

UNITED STATES PATENT AND TRADEMARK OFFICE

---

BEFORE THE PATENT TRIAL AND APPEAL BOARD

---

AMAZON.COM, HULU, LLC, and NETFLIX, INC.,  
Petitioner,

v.

DIGITAL MEDIA TECHNOLOGIES, INC.,  
Patent Owner.

---

Case IPR2017-00284  
Patent 8,964,764 B2

---

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

LEE, *Administrative Patent Judge.*

DECISION  
Denying Institution of *Inter Partes* Review  
37 C.F.R. § 42.108(b)

## I. INTRODUCTION

### A. Background and Summary

On November 23, 2016, Petitioner<sup>1</sup> filed a Petition (Paper 2, “Pet.”) to institute *inter partes* review of claims 1–37 of U.S. Patent No. 8,964,764 B2 (Ex. 1001, “the ’764 patent”). On March 9, 2017, Patent Owner<sup>2</sup> filed a Preliminary Response (Paper 8, “Prelim. Resp.”).<sup>3</sup> To institute an *inter partes* review, we must determine that the information presented in the Petition shows “that there is a reasonable likelihood that the petitioner would prevail with respect to at least 1 of the claims challenged in the petition.” 35 U.S.C. § 314(a). Having considered the arguments and evidence presented by Petitioner, we determine that Petitioner has *not* demonstrated a reasonable likelihood that it would prevail in establishing the unpatentability of any one of claims 1–37 of the ’764 patent.

### B. Related Matters

Petitioner indicates that the ’764 patent and related U.S. Patent No. 9,300,657 B2 were asserted by Patent Owner against Petitioner in *Digital Media Technologies Inc. v. Amazon.com, Inc.*, Case No. 4:16-cv-00244 (N.D. Fla.), *Digital Media Technologies Inc. v. Hulu, LLC*, Case No. 4:16-cv-00245 (N.D. Fla.), and *Digital Media Technologies Inc. v. Netflix, Inc.*, Case No. 4:16-cv-00243 (N.D. Fla.). Pet. 2. Patent Owner additionally identifies *inter partes* review proceeding IPR2017-00285 as involving related U.S. Patent No. 9,300,657 B2. Paper 5, 2.

---

<sup>1</sup> Amazon.Com, Inc., Hulu, LLC, and Netflix, Inc.

<sup>2</sup> Digital Media Technologies, Inc.

<sup>3</sup> The response relies on the Declaration of Ivan Zatkovich (Ex. 2001).

C. The '764 Patent

The '764 patent provides a multimedia networking system that can be either wired or wireless. Ex. 1001, 2:45–48. It allows for the importation of content from an external content provider via the Internet. *Id.* at 2:52–54. A user can freely import, create, and share content within the network. *Id.* at 3:15–16. The system allows the user to control system functions from any component linked to the network and properly designated to access the network. *Id.* at 3:49–51.

Claim 1 is the only independent claim of all challenged claims and is reproduced below:

1. A multimedia system, comprising:  
an external control server configured to:
  - receive a request from a client device via a wide area network requesting protected content to be sent to the client device;
  - receive client device authentication information from the client device, the client device authentication information comprising at least information related to a user authentication and a device authorization;
  - validate the client device authentication information according to predetermined criteria;
  - send protected content location information to the client device, the protected content location information being associated with a location of the protected content;
  - encrypt, in response to receiving a request for a content license from the client device via the wide area network, the request comprising information related to a location of the content license and being based on a determination by the client device that the protected content is encrypted and requires a content license, the content license using a public key associated with the client device, the content license comprising a content

key which the client device uses to decrypt the protected content and usage parameters specifying terms under which the protected content can be consumed; and

send the encrypted content license to the client device, the client device using a private key associated with the client device to decrypt the content license and using the content key to decrypt the protected content for use according to usage parameters specified by the content license;

and

an external content server configured to:

receive a request for the protected content from the client device, the request comprising the protected content location information provided by the external control server; and

send the protected content to the client device.

Ex. 1001, 23:46–24:18.

D. Evidence Relied Upon by Petitioner

Petitioner relies on the following references:<sup>4</sup>

|         | <b>Reference</b>                      | <b>Date</b>                 | <b>Exhibit</b> |
|---------|---------------------------------------|-----------------------------|----------------|
| Bi      | PCT Int’l Pub. App.<br>WO 02/45316 A2 | Published June 6,<br>2002   | Ex. 1006       |
| Peinado | U.S. Pub. App. 2003/0078853<br>A1     | Published April 24,<br>2003 | Ex. 1007       |
| Reisman | U.S. Pub. App. 2003/0229900<br>A1     | Published Dec. 11,<br>2003  | Ex. 1008       |

Petitioner also relies on the Declaration of Aviel Rubin, Ph.D.

Ex. 1003.

---

<sup>4</sup> The earliest possible effective filing date of the ’764 patent that potentially may be established by Patent Owner is May 19, 2004. Ex. 1001, (60) (62).

E. The Asserted Grounds

Petitioner asserts the following grounds of unpatentability:

| Claim(s) Challenged                       | Basis    | References               |
|---|----------|--------------------------|
| 1–37                                      | § 103(a) | Bi and Peinado           |
| 3–6, 8, 10, 11, 13–16, 22, 33, 35, and 37 | § 103(a) | Bi, Peinado, and Reisman |

II. ANALYSIS

The question of obviousness is resolved on the basis of underlying factual determinations including: (1) the scope and content of the prior art; (2) any differences between the claimed subject matter and the prior art; (3) the level of ordinary skill in the art; and (4) objective evidence of nonobviousness. *Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966). One seeking to establish obviousness based on more than one reference also must articulate sufficient reasoning with rational underpinning to combine teachings. *See KSR Int’l Co. v. Teleflex, Inc.*, 550 U.S. 398, 418 (2007).

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).

A. Claim Construction

In an *inter partes* review, claim terms in an unexpired patent are interpreted according to their broadest reasonable construction in light of the specification of the patent in which they appear. 37 C.F.R. § 42.100(b); *Cuozzo Speed Techs., LLC v. Lee*, 136 S. Ct. 2131, 2142–46 (2016). Consistent with that standard, claim terms also are given their ordinary and

customary meaning, as would be understood by one of ordinary skill in the art in the context of the entire disclosure. *See In re Translogic Tech., Inc.*, 504 F.3d 1249, 1257 (Fed. Cir. 2007). There are, however, two exceptions to that rule: “1) when a patentee sets out a definition and acts as his own lexicographer,” and “2) when the patentee disavows the full scope of a claim term either in the specification or during prosecution.” *Thorner v. Sony Comp. Entm’t Am. LLC*, 669 F.3d 1362, 1365 (Fed. Cir. 2012).

If an inventor acts as his or her own lexicographer, the definition must be set forth in the specification with reasonable clarity, deliberateness, and precision. *Renishaw PLC v. Marposs Societa’ per Azioni*, 158 F.3d 1243, 1249 (Fed. Cir. 1998). It is improper to add into a claim an extraneous limitation, i.e., one that is added wholly apart from any need for the addition. *See, e.g., Hoganas AB v. Dresser Indus., Inc.*, 9 F.3d 948, 950 (Fed. Cir. 1993); *E.I. du Pont de Nemours & Co. v. Phillips Petroleum Co.*, 849 F.2d 1430, 1433 (Fed. Cir. 1988). Although it is improper to read a limitation from the specification into the claims, *In re Van Geuns*, 988 F.2d 1181, 1184 (Fed. Cir. 1993), claims still must be read in view of the specification of which they are a part. *Microsoft Corp. v. Multi-Tech Sys., Inc.*, 357 F.3d 1340, 1347 (Fed. Cir. 2004).

Only terms which are in controversy need to be construed, and only to the extent necessary to resolve the controversy. *See Wellman, Inc. v. Eastman Chem. Co.*, 642 F.3d 1355, 1361 (Fed. Cir. 2011); *Vivid Techs., Inc. v. Am. Sci. & Eng’g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999).

*“the content license comprising a content key which the client device uses to decrypt the protected content and usage parameters specifying terms under which the protected content can be consumed”*

Claim 1 recites the phrase “the content license comprising a content key which the client device uses to decrypt the protected content and usage parameters specifying terms under which the protected content can be consumed.” Ex. 1001, 24:1–5. There are two possible ways to read this phrase. The first reading is that the phrase defines the two parts of a content license, i.e., content key and usage parameters. The second reading is that the phrase first specifies that the content license comprises a content key, and then defines how the content key is used, i.e., to decrypt protected content and also to decrypt usage parameters specifying terms under which the protected content can be consumed. Patent Owner urges the first reading. Petitioner urges the second reading. For reasons discussed below, we agree with Patent Owner, and construe the phrase as specifying that the content license comprises (1) “a content key which the client device uses to decrypt the protected content,” and (2) “usage parameters specifying terms under which the protected content can be consumed.”

Another clause within claim 1 recites: “the client device using a private key associated with the client device to decrypt the content license and using the content key to decrypt the protected content for use *according to usage parameters specified by the content license.*” Ex. 1001, 24:7–11 (emphasis added). Consistent with the clause at issue that is being construed, this other clause within claim 1 reiterates that the content key is used to decrypt the protected content. Importantly, however, this other clause makes clear that usage parameters are specified by the content

license. That is a strong indication that the first reading is correct and that usage parameters are a part of the content license.

Another reason in support of the first reading is that a content license logically is expected to include the conditions of usage for the licensed content, i.e., the usage parameters. Still another reason in support of the first reading is that the term “usage parameters” is not previously defined in claim 1, and thus the first reading serves to introduce “usage parameters” by specifying that they are comprised within the content license. In contrast, the second reading would leave unexplained and uncertain where usage parameters specifying the terms of consumption would be located. Although not by themselves determinative, these observations add to the evidentiary weight as a whole more in support of the first reading than the second.<sup>5</sup>

Petitioner points to no embodiment in the '764 patent in which usage parameters specifying the terms of consumption are not a part of the content license and we can find no such disclosure. Similarly, Petitioner points to no embodiment in the '764 patent in which the content key is used to decrypt the usage parameters and we can find no such disclosure. These observations also are not by themselves determinative, but they add to the evidentiary weight as a whole more in support of the first reading than the second.

---

<sup>5</sup> Patent Owner asserts that during prosecution, it represented to the Examiner that the content license comprises both the content key and usage parameters. Prelim. Resp. 7–8 (citing Ex. 1004, 346–48). We have reviewed the cited portion of the prosecution history, and find no such representation. The Applicant simply reiterated the entirety of the recited clause at issue as something not disclosed by the prior art. That is insufficient to indicate one way or the other with respect to the issue at hand.

For the foregoing reasons, we construe the phrase “the content license comprising a content key which the client device uses to decrypt the protected content and usage parameters specifying terms under which the protected content can be consumed” as specifying that the content license comprises (1) “a content key which the client device uses to decrypt the protected content,” and (2) “usage parameters specifying terms under which the protected content can be consumed.”

B. Alleged Unpatentability of  
Claims 1–37 as Obvious over Bi and Peinado

Claim 1 is independent and all other claims depend, directly or indirectly, from claim 1. For reasons discussed below, Petitioner has not shown a reasonable likelihood that it would prevail in establishing unpatentability of any one of claims 1–37 as obvious over Bi and Peinado.

1. Bi

Bi discloses a digital content distribution and subscription system for digital data files which provide subscribers music or video from locally-stored digital files or on demand for a fee. Ex. 1006, 2:20–22. The system optionally provides streaming digital data. *Id.* at 2:22–23. The subscription service may be accessed from a client computing platform, and the client computing platform “can encompass anything from general-purpose devices, such as a personal computer, to open fixed function devices, such as a set-up box that connects to a television set.” *Id.* at 16:18–20.

To help ensure that downloads of digital content data are made only by authorized subscribers, Bi’s system uses a subscriber login procedure and unique tokens to identify digital content data such that a download address is only valid for a specific subscriber during a specific time period. *Id.* at 14:9–16. Bi further describes the optional use of a digital rights

management system, and identifies the Microsoft Windows Media Rights Manager as an example:

A Digital Rights Management software system 140 may also be provided and functions as an additional level of protection for the digital content data 108 to prevent access to or playback of the digital content data 108 through encryption of the digital content data 108 and the use of access or playback licenses. Decryption of the digital content data 108 for access to or playback of the digital content data 108 requires the subscriber on the client computing platform 100 to have specific access or playback licenses for the digital content data 108. The access or playback licenses are obtained from license servers 102 and *are handled in a manner corresponding to the specific requirements of the digital rights management 140 implementation used*, for example, Microsoft Windows Media Rights Manager.

*Id.* at 14:17–25 (emphasis added).

Bi describes that once a user is authenticated, the user on a client computing platform may access a digital content catalog through one or more application servers. *Id.* at 11:24–26. Bi also describes that after a user on a client computing platform has determined what digital content data to download, the client computing platform accesses this digital content data through one or more content servers. *Id.* at 11:32–34. Bi further describes that where the digital content data is kept in a secure or protected format, the client computing platform must also obtain access or playback licenses.<sup>6</sup> *Id.* at 11:35 to 12:7. In that connection, Bi states: “The client computing platform 100 accesses the license servers 102 to obtain these access or playback licenses, using, for example, Microsoft Windows Media Rights

---

<sup>6</sup> Bi describes that an aspect of its system is that the selected digital files are downloaded in an encrypted format and that a key is downloaded to the subscriber to enable the content to be decrypted. Ex. 1006, 10:7–10.

Manager, for digital rights management.” *Id.* at 12:7–9; *see also id.* at 27:25–28 (“the license server 102 obtains the license for the specific digital content data 108 in step 234 in a manner corresponding to the requirements of the digital rights management implementation used, for example, Microsoft Windows Media Rights Manager.”).

## 2. Peinado

Peinado discloses a method for implementing digital rights management. Ex. 1007, Abstr. The method operates as follows:

When a user attempts to render the digital content on a computing device, the rendering application invokes a Digital Rights Management (DRM) system on such user’s computing device. If the user is attempting to render the digital content for the first time, the DRM system either directs the user to a license server to obtain a license to render such digital content in the manner sought, or transparently obtains such license from such license server without any action necessary on the part of the user.

*Id.* at (0011).

The license includes (1) a decryption key “KD” that decrypts the encrypted digital content, (2) a decryption of the rights conferred by the license and related conditions (hereinafter “rights description”), and (3) a digital signature that ensures the integrity of the license. *Id.* at (0011)–(0014). Each license specifies whether the user has rights to play the digital content based on any of several factors, including who the user is, where the user is located, what type of computing device the user is using, what rendering application is calling the DRM system, the date, and the time, etc. *Id.* at (0136). The rights description may limit the license to a pre-determined number of plays or a predetermined play time. *Id.*

The DRM system on the user's computing device is equipped with a "black box" that includes a public/private key pair, a version number, and a unique signature. *Id.* at (0016). The public key is made available to the license server for the purpose of encrypting portions of the issued license, thereby binding such license to such black box, and the private key is made available to the to the black box only, for the purpose of decrypting information encrypted with the corresponding public key. *Id.*

Specifically, when a license is requested, the client machine sends the black box public key, version number, and signature to the license server, as well as an identification of the digital content for which a license is requested. *Id.* at (0017). Then, the license server uses the black box public key to encrypt the decryption key, and the decryption key to encrypt the license terms. *Id.* Thereafter, the license server downloads the encrypted decryption key and the encrypted license terms to the user's computing device along with a license signature. *Id.*

Peinado describes the generated license as follows:

In one embodiment of the present invention, and as seen in FIG. 8, the generated license 16 includes:

[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[d] in the license request (i.e., (PU-BB (KD)));

[0164] a digital signature from the license server 24 (without any attached certificate) based on (KD (DRL)) and (PU-BB (KD)) and encrypted with the license server 24 private key (i.e., (S (PR-LS))); and

[0165] the certificate that the license server 24 obtained previously from the content server 22, such certificate indicating that the license server 24 has the authority from the content server 22 to issue the license 16 (i.e., (CERT (PU-LS) S (PR-CS))).

*Id.* at (0160)–(0165) (emphases added).

### 3. Discussion

Our claim construction, as discussed above, is determinative of this alleged ground of unpatentability. Specifically, as a matter of claim construction, we determined that the content license includes (1) a content key, and (2) usage parameters specifying terms under which the protected content can be consumed. Another portion of claim 1 recites that the external control server is configured to encrypt “the content license using a public key associated with the client device.” Ex. 1001, 23:61–24:1. Because the content license is recited expressly as comprising a content key and usage parameters specifying terms under which the protected content can be consumed, we determine the limitation that the server is configured to encrypt the content license using a public key requires use of the public key to encrypt both (1) the content key and (2) the usage parameters.

Petitioner asserts that under the broadest reasonable interpretation, the limitation that the server is configured to encrypt the content license can be met simply by encrypting some component of the content license with a public key, e.g., the content key without the usage parameters. Pet. 38. We disagree. Claim 1 expressly recites that the content license comprises usage parameters specifying terms under which the protected content can be

consumed, and such usage parameters are the essence of any content license and not an insignificant addition by any reasonable standard. To whatever extent the broadest reasonable interpretation possibly may allow some part of the content license to be excepted from the requirement of being encrypted by use of the public key associated with the client device, the usage parameters could not be that part. Petitioner further notes that the '764 patent discloses an embodiment that encrypts and sends the content key and the usage parameters separately. *Id.* That observation, although true, does not persuade us that encrypting the content license by using a public key can be met without encrypting the usage parameters of the license by using a public key. In summary, we determine that excepting the usage parameters in the manner urged by Petitioner is an unreasonable interpretation of the claim.

Another portion of claim 1 recites “using a private key associated with the client device to decrypt the content license.” *Id.* at 24:7–8. Thus, as is noted by Patent Owner (Prelim. Resp. 14–15), claim 1 requires asymmetric encryption/decryption of both (1) the content key and (2) the usage parameters specifying terms under which the protected content can be consumed. Specifically, a public key is used for their encryption, and a private key is used for their decryption. The same key is not used for both encryption and decryption. As we explain below, Petitioner has not adequately accounted for this feature of independent claim 1, i.e., asymmetric encryption/decryption of the usage parameters specifying terms under which the protected content can be consumed.

First, Petitioner observes that Peinado discloses encrypting the decryption key, which corresponds to the claimed content key, with the

public key, and encrypting the Digital Rights License, which corresponds to the usage parameters, with the decryption key. Pet. 39 (citing Ex. 1007 (162), (163), (188), (189)). Petitioner further observes that a computing device needs to decrypt the decryption key prior to using the decrypted decryption key to decrypt the Digital Rights License. *Id.* (citing Ex. 1007 (202)). According to Petitioner, that in effect means all data encrypted by the decryption key ultimately are locked and protected with the black box public key. *Id.* (citing Ex. 1003 ¶ 171). On that basis, Petitioner argues that a person of ordinary skill in the art (“POSITA”) would understand that encryption and decryption of the Digital Rights License is mathematically related to the black box’s public key because the black box’s private key is needed to decrypt the Digital Rights License by first decrypting the decryption key with the private key. Petitioner further argues that a POSITA would understand that the Digital Rights License is asymmetrically encrypted with the black box’s public key because the symmetric key used to encrypt and decrypt the Digital Rights License is itself asymmetrically encrypted with the black box’s public key.

Petitioner’s argument is unpersuasive. Peinado’s symmetric encryption of the Digital Rights License is unchanged regardless of how the symmetric key is obtained. It is an immutable fact that in Peinado the same key is used to encrypt and decrypt the Digital Rights License. That the key itself may, in turn, be asymmetrically encrypted while being transferred to a computing device does not alter symmetric encryption of the Digital Rights License. In summary, the key that encrypts the Digital Rights License is the decryption key and not the public key that encrypts the decryption key.

In the alternative, Petitioner argues that it would have been obvious to one with ordinary skill in the art “to directly encrypt the digital rights license (*i.e.*, the claimed usage parameters) with the black box public key.” Pet. 40.

In that connection, Petitioner asserts:

Peinado merely provides a suggestion to employ an encryption scheme on the Digital rights License. Peinado states that the Digital Rights License is “perhaps” encrypted with the decryption key (*i.e.*, the claimed content key). *Id.* at [0162], [0188]; *see also* claims 20, 48, 73, 99. Notably, Peinado states that how or if the Digital Rights License is encrypted is not critical to its disclosure. *Id.* at [0166], [0202]. A POSITA would understand that Peinado’s usage of “perhaps,” especially in light of Peinado’s discussion that the encryption of the Digital Rights License is not a critical aspect, is a suggestion to employ any encryption technique. Rubin Decl. ¶ 173. A POSITA would understand that any known technique to encrypt the Digital Rights License, including using the black box’s public key, could be employed. *Id.*

*Id.* at 40–41. Petitioner explains:

Bi teaches encrypting sensitive data sent over the Internet with a public key (Bi at 47-31-35) and Peinado communicates the Digital Rights License over the Internet (Peinado at [0010], [0039]). A POSITA would have been motivated by Bi’s suggestion to encrypt sensitive data over the Internet with a public key and Peinado’s teachings of public key encryption to encrypt the Digital Rights License with the black box’s public key. Rubin Decl. ¶ 174. Accordingly, instead of encrypting the Digital Rights License with the decryption key (a symmetric key), a POSITA would have found it obvious to employ asymmetric encryption and encrypt the Digital Rights License (*i.e.*, the claimed usage parameters) with the black box public key. Rubin Decl. ¶ 174. Thus, the Bi-Peinado combination teaches encrypting both the content key (*i.e.*, the decryption key) and the usage parameters (*i.e.*, the Digital Rights License) with the black box public key.

*Id.* at 41–42. For reasons discussed below, we are unpersuaded by Petitioner’s alternative argument.

We disagree with Petitioner’s treating Peinado’s disclosure of optionally encrypting the Digital Rights License, and doing so with a symmetric key, as an affirmative suggestion to employ any technique to encrypt the Digital Rights License, including use of an asymmetric public/private key pair to encrypt/decrypt the Digital Rights License. That is tantamount to asserting as obvious anything that could have been used. But that is not the law. The mere fact that the prior art may be modified in the manner urged by a proponent of obviousness does not make the modification obvious unless the prior art suggests the desirability of the modification. *See In re Fritch*, 972 F.2d 1260, 1266 (Fed. Cir. 1992). There must be reasoning with rational underpinning to support a conclusion of obviousness. *See In re Kahn*, 441 F.3d 977, 988 (Fed. Cir. 2006).

Petitioner has not shown sufficiently that the prior art would have suggested to one with ordinary skill in the art the desirability of encrypting the Digital Rights License of Peinado asymmetrically with a public key. Petitioner notes that Bi teaches asymmetrically encrypting sensitive data sent over the Internet with a public key, and that Peinado communicates its Digital Rights License over the Internet. Pet. 41. On that basis, Petitioner argues that a POSITA would have been motivated to encrypt Peinado’s Digital Rights License with a public key. *Id.* But Petitioner’s characterization of Bi’s disclosure is inaccurate. Bi does not disclose that in general all sensitive data on the Internet should be encrypted asymmetrically with a public key. Rather, it only discloses asymmetric encryption of “tokens” that are transmitted over the Internet. Ex. 1006, 47:31–35. And

tokens, as described in Bi, are codes used to authenticate that which is downloaded, such as “a randomly generated alphanumeric string of a predetermined or random length.” *Id.* at 47:9–14. Such tokens do not correspond to licenses, and are not comparable to the claimed usage parameters specifying terms under which the protected content can be consumed. We are not sufficiently persuaded that Bi’s disclosure of asymmetric encryption of tokens with a public key would have motivated one with ordinary skill in the art to modify Peinado’s symmetric encryption of its Digital Rights License so that the Digital Rights License is encrypted asymmetrically with a public key.

Each of claims 2–37 depends, directly or indirectly, from claim 1. The same deficiencies discussed above with respect to claim 1 carry through to each of dependent claims 2–37 by reason of their incorporation of all of the limitations of claim 1.

For the foregoing reasons, we determine that Petitioner has not shown a reasonable likelihood that it would prevail in establishing the unpatentability of any of claims 1–37 as obvious over Bi and Peinado.

C. Alleged Unpatentability of Claims 3–6, 8, 10, 11, 13–16, 22, 33, 35, and 37 as Obvious over Bi, Peinado, and Reisman

Each of claims 3–6, 8, 10, 11, 13–16, 22, 33, 35, and 37 depends, directly or indirectly, from independent claim 1. We have reviewed the Petition and find that Petitioner’s reliance on and application of Reisman to these claims do not cure the above-noted deficiencies of Bi and Peinado with respect to claim 1. We determine that Petitioner has not shown a reasonable likelihood that it would prevail in establishing unpatentability of any of

claim 3–6, 8, 10, 11, 13–16, 22, 33, 35, and 37 as obvious over Bi, Peinado, and Reisman.

### III. CONCLUSION

Petitioner has not shown a reasonable likelihood that it would prevail in establishing unpatentability of any of claims 1–37 of the '764 patent as obvious over Bi and Peinado.

Petitioner has not shown a reasonable likelihood that it would prevail in establishing unpatentability of any of claims 3–6, 8, 10, 11, 13–16, 22, 33, 35, and 37 of the '764 patent as obvious over Bi, Peinado, and Reisman.

### IV. ORDER

it is

ORDERED that the Petition is *denied*, and no trial is instituted with respect to any claim of U.S. patent No. 8,964,764 B2.

IPR2017-00284  
Patent 8,964,764 B2

COUNSEL FOR PETITIONER:

Chun Ng  
Miguel Bombach  
Matthew Moffa  
Matthew Bernstein  
Martin Gilmore  
[cng@perkinscoie.com](mailto:cng@perkinscoie.com)  
[mbombach@perkinscoie.com](mailto:mbombach@perkinscoie.com)  
[mmoffa@perkinscoi.com](mailto:mmoffa@perkinscoi.com)  
[mbernstein@perkinscoie.com](mailto:mbernstein@perkinscoie.com)  
[mgilmor@perkinscoi.com](mailto:mgilmor@perkinscoi.com)

COUNSEL FOR PATENT OWNER:

Stephen Risley  
Robert Blaha  
[steverisley@kentrisley.com](mailto:steverisley@kentrisley.com)  
[rblaha@srtslaw.com](mailto:rblaha@srtslaw.com)