UNITED STATES PATENT AND TRADEMARK OFFICE
_____

BEFORE THE PATENT TRIAL AND APPEAL BOARD
_____

AMAZON.COM, INC., HULU, LLC, AND NETFLIX, INC.,
Petitioners,

v.

DIGITAL MEDIA TECHNOLOGIES, INC.,
Patent Owner.
_____

Case No. IPR2017-00285
Patent No. 9,300,657 B2
_____

Before JAMESON LEE, HUBERT C. LORIN, and STACEY G. WHITE,
Administrative Patent Judges.

LORIN, *Administrative Patent Judge*.

DECISION
Denying Institution of *Inter Partes* Review
35 U.S.C. § 314 and 37 C.F.R. § 42.108

I. INTRODUCTION

A. Background

Amazon.com, Inc., Hulu, LLC, and Netflix, Inc., ("Petitioner") filed a

Petition requesting *inter partes* review of claims 1–55 of U.S. Patent No.

9,300,657 (Ex. 1002, "the '657 patent") pursuant to 35 U.S.C. §§ 311–319. Paper 2 ("Pet."). Digital Media Technologies, Inc. ("Patent Owner") filed a Preliminary Response to the Petition (Paper 8, "Prelim. Resp.").

We have jurisdiction under 35 U.S.C. § 314.

Upon consideration of the arguments and evidence presented by Petitioner and Patent Owner, we are not persuaded that Petitioner has demonstrated, under 35 U.S.C. § 314(a), a reasonable likelihood that it would prevail in showing the unpatentability of any of the challenged claims. Accordingly, we do not institute an *inter partes* review of any claim.

B. Related Proceedings

Petitioner notifies us that:

The '657 patent and related U.S. Patent No. 8,964,764 have been asserted against Petitioners in ongoing patent infringement lawsuits brought by Patent Owner in *Digital Media Technologies, Inc. v. Amazon.com, Inc.,* Case No. 4:16-cv-10 00244 (N.D. Fla.) (filed April 26, 2016), *Digital Media Technologies, Inc. v. Hulu, LLC,* Case No. 4:16-cv-00245 (N.D. Fla.) (filed April 26, 2016), and *Digital Media Technologies, Inc. v. Netflix, Inc.,* Case No. 4:16-cv-00243 (N.D. Fla.) (filed April 25, 2016). Petitioners are concurrently filing an IPR petition on U.S. Patent No. 8,964,764 [IPR2017-00284].

Pet. 2.

C. The '657 patent (Ex. 1002)

1. Effective Filing Date

Petitioner indicates that

[t]he '657 patent issued on March 29, 2016 from U.S. Patent Application No. 14/490,033 ['033 application] filed September 18, 2014. It claims priority to a chain of prior applications filed

> on or after May 19, 2005 and the benefit of U.S. Provisional
> Patent Application No. 60/572,365 filed May 19, 2004.
> Therefore, the earliest priority date available to the '657 patent
> is May 19, 2004.

Pet. 5. This is in accord with the information recited on the cover of the
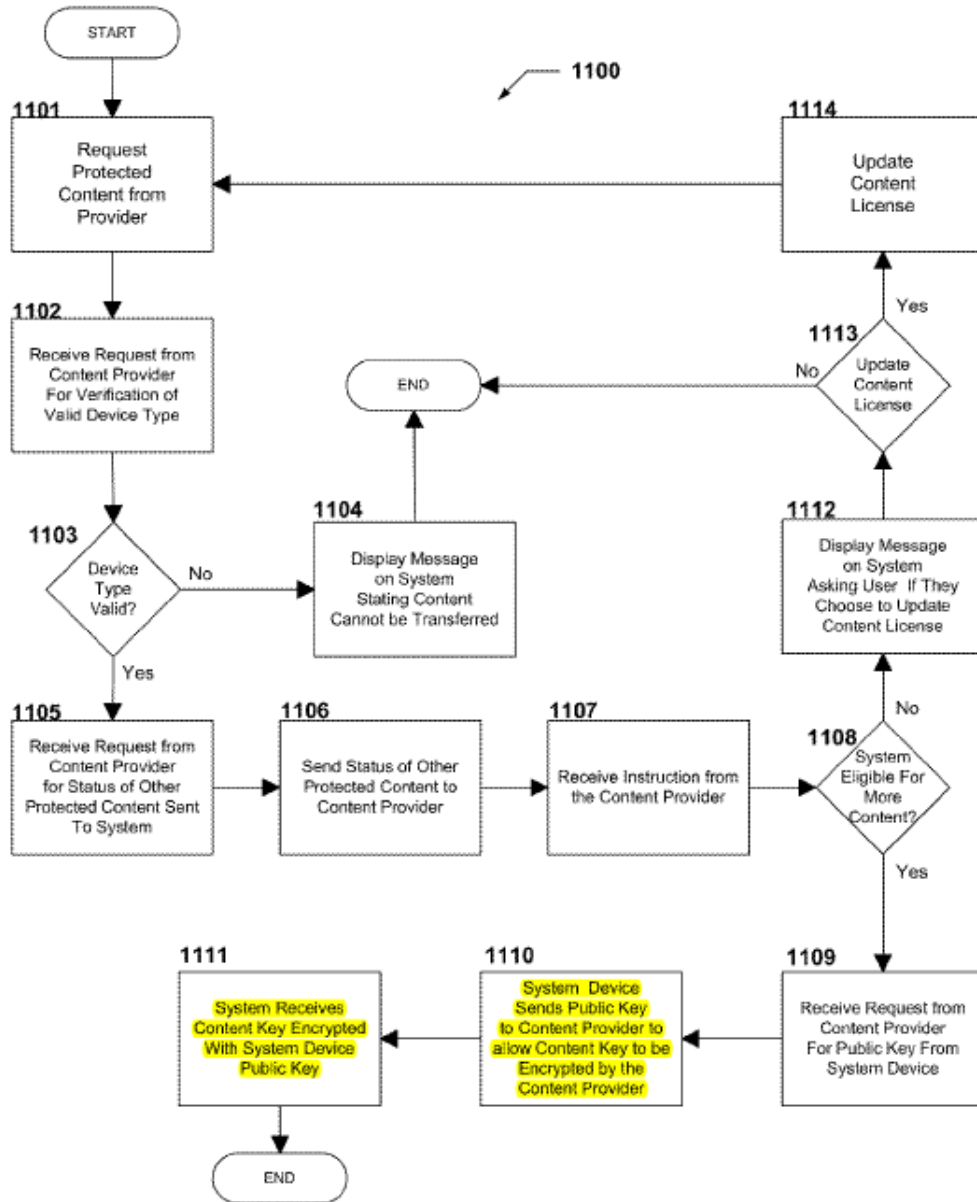
'657 patent.

2. Disclosure

The '657 patent, titled "Multimedia Network System with Content

Importation, Content Exportation, and Integrated Content Management,"

discloses systems and methods for managing digital information via

networked multimedia systems. According to the patent,

> [t]he issue of content protection (for the content being
> downloaded from the content provider) has been a major
> obstacle to allowing consumers to rent or purchase digital video
> disk (DVD) quality video via the internet, or some other data
> network. Thus, a system is needed which will provide
> protection for the content downloaded while, at the same time,
> will allow ease of use and convenience for the consumer.

Ex. 1002, col. 1, ll. 30–37. When a device requests protected content from

an external content provider, the device determines if it is eligible to receive

the protected content. If so, then the system "receives a request from the

content provider for the public key from the system device." *Id* at col. 19, ll.

65–67. In this way, the system accomplishes content protection.

> Next at step 1110, the system device sends its public key to the
> content provider so that the content key sent from the content
> provider can be encrypted with the system device's public key.
> At step 1111, the system 100 receives the content key that is
> encrypted with the system device's public key and the content,
> which is encrypted using the content key. The process 1100 of
> requesting protected content from the content provider ends.

Id at col. 20, ll. 1–8, referring to Fig. 11 (reproduced below, highlighting added for the encryption steps).

START

1100

1101
Request Protected Content from Provider

1114
Update Content License

1102
Receive Request from Content Provider For Verification of Valid Device Type

END

1113
Update Content License

Yes

No

1103
Device Type Valid?

No

1104
Display Message on System Stating Content Cannot be Transferred

1112
Display Message on System Asking User If They Choose to Update Content License

Yes

1105
Receive Request from Content Provider for Status of Other Protected Content Sent To System

1106
Send Status of Other Protected Content to Content Provider

1107
Receive Instruction from the Content Provider

1108
System Eligible For More Content?

No

Yes

1111
System Receives Content Key Encrypted With System Device Public Key

1110
System Device Sends Public Key to Content Provider to allow Content Key to be Encrypted by the Content Provider

1109
Receive Request from Content Provider For Public Key From System Device

END

Figure 11

4

3. Claims

The '657 patent has 55 claims, all of which are challenged.

Independent claim 1 is illustrative.

1.   A multimedia management system for managing distribution and use of content, the multimedia management system comprising:

at least one external control server communicatively connected to a network; and

at least one external content server communicatively connected to the network;

wherein the at least one external control server is configured to:

receive a request for protected content from at least one multimedia client via the network, the at least one multimedia client being associated with at least one user subscription, the request comprising a request for a content license associated with the protected content;

receive a device identification from the at least one multimedia client, the device identification comprising a device type associated with the at least one multimedia client, the device type comprising at least one of: information related to a user authentication or a device authorization;

validate the device identification against a list of acceptable device types;

encrypt the content license with a public key associated with the at least one multimedia client; and

transmit the encrypted content license to the at least one multimedia client via the network;

wherein the at least one external content server is configured to:

transmit the protected content to the at least one multimedia client via the network.

There are three independent claims: claim 1 to a "multimedia management system for managing distribution and use of content"; claim 30 to a method; and, claim 55 to a "multimedia management system for managing distribution and use of protected content." They parallel each other. Claim 1 is drafted in apparatus terms; that is, elements are "configured to" perform certain functions, such as to "encrypt the content license with a public key associated with the at least one multimedia client." Claim 30 is drafted in process terms; that is, by way of steps, such as "encrypting, in the at least one external control server, a content license with the public key associated with the at least one multimedia client." Claim 55 also is drafted in apparatus terms but by way of mean-plus-function language, e.g., "means for encrypting, in the at least one external control server, a content license associated with the protected content with the public key associated with the at least one multimedia client."

Claims 2–29 depend from claim 1 and claims 31–54 depend from claim 30. Claims 2–29 and claims 31–54 generally parallel each other. For example, see claims 28 and claim 54:

> 28. The multimedia management system of claim 1, wherein the content license comprises a decryption key with which the at least one multimedia client can decrypt the protected content using the decryption key as at least one input parameter for a decryption algorithm and usage parameters specifying terms under which the protected content can be consumed.

> 54. The method of claim 30, wherein the content license comprises a decryption key with which the at least one multimedia client can decrypt the protected content using the decryption key as at least one input parameter for a decryption algorithm and usage parameters specifying terms under which the protected content can be consumed.

6

D. References

Petitioner relies on the following references:

Name	Reference	Ex. No.
Bi	WO 02/45316 A2, pub. June 6, 2002	1006
Peinado et al.	U.S. 2003/0078853 A1, pub. Apr. 24, 2003	1007
Reisman	U.S. 2003/0229900 A1, pub. Dec. 11, 2003	1008
Meffert et al.	U.S. 2002/0059144 A1, pub. May 16, 2002	1009
Pasieka	WO 00/74301 A1, pub. Dec. 7, 2000	1010

F. Grounds Asserted

Petitioner contends that claims 1–55 of the '657 patent are unpatentable under the following four grounds:

Ground	Basis	Prior Art	Claims
I	§ 103	Bi and Peinado	1–3, 5–24, 27, 28, 30–32, and 34–55
II	§ 103	Bi, Peinado, and Reisman	26
III	§ 103	Bi, Peinado, and Meffert	25 and 29
IV	§ 103	Bi, Peinado, and Pasieka	4 and 33

Pet. 17–68.

Petitioner also relies on the declaration testimony of Dr. Aviel Rubin (Ex. 1003) as support for the various contentions.

II. ANALYSIS

A. Inter Partes Review Eligibility

The Petition has been accorded a filing date of November 23, 2016 (Paper 4, 1), which is less than nine months after the March 29, 2016 issue date of the '657 patent.

A petition for *inter partes* review shall be filed after the later of nine months after the grant of a patent, or if a post-grant review is instituted under chapter 32, the date of the termination of such post-grant review. 35 U.S.C. § 311(c). Section 311(c) does not apply, however, to a petition for *inter partes* review of a patent that is not a patent described in section 3(n)(1) of the Leahy-Smith America Invents Act ("AIA"). Pub. L. No. 112–274, § 1(d)(1), 126 Stat. 2456 (2013). Similarly, our rules require that a petition for *inter partes* review must not be filed nine months or less from the grant of the challenged patent if it "is a patent described in section 3(n)(1) of the [AIA]." 37 C.F.R. § 42.102(a)(1). If the patent is not one described in section 3(n)(1) of the Leahy-Smith America Invents Act, then the petition must be filed after the date of the grant of the patent, if no post-grant review has been instituted for a patent. *See* 37 C.F.R. § 42.102(a)(2) – "If the patent is a patent that is not described in section 3(n)(1) of the Leahy-Smith America Invents Act, [the petition must be filed after] the date of the grant of the patent" (not requiring filing after nine months from the date of the grant of the patent).

Section 3(n)(1) of the AIA states that such patents include those issuing from an application that contains or contained at any time a claim having an effective filing date, as defined in 35 U.S.C. § 100(i), on or after "the expiration of the 18-month period beginning on the date of the

enactment of" the AIA. Because the AIA was enacted on September 16, 2011 (Pub. L. No. 112–29, 125 Stat. 284), patents described in section 3(n)(1) include those with at least one claim having an effective filing date on or after March 16, 2013.

The parties have not spoken to this issue of whether any claim of the challenged the '657 patent has an effective filing date on or after March 16, 2013. Nevertheless, Petitioner has not identified any element of any claim as possibly lacking support in parent Application 13/109,202.

Based on our review of the record before us, on its face, the '657 patent claims priority to the application that led to U.S. Patent No. 8,868,687; that is, the '657 patent is a continuation of Application 13/109,202, filed May 17, 2011, and facially shares essentially the same disclosure. At this time, we are not aware of any subject matter in the claims of the '657 patent that would break the chain of priority between the claims and the May 11, 2011 parent application. At this stage we assume all challenged claims are entitled to an effective filing date of May 17, 2011. Thus, on the record before us, we are persuaded that all of the '657 patent claims would have an effective filing date of at least May 11, 2011, which is prior to the March 16, 2013 enactment date of § 3(n)(1). It follows therefrom that we are persuaded that the challenged patent is not a patent as described in Section 3(n)(1) of the AIA.

Accordingly, since the record supports viewing the '657 patent as not a patent as described in section 3(n)(1) of the AIA, a petition for *inter partes* review may be filed within nine months from granting of the '657 patent, so long as a post-grant review has not been instituted. As such, we determine

that the Petition does not violate either 35 U.S.C. § 311(c) or 37 C.F.R.
§ 42.102(a)(1).

B. Level of Ordinary Skill in the Art

With regard to the level of ordinary skill in the art, we determine that
no express finding is necessary, on this record, and that the level of ordinary
skill in the art is reflected by the prior art of record. *See Okajima v.
Bourdeau*, 261 F.3d 1350, 1355 (Fed. Cir. 2001); *In re GPAC Inc*., 57 F.3d
1573, 1579 (Fed. Cir. 1995); *In re Oelrich*, 579 F.2d 86, 91 (CCPA 1978).

C. Claim Construction

In an *inter partes* review, "[a] claim in an unexpired patent shall be
given its broadest reasonable construction in light of the specification of the
patent in which it appears." 37 C.F.R. § 42.100(b); *see also Cuozzo Speed
Techs., LLC v. Lee*, 136 S. Ct. 2131, 2144–46 (2016) (upholding the use of
the broadest reasonable interpretation standard). Under the broadest
reasonable interpretation standard, claim terms are generally given their
ordinary and customary meaning in view of the specification, as would be
understood by one of ordinary skill in the art at the time of the invention. *In
re Translogic Tech., Inc.*, 504 F.3d 1249, 1257 (Fed. Cir. 2007).
Furthermore, only those terms that are in controversy need to be construed,
and only to the extent necessary to resolve the controversy. *Vivid Techs.,
Inc. v. Am. Sci. & Eng'g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999).

1. The "encrypt the content license with a public key associated with the at
least one multimedia client" limitation of claim 1.

On the present record, the "encrypt the content license with a public key associated with the at least one multimedia client" limitation of claim 1 is in controversy and resolving its construction is necessary to resolve the controversy.

The "encrypt the content license with a public key associated with the at least one multimedia client" limitation of claim 1, when plainly read, calls for a public key associated with a multimedia client and employing the public key to encrypt a content license. The question is: what does the "content license" contain?

"Claim construction begins, as it must, with the words of the claims." *Vehicular Techs. Corp. v. Titan Wheel Int'l*, Inc. 141 F.3d 1084, 1088 (Fed. Cir. 1998). According to claim 1, the "content license [is] associated with [a] protected content." Notwithstanding that claim 1 does not otherwise characterize the contents of the "content license," the recited association of the "content license" to the "protected content" creates an inference that the "content license" contains certain license data related to the associated "protected content." This comports with claim 9 which further limits the multimedia management system (claim 1) such that it comprises a computing device "configured to store the protected content" (claim 8) as well as "the content license" (claim 9). It necessarily follows from performing a computer-enabled *storing* of the "content license" that the "content license" of claim 1 contains certain license data and that that data are related to the associated "protected content."

The written description is "always highly relevant" in construing a claim, and "it is the single best guide to the meaning of a disputed term." *Vitronics Corp. v. Conceptronic, Inc.*, 90 F.3d 1576, 1582 (Fed. Cir. 1996).

11

However, the '657 patent specification does not define the "content license."
It is disclosed as the subject of discussions about

a. the advantages of the invention (col. 5, ll. 17–20; col. 5, ll. 33–35; col.
    5, ll. 39–40; and, col. 8, ll. 61–63);

b. methods of renewing a content license (col. 14, ll. 37–45); and,
    methods of updating a content license (col. 11, ll. 14–16; col. 20, ll.
    9–20; col. 22, ll. 1–4; col. 22, ll. 18–21; col. 22, ll. 37–38; col. 22, ll.
    62–col. 23, l. 2; Figs. 7, 11, 15, 16, 17A and Fig. 17B).

But the '657 patent specification does not otherwise provide insight into
what the claim phrase "content license" covers.

Petitioner does not propose a specific construction for the phrase
"encrypt the content license with a public key associated with the at least
one multimedia client" limitation of claim 1.

Patent Owner states that "[i]n claim 1 of the '657 Patent, the content
license, which contains both the content key and usage parameters, is
asymmetrically encrypted with the content key." Prelim. Response 31. But
claim 1 is not so narrow in scope. It does not mention a "content key" and
the "content license" is not expressly defined as "contain[ing] both [a]
content key and usage parameters" as Patent Owner states.

Accordingly, we conclude that, under the broadest reasonable
interpretation, the term "content license" of claim 1 comprises at least
certain license data related to the associated "protected content."

This interpretation of "content license" of claim 1 applies equally to
claims 30 and 55 which include limitations to encrypting a content license
with a public key of similar scope.

2. The decryption key limitation of claim 28.

Claim 28, which depends from claim 1, further limits the "content license" such that it

> comprises a decryption key with which the at least one multimedia client can decrypt the protected content using the decryption key as at least one input parameter for a decryption algorithm and usage parameters specifying terms under which the protected content can be consumed.

Ex. 1002 col. 25 ll. 41–49.

Accordingly, the broadest reasonable interpretation of "content license" in the context of the subject matter defined by claim 28 is that it comprises a decryption key *as well as* usage parameters specifying terms under which the protected content can be consumed.

> Petitioner states that, with respect to claim 28,

> it is unclear if the content license: (1) comprises a content key[1], where the content key is used to decrypt protected content and the content key is also used to decrypt usage parameters; or (2) comprises a content key used to decrypt protected content and the content license also comprises usage parameters.

Pet. 52.

Patent Owner takes issue with Petitioners' construction of claim 28, arguing that claim 28 is not "open to two possible interpretations of usage parameters." Prelim. Response 32. According to the Patent Owner, "[t]he language of [claim 28] of the '657 Patent clarifies that the content key is employed to decrypt only the protected content, while the content license comprises both the content key and the usage parameters." Prelim Response

---

[1] Both Petitioners and Patent Owner use the phrase "content key," presumably referring to the "decryption key" that claims 1 and 28 actually use.

34. Patent Owner further states that "[i]n dependent claims 28 and 54 of the '657 Patent, the content license, which contains both the content key and the usage parameters, is asymmetrically encrypted using the client device public key." Prelim. Response 12.

Both the Petitioner and Patent Owner appear to agree that the claim 28 "content license" comprises a decryption key. The disagreement is over whether the claim 28 "content license" necessarily also includes usage parameters. However, it is not necessary to resolve this disagreement in order to determine whether Petitioner has demonstrated a reasonable likelihood that it would prevail with respect to at least one of the claims challenged in the Petition. Given that the "content license" of claim 1 is reasonably broadly construed to comprise certain license data related to the associated "protected content" and that claim 28 depends from claim 1, it follows that the claim 28 "content license" comprises, in addition to a decryption key, certain license data related to the associated "protected content." It is sufficient to find claim 28 is reasonably broadly construed to encompass encrypting a content license with a public key associated with the multimedia client where the "content license" contains, at a minimum, (a) a decryption key and (b) certain license data related to the associated "protected content."

The construction of "content license" of claim 28 applies equally to claim 54 which is of similar scope.

D. Overview of the Prior Art References

1. Bi

Bi discloses a digital content distribution and subscription system. "An important aspect of the invention is that the selected digital audio or video files are downloaded in an encrypted format." Ex. 1006, 10:7–8. To use the encrypted files requires one to first decrypt the files via a key.

> Once the customer information is verified, the selected digital audio files are downloaded from the Digital Content Storage data store 22 as well as a "key" is downloaded from the license server 44 to the subscriber's computing platform 100 (FIG. 6), such as a PC. [T]the license "key" is used to decode or decrypt the encrypted digital audio files.

Id. at 10:21–24.

2. Peinado

Peinado discloses an enforcement and method for implementing digital rights management (DRM). According to Peinado, the DRM system decrypts encrypted digital content if a user has a valid license for the digital content and the right to play the digital content according to the license rules in the valid license. Ex. 1007 (0116). The DRM system involves interacting with a black box in a user's computing device, the black box performing encryption and decryption functions for the user's computing device. *Id.* (0098). The black box includes a private/public key pair. *Id.* at (0016). When a user requests a license, the client machine sends the black box public key to a license server. According to Peinado, the downloaded license comprises a rights description and the decryption key. *See* Peinado paragraphs 162 and 163. "The license server uses the black box public key to encrypt the decryption key, and the decryption key to encrypt the license

terms, then downloads the encrypted decryption key and encrypted license terms to the user's computing device along with a license signature." *Id.* (0017). The black box is caused to decrypt the decryption key and license terms, and if the user is allowed to play protected content according to the license, to play such content, "[t]he black box decrypts the encrypted digital content." *Id.* (0018).

3. Reisman

Reisman "is directed generally to interactive television and similar interactive hypermedia such as from television or Internet sources, and more particularly to the provision and use of user interfaces that permit interaction using multiple coordinated device sets." Ex. 1008 (0002).

4. Meffert

Meffert "is directed generally to implementations of public key infrastructure (PKI) based encryption and specifically to harnessing the advantages of PKI to provide encryption of and controlled access to data including, but not limited to, email, email attachments, streaming media, XML along with other transaction formats, and wireless communication data." Ex. 1009 (0002).

5. Pasieka

Pasieka is directed to "provid[ing] a method and device for generating a public/private key pair at a client processor that does not require substantial computing resources." Ex. 1010, 3:10–12.

E. Ground I

Petitioners challenge claims 1–3, 5–24, 27, 28, 30–32, and 34–55 as obvious under 35 U.S.C. § 103(a) over Bi and Peinado. Pet. 4, 48–55.

Claim 1

The "encrypt the content license with a public key associated with the at least one multimedia client" limitation of claim 1 is reasonably broadly construed as encrypting a content license with a public key associated with the multimedia client where the "content license" contains at least certain license data related to the associated "protected content." *See* § II.C.2.

With respect to said limitation, the Petitioner argues the following:

Bi instructs a POSITA to look to a particular DRM implementation for details of licensing, and a POSITA would look to the teachings of Peinado details of encrypting content licenses and details regarding the contents of a license. A POSITA would have been motivated to encrypt a license before sending it to a client device because it is desirable to prevent easy modifications to protected content, and Peinado describes encrypting a content license at the content license server responsive to license requests from the client device. See Peinado at [0163]; Rubin Decl. ¶269. Unencrypted content licenses and keys leave content unprotected. Rubin Decl. ¶269. Accordingly, it would be natural for a POSITA to incorporate Peinado's teachings of content licenses and encryption of those content licenses. Id.

Peinado teaches encrypting a content license at a license server according to a public key associated with the multimedia client. Peinado teaches a "black box" at the client machine that performs decryption with a public/private key pair. Peinado at [0016]. The public key is made available to the license server to "encrypt[] portions of the issued license." *Id.* The content license includes inter alia a "decryption key (KD) for the digital content" that is encrypted by the license server with the user's

computing device's black box public key. *Id.* at [0160]–[0163];
[0181], [0189], [0017]; *see also id.* at [0012] (stating that the
"decryption key (KD) . . . decrypts the encrypted digital
content."); *see also* [0162] (stating that the digital rights license
is encrypted). Indeed, encrypting sensitive data, such as content
licenses, is the core purpose of DRM systems. Rubin Decl.
¶270. Accordingly, Peinado teaches encrypting the content
license with a public key associated with the at least one
multimedia client (the client's black box public key).

Pet. 37–38.

Patent Owner disagrees, arguing *inter alia* that the claims provide for

a "single-step license encryption scheme" in contrast to "Peinado's two-step

license encryption scheme of symmetrically encrypting the digital rights

license and then asymmetrically encrypting the decryption key." Prelim.

Resp. 57.

The evidence favors the Patent Owner's position.

The passages from Peinado that the Petitioner relies upon are

reproduced below:

- [0012] a decryption key (KD) that decrypts the encrypted digital
  content;

- [0016] The public key is made available to the license server for
  purposes of encrypting portions of the issued license, thereby
  binding such license to such black box.

- [0017] When a user requests a license, the client machine sends the
  black box public key, version number, and signature to the license
  server, and such license server issues a license only if the version
  number is current and the signature is valid. A license request also
  includes an identification of the digital content for which a license
  is requested and a key ID that identifies the decryption key
  associated with the requested digital content. The license server
  uses the black box public key to encrypt the decryption key, and
  the decryption key to encrypt the license terms, then downloads the

encrypted decryption key and encrypted license terms to the user's computing device along with a license signature.

- [0160] Once all the terms of the license 16 have been negotiated and agreed to by both the license server 24 and user (step 715), a digital license 16 is generated by the license server 24 (step 719), where such generated license 16 is based at least in part on the license request, the black box 30 public key (PU-BB), and the decryption key (KD) for the digital content 12 that is the basis of the request as obtained from the content-key database 20.

- [0161] the content ID of the digital content 12 to which the license 16 applies;

- [0162] a Digital Rights License (DRL) 48 (i.e., the rights description or actual terms and conditions of the license 16 written in a predetermined form that the license evaluator 36 can interrogate), perhaps encrypted with the decryption key (KD) (i.e., KD (DRL));

- [0163] the decryption key (KD) for the digital content 12 encrypted with the black box 30 public key (PU-BB) as receive in the license request (i.e.,(PUBB (KD));

- [0181] Referring now to FIG. 5B, and assuming, now, that the license evaluator 36 has found at least one valid license 16 and that at least one of such valid licenses 16 provides the user with the rights necessary to render the corresponding digital content 12 in the manner sought (i.e., is enabling), the license evaluator 36 then selects one of such licenses 16 for further use (step 519). Specifically, to render the requested digital content 12, the license evaluator 36 and the black box 30 in combination obtain the decryption key (KD) from such license 16, and the black box 30 employs such decryption key (KD) to decrypt the digital content 12. In one embodiment of the present invention, and as was discussed above, the decryption key (KD) as obtained from the license 16 is encrypted with the black box 30 public key (PU-BB(KD)), and the black box 30 decrypts such encrypted decryption key with its private key (PR-BB) to produce the decryption key (KD) (steps 521, 523). However, other methods of obtaining the decryption key (KD) for the digital content 12 may

19

be employed without departing from the spirit and scope of the present invention.

- [0189] the decryption key (KD) for the digital content 12 encrypted with the black box 30 public key (PU-BB) (i.e.,(PU-BB (KD));

Petitioner's position is that "Peinado describes encrypting a content license." Pet. 37 (relying on Rubin Decl. ¶269).

Peinado [0012] does not describe or teach encrypting a "content license" in the manner recited in the challenged claims. When a user attempts to render digital content for the first time, a Digital Rights Management (DRM) system on a user's computing device provides the means for obtaining a license. *See* Peinado [0011]. "The license includes:" ([0011]) "a decryption key that decrypts the encrypted digital content;" [0012]. Peinado [0012] simply discloses encrypting one element of Peinado's license with a public key; that is, a decryption key. The other elements of Peinado's license are "a description of the rights [] conferred by the license and related conditions" [0013], and "a digital signature that ensures the integrity of the license" [0013]. There is no indication that these other elements are encrypted with a public key.

Peinado [0016] also does not describe or teach encrypting a "content license" as required by the challenged claims. This so because the "content license" has been reasonably broadly construed to include at least certain license data (see C. above). By contrast, Peinado [0160] does not indicate that the encrypted portion includes license data and thus Peinado [0016] does not describe that the black box public key is used to encrypt license data.

According to Peinado [0017], "[t]he license server uses the black box public key to encrypt the decryption key, and the decryption key to encrypt the license terms." Given that the decryption key is an element of the license (see [0012]), and the black box public key is used to encrypt the decryption key (see [0017]), then it follows that the portion of the issued license ([0016]) that the black box public encrypts is the decryption key.

Peinado [0160] also does not describe or teach encrypting a "content license" as required by the challenged claims, which is reasonably broadly construed to include at least encrypting license data by a public key. Rather, it describes a generated license "based at least in part on" the black box public key.

Peinado [0161]–[0163] does not describe or teach encrypting a "content license" as required by the challenged claims, which is reasonably broadly construed to include at least encrypting license data by a public key. They disclose some of the elements of a generated license; that is, "the content ID of the digital content" ([0161]); "a Digital Rights License" ([0162]); and, "the decryption key" for the encrypted digital content ([0163]). Like Peinado [0011]–[0013], they disclose elements of the Peinado license, but there is no disclosure that license terms are encrypted with a public key.

Peinado [0181] and [0189] do not describe or teach encrypting a "content license" as required by the challenged claims, because it conveys nothing about encryption of anything that corresponds to the license data of the content license.

The evidence indicates that Peinado's black box public key that the license server receives from the client *only* encrypts the decryption key

contained in the license. It does not encrypt anything that constitutes license data which, according to our interpretation of "content license," must be in the content license. Thus, Peinado does not disclose encrypting the "content license" as claimed.

Claim 1 requires "encrypting the content license with a public key associated with the at least one multimedia client." Because Peinado discloses that the black box public key only encrypts the decryption key of the content license, but not any license data, it does not disclose encrypting a content license with a public key associated with the at least one multimedia client (the client's black box public key) as claimed.

Claims 30 and 55

Independent claims 30 and 55, like claim 1, provide for encrypting a content license with a public key. Because Peinado discloses that the black box public key only encrypts the decryption key of the content license, it does not in fact disclose encrypting a content license with a public key associated with the at least one multimedia client (the client's black box public key) as claimed.

Claims 2, 3, 5–24 and 27

Claims 2, 3, 5–24 and 27 depend from claim 1 and therefore include the claim 1 "encrypting the content license with a public key associated with the at least one multimedia client" limitation. Petitioner's position that "Peinado describes encrypting a content license" and "Peinado teaches encrypting a content license" (Pet. 37) applies to claims 2, 3, 5–24 and 27.

See Pet. 41–52. We disagree for the reasons discussed with respect to the challenge of claim 1.

Claims 28 and 54

Claim 28, and claim 54 which parallels claim 28, are reasonably broadly construed as encrypting a content license with a public key associated with the multimedia client where the "content license" contains at least (a) certain license data related to the associated "protected content" and (b) a decryption key.

Petitioner's position that "Peinado describes encrypting a content license" and "Peinado teaches encrypting a content license" (Pet. 37) applies to claims 28 and 54, albeit claims 28 and 54 further limit the content license to include a decryption key. *See* Pet. 52–54 and 59, respectively.

However, because Peinado discloses that the black box public key only encrypts the decryption key of the content license, it does not in fact disclose encrypting a content license with a public key associated with the at least one multimedia client (the client's black box public key) as claimed.

Claims 31, 32 and 34–53

Claims 31, 32 and 34–53 depend from claim 30 and therefore include the claim 30 limitation to encrypting a content license with a public key. Petitioner's position that "Peinado describes encrypting a content license" and "Peinado teaches encrypting a content license" (Pet. 37) applies to claims 31, 32 and 34–53. *See* Pet. 55–59. We disagree for the reasons discussed with respect to the challenge of claim 1.

F. Ground II

Petitioner challenges claim 26 as obvious under 35 U.S.C. § 103(a) over Bi, Peinado, and Reisman.

Claim 26 depends from claim 1 and therefore includes the claim 1 "encrypting the content license with a public key associated with the at least one multimedia client" limitation. Petitioner's position that "Peinado describes encrypting a content license" and "Peinado teaches encrypting a content license" (Pet. 37) applies to claim 26. See Pet. 62–63. We disagree for the reasons discussed with respect to the challenge of claim 1.

For the above reasons, we determine that the Petition does not establish a reasonable likelihood that claim 26 is unpatentable over Bi, Peinado, and Reisman.

G. Ground III

Petitioner challenges claims 25 and 29 as obvious under 35 U.S.C. § 103(a) over Bi, Peinado, and Meffert. Pet. 4, 48–55.

Claims 25 and 29 depend from claim 1 and therefore each include the claim 1 "encrypting the content license with a public key associated with the at least one multimedia client" limitation. Petitioners' position that "Peinado describes encrypting a content license" and "Peinado teaches encrypting a content license" (Pet. 37) applies to claims 25 and 29. See Pet. 63–65. We disagree for the reasons discussed with respect to the challenge of claim 1.

H. Ground IV

Petitioner challenges claims 4 and 33 as obvious under 35 U.S.C. § 103(a) over Bi, Peinado, and Pasieka. Pet. 4, 48–55.

Claims 4 and 33 depend from claims 1 and 30, respectively, and therefore they also require encrypting the content license with a public key associated with the at least one multimedia client. Petitioner's position that "Peinado describes encrypting a content license" and "Peinado teaches encrypting a content license" (Pet. 37) applies to claims 4 and 33. See Pet. 66–68. We disagree for the reasons discussed with respect to the challenge of claim 1.

III. CONCLUSION

For the foregoing reasons, we determine that Petitioner has not demonstrated a reasonable likelihood that it would prevail with respect to at least one of the claims challenged in the Petition. We do not institute an *inter partes* review on any of claims 1–55 of the '657 patent on any ground.

IV. ORDER

It is

ORDERED that the Petition is *denied*, and that we do not institute an *inter partes* review of any claim of claims 1–55 of the '657 patent.

PETITIONER:

Chun M. Ng
Matthew C. Bernstein
Martin E. Gilmore
Miguel J. Bombach
Matthew J. Moffa
PERKINS COIE LLP
CNg@perkinscoie.com
MBernstein@perkinscoie.com
MGilmore@perkinscoie.com
MBombach@perkinscoie.com
MMoffa@perkinscoie.com

PATENT OWNER:

Stephen R. Risley
KENT & RISLEY LLC
steverisley@kentrisley.com

Robert A. Blaha
SMITH TEMPEL BLAHA LLC
rblaha@srtslaw.com