrust characterizes the OSP as merely “software that executes processes that make enforcement of control information possible.” *Id.* at 29.

Further, Intertrust contends that the OSP “carries out its functions without any regard to the specific rental software being processed or the specific target computer 14 it is executed on.” PO Resp. 30–31 (citing Ex. 1007, 11:41–43; Ex. 2026, 130:23–131:10, 131:23–132:12; Ex. 2024 ¶ 86). And Intertrust argues that it is not the OSP, itself, that governs the use of a digital file, but the RCM or the patched operating system, which also includes other system-level information and enforcement processes “that are (at best) related to control information, not information and programming that conveys permissions, restrictions, and/or conditions that control operations on or use of the rental software.” *Id.* at 31–33 (citing Ex. 1002 ¶ 84; Ex. 1007, 13:6–23; Ex. 2024 ¶¶ 87–89).

We disagree. As we discuss above, we construe “control information” to mean “information and/or programming controlling operations on or use of a digital file or electronic item.” *See supra* part III.B.1. There is no

requirement in claim 24, or the '304 patent as a whole, that all control information must convey permissions, restrictions or conditions.

We also find persuasive Dolby's argument, in its Reply, that control information need not necessarily carry out functions with specific regard for the digital file, such as the particular software being run on Hornbuckle's target computer 14. *See* Pet. Reply 4–5 (citing Ex. 1001, 18:46–19:10). The '304 patent discloses that “control information may be specifically associated with one or more pieces of electronic content and/or it may be employed as a general component of the operating system capabilities of a VDE installation.” Ex. 1001, 18:59–62. It also states that control elements can “reflect and enact content[-]specific and/or more generalized administrative (for example, general operating system) control information.” *Id.* at 18:63–65.

Also, Dolby persuasively argues that claim 24 only requires that the control information is at least “part” of what governs the use of the digital file. Pet. Reply 6. Dolby argues, and we agree, that even though Hornbuckle's rights control system includes a larger system and an RCM, “[t]he OSP is integral to governing the use of the software,” and “the RCM does not govern the use of content without the OSP.” *Id.* (citing Ex. 1007, 11:35–38). Dolby persuasively argues that “the OSP is programming that performs decryption and time-keeping operations, even if it makes use of hardware RCM.” *Id.* at 6–7 (citing Ex. 1007, 14:31–46). Hornbuckle's OSP is a set of procedures that can be enacted for controlling the use of the software on target computer 14, and is thus control information.

(2) *Whether the OSP Continues to Be “the First Entity’s Control Information” in the Target Computer*

Next, Intertrust argues that Hornbuckle’s OSP cannot be control information, and specifically it cannot be “the first entity’s control information,” because “it is a *patch*—an update—that is installed on the existing operating system at the target computer 14 and provides additional functionality to that existing operating system.” PO Resp. 34 (citing Ex. 1007, 11:35–45, 13:53–55; Ex. 2026, 127:13–17). Thus, according to Intertrust, once the operating system of target computer 14 is patched using the OSP, “the OSP itself effectively ceases to exist” and it is the operating system that would actually govern the use of the digital software. *Id.* at 34–35 & n.7 (citing Ex. 1007, 11:35–40, 13:53–55; Ex. 2024 ¶ 92 & n.4; Ex. 2026, 127:13–24). Because claim 24 “requires that the same ‘control information’ that was received separately from the digital file (limitation 24[b]) must also be used to govern a use of the digital file (limitation 24[c]),” and must continue to be “the first entity’s control information,” Intertrust argues that Dolby has failed to show, with sufficient particularity, how Hornbuckle meets these limitations. *Id.* at 35–37 (citing Ex. 1007, 10:36–40; Ex. 2024 ¶¶ 93–95; 37 C.F.R. § 42.104(b)(4)–(4)); *see also* PO Sur-reply 11 (citing Ex. 2024 ¶ 95).

In its Reply, Dolby responds that the phrase “receiving the first entity’s control information” does not require the control information to “belong” to the first entity forever, but rather “only requires that the control information belong to the first entity at the time it is transmitted/received.” Pet. Reply 7–8 & n.3 (citing Ex. 1001, 10:60–63, 10:65–67). According to Dolby, “Hornbuckle’s OSP is transmitted from the host computer 12 and

therefore is the first entity's (the host computer's) control information that is used to govern, in part, use of the file at the computing system." *Id.* (citing Ex. 1007, 5:5–10, 11:57–60).

Dolby also disagrees that, after patching the operating system, the OSP ceases to exist. Pet. Reply 8–10. According to Dolby, "the OSP does not disappear; it is simply added to the existing code." *Id.* at 8. Dolby contends that after the patch, the OSP is incorporated into and becomes "an addition to the operating system," and "Hornbuckle consistently states that the 'OSP module' is being used in its system." *Id.* at 9 (citing Ex. 1007, 11:45–53, 12:68–13:9, 13:14–20, 13:34–53).¹²

Having considered the arguments on both sides, including Intertrust's arguments in its Sur-reply, which we address in our analysis below, we find Dolby's arguments persuasive. First, as we discuss above, we agree with Dolby that claim 24 does not require that the control information "belong" to the first entity in the sense that the first entity exercises continuing control over the control information after submitting it to the computing system. *Supra* part III.B.4. We also find Dolby's argument persuasive that, in Hornbuckle, the OSP does not cease to exist, but becomes incorporated into the operating system of target computer 14, which then uses the same processes and data to govern use of the software. Although the first entity's control information continues to reflect the interests of the first entity, the '304 patent imposes no requirement that the control information remain

¹² In passing, Dolby argues in its Reply that the act itself of "patching the operating system" is a use of the first entity's control information. Pet. Reply 9. Intertrust contends that this is an improper new argument. *See* PO Sur-reply 8–9. Because we find Dolby's arguments in the Petition persuasive, we need not address this issue.

unmodified after the first entity sends it. *See, e.g.*, Ex. 1001, 57:18–19 (“‘Rules and controls’ may self limit if and how they may be changed.”); *id.* at 57:34–35, Fig. 2A (showing a content creator 102’s control information being modified by distributor 106 for use by content user 112, and distinguishing between the situation where the content creator’s control information is “modified” and when its control information is “replaced”). Although the OSP in Hornbuckle’s system is transformed when it is used to patch the operating system, the OSP’s control information—consisting of the methods and associated data for controlling operations on or use of the software package—still exists after the patch.

In its Sur-reply, Intertrust concedes that “[t]he ’304 patent does generally describe[] that in some embodiments control information may include a component of an operating system.” PO Sur-reply 2 (citing Ex. 1001, 18:59–62). But Intertrust contends that Hornbuckle’s OSP still fails to meet the requirement, in claim 24, that the control information is received at the computing system “separately from the digital file it controls.” *Id.* at 2–3. According to Intertrust, this is because the operating system is already part of target computer 14, and is patched, not “received.” *Id.*

We disagree. Dolby’s contention is that the OSP—not the un-patched operating system—contains control information as recited in claim 24, and that the OSP is received separately from the digital file. The un-patched operating system in target computer 14 is not part of the control information according to Dolby’s analysis, and it is the control information in the patch (the OSP module) that governs the use of the digital software. *See* Pet. 27–30.

Intertrust also contends that Dolby's argument that the OSP module "does not disappear" is merely attorney argument, and that Dolby does not submit expert testimony to rebut Dr. Jakobsson's testimony. PO Sur-reply 6–8 (citing Ex. 2024 ¶ 92; *Butamax Advanced Biofuels LLC v. Genvo, Inc.*, IPR2013-00539, Paper 33 at 42 (PTAB Mar. 3, 2015) (declining to reject expert testimony as to the level of ordinary skill, where the rebuttal was merely attorney argument)). And Intertrust contends that Dolby's argument that the "OSP module" carries out "control information" functions is merely a "grammatical shorthand" in Hornbuckle to describe functions performed by the patched operating system. PO Sur-reply 7–8 (citing Ex. 2024 ¶ 92; Ex. 2026, 127:13–24).

We disagree that Dolby's argument that the OSP module continues to operate in the patched system is merely attorney argument. As supporting evidence, Dolby persuasively points to passages in Hornbuckle indicating that the "OSP module" (i.e., part of the patched operating system) continues to perform functions for controlling the use of the protected software. *See* Pet. Reply 9 (citing Ex. 1007, 11:45–53, 12:68–13:9, 13:14–20, 13:34–53). We also disagree that Dolby's argument is inconsistent with Dr. Jakobsson's uncontested testimony that the OSP becomes incorporated into, and becomes part of, the operating system of target computer 14, and that the updated operating system is not the same as the OSP. Ex. 2024 ¶¶ 92–93 (citing Ex. 1007, 11:35–45, 13:53–55; Ex. 2026, 127:13–17). Since these points are undisputed, Dolby did not need to rebut it with expert testimony. Dolby's argument does not hinge on the OSP remaining separate and unmodified before it controls use of the rental software.

We also disagree with Intertrust that it is merely grammatical shorthand for Hornbuckle to say that the “OSP module” is performing the functions of control information. Hornbuckle clearly indicates that the procedures and data of the OSP module—the control information—remain intact after the operating system is patched, and they continue to function, as control information, in governing the use of the protected software. *See* Ex. 1007, 11:45–53, 12:68–13:9, 13:14–20, 13:34–53.

Finally, Intertrust argues in its Sur-reply that neither the OSP in Hornbuckle nor the patched operating system are the “first entity’s control information” because they do not belong to host computer 12, and that Dolby did not argue that the OSP belongs to host computer 12 before its Reply, and the argument is thus untimely. PO Sur-reply 9–11.

We disagree that Dolby’s arguments about whether the OSP is the first entity’s control information are untimely. In its Petition, Dolby argued that Hornbuckle’s system (1) “seeks to distribute rental software in secure ways by installing programmable modules [i.e., the OSP module] onto a target user’s computer that prevent unauthorized use,” (2) sends reporting data back to “the host computer distributing the software,” and (3) “impede[s] a user [of the target computer] from tampering with the system.” Pet. 19 (citing Ex. 1007, 3:37–40; then citing *id.*, code (57); and then citing *id.* at 12:23–33; Ex. 1002 ¶¶ 66–67). Dolby also makes clear that host computer 12 is the source of the rental software package. Pet. 26–30.

Thus, Dolby provided ample evidence, in its Petition, that host computer 12 is the distributor of the rental software and also the distributor of control information, including the OSP module, that protects its interests in preventing a user from tampering with the system or obtaining

unauthorized use of the software. In its Reply, Dolby merely clarified its position, but did not introduce new evidence and did not make any contentions that were meaningfully distinct from what it presented in its Petition. Thus, we do not consider Dolby's arguments in the Reply to be untimely.

We also find Dolby's arguments persuasive that the OSP module "belongs to" the software distributor (i.e., host computer 12). Pet. Reply 8. As the Texas court stated, "there may be a variety of ways in which the information might belong to the first entity." Ex. 2007, 56. But the situation in Hornbuckle is analogous, in the '304 patent, to the control information (110) that belongs to VDE rights distributor 106, as shown in Figure 2 of the '304 patent (reproduced above in part II.B). Rules and controls 110 originate with rights distributor 106, they specify control information relating to the distribution model, and they govern how downstream content user 112 uses the content. *See* Ex. 1001, 56:7–18. Rights distributor 106 may be the content creator, or may simply be distributing content from another entity 102. *Id.* at 56:37–38. In Hornbuckle, host computer 12 takes on the same role as rights distributor 106 in the '304 patent.

Intertrust points out that the Texas court rejected "[d]efendants' proposal that 'first entity's control information' in claim 24 somehow may mean control information simply received from a first entity is . . . not reasonable." PO Sur-reply 10 (emphasis omitted) (quoting Ex. 2007, 55). This is because, in the embodiments captured in dependent claims 26 and 27, the first entity's control information is received via a second entity. *See* Ex. 2007, 55; *see also* Ex. 1001, 328:21–27. This would be similar to the embodiment shown in Figure 2 or 2A of the '304 patent, in which content

user 112 receives content creator 102's control information via distributor 106. *See* Ex. 1001, Figs. 2, 2A.

But Dolby's contention does not hinge on us construing "first entity's control information" based on which entity directly sent the control information. More pertinent is that, in the case of Hornbuckle, the OSP module originated with host computer 12, which is distributing the software, and the OSP module governs use of the rental software *for* the software distributor who distributed it, to protect the distributor's interests in controlling use of the software. *See* Pet. Reply 8 ("Hornbuckle's OSP is transmitted from the host computer 12 and therefore is the first entity's (the host computer's) control information that is used to govern, in part, use of the file at the computing system.").

Thus, we find that Dolby has persuasively shown that Hornbuckle's OSP module is "the first entity's control information."

(3) *Whether the Encryption Key is Control Information*

Independently of OSP module, Dolby also argues that Hornbuckle's encryption key is control information. *See* Pet. 24, 27, 30. Dolby contends that "[t]he rental software package will only run on the particular target computer 14 with an encryption key corresponding to the encryption key used by host computer 12 to encrypt the key module." Pet. 21 (citing Ex. 1001, 12:36–43). Thus, Dolby asserts that the "the rental software cannot be used without the encryption key." Pet. 22 (citing Ex. 1001, 12:25–29).

Intertrust's responsive arguments rely on its proposed construction of "control information" that narrows the earlier district court constructions to

exclude a simple cryptographic key, which we address above. *See* PO Resp. 37–42; *supra* part III.B.1(b). In particular, Intertrust argues that Hornbuckle’s encryption key is not a “critical key,” and thus cannot be control information, because it “is received at the RCM 18 from an external source (*e.g.*, host computer 12) in encrypted form,” and *another* key—a private key—is used to decrypt that encryption key. *Id.* at 42 (citing Ex. 1007, 12:9–21). Thus, according to Intertrust, the key that target computer 14 receives is not the private (critical) key. *Id.* (citing Ex. 2024 ¶ 103).

We disagree with Intertrust, and we find Dolby’s arguments persuasive. As we discuss above, our construction of “control information” does not depend on the source of the key, or whether it is a private key, but on whether the key functions as information controlling operations on or use of a digital file or electronic item. In Hornbuckle, the key, distributed as part of the retail software, is enacted for controlling use of the rental software. *See* Ex. 1007, 12:25–27 (“Without the encryption key, decryption of the key module of the rental software at the target computer 14 is essentially impossible”); *id.* at 12:38–40 (“[A] downloaded rental software package will only run on the particular target computer 14 having [the right] encryption key”). This is true even though the received key is encrypted and must be decrypted by another key that is not received from the first entity.

For the above reasons, we find that Dolby has shown that Hornbuckle discloses limitations 24b and 24c.

(d) Limitation 24d

Limitation 24d recites “reporting information relating to the use of the digital file to the first entity.” Ex. 1001, 328:8–9. Dolby contends that

Hornbuckle discloses this limitation because its system records “[t]he elapsed time between the starting and stopping of the rental program, as well as the time and date information” in “RCM 18 for subsequent offline processing.” Pet. 23 (citing Ex. 1007, 13:20–23). According to Dolby, RCM 18 uploads this information to host computer 12. *Id.* (citing Ex. 1007, 3:33–36, 6:21–29, 9:25–26; Ex. 1002 ¶ 75).

Intertrust does not contest these arguments, and we find Dolby’s arguments persuasive.

(e) Limitation 24e

Limitation 24e recites “wherein at least one aspect of the computing system is designed to impede the ability of a user of the computing system to tamper with at least one aspect of the computing system’s performance of one or more of said using and reporting steps.” Ex. 1001, 328:10–15.

Dolby argues that Hornbuckle discloses this limitation because its encryption key is inaccessible to the user and, thus, “the user’s ability to tamper with the encryption key, which is used in governing the use of the rental software, is impeded.” Pet. 23 (citing Ex. 1007, 12:36–37). Dolby also contends that RCM 18 will destroy the encryption key if anyone tampers with RCM 18, and the OSP module will erase the software from target computer 14 if it is disconnected from RCM 18. *Id.* at 23–24 (citing Ex. 1007, 12:23–29, 13:34–44, 14:1–8). Thus, Dolby argues that “the user is prevented from using, stealing, copying, vandalizing, . . . modifying the software, and . . . circumventing the accounting of the rental usage.” *Id.* at 24 (citing Ex. 1007, 12:25–29, 13:34–44).

Intertrust argues that Hornbuckle’s OSP cannot be both the “control information” and the “aspect of the computing system” designed to impede

tampering. PO Resp. 33 (citing Ex. 2024 ¶ 90). Intertrust also argues, in its Sur-reply, that claim 24 “implicitly require[s] that the ‘aspect of the computing system’ of limitation 24[e] be different from the control information used to govern content use.” PO Sur-reply 4. According to Intertrust, this is because the tamper-resistance limitation is a “design” aspect of the computing system, so it can’t be something that is the result of something that is received externally from the computing system. *Id.* at 5 (citing Ex. 1001, 64:1–66:53 (describing a “tamper-resistant hardware security barrier” for an SPU)). Also, according to Intertrust, if the OSP could be both the control information and the aspect for impeding tampering, “the control information would be illogically and improperly tasked with impeding tampering with *its own use.*” *Id.*

We disagree. We find nothing in claim 24, or in the ’304 patent as a whole, requiring that control information cannot also be part of an aspect of the computing system designed to impede tampering. Claim 24 is a method claim, and limitation 24e is a “wherein” clause introducing a functional “aspect” of the computer system as a whole. So this “aspect” need not be in the form of an element of the computer system other than the control information. Also, the ’304 patent contemplates that the computing system’s tamper-resistance aspect may take the form of functional software features, and these features may involve encryption keys or other control information. *See, e.g.*, Ex. 1001, 22:20–25 (“VDE may employ . . . compartmentalization of . . . stored control information (including differentially tagging such stored information to ensure against substitution and tampering)”); *id.* at 60:24–28 (tamper resistant barrier 502 can be “formed by security features such as ‘encryption’”); *id.* at 65:5–19 (tamper resistance may include

“further modules providing additional security protections such as requiring password or other authentication to operate”); *id.* at 81:49–82:21 (describing a “software-based tamper resistant barrier”); *id.* at 128:45–46 (describing load modules as “[s]ecure (tamper-resistant) executable code”).

Also, Dolby’s contentions do not rely on the OSP, alone, to provide tamper resistance. According to Dolby, other aspects of Hornbuckle’s computing system that are designed to impede tampering include the encryption key and RCM 18. *See* Pet. 33–35. RCM 18 is the aspect of the system that, most directly, is designed to impede tampering, because RCM 18 includes “programmable modules for preventing unauthorized use, copying, vandalism and modification of downloadable data and programs during or after transmission to the target computer,” and “[i]f the RCM 18 is tampered with in any manner, the encryption key is destroyed,” thus preventing tampering. Pet. 33–34 (emphasis omitted) (first quoting Ex. 1001, 3:37–41; then quoting *id.* at 12:23–29). RCM 18 also sends signals in response to queries from the OSP module to indicate that it is still connected to target computer 14, or otherwise the OSP module will terminate and erase the protected software to protect it from theft, vandalism, or other unauthorized modification. Pet. 34 (citing Ex. 1001, 13:34–44).

For the above reasons, we find that Hornbuckle discloses limitation 24(e).

3. Conclusion

For the above reasons, we find that Dolby has shown, by a preponderance of the evidence, that Hornbuckle discloses identically each

limitation of claim 24. Therefore we find that claim 24 is unpatentable as anticipated by Hornbuckle.

D. GROUND BASED ON KATZNELSON AND NARASIMHALU

For its second ground, Dolby alleges that claim 24 is unpatentable under § 103(a) as obvious over Katznelson in view of Narasimhalu. Pet. 7, 35–54.

A claim is unpatentable under § 103 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 24 is unpatentable under 35 U.S.C. § 103(a) as obvious over Katznelson in view of Narasimhalu. We present our findings and conclusions below.

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:

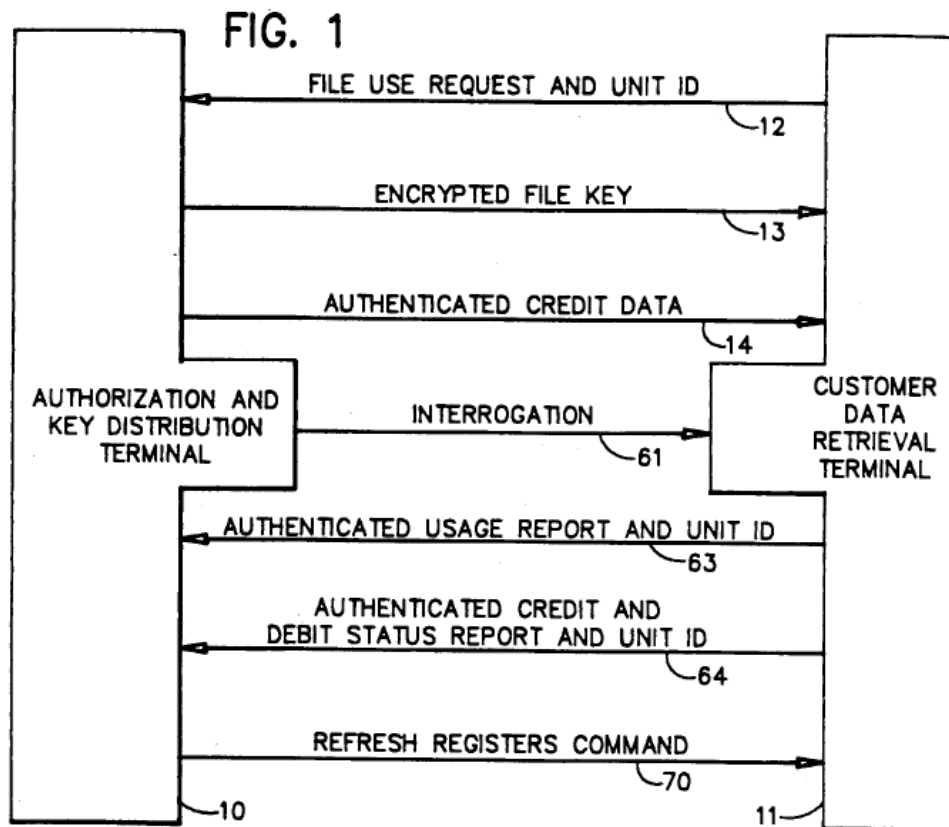


Figure 1, above, depicts “an authorization and key distribution terminal 10 and a customer data retrieval terminal 11,” of which there may be many

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.

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.

Thus, retrieval control unit 22 has two data inputs: authenticated credit data signal 41 (i.e., the authenticated version of credit data signal 14 received from authorization and key distribution terminal 10), and authenticated cost data signal 51 (i.e., the authenticated version of cost data signal 48 received from the ROM or CD-ROM medium storing the digital file). Credit data signal 14/41 “indicates an amount of credit to be extended to the customer terminal . . . for retrieval of data from the file identified in the file use request signal 12.” Ex. 1005, 2:35–38. Cost data signal 48/51 “indicates the cost associated with retrieving the given encrypted block of data.” *Id.* at 3:17–19.

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.

Customer data retrieval terminal 11 also has facilities for generating authenticated usage reports 62 and authenticated credit and debit status reports 68. *See* Ex. 1005, 4:65–5:35.

2. *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.

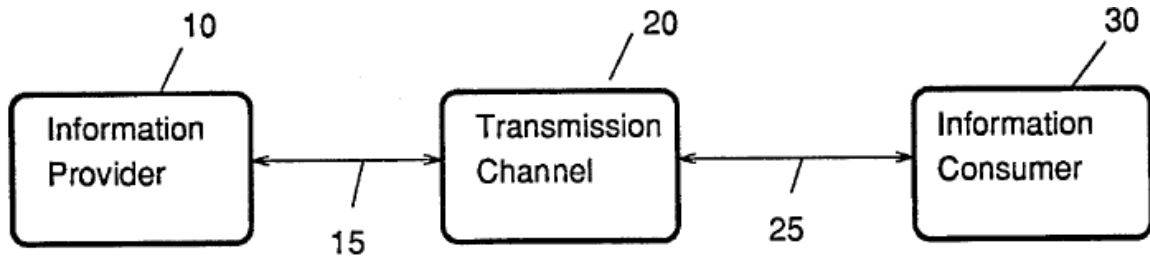


Figure 1, above, depicts information provider 10, which communicates to information consumer 30 over transmission channel 20 via paths 15 and 25. Ex. 1004, 4:48–54. Information Consumer 30 represents “one or more end users of information.” *Id.* at 4:58–60.

Information Consumer 30 has a tamper-proof controlled access device to access the information in the distributed medium. Ex. 1004, 6:47–49.

Figure 6, reproduced below, is an example of such an access device:

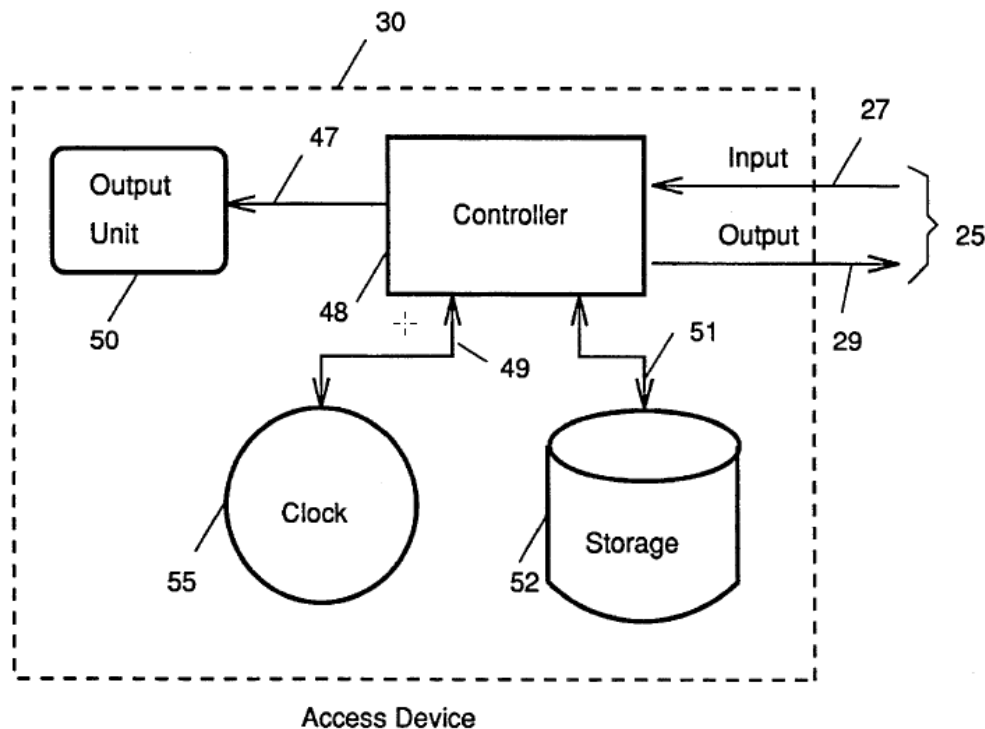


Figure 6

Figure 6, above, depicts an access device (dashed line) modeling Information Consumer 30, which includes controller 48, storage 52, clock 55, and output unit 50. Ex. 1004, 8:38–53. Controller 48 controls the flow of information through input channel 27 and output channel 29. *Id.* at 8:40–42, 8:53–55. “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.

3. *Reason to Combine Katznelson and Narasimhalu*

Dolby argues that a person of ordinary skill in the art would have had reason to “modify Katznelson’s system to include a tamper-proof device for enclosing controllers, memories, clocks, and other circuitry in a secure environment, as taught by Narasimhalu, so that a user is impeded from tampering with aspects of controlling and using the digital file.” Pet. 42 (emphasis omitted) (citing Ex. 1004, 7:3–6, 8:55–59). Noting that Katznelson discloses secure memory storing a unit key, but not securing other aspects of its system, Dolby argues that a person of ordinary skill “would have been motivated to make additional circuitry and transmission channels tamper-proof, including those used to decrypt files and govern use of the files, such as Katznelson’s transmission channels and processing circuitry used with respect to the credit and cost signals.” *Id.* (emphasis omitted). In addition, Dolby argues that a skilled artisan would have expected success in this combination because there were several other known successful ways (including in Hornbuckle) to implement a tamper-proof device. *Id.* at 42–43 (citing Ex. 1006, 3:33–38, 4:5–12, 6:12–44; Ex. 1007; Ex. 1002 ¶¶ 38–42).

Intertrust does not contest these arguments. *See* PO Resp. 42–60. We find Dolby’s asserted reasons to combine Katznelson and Narasimhalu persuasive for the reasons in the Petition.

4. *Preamble and Limitations 24a, 24d, and 24e.*

Dolby contends that Katznelson discloses (1) “[a] method for monitoring use of a digital file at a computing system” according to the preamble, Pet. 43–44; (2) “receiving the digital file” according to limitation 24a, either as a ROM or a CD-ROM, Pet. 45–46; and (3) “reporting information relating to the use of the digital file to the first entity” (that is, authorization and key distribution terminal 10) according to limitation 24d, Pet. 50–51. Dolby also contends that Katznelson, in light of Narasimhalu, teaches designing an aspect of the computer system that impedes tampering according to limitation 24e, and that a person of ordinary skill in the art would have had reason to combine the two references. Pet. 51–54.

Intertrust does not contest Dolby’s arguments regarding the preamble or limitations 24a, 24d, or 24e. We find these arguments persuasive for the reasons Dolby provides in the Petition.

5. *Limitations 24b and 24c*

For limitation 24b and 24c, Dolby identifies Katznelson’s credit data signal 14 as the “control information.” *See* Pet. 39, 46. According to Dolby, Katznelson’s credit data signal 14 “is control information that indicates an amount of credit to be extended to the customer [data retrieval] terminal 11 for retrieval of data from the requested file.” Pet. 37 (citing Ex. 1005, 2:35–38); *see also* Pet. 46 (credit data signal 14 “indicates an amount of credit available for retrieval of data from the requested file”). Dolby argues that

customer data retrieval terminal 11 “is only permitted to decrypt the encrypted data [in the content file] if sufficient credit exists to cover the cost of retrieving a requested file.” *Id.* at 37 (emphasis omitted) (citing Ex. 1005, 4:11–43). Thus, according to Dolby, “the customer terminal limits the amount of data retrieved based on credit data signal 14.” *Id.* (emphasis omitted) (citing Ex. 1005, code (57), 1:16–22, 2:35–38). Dolby also contends that credit data signal 14 is control information because it reflects “a permission to use the requested file for the credited amount” and indicates “how the file is distributed, used, decrypted, [and] paid for.” Pet. 46–50 (citing Ex. 1005, code (57), 1:16–20, 1:59–2:6, 2:28–38, 3:45–51, 4:26–37, 9:3–14, Figs. 2, 6; Ex. 1002 ¶¶ 130–134, 141).

Intertrust disagrees that Katznelson’s credit data signal 14 is control information that governs use of a digital file. PO Resp. 43 (citing Ex. 2024 ¶ 104). Intertrust’s arguments fall into three main categories: (a) that credit data signal 14 is simply “an amount of credit” and not control information, unlike other aspects of Katznelson’s customer data retrieval terminal 11; (b) that credit data signal 14 is not a “permission” to use a file because it does not identify any specific file; and (c) that credit data signal 14 is not a “budget” as described in the ’304 patent. We address these issues in turn.

(a) Whether Credit Data Signal 14 Is Merely an Input to Katznelson’s Other Control Information

First, Intertrust argues that credit data signal 14, being simply “an amount of credit,” is merely an input or operand that is *used by* Katznelson’s control information, and is not control information itself. PO Resp. 46 (quoting Ex. 1005, 2:36). According to Intertrust, the control information in Katznelson’s system includes cost data signal 48 and authenticated cost data

signal 51, which “specif[y] how much a particular block of data costs,”¹³ and the rule “that data blocks may only be retrieved if the accumulated credits compared to the sum data costs, including the cost data signal 48/51, are sufficient to merit authorization.” *Id.* (citing Ex. 1005, 4:20–37). But unlike signals 48 and 51 and the underlying calculation they are a part of, Intertrust argues that credit data signal 14 “merely serves as an input that is used by the control information that dictates how much a particular data block costs in order to ultimately determine whether to allow data block retrieval.” *Id.* (citing Ex. 2024 ¶ 108); *see also* PO Sur-reply 20–21. Although Intertrust acknowledges “[t]hat Katznelson’s credit data signal 14 may in some cases provide sufficient credit such that the accumulated credit signal 54 exceeds the sum cost signal 53 and ultimately allow[s] for the retrieval of a block of data,” Intertrust contends that this “does not change the nature of the credit data signal 14 as an input/operand that is used by the actual control information.” PO Resp. 47 (citing Ex. 2024 ¶ 109).

Intertrust similarly contends that Katznelson’s credit data signal 14 “does not represent ‘enactable data’ as that phrase was used in the Texas court’s claim construction order,” because in Intertrust’s view, “the scope of ‘enactable data’ in the context of the challenged claim is information and/or programming that conveys some permission, restriction, and/or condition that controls operations on or use of protected content.” PO Resp. 47–48 (citing Ex. 2007, 38–39; Ex. 2024 ¶ 110). According to Intertrust, “credit

¹³ Intertrust argues that Dolby would not be able to rely on cost data signal 48 as the control information, because it accompanies the ROM or CD-ROM that holds the digital file, and is thus not “receiv[ed] . . . separately from the digital file.” PO Resp. 59–60 & n.12 (quoting Ex. 1001, 328:2–3) (citing Ex. 1005, 3:58–66; Ex. 2024 ¶¶ 128–129).

data signal 14 fails to do this” because it “is supplied as *an input* to Katznelson’s data retrieval unit 22 . . . , analogous to the amount of money a customer hands over at a cash register.” *Id.* at 49 (citing Ex. 1005, 2:35–38, 3:37–51).¹⁴ Intertrust contrasts this with Katznelson’s “cost data signal 48/51 that conveys how much a particular block of data costs and Katznelson’s data retrieval unit 22 that determines whether the cost indicated in that cost data signal 48/51 has been satisfied.” *Id.* (citing Ex. 2024 ¶ 111).

Further, Intertrust argues that, since “credit data signal 14 does not in and of itself constitute control information,” it does not matter that what Intertrust regards as the *actual* control information (i.e., cost data signal 48/51 and data retrieval unit 22) governs the use of the digital file in conjunction with credit data signal 14, because the “at least in part” language in limitation 24c would still require credit data signal 14, itself, to be control information. PO Resp. 54–56 (citing Ex. 2024 ¶¶ 121–122).

Intertrust’s arguments rely on its proposed construction of “control information” that requires a permission, restriction, or condition and excludes data, associated with control methods, that is merely an “input” to those methods. As we discuss above, we disagree with Intertrust’s proposal to narrow the construction of “control information” in these ways. *See supra* part III.B.1(c). In addition, Intertrust fails to make a meaningful distinction between Katznelson’s credit data signal 14 and cost data signal 48, which are both inputs to the same overall calculation that determines whether a

¹⁴ Intertrust argues that the status of Katznelson’s credit data signal 14 as a “mere input” is true, regardless of whether previous credits are accumulated in credit data register 27 or previous debits are accumulated in debit register 28. PO Resp. 49 (citing Ex. 2024 ¶ 112).

user has access to the digital file. Intertrust acknowledges that signals 48 and 51 are control information, likely because the '304 patent explicitly states that “how much [content usage] costs” is a form of “rules and controls.” *See* PO Resp. 46; *id.* at 56 (citing Ex. 1001, 56:63–64). But cost data signal 48 is no less an input or operand to the calculation occurring in retrieval control unit 22 than is credit data signal 14. *See* Ex. 1005, 4:20–37, Fig. 2. We also disagree that there is any meaningful distinction in the construction of “control information” that would allow us to determine that a debit-side input to a calculation is control information but a credit-side input is not.

(b) Whether Credit Data Signal 14 Is a “Permission”

Next, Intertrust disputes Dolby’s contentions that Katznelson’s credit data signal 14 is a “permission to use the requested file for the credited amount,” or that it governs use of the digital file by “indicat[ing] an amount of credit available” that dictates “the amount of the digital file available.” PO Resp. 50 (alteration in original) (first quoting Pet. 46–47; and then quoting Pet. 49–50) (citing Ex. 2024 ¶ 113). According to Intertrust, this is because customer data retrieval terminal 11’s use of request signal 12 “does not identify any particular blocks of data the user actually wishes to access—or notably the blocks’ associated costs.” *Id.* (citing Ex. 1005, 3:6–20). Intertrust also argues that “credit data signal 14 is not even tied to any particular *file* (in addition to not being tied to any particular block of data of a file).” *Id.* at 52 (citing Ex. 2026, 106:21–107:10, 108:21–109:3; Ex. 2024 ¶ 117). And Intertrust argues that “there is no assurance that the credit extended by the credit data signal 14 is even sufficient to pay for retrieval of the data blocks the user ultimately requests.” *Id.* at 53 (citing Ex. 2024 ¶ 118); *see also* PO Sur-reply 22–24.

Similarly, Intertrust contests Dolby's contention that Katznelson receives from authorization and key distribution terminal 10 control information including "how the file is distributed, used, decrypted, [and] paid for." PO Resp. 58 (alteration in original) (quoting Pet. 46). According to Intertrust, "credit data signal 14, which simply includes an amount [of] credit, has no bearing on how the ROM 37 arrives at the customer terminal," and is not control information with respect to the use, decryption, or payment because it is merely an input, it is not "enactable data," and it is not a permission to use any particular file for the credited amount, nor does it indicate the amount of the requested file available for use. *Id.* at 58–59 (citing Ex. 2024 ¶ 127).

In its Reply, Dolby argues that "[Intertrust's] argument is irrelevant" because the '304 patent imposes no requirement that control information must identify a particular file, or a particular cost. Pet. Reply 17. Dolby contends that the '304 patent explicitly states that control information "may be employed as a general component of the operating system capabilities" and may involve "generalized administrative tasks." *Id.* (emphasis omitted) (quoting Ex. 1001, 18:61–62) (citing Ex. 1001, 18:46–19:10).

Dolby also points out that, according to Katznelson, file use request signal 12 *does* identify the file, and Katznelson characterizes it as a request to access a particular file. *See* Pet. Reply 18 (citing Ex. 1005, 3:45–49, 3:52–54); Ex. 1005, 2:11–13 ("The file use request signal [12] identifies the file for which retrieval authorization is requested . . ."). According to Dolby, "[t]hat the credit may be used for other files from the same vendor, or that the credit may be insufficient on its own to access the file, or that a cost is later compared to the credit" are not important, because "the credit serves as

the basis to determine whether permission to use the requested file for the credited amount will be granted.” *Id.* at 18.

As we discuss above, our construction of “control information” does not require it to convey a “permission,” much less a permission to use a particular file or a particular set of file blocks at a particular cost. *See supra* part III.B.1(a). Nevertheless, Dolby has persuasively shown that Katznelson’s credit data signal 14 is a type of permission, because authorization and key distribution terminal 10 issues credit data signal 14 in response to request signal 12 to access a particular file (*see* Ex. 1005, 2:11–13), and Katznelson states that, as a result of receiving credit data signal 14, “authorization has been granted for the customer [data retrieval] terminal 11 to retrieve data from the requested file.” Ex. 1005, 3:52–54; *see also id.* at 10:6–11 (“authorizing said retrieval by providing . . . a credit signal for use in limiting the amount of data to be retrieved *from said file*; . . . limiting the amount of data retrieved *from said file* in accordance with said credit signal” (emphasis added)).

We also agree with Dolby that the manner of calculating the cost, or the question of whether or not authorization and key distribution terminal 10 knows the cost of the requested file, is not relevant to the question of whether credit data signal 14 is control information, either under our construction of the term or Intertrust’s proposed narrower construction of the term.

(c) Whether Credit Data Signal 14 Is a “Budget”

Next, Intertrust argues that Dolby “does not cite to any portion of the ’304 patent specification that describes control information as simply credit/money used to purchase access to protected content.” PO Resp. 56

(citing Pet. 46 n.9; Ex. 1001, 46:42–55). Intertrust also argues that “Katznelson’s credit data signal 14 does not specify either *how* content usage is to be paid for (e.g., credit card, Swiss francs, etc.), nor how much content usage costs.” *Id.* (citing Ex. 2024 ¶ 123).

Intertrust acknowledges that the ’304 patent discloses that “budgets” can be control information if they “limit[] how much content usage is permitted,” “*specify*[] . . . limitations on usage of information content,” and “*specify* . . . how much . . . content . . . can be used.” PO Resp. 56 (omissions and first alteration in original) (first quoting Ex. 1001, 58:60–61; and then quoting *id.* at 59:53–59). But Intertrust contends that such “a budget-based control is the information/programming that conveys a limitation on content access,” rather than “merely an input that is used by the control information to determine whether access should be granted.” *Id.* at 56–57 (citing Ex. 2024 ¶ 124). Intertrust also disputes that Katznelson’s credit data signal 14 specifies “how much of the total information content . . . can be used and/or copied,” because “the amount of credit supplied by credit data signal 14 is not tied to any particular *block* of data, nor any anticipated costs.” *Id.* at 57–58 (quoting Ex. 1001, 57:38–61; Ex. 1005, 3:49–51, 4:20–39) (citing Ex. 2024 ¶ 126).

In its Reply, Dolby argues that the ’304 patent contemplates that “[s]imple budget allowances” are within the scope of the term “control information.” Pet. Reply 14–15 (citing Ex. 1001, 54:66–55:10, 59:35–59). Dolby points to Figure 85 of the ’304 patent, which indicates budgets in the form “Budget=\$22,000” or “Budget=\$8000.” *Id.* at 15 (citing Ex. 1001, 319:42–61, Fig. 85). Dolby contends that “[b]udgets (Budget=\$) are not patentably distinguishable from Katznelson’s credits (Credit=\$). Both

specify to the recipient how much money/credit they have available for use.”
Id. at 16.

In its Sur-reply,¹⁵ Intertrust argues that Dolby improperly raised its argument “that Katznelson’s credit data signal is control information because it is purportedly ‘not patentably distinguishable’ from ‘budgets.’” PO Sur-reply 16 (citing Pet. Reply 13–16, 19). We disagree that Dolby improperly raised this issue in its Reply, because the argument is responsive both to our Institution Decision (Paper 13, 44) and Intertrust’s Response (PO Resp. 48, 56–57). The argument also does not represent any meaningful departure from Dolby’s arguments in the Petition, and Intertrust has had a fair opportunity to be heard on the issue, both in its Response and in its Sur-reply.

As to the merits of this issue, Intertrust argues that the simple budget limits disclosed in the ’304 patent are distinguishable from Katznelson’s credit data signal 14: whereas the budget limits in the ’304 patent “are ‘created’ by the VDE operator to set *limits on usage*,” credit data signal 14 is a “credit/money actually used to pay for content and (expended until the budget limit is reached).” PO Sur-reply 17–18 (citing Ex. 1001, 270:7–271:19); *see also id.* at 18–19 & n.10 (citing Ex. 1001, 27:47–58, 36:37–48, 57:60–58:6, 58:7–58:15, 296:51–297:2; Ex. 2024 ¶¶ 124–126). Intertrust also argues that credit data signal 14 is “not a budget limit because the

¹⁵ Intertrust notes that Dolby’s Reply makes reference to two arguments that Dolby made in another proceeding, but not in this one, for which Intertrust allegedly did not “provide any meaningful rebuttal.” *See* PO Sur-reply 15–16 & n.9 (emphasis omitted) (citing Pet. Reply 19–20). Because Intertrust did not make these arguments in this proceeding, we do not address these arguments in this decision.

credits . . . are merely added to the preexisting balance in credit register 27.”
Id. at 19–20.

We disagree. Although Katznelson’s credit data signal 14 need not be a “budget” as described in the ’304 patent to be control information, we find Dolby’s arguments persuasive that a person of ordinary skill in the art would have regarded credit data signal 14 as equivalent to a simple budget limit, and thus within the scope of “control information,” for the following reasons.

First, the ’304 patent clearly teaches that “control information” includes a simple budget that limits how much content can be used. *See* Ex. 1001, 54:66–55:10 (“rules and controls” for an office may include “a maximum usage budget for each individual user and/or group within the office”), 59:35–59 (“Budgets . . . can specify, for example, how much of the total information content . . . can be used and/or copied.”). And the ’304 patent teaches that this limit can be expressed in terms of a monetary value. *See id.* at Fig. 85 (“Budget=\$22,000”). As Dolby correctly argues, the ’304 patent does not require that a budget or other control information “follow any specific syntax” to achieve the desired functionality. Pet. Reply 17; *see also* Ex. 1001, 146:46–56, 147:12–15 (teaching that a “budget” may be expressed in many, non-exclusive ways, including an “[a]scending count of uses,” a “descending count of permitted use, e[.]g., remaining budget,” or “usage limits since a specific time.”).

We acknowledge that Katznelson’s credit data signal 14 is not quite as simple as a fixed limit on data usage such as “Budget=\$22,000,” because the usage limit is accumulated in credit register 27 as, potentially, the sum of multiple credit data signals 14. *See* Ex. 1005, 45–51, Fig. 2. This is because,

in response to each file use request signal 12, authorization and key distribution terminal 10 only authorizes enough credit, at any one time, to allow the user to retrieve a specific amount of data from the requested file. *See* Ex. 1005, 2:7–38. But credit data signal 14 is still, in function and effect, a budget limit that restricts customer data retrieval terminal 11 from using more than a specified amount of data in a digital file.

Second, we disagree with Intertrust that Katznelson’s credit data signal 14 is merely money that “pays for content.” *See* PO Sur-reply 17–18. In Katznelson’s system, there is a separate “customer account associated with the customer [data retrieval] terminal 11,” which authorization and key terminal 10 consults (in addition to factors such as eligibility and credit worthiness) before issuing credit data signal 14. *See* Ex. 1005, 2:21–26. Thus, Katznelson’s description of credit data signal 14 does not limit the manner in which a customer may pay for the content or otherwise receive authorization to access the content—that is an issue left to authorization and key distribution terminal 10. What credit data signal 14 provides is a limit on the amount of data (in terms of its cost) that the user can access from the requested file. We agree with Dolby that such a credit limit is not materially different than a simple budget limit such as “Budget=\$22,000.” *See* Pet. Reply 16.

6. *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. 60–65.

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 21–22), 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.*, IPR2020-00661, Paper 17 at 63–67 (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 distributing 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. 61 (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 61 (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. 61–62. 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 '304 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 24 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 '304

patent as the most valuable patent family, based on a patent value index created by Unified Patents. PO Resp. 62–63 (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 24.

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 ’304 patent or claim 24. Also, Intertrust has not identified anything in the IAM article that ascribes the value of this patent family to any aspect of claim 24, 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. 63–64 (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 63–64 (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 64 (quoting Ex. 2036, 2). According to Intertrust, the praise

from these two articles relates to the use of control information (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 63–64; *see also* PO Sur-reply 25 (citing Ex. 2035, 2) (arguing that the first article specifically describes a unique combination of features that includes control information and tamper impedance).

In its Reply, Dolby contends that these features (control information and tampering impedance) already existed in the prior art and thus cannot be the basis of a nexus to claim 24. *See* Pet. Reply 22.

We agree with Dolby that the *Fortune* articles fail to provide a nexus to the claimed invention. Intertrust acknowledges that Katznelson already discloses the idea of rules and controls, at least in the form of cost data signal 48/51 and the logic within retrieval control unit 22. *See* PO Resp. 46; PO Sur-reply 20. Although this control information is received together with the digital file, Intertrust concedes that the *Fortune* articles do not include praise for the idea that control information is received separately from the digital file, as recited in limitation 24b. *See* PO Sur-reply 25–26. Intertrust also does not challenge Dolby’s contention that Narasimhalu discloses a tamper-resistant container, or that it would have been obvious to combine that container with Katznelson’s customer data retrieval terminal 11. *See supra* part III.D.3.

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 Katznelson, in light of Narasimhalu, discloses all the limitations of claim 24, including the limitations praised in the *Fortune* articles. To the extent that the *Fortune* article is praising the combination of “rules and controls” and a device that impedes tampering, Intertrust does not contest Dolby’s argument that Narasimhalu discloses the tamper impedance function of limitation 24e, or that a person of ordinary skill in the art would have had reason to combine these teachings with Katznelson.

(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. 64–65.

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 24. Thus, we assign little weight to Intertrust’s unsupported arguments on commercial success and copying.

7. *Conclusion for Second Ground*

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 24 would have been obvious over the combination of Katznelson and Narasimhalu, and is thus unpatentable.

IV. CONCLUSION¹⁶

For the reasons given above, Dolby has shown by a preponderance of the evidence that claim 24 of the '304 patent is unpatentable, as summarized in the following table:

Claims	35 U.S.C. §	Reference(s)/ Basis	Claims Shown Unpatentable	Claims Not Shown Unpatentable
24	102(a)	Hornbuckle	24	
24	103(a)	Katznelson, Narasimhalu	24	
Overall Outcome			24	

¹⁶ 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).

V. ORDER

In consideration of the foregoing, it is

ORDERED that claim 24 of the '304 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.

IPR2020-00662
Patent 6,640,304 B2

For PETITIONER:

Scott McKeown
Mark D. 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
razmessengerian@quinnemanuel.com
tigranguledjian@quinnemanuel.com
scottflorance@quinnemanuel.com