

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

DOLBY LABORATORIES, INC.,
Petitioner,

v.

INTERTRUST TECHNOLOGIES CORPORATION,
Patent Owner.

IPR2020-00663
Patent 7,406,603 B1

Before MICHAEL R. ZECHER, KIMBERLY McGRAW, and
CHRISTOPHER L. OGDEN, *Administrative Patent Judges*.

McGRAW, *Administrative Patent Judge*.

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

I. INTRODUCTION

Petitioner, Dolby Laboratories, Inc., filed a Petition requesting *inter partes* review of claims 1 and 2 of U.S. Patent No. 7,406,603 B1 (Ex. 1001, “the ’603 patent”). Paper 2 (“Pet.”). Patent Owner, Intertrust Technologies Corporation, filed a Preliminary Response. Paper 6 (“Prelim. Resp.”). Petitioner subsequently filed an authorized Reply (Paper 7, “Pet. Reply”) and Patent Owner filed an authorized corrected Sur-reply (Paper 9, “PO Sur-reply”).

Institution of an *inter partes* review is authorized by statute when “the information presented in the petition . . . and any response . . . shows that there is a reasonable likelihood that the petitioner would prevail with respect to at least 1 of the claims challenged in the petition.” 35 U.S.C. § 314(a); *see* 37 C.F.R. § 42.108. Upon consideration of the submitted evidence and argument, we conclude the information presented does not show there is a reasonable likelihood that Petitioner would prevail in establishing the unpatentability of at least one of the challenged claims of the ’603 patent.

A. *Real Parties-in-Interest*

Petitioner identifies Dolby Laboratories, Inc., a Delaware corporation, and Dolby Laboratories, Inc., a California corporation, as real parties-in-interest. Pet. 3. Petitioner further identifies (1) Cinemark Holdings, Inc., (2) AMC Entertainment Holdings, Inc., and (3) Regal Entertainment Group (hereinafter “Cinemas” or the “Texas Defendants”), as real parties-in-interest “out of an abundance of caution, to avoid any dispute about such status based on any alleged business relationship between the Cinemas and Petitioner.” *Id.*

Patent Owner identifies itself as the real party-in-interest. Paper 4 (Patent Owner's Mandatory Notices), 2.

B. The '603 Patent

The '603 patent, titled "Data Protection Systems and Methods" is directed to "systems and methods for inspecting, classifying, controlling, and/or modifying the processing of protected electronic content to provide enhanced resistance to attempts to circumvent content protection."

Ex. 1001, code (54), 1:25–29. The application giving rise to the '603 patent was filed on August 31, 2000, and claims priority to U.S. Provisional App. No. 60/151,790 (Ex. 1004), filed on August 31, 1999. *Id.* at codes (21), (22), (60).

Figure 5 of the '603 patent is reproduced below.

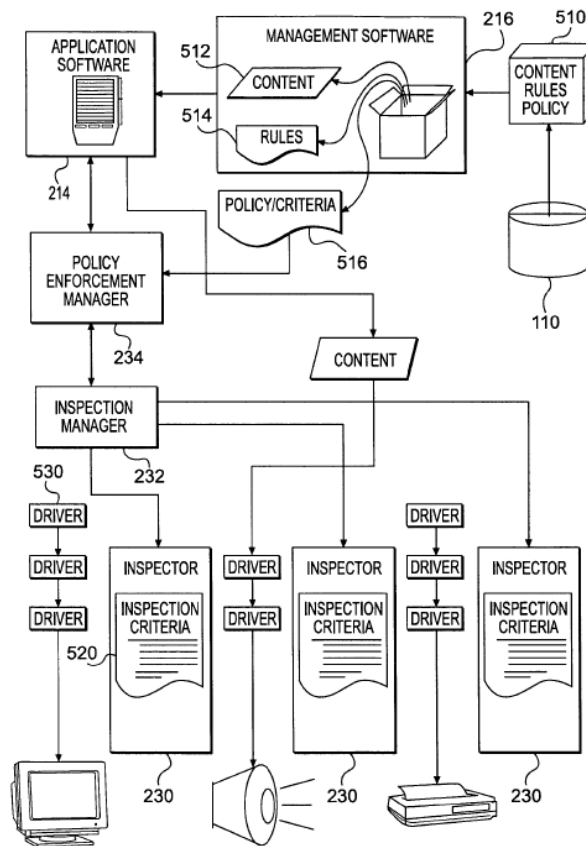


FIG. 5

Figure 5 depicts a system and method for protecting content by inspecting drivers, software, or hardware modules and using the inspection results, along with predefined policies, to control processing or use of the content. *Id.* at 4:26–30, 19:65–66. As shown in Figure 5, application software 214 (for example, a music player providing a user interface for selecting songs from a play list) may call management software 216 (for example, a digital rights management (“DRM”) program) to check and enforce a set of policies or rules associated with the song to determine whether the user is authorized to play (or otherwise act on) the song. *Id.* at 10:31–39. Management software 216 may receive digital content from an external source (such as hard drive 110 or network 136) via secure container

510. *Id.* at 19:67–20:2. Secure container 510 may contain digital content file 512, rules 514 governing use of content, and policy criteria 516 governing the security to be applied while using content in accordance with rules 514. *Id.* at 20:2–6. Management software 216 is operable to release content file 512 from container 510 to application software 214 in accordance with the rules 514 that govern the content’s use—for example, upon receipt of a predefined payment from the user. *Id.* at 20:16–21.

Upon releasing content file 512 from container 510, management software 216 may also release policy criteria 516 to policy enforcement manager 234, inspection manager 232, or inspectors 230. *Id.* at 20:36–41. Inspectors 230 may use lists of criteria 520 (including, for example, public keys to verify cryptographic signatures in a driver) to check appropriate drivers 530 and report the results to inspection manager 232 or policy enforcement manager 234, which evaluates the security of the system by applying the policy to the inspection data. *Id.* at 16:25–29, 20:41–46. If the results indicate that defensive action is warranted, an appropriate signal may be sent to application 214 or management software 216. *Id.* at 20:46–48.

Figure 6 of the '603 patent is reproduced below.

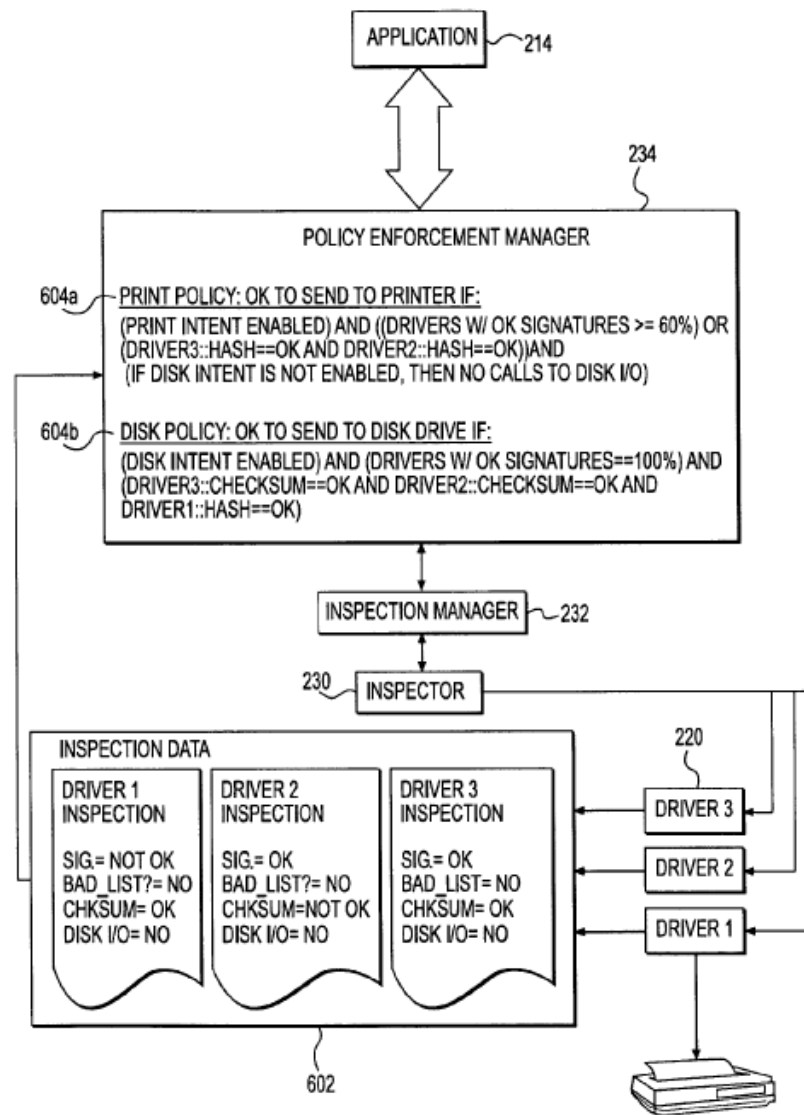


FIG. 6

Figure 6 depicts an application of a policy for processing content obtained by inspectors 230. *Id.* at 4:31–32, 20:49–50. Policy enforcement manager 234 may contain various policies 604 about a given item of electronic content. *Id.* at 20:50–53. Figure 6 shows two such policies 604a and 604b, one governing the release of a content file to a printer, and the

other governing the release of the content file. *Id.* at 20:53–56. Print policy 604a indicates that the content file may be sent to the printer as long as the rules 514 allow printing of the content (the print intent is enabled). *Id.* at 20:58–61. Disk policy 604b indicates that the content file may be sent to the disk drive as long as drivers 220 for handling the content on its way to the printer satisfy certain conditions. *Id.* at 20:61–65.

Inspectors 230 may gather data 602 needed by policy enforcement manager 234 to evaluate logical policy expressions 604. *Id.* at 20:65–67. For example, inspectors 230 may check any cryptographic signatures associated with the drivers in the appropriate driver chain, compute the hash of a driver and compare it to lists of known “good” or “bad” drivers, compute the checksum of all or part of a driver, or check for calls to certain interfaces such as disk input/output. *Id.* at 21:1–7. Upon receiving inspection data 602, policy enforcement manager 234 is operable to determine whether appropriate policy criteria 604 have been satisfied, and permit the release of the content or take appropriate defensive action. *Id.* at 21:7–11.

The ’603 patent identifies several heuristic approaches that may be used to identify a driver as “probably unacceptable.” *Id.* at 17:66–18:2. First, the system may scan for the use of certain “system interfaces” indicating undesirable behavior or known to be undesirable. *Id.* at 18:3–19. Second, the system may “monitor and analyze the dynamic timing operations performed by the module to identify anomalous timing characteristics indicative of invalid and/or malicious activities.” *Id.* at 18:34–37. Third, the system may determine whether content is being directed through an unapproved streaming channel. *Id.* at 19:24–29. When

an unauthorized module is detected during processing of protected content, the system may (1) return an error and deny the operation; (2) remove or disable the offending module and deny the operation; or (3) damage the content, but permit the operation to continue. *Id.* at 22:2–9.

C. Illustrative Claim

Petitioner challenges claims 1 and 2 in this proceeding. Claim 1, the only challenged independent claim, is reproduced below with formatting and bracketing added for clarity.

1. A method for protecting electronic media content from unauthorized use by a user of a computer system, the method including:
 - [a] receiving a request from a user of the computer system to use a piece of electronic media content;
 - [b] identifying one or more software modules responsible for processing the piece of electronic media content and enabling use of the piece of electronic media content by the user;
 - [c] processing at least a portion of said piece of electronic media content using at least one of the one or more software modules;
 - [d] evaluating whether the at least one of the one or more software modules process the portion of the electronic media content in an authorized manner,
 - [e] the evaluating including at least one action selected from the group consisting of:
 - [i] evaluating whether the at least one of the one or more software modules make calls to certain system interfaces;
 - [ii] evaluating whether the at least one of the one or more software modules direct data to certain channels;
 - [iii] analyzing dynamic timing characteristics of the at least one of the one or more software modules for anomalous timing characteristics indicative of invalid or malicious activity;

[f] denying the request to use the piece of electronic media content if the evaluation indicates that the at least one of the one or more software modules fail to satisfy a set of predefined criteria.

Ex. 1001, 23:46–24:9.

D. Prior Art and Asserted Grounds

Relying on the declaration testimony of Dr. Vijay H. Madiseti (Ex. 1002), Petitioner asserts that claims 1 and 2 are unpatentable based on the following grounds:

Claims Challenged	35 U.S.C. §	Reference(s)/Basis
1, 2	103(a) ¹	Griswold ²
1, 2	103(a)	England ³

II. GROUNDS OF THE PETITION

Petitioner contends claims 1 and 2 would have been obvious over both Griswold and England. For the reasons below, we determine that Petitioner has not shown a reasonable likelihood that it will prevail in showing that at least 1 claim is unpatentable and, therefore, we deny institution of *inter partes* review of the '603 patent.

A. Legal Standards

A claim is unpatentable under 35 U.S.C. § 103(a) if “the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the

¹ The Leahy-Smith America Invents Act (“AIA”), Pub. L. No. 112-29, 125 Stat. 284, 287–88 (2011), amended 35 U.S.C. § 103, effective March 16, 2013. Because the application from which the '603 patent issued was filed before this date, the pre-AIA version of § 103 applies. *See* Ex. 1001, codes (21) and (22).

² US 5,940,504, issued August 17, 1999 (Ex. 1006, “Griswold”).

³ US 6,820,063, issued November 16, 2004 (Ex. 1005, “England”).

invention was made to a person having ordinary skill in the art to which said subject matter pertains.” *KSR Int’l Co. v. Teleflex Inc.*, 550 U.S. 398, 406 (2007). The question of obviousness is resolved on the basis of underlying factual determinations, including (1) the scope and content of the prior art; (2) any differences between the claimed subject matter and the prior art; (3) the level of skill in the art; and (4) when in evidence, objective evidence of obviousness or non-obviousness, i.e., secondary considerations. *See Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966).

“In an [*inter partes* review], the petitioner has the burden from the onset to show with particularity why the patent it challenges is unpatentable.” *Harmonic Inc. v. Avid Tech., Inc.*, 815 F.3d 1356, 1363 (Fed. Cir. 2016) (citing 35 U.S.C. § 312(a)(3) (requiring *inter partes* review petitions to identify “with particularity . . . the evidence that supports the grounds for the challenge to each claim”); *see also* 37 C.F.R. § 42.104(b) (requiring a petition for *inter partes* review to identify how the challenged claim is to be construed and where each element of the claim is found in the prior art patents or printed publications relied upon). Apart from limited circumstances not present here, this burden does not shift to Patent Owner. *See Dynamic Drinkware, LLC v. Nat’l Graphics, Inc.*, 800 F.3d 1375, 1378 (Fed. Cir. 2015) (discussing the burden of proof in *inter partes* review). Furthermore, Petitioner cannot satisfy its burden of proving obviousness by employing “mere conclusory statements.” *In re Magnum Oil Tools Int’l, Ltd.*, 829 F.3d 1364, 1380 (Fed. Cir. 2016).

B. Level of Ordinary Skill in the Art

In determining whether an invention would have been obvious at the time it was made, we consider the level of ordinary skill in the pertinent art at the time of the invention. *Graham*, 383 U.S. at 17. Petitioner contends that a person of ordinary skill in the art at the time the '603 patent was filed (a "POSITA") would have had a minimum of a bachelor's degree in computer science, electrical engineering, mathematics, or a related field, and approximately two years of relevant experience or equivalent study in electronic data protection, electronic content protection, or digital rights management. Pet. 16. Petitioner further states that additional graduate education could substitute for professional experience, or significant experience in the field could substitute for formal education. *Id.* (citing Ex. 1002 ¶¶ 47–48).

Patent Owner sets forth a similar definition, stating that a POSITA would have 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. Prelim. Resp. 19. Patent Owner states that the positions set forth in its Preliminary Response would be the same under either parties' proposal. *Id.*

The parties' proposals do not differ in any meaningful way to the issues in dispute. We adopt Petitioner's definition of a POSITA, except that we delete the qualifier "a minimum" to eliminate vagueness as to the appropriate level of education. The qualifier expands the range without an upper bound, i.e., encompassing a Ph.D. degree and beyond, and thus does

not meaningfully indicate the level of ordinary skill in the art. This definition of a person of ordinary skill in the art is supported by the testimony of Dr. Madisetti and is commensurate with the level of ordinary skill as reflected in the prior art and the '603 patent. We note, however, that our analysis would be the same under either parties' definition of a POSITA.

C. Claim Construction

For petitions filed on or after November 13, 2018, such as here, we apply the same claim construction standard that would be used to construe the claim in a civil action under 35 U.S.C. § 282(b), including 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. 37 C.F.R. § 42.100(b) (2018); *Phillips v. AWH Corp.*, 415 F.3d 1303 (Fed. Cir. 2005) (en banc).

1. “predefined criteria”

Petitioner asserts that the term “predefined criteria” recited in claim 1 should be construed to mean “conditions or characteristics determined in advance against which to check the structure and/or behavior of one or more software modules.” Pet. 16–18 (citing Ex. 1002 ¶¶ 67–72). To support this proposed construction, Petitioner states that the '603 patent describes “inspector modules that ‘are operable to check the structure and/or behavior of drivers, software, and/or hardware against predefined criteria.’” *Id.* at 17 (emphasis omitted) (quoting Ex. 1001, 15:36–62); *see also id.* (citing Ex. 1001, 16:25–34, 23:63–24:4).

Patent Owner contends that the term “predetermined criteria” does not require construction and should be given its plain and ordinary meaning.

Prelim. Resp. 21. Patent Owner further asserts that construction of this term is not necessary to resolve the matters presently in dispute. *Id.*

We agree that no explicit construction of this phrase is necessary for our decision on whether to institute. *See Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.*, 868 F.3d 1013, 1017 (Fed. Cir. 2017) (“[W]e need only construe terms ‘that are in controversy, and only to the extent necessary to resolve the controversy.’” (quoting *Vivid Techs., Inc. v. Am. Sci & Eng’g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999))).

2. “predefined policy”

Petitioner contends the term “predefined policy” as recited in claim 2 should be construed to mean “one or more rules determined in advance governing the processing of content.” Pet. 18–19 (citing Ex. 1002 ¶¶ 73–74). To support this proposed construction, Petitioner states that the ’603 patent describes that “use of the electronic media content by a software module is in accordance with ‘a set of rules or policy controls’ governing ‘whether it will allow, modify, or disallow downstream processing operations on protected content.’” *Id.* at 18 (internal quotation marks omitted) (quoting Ex. 1001, 2:56–64); *see also id.* at 18–19 (citing Ex. 1001, 20:56–65).

Patent Owner contends that the term “predefined policy” does not require construction and should be given its plain and ordinary meaning. Prelim. Resp. 21. Patent Owner further asserts that construction of this term is not necessary to resolve the matters presently in dispute. *Id.* at 21–22.

We agree that no explicit construction of this phrase is necessary for our decision on whether to institute.

3. “evaluating whether the at least one of the one or more software modules direct data to certain channels”

Petitioner contends that claim 1 recites a Markush group:

evaluating whether the at least one of the one or more software modules process the portion of the electronic media content in an authorized manner, [e] the evaluating including at least one action selected from the group consisting of:

- [i] evaluating whether the at least one of the one or more software modules make calls to certain system interfaces;
- [ii] evaluating whether the at least one of the one or more software modules direct data to certain channels;
- [iii] analyzing dynamic timing characteristics of the at least one of the one or more software modules for anomalous timing characteristics indicative of invalid or malicious activity.

Pet. 19 (bracketed material added). Petitioner, therefore, asserts that it need only show that the prior art discloses one of the recited options of the Markush Group in order to render this claim element unpatentable. *Id.* (citing *Fresenius USA, Inc. v. Baxter Intern., Inc.*, 582 F.3d 1288, 1298 (Fed. Cir. 2009)). Petitioner also asserts that the parties proposed different constructions for the phrase recited in claim element 1[e.ii] during the district court proceeding and that the Petition applies the construction proposed by Patent Owner. *Id.* at 20–21.

Patent Owner responds that this phrase does not require construction beyond its plain meaning. Prelim. Resp. 22. Patent Owner further asserts that construction of this term is not necessary to resolve the matters presently in dispute. *Id.*

We agree that claim element 1[e] recites a Markush group and determine that no further construction of this claim element is necessary for our decision on whether to institute.

4. *Order of Processing and Evaluating Steps*

Patent Owner additionally raises the fact that, in the Texas Actions, the district court construed claim 1's step of "processing at least a portion of said piece of electronic media content using at least one of the one or more software modules" as occurring before the step of "evaluating whether the at least one of the one or more software modules process the portion of the electronic media content in an authorized manner." Prelim. Resp. 23 (citing Ex. 2007, 53). Patent Owner contends that this construction is not pertinent to the parties' controversy and issues raised in the Petition. *Id.* Petitioner does not propose its own construction with respect to the ordering of these claim steps. *See, e.g.*, Pet. 16–21 (setting forth Petitioner's positions on claim construction).

We agree that a determination of the whether claim 1 requires the recited method steps to be performed in any particular order is not necessary for our decision on whether to institute. *See Nidec*, 868 F.3d at 1017 (quoting *Vivid Techs.*, 200 F.3d at 803).

D. Asserted Unpatentability of Claims 1 and 2 over Griswold

Petitioner contends that claims 1 and 2 would have been obvious under 35 U.S.C. § 103(a) over Griswold (Ex. 1006). *See* Pet. 22–41; Pet. Reply 8–9. Patent Owner responds that Griswold fails to teach, *inter alia*, identifying a software module responsible for processing electronic media content as required by claim element 1[b]. Prelim. Resp. 43–47; PO Sur-Reply 8–9. For the following reasons, we determine that Petitioner has not

demonstrated a reasonable likelihood it would prevail in showing that claims 1 and 2 would have been obvious over Griswold.

1. Overview of Griswold

Griswold, titled “Licensing Management System and Method in Which Datagrams Including an Address of a Licensee and Indicative of Use of a Licensed Product Are Sent from the Licensee’s Site,” is directed to systems and methods “for managing licenses of products such as computer software, video games, CD-ROM information, movies and other video products, music and other audio products, [and] multimedia products.” Ex. 1006, codes (54), (57), 1:16–20. In a preferred embodiment, the licensed product can include both data portion 1B, (the protected information such as CD-ROM database information, video information, audio information) as well as “software which controls the information.” *See id.* at 5:19–28. By “including in product 1 both information and the software which controls the information, product 1 is an executable product.” *Id.* at 5:33–35.

Figure 1 of Griswold is reproduced below.

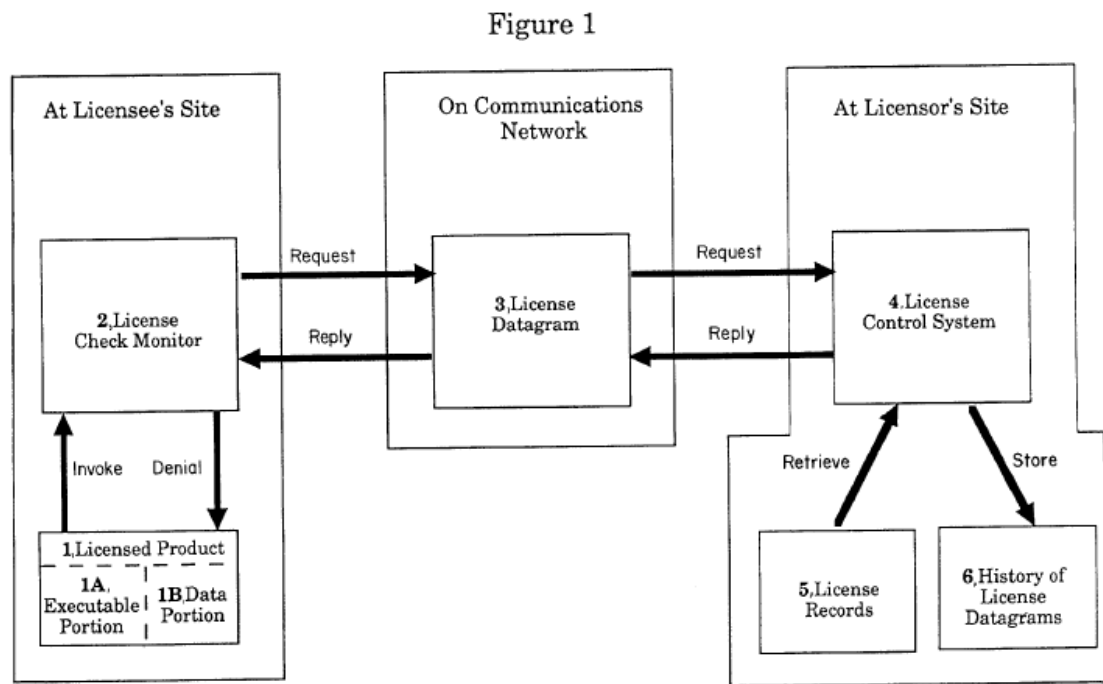


Figure 1 depicts a block diagram according to an embodiment of Griswold. *Id.* at 4:53–55. As shown in Figure 1, licensed product 1, located at the licensee's site, includes functional or executable portion 1A and data portion 1B. *Id.* at 5:19–21. Portion 1A may be a computer software product or any other kind of information product used to control use of portion 1B. *Id.* at 5:21–23. For example, if portion 1B is CD-ROM database information, portion 1A may enable the licensee to search indexes and display text. *Id.* at 5:23–25. If portion 1B is video information, portion 1A may control the display of the video information. *Id.* at 5:25–27. If portion 1B is audio information, portion 1A may play the audio information. *Id.* at 5:27–28. And if portion 1B is an electronic book, portion 1A may display and turn pages. *Id.* at 5:28–30.

In another embodiment, data portion 1B and functional portion 1A are not together, but are provided separately. Griswold explains that “it is also possible to include the software which controls the information in the networked machine at the licensee’s site,” such that “product 1 is split, with part of it on media and part on the licensee’s machine. By doing this, some space can be saved on the media containing product 1, but the capabilities of these products will be limited by *the standard functions* available on these machines.” *Id.* at 11:36–43.

In operation, the licensee’s site and a licensor’s site may communicate license datagrams 3 to each other over a communications network for approving or denying use of licensed product 1. *Id.* at 5:38–58. License datagrams 3 are messages that describe information related to the use of a licensed product 1. *Id.* at 5:44–45. Data 23, which is a part of datagram 3, contains a number of fields. *Id.* at 6:44–46. For example, field product model number 24 and datagram number 25 identifies product 1 and datagram 3, respectively. *Id.* at 6:46–48.

2. *Analysis*

a) *Claim element 1[b]*

Claim element 1[b] recites the step of:

identifying one or more software modules responsible for processing the piece of electronic media content and enabling use of the piece of electronic media content by the user;

Ex. 1001, 23:51–54.

Petitioner argues Griswold’s split embodiment, where the software used to process the protected content is separate from the content, teaches this claim element in two ways. Pet. 30–33 (citing Ex. 1006, 5:19–33, 5:44–

45, 6:37–51, 11:28–43, Fig. 1; Ex. 1002 ¶¶ 89–93, 107). First, Petitioner contends a POSITA would have understood that, in Griswold’s split embodiment, the monitor at the licensee’s site must first identify the software (the asserted software module) in order for the software to be used together with the content. *Id.* at 33 (citing Ex. 1002 ¶ 93). Second, Petitioner contends a POSITA would have understood that the monitor at the licensee’s site must identify the software so that information identifying the software can be transmitted in the license datagram for evaluation at the licensor’s site. *Id.* (citing Ex. 1002 ¶ 93).

Patent Owner responds that Petitioner has not sufficiently shown that Griswold teaches *identifying a software module* responsible for processing electronic media content as required by claim element [b]. Prelim. Resp. 43–47.

We agree with Patent Owner.

To support both arguments, Petitioner states Griswold’s licensed product 1 can include an “executable portion” or “functional portion” (a software module) that is used to control use of (responsible for processing) data portion 1B (electronic media content). *See, e.g.*, Pet. 30; *see also id.* at 31 (stating that, as shown in Fig. 1, product 1 may include data portion 1B and functional portion 1A such as computer software product or any other kind of information product used to control use of data portion 1B). Petitioner explains that, although “the software is depicted in Figure 1 as part of the licensed product, Griswold also discloses that the software that controls or processes the content may be on the licensee’s computer separate from the content.” *Id.* at 24. Petitioner further explains that in “this

embodiment, the software is not limited to software provided by the licensor.” *Id.* (citing Ex. 1002 ¶ 79).

With respect to Petitioner’s first argument, Petitioner contends that “a POSITA would have understood that in the embodiment where the software is separate from the content[,] the monitor at the licensee’s site must first identify the software in order for the software to be used together with the content” *Id.* at 33 (citing Ex. 1002 ¶ 93), *id.* at 25 (citing Ex. 1002 ¶ 81). Petitioner, however, does not provide sufficient evidence to support its contention. Although Petitioner cites to the declaration testimony of Dr. Madisetti to support its argument, Dr. Madisetti’s testimony merely repeats verbatim what is stated in the Petition and provides no additional persuasive facts or objective evidence to support his conclusion. *See* Ex. 1002 ¶ 93; *see also id.* at ¶¶ 77–82. To satisfy its burden of proving obviousness a petitioner cannot employ mere conclusory statements. *In re Magnum Oil Tools Int’l*, 829 F.3d at 1380; *see also In re Geisler*, 116 F.3d 1465, 1470 (Fed. Cir. 1997) (explaining that attorney arguments and conclusory statements that are unsupported by factual evidence are entitled to little probative value).

We are also not persuaded by Petitioner’s second argument that “a POSITA would have understood that in the embodiment where the software is separate from the content[,] the monitor at the licensee’s site must first identify the software . . . so that information identifying the software can be transmitted in the license datagram for evaluation at the licensor’s site.” Pet. 33 (citing Ex. 1006, 5:44–45, 6:37–51; Ex. 1002 ¶ 93). Petitioner does not provide sufficient evidence or argument either that the license datagram provides information about the software (as opposed to the licensed product

itself) or a reason why a POSITA would have understood information about the software would be provided in the datagram for evaluation at the licensor's site.

To support this second argument, Petitioner states Griswold's license check system involves sending a "request datagram" or a "license datagram" to the licensor's site in order to obtain approval to use the licensed product. Pet. 24–25 (citing Ex. 1006, 3:62–4:5, 5:44–52). Petitioner contends Griswold's "license datagram 3 describes information related to the use of licensed product 1, including an identification of product 1 (*i.e.*, the software)." *Id.* at 25 (citing Ex. 1006, 5:44–45, 6:37–51); *see also id.* at 33 (citing Ex. 1006, 5:44–45, 6:37–51; Ex. 1002 ¶ 93). Griswold, however, does not state that license datagram 3 identifies the software separately from the product. Rather, Griswold states that datagram 3 contains a number of fields, including product model number 24 that identifies product 1. Ex. 1006, 6:45–48. Thus, we disagree with Petitioner's assertion that license datagram 3 identifies the software separately from the product. Petitioner's contention that a POSITA would have understood that, in the embodiment where the software is separate from the content, the monitor must first identify the software so that information identifying the software can be transmitted in the license datagram for evaluation at the licensor's site, is conclusory and unsupported. *See* Pet. 33 (citing Ex. 1002 ¶ 93).

Thus, Petitioner has not sufficiently shown that Griswold teaches the limitations of claim element 1[b].

b) Conclusion

For the foregoing reasons, Petitioner has not shown sufficiently that Griswold teaches all the limitations of claim 1. Accordingly, Petitioner has

not shown a reasonable likelihood that it will prevail in establishing that claim 1, or its dependent claim 2, would have been obvious over Griswold.

E. Asserted Unpatentability of Claims 1 and 2 over England

Petitioner contends that claims 1 and 2 would have been obvious under 35 U.S.C. § 103(a) over England (Ex. 1005). *See* Pet. 42–58; Pet. Reply 9–10. Patent Owner responds that England fails to disclose “evaluating whether the at least one of the one or more software modules make calls to certain system interfaces” as recited in claim element 1[e][i], or “evaluating whether the at least one of the one or more software modules direct data to certain channels” as recited in claim element 1[e][ii]. Prelim. Resp. 50–56; Sur-reply 9–10.

For the reasons stated below, we determine that Petitioner has not demonstrated a reasonable likelihood it would prevail in showing that claims 1 and 2 would have been obvious under § 103(a) over England.

1. Overview of England (Ex. 1005)

England, titled “Controlling Access to Content Based on Certificates and Access Predicates,” is directed to systems and methods for controlling access to downloaded content based on a rights manager certificate and digital rights specified in an access predicate. Ex. 1005, codes (54), (57). England describes a series of processes and data structures on a subscriber computer for controlling the loading of a digital rights management operating system (DRMOS), identifying the DRMOS and trusted applications to a content provider, and securing content downloaded by the provider to a subscriber computer. *Id.* at 10:39–44.

Figure 2 of England is reproduced below.

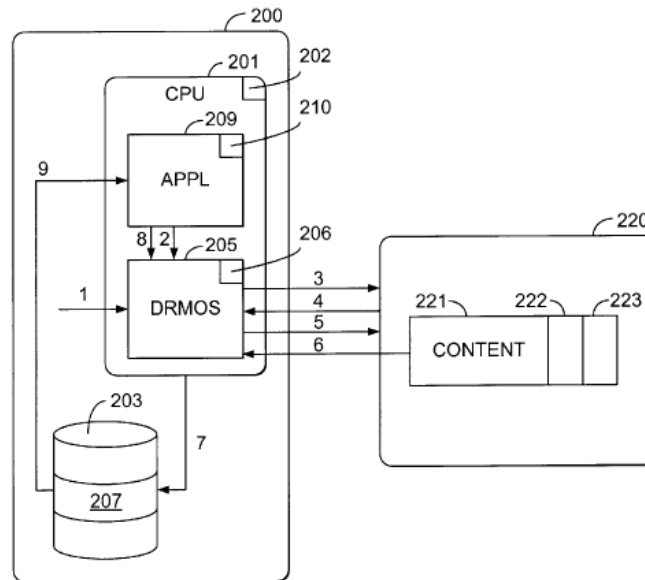


Fig. 2

Figure 2 of England depicts a system-level overview according to one embodiment. *Id.* at 4:37–38, 8:25–27. Subscriber computer 200, such as a client computer, contains a plurality of program modules (including an operating system (“OS”), application programs, program modules, and program data), and is connected to content provider server computer 220 (“provider”) through a wide-area network. *Id.* at 6:26–29, 8:26–29.

DRMOS 205, with its identity 206, is loaded into central processing unit (“CPU”) 201 of the subscriber computer through a loading process (step 1). *Id.* at 8:59–61. DRMOS 205 loads and executes only OS components that it identifies as respecting digital rights (“trusted”) and allows access to downloaded content only by similarly trusted applications. *Id.* at 8:45–50, 8:63–64. DRMOS 205 prevents applications it identifies as non-trusted from gaining access to content stored on the subscriber computer. *Id.* at 8:64–67. Trusted application 209, which accesses and handles certain types

of content, may be identified through a rights manager certificate 210. *Id.* at 9:3–11. Application 29 may request the download of content 221 from provider 220 (step 2). *Id.* at 9:26–28. DRMOS 205 may send a message to provider 220 requesting the content (step 3), and the content provider may transmit a challenge message to the DRMOS 205 asking for the identity of CPU 201, DRMOS 205, and application 209 (step 4). *Id.* at 9:28–32. DRMOS 205 may transmit a response message containing a certificate 202 for the CPU 201, its own identity 206, and the rights manager certificate for the application 209 (step 5). *Id.* at 9:32–35.

If a trust relationship is established, the provider may download the content 221 (step 6), access predicate 222, and license 223 to DRMOS 205 on subscriber computer 200. *Id.* at 9:65–10:2. Access predicate 222 may specify the properties an application must have to process content 221 and specific applications (or families thereof) allowed to process the content. *Id.* at 10:5–7. License 223 may place restrictions on an approved application's use of content 221, which may be monitored by DRMOS 205 and terminated if the license is violated. *Id.* at 4:9–11, 10:7–8, 10:34–36.

2. *Analysis*

Claim 1 is directed to a method for protecting electronic media content from unauthorized use that includes evaluating whether software modules process a portion of electronic media content in an authorized manner. Ex. 1001, 23:46–24:8.

Claim element 1[e] requires that:

[e] the evaluating including at least one action selected from the group consisting of:

[i] evaluating whether the at least one of the one or more software modules make calls to certain system interfaces;

[ii] evaluating whether the at least one of the one or more software modules direct data to certain channels;

[iii] analyzing dynamic timing characteristics of the at least one of the one or more software modules for anomalous timing characteristics indicative of invalid or malicious activity;

Id. at 23:60–24:4 (bracketed material added). Petitioner asserts England satisfies the limitations of claim element 1[e] by teaching the limitations recited in either claim element 1[e][i] or 1[e][ii]. Pet. 51–54; *see also id.* at 52 n.10 (stating “Petitioner need only show that the prior art discloses one of the recited options in order to invalidate this claim element”).

a) Claim element 1[e][i]

Petitioner contends a POSITA would have understood England to teach “evaluating whether . . . software modules make calls to certain interfaces” as recited in claim element 1[e][i]. Pet. 51–53 (citing Ex. 1002 ¶¶ 131–133, 150; Ex. 1010, 4:4–11; Ex. 1011, 16:23–25; Ex. 1012, 14; Ex. 1013, 5:11–20; Ex. 1014, 243; Ex. 1017; Ex. 1018, 3). In particular, Petitioner contends that England teaches detecting whether a user attempts to load a kernel debugger into memory. *Id.* at 52. Petitioner asserts that a POSITA would have understood that “loading a kernel debugger” “involves making a call to certain system interfaces” and, “in order to determine

whether the user attempts to load a kernel debugger” into memory, “a POSITA would have understood to evaluate whether the trusted application makes calls to certain system interfaces.” *Id.* at 52–53.

We are not persuaded by Petitioner’s arguments. Claim element 1[e][i] requires evaluating whether *software modules* make calls to certain interfaces. Petitioner contends that England’s *trusted application*, *not the kernel debugger*, is the recited software module. *See, e.g.*, Pet. 51 (stating England’s “trusted application 209” is a software module); *see also id.* at 52–53 (discussing England’s kernel debugger without asserting the kernel debugger is a software module). Even if we agree with Petitioner that a POSITA would have understood England to teach that loading a kernel debugger into memory involves making calls to system interfaces, Petitioner does not sufficiently explain how a POSITA would have understood that determining whether a user attempts to load a kernel debugger into memory teaches evaluating whether England’s *trusted application* (the asserted software modules) makes calls to certain system interfaces. *See id.*

To support its contentions that a POSITA would have understood England to teach that loading a kernel debugger into memory involves making calls to certain system interfaces, including the “ptrace” and “/proc” interfaces in UNIX systems, Petitioner asserts that “ptrace” and “/proc” are well-known debugger interfaces; that the “ptrace” interface allows one process to control another and to gain access to the memory of the controlled process; and that the “/proc” interface was “used to read data from the memory of a running process.” *Id.* at 52 (citing Ex. 1010, 4:4–11; Ex. 1011, 16:23–25; Ex. 1012, 14; Ex. 1013, 5:11–20; Ex. 1014, 243; Ex. 1017; Ex. 1018, 3).

Even if we accept that these assertions are true, however, Petitioner, does not sufficiently explain how these assertions regarding the kernel debugger support Petitioner’s conclusion that “[t]hus, in order determine whether the user attempts to load a *kernel debugger* for copying content stored in memory” a “POSITA would have understood to evaluate whether the *trusted application* makes calls to certain interfaces.” *Id.* at 52–53 (citing Ex. 1002 ¶¶ 131–133, 150) (emphasis added). Conclusory statements are not sufficient to satisfy a Petitioner’s burden of proving obviousness. *See Magnum Oil Tools*, 829 F.3d at 1380.

Notably, in response to Patent Owner’s arguments that Petitioner failed to sufficient show England’s trusted application makes a call to system’s interfaces as required by claim element 1[e][i] (*see* Prelim. Resp. 51–53), Petitioner does not affirmatively assert that England’s trusted application makes a call to system interfaces. *See* Pet. Reply 9–10. Rather, Petitioner merely replies that “England teaches making a call to an interface such that a “ptrace” or “/proc” causes the debugger to load. *Id.* at 10. Petitioner’s unsupported assertions are insufficient to show that England teaches a *software module* that makes calls to system interfaces as required by claim element 1[e][i].

Thus, for the foregoing reasons, we determine Petitioner has not sufficiently shown that England teaches a software module that makes calls to system interfaces as required by claim element 1[e][i].

b) Claim element 1[e][ii]

Petitioner contends that England teaches “evaluating whether . . . software modules direct data to certain channels,” as required by claim element 1[e][ii] by “monitoring and enforcing the trusted application’s

‘sublicense rights’).” *See* Pet. 53–54 (citing Ex. 1005, 15:54–58, 19:32–55; Ex. 1002 ¶¶ 134–137, 150) (emphasis omitted); Pet. Reply 10. In particular, Petitioner contends that England disclose a license, which can specify sublicense rights 1107, that permits the trusted application on an upstream computer (software module) to validate and share content (direct data) with sublicensed downstream computers. Pet. 53 (citing Ex. 1005, 19:32–55). Petitioner further contends that England teaches monitoring the use of content by the trusted application and terminating the trusted application’s use of the content if the trusted application “violates the sublicense rights by sharing content with non-validated computers.” *Id.* (citing Ex. 1002 ¶ 136). Petitioner further asserts that determining if the trusted subscriber violates the license limitations by sharing content with non-validated computers, “involves determining whether the downstream computers are validated.” *Id.* at 53–54 (citing Ex. 1002 ¶¶ 136–137); Pet. Reply 10.

Petitioner further contends that it would have been obvious to a POSITA to terminate the underlying use of the content by the upstream subscriber (as opposed to terminating only the ability to sublicense). Pet. 54 (citing Ex. 1002 ¶ 137). Specifically, Petitioner asserts:

it would have been obvious to a POSITA, in view of England’s disclosures to terminate the trusted application on the upstream subscriber computer (and renounce the trusted application’s trusted status) if the application is used to share content with nonvalidated computers in violation of sublicense rights 1107, which involves determining whether the downstream computers are validated. ([Ex. 1002] ¶ 137.) This is because, like the kernel debugger example, there is a heightened interest of content providers to protect against unauthorized copying, and shutting down users exhibiting this type of behavior is

critical to ensuring unauthorized content is not propagated over networks. (*Id.*)

Id. (emphasis omitted).

Patent Owner responds that England does not teach detecting whether the trusted application directed data to *certain* channels (certain “non-validated computers”), as required by claim element 1[e][ii]. Patent Owner contends that England teaches that its trusted application is presented with a binary choice: it may either (1) issue a sublicense that allows *any and all* downstream computers to access content subject to certain license rights, or (2) not issue a sublicense to *any and all* downstream computers. *See* Prelim. Resp. 55 (citing Ex. 1005, 19:36–50). Patent Owner contends that England does not disclose evaluating whether the trusted application attempts to issue a sublicense to only *certain*, validated computers and not to other non-validated computers, nor has Petitioner presented any argument that such an embodiment would have been obvious. *Id.* at 55–56. Patent Owner further contends that England does not provide any disclosure of what criteria determines which downstream computers are valid, how any such criteria would be supplied to the trusted application, how the trusted application would apply any such criteria, or any other number of other details necessary to even suggest, let alone disclose, such an embodiment. *Id.* at 56.

We agree with Patent Owner. Petitioner does not sufficiently show that England teaches evaluating whether data is directed to *certain* channels, as required by claim element 1[e][ii]. Even if we agree with Petitioner that England teaches determining whether its trusted application violates sublicense rights 1107 by sharing content with non-validated computers, Petitioner has not sufficiently explained how this disclosure teaches or

suggests evaluating whether the trusted application directs data to *certain* channels.

Petitioner does not point to any disclosure in England that the trusted application can issue sublicense to only certain validated down-stream computers and not to other non-validated downstream computers; nor has Petitioner presented any argument that such an embodiment would have been obvious. *See generally* Pet.; Pet. Reply; Prelim. Resp. 56. Nor does Petitioner explain why it would have been obvious to determine if the trusted application violates its license by determining if the trusted application has shared content with *certain* downstream computers. Rather, Petitioner asserts the “subscriber computer can share content only with downstream computers that are validated,” and that it would have been obvious “to terminate the trusted application on the upstream subscriber computer (and renounce the trusted application’s trusted status) if the application is used to share content with non-validated computers in violation of sublicense rights 1107, which involves determining whether the downstream computers are validated.” Pet. Reply 10 (citing Pet. 54). Such assertions do not establish that England teaches evaluating whether the asserted software modules direct data to *certain* channels, as required by claim element 1[e][ii].

As such, Petitioner has not sufficiently shown that England teaches the limitations of claim element 1[e][ii].

a) Conclusion

For the foregoing reasons, Petitioner has not sufficiently shown that England teaches or suggests at least one of the three options recited in claim element 1[e] and thus, has not shown a reasonable likelihood that it will

prevail in establishing that claim 1, or claim 2 which depends therefrom, would have been obvious over England.

III. CONCLUSION

For the foregoing reasons, we determine that Petitioner fails to demonstrate a reasonable likelihood that it would prevail in showing at least one of the challenged claims of the '603 patent is unpatentable.

Accordingly, the Petition is *denied*, and no trial is instituted.

IV. ORDER

It is hereby

ORDERED that the Petition is *denied* as to all challenged claims of the '603 patent and no trial is instituted.

IPR2020-00663
Patent 7,406,603 B1

FOR PETITIONER:

Scott A. McKeown
Mark Rowland
Christopher M. Bonny
ROPES & GRAY LLP
scott.mckeown@ropesgray.com
mark.rowland@ropesgray.com
christopher.bonny@ropesgray.com

Leslie Spencer
DESMARAIS LLP
lspencer@desmaraisllp.com

FOR PATENT OWNER:

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