

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

OPENTV, INC.

Petitioner

v.

CISCO SYSTEMS, INC., CISCO TECHNOLOGY INC., SCIENTIFIC-
ATLANTA, LLC, SCIENTIFIC-ATLANTA, INC. AND NDS AMERICAS INC.

Patent Owner

CASE: Unassigned

Patent No. 7,505,592 B2

**PETITION FOR *INTER PARTES* REVIEW
OF U.S. PATENT NO. 7,505,592 B2**

TABLE OF CONTENTS

EXHIBIT LIST	v
I. INTRODUCTION	1
II. MANDATORY NOTICES UNDER 37 C.F.R. § 42.8(A)(1)	1
A. REAL PARTY IN INTEREST	1
B. RELATED MATTERS	1
C. NOTICE OF LEAD AND BACKUP COUNSEL	2
D. SERVICE INFORMATION	2
III. REQUIREMENTS FOR INTER PARTES REVIEW	2
A. GROUND FOR STANDING.....	3
B. IDENTIFICATION OF CHALLENGE.....	3
1. Claims Challenged	3
2. The Prior Art	3
3. Supporting Evidence Relied Upon For The Challenge	4
4. The Statutory Ground(s) of Challenge & Legal Principles	4
5. Claim Construction under 37 C.F.R. § 42.100(b).....	5
6. How the Claims Are Unpatentable Under the Statutory Ground Identified in Paragraph (b)(2) of 37 C.F.R. § 42.104.....	5
IV. OVERVIEW OF THE ‘592 PATENT	5
A. PRIORITY DATE OF THE ‘592 PATENT	5
B. PERSON OF ORDINARY SKILL IN THE ART	6
C. BRIEF DESCRIPTION OF THE ‘592 PATENT	6
D. SUMMARY OF PROSECUTION HISTORY OF THE ‘592 PATENT.....	8
E. PROPOSED CLAIM CONSTRUCTION.....	9
1. “Service Instance”	9
2. “Communications Device”	10

TABLE OF CONTENTS
(continued)

3.	“Remote Client Devices”	10
4.	“Entitled to receive”	11
5.	“Subscriber Premises”	11
6.	“Subscriber”	12
7.	“Format protocol”	12
8.	“Accessible”	13
V.	THERE IS A REASONABLE LIKELIHOOD THAT AT LEAST ONE CLAIM OF THE ‘592 PATENT IS UNPATENTABLE	13
A.	IDENTIFICATION OF THE REFERENCES AS PRIOR ART.....	13
B.	SUMMARY OF INVALIDITY POSITIONS	14
C.	DIFFERENT INVALIDITY POSITIONS AGAINST EACH CLAIM ARE INDEPENDENT, DISTINCTIVE AND NOT REDUNDANT	15
VI.	DETAILED EXPLANATION OF THE GROUNDS FOR UNPATENTABILITY	16
A.	ANTICIPATION.....	16
1.	Claims 1-2, 6-8, 12-13, and 17-20 are Unpatentable Under 35 U.S.C. § 102(b) as Being Anticipated by Payton.....	16
2.	Claims 1-4, 6-10, 12-15 and 17-20 Are Unpatentable Under 35 U.S.C. § 102(e) As Being Anticipated By Hicks	33
		33
B.	OBVIOUSNESS	55
1.	Claims 2, 8 and 13 Are Unpatentable Under 35 U.S.C. § 103(a) over Hicks and Egli	55
2.	Claims 3-5, 9-11 and 14-16 Are Unpatentable Under 35 U.S.C. § 103(a) over Hicks and Safadi.....	56

TABLE OF CONTENTS
(continued)

3.	Claim 6 is Unpatentable Under 35 U.S.C. § 103(a) over Hicks and Putterman	59
VII.	CONCLUSION.....	60

EXHIBIT LIST

- Ex. 1001 U.S. Patent No. 7,505,592 B2 (“the ‘592 Patent”)
- Ex. 1002 U.S. Patent No. 5,790,935 (“Payton”)
- Ex. 1003 U.S. Patent No. 7,698,723 (“Hicks”)
- Ex. 1004 U.S. Patent Pub. No. 2002/0146237 (“Safadi”)
- Ex. 1005 U.S. Patent Pub. No. 2003/0110234 (“Egli”)
- Ex. 1006 U.S. Patent Pub. No. 2003/0135859 (“Putterman”)
- Ex. 1007 Michael Perkins, Ph.D. Declaration (with Appendices)
- Ex. 1008 Prosecution File History of the ‘592 Patent
- Ex. 1009 Prior Art Matrix
- Ex. 1010 IEEE Dictionary Evidence

Pursuant to 35 U.S.C. § 311 and 37 C.F.R. § 42.100, OpenTV, Inc. (“Petitioner”), petitions for *inter partes* review of claims 1-20 of U.S. Pat. No. 7,505,592 B2 (“the ‘592 Patent”, Exhibit 1001), assigned to Scientific-Atlanta, Inc. Based on information and belief, Scientific-Atlanta, Inc., Scientific-Atlanta, LLC, Cisco Systems, Inc., Cisco Technology Inc., and NDS Americas Inc. (collectively “Cisco”) each may have, or are represented by Cisco to have, or have had, ownership interest in the ‘592 Patent. Accordingly, these entities are collectively referred to as “Patent Owner” in this Petition.

I. INTRODUCTION

This Petition demonstrates that there is a reasonable likelihood that Petitioner will prevail with respect to at least one of the claims challenged in this petition and thus a trial for *inter partes* review must be instituted. Evidence in this Petition demonstrates that claims 1-20 of the U.S. Patent No. 7,505,592 B2 (“the ‘592 Patent”) are unpatentable under 35 U.S.C. § 102 and/or § 103. Petitioner respectfully requests claims 1-20 be rejected and cancelled.

II. MANDATORY NOTICES UNDER 37 C.F.R. § 42.8(A)(1)

A. REAL PARTY IN INTEREST

Petitioner OpenTV, Inc. is the real party in interest and is wholly owned by Kudelski S.A., which is publicly traded on the SIX Swiss Exchange.

B. RELATED MATTERS

The '592 Patent and U.S. Patent Nos. 6,252,964 B1 and 6,744,892 B2 are being asserted against Petitioner in an on-going patent infringement lawsuit brought by Patent Owner in *Cisco Systems, Inc. et al. v. OpenTV Inc. et al.*, 5:13-cv-00282, filed in the Northern District of California on January 18, 2013.

5 In addition, Petitioner is concurrently filing petitions for inter partes review of U.S. Patent Nos. 6,252,964 B1 and 6,744,892 B2 asserted in the above litigation.

C. NOTICE OF LEAD AND BACKUP COUNSEL

Pursuant to 37 C.F.R. § 42.8(b)(3) and 42.10(a), Petitioner appoints **Amy E. Simpson** (Reg. No. 54,688) as its lead counsel, and **Bing Ai** (Reg. No. 43,312) and
10 **Nicholas T. Bauz** (Reg. No. 41,604) as its back-up counsel, all at the mailing address of Perkins Coie LLP, 11988 El Camino Real, Suite 200, San Diego, CA 92130, contact numbers of 858-720-5700 (phone) and 858-720-5799 (fax), and the following email for service and all communications:

opentv-cisco-ipr@perkinscoie.com

15 Pursuant to 37 C.F.R. § 42.10(b), a Power of Attorney accompanies this Petition.

D. SERVICE INFORMATION

Service information for lead and back-up counsel is provided in the designation of lead and back-up counsel above.

III. REQUIREMENTS FOR *INTER PARTES* REVIEW

20 As set forth below and pursuant to 37 C.F.R. § 42.104, each requirement for *inter partes* review of the '592 Patent is satisfied.

A. GROUND FOR STANDING

Pursuant to 37 C.F.R. § 42.104(a), Petitioner hereby certifies that the ‘592 Patent is available for *inter partes* review and that the Petitioner is not barred or estopped from requesting *inter partes* review challenging the claims of the ‘592 Patent on the grounds identified herein.

B. IDENTIFICATION OF CHALLENGE

Pursuant to 37 C.F.R. § 42.22(a)(1) and 42.104(b), the precise relief requested by Petitioner is that the Patent Trial and Appeal Board (“PTAB”) invalidate the ‘592 Patent.

1. Claims Challenged

Claims 1-20 of the ‘592 Patent are being challenged in this Petition.

2. The Prior Art

The PTAB applies U.S. law in conducting an *inter partes* review. 35 U.S.C. §§ 311-319. Unpatentability is proven by a preponderance of the evidence. U.S.C. § 316. *Inter partes* review of the ‘592 Patent is requested in view of the following references:

- U.S. Patent No. 5,790,935 to Payton (“Payton;” Ex. 1002), which issued on August 4, 1998 and is prior art under 35 U.S.C. § 102(b).
- U.S. Patent No. 7,698,723 B2 to Hicks, III (“Hicks;” Ex. 1003), which issued on April 13, 2010 and is prior art under 35 U.S.C. § 102(e).

- U.S. Patent Pub. No. 2002/0146237 to Safadi (“Safadi,” Ex. 1004),
published on October 10, 2002 and is prior art under 35 U.S.C. § 102(e)
- U.S. Patent Pub. No. 2003/0110234 to Egli et al. (“Egli,” Ex. 1005)
published on June 12, 2003 and is prior art under 35 U.S.C. § 102(e)
- 5 • U.S. Patent Pub. No. 2003/0135859 (“Putterman,” Ex. 1006) published
on July 17, 2003 and is prior art under 35 U.S.C. § 102(e)

3. Supporting Evidence Relied Upon For The Challenge

The evidence to support the challenge and the identification of where in each
numbered exhibit the challenge is supported, is provided below.

10 Attached to this petition as Exhibit 1007 is the declaration of Michael
Perkins (“Ex. 1007, Perkins Decl.”). Dr. Perkins’ declaration supports the grounds
in this petition showing that there is a reasonable likelihood that Petitioner will
prevail with respect to at least one of the challenged claims and that each
challenged claim is not patentable. *See* 35 U.S.C. § 314(a).

15 4. The Statutory Ground(s) of Challenge & Legal Principles

The patentability of claims 1-20 of the ‘592 Patent and the review requested
in this Petition are governed by statutory provisions 35 U.S.C. §§102 and 103 that
were in effect on and before March 15, 2013. The new 35 U.S.C. §§102 and 103
under the America Invents Act of 2011 that took effect on March 16, 2013 are not
20 applicable to this Petition and the associated *inter partes* review. In addition,

statutory provisions 35 U.S.C. §§311 through 319 that took effect on September 16, 2012 govern the *inter partes* review requested by this Petition.

5. Claim Construction under 37 C.F.R. § 42.100(b)

A claim subject to *inter partes* review shall be given by the Patent Office

5 “its broadest reasonable construction in light of the specification of the patent in which it appears” to one of ordinary skill in the art.

6. How the Claims Are Unpatentable Under the Statutory Ground Identified in Paragraph (b)(2) of 37 C.F.R. § 42.104

An explanation of how claims 1-20 of the ‘592 Patent are unpatentable

10 under the statutory grounds identified above, including the identification of where each element of the claim is found in the prior art patents or printed publications, is provided in Section VII below.

IV. OVERVIEW OF THE ‘592 PATENT

A. PRIORITY DATE OF THE ‘592 PATENT

15 The ‘592 Patent is a continuation of U.S. Patent No. 7,181,010 filed on March 6, 2003, which in turn is a continuation-in-part of U.S. Patent No. 6,748,080 filed on May 24, 2002. Based on the record, there is no reason to believe that the priority date of the independent claims of the ‘592 Patent is earlier than May 24, 2002. Dependent claims 2, 8 and 13 are not supported by the original disclosure
20 (‘080 Patent) and therefore receive a later priority date. Based on the available record to date, the priority dates for the claims challenged in this Petition are

assumed to be May 24, 2002 for claims 1, 3-7, 9-12, and 14-20 and March 6, 2003 for claims 2, 8, and 13.

B. PERSON OF ORDINARY SKILL IN THE ART

A person of ordinary skill in the art in the field of the '592 Patent in 2002

5 would have been someone with at least a bachelor degree in Electrical Engineering, Computer Science or Mathematics, with about three years of additional working experience in cable, internet or satellite video delivery systems and a general familiarity with content security techniques such as Conditional Access (CA), digital rights management (DRM) or content encryption. *See* Ex. 10 1007, Perkins Decl., 8-11.

C. BRIEF DESCRIPTION OF THE '592 PATENT

The '592 Patent is directed to residential entertainment systems wherein a digital content server, located at the subscriber's premise, acts as a middleman between the content distribution system/providers (e.g., cable or satellite TV) and 15 the remote client-receivers (e.g., laptops, PDAs, etc.) also located at the subscriber's premises. *See* Abstract, Fig. 1. Specifically, the content server, also referred to as a digital subscriber communication terminal ("DSCT"), stores audio and video received from content distribution providers/systems (cable or satellite TV) and then transmits content to client-receivers connected on a local area 20 network (LAN) throughout the subscriber's premises. *See* 3:1-13. In sum, the

DSCT is the interface between the client-receivers in a home/building and the cable or satellite TV distribution system.

The '592 Patent recognizes that placing a DSCT with storage and transmission capabilities within a local or home network presents security and content protection issues. Specifically, the '592 Patent states that “*local area networks introduce security and control concerns for the operators of the subscriber network systems due to issues such as payment, theft of services, and privacy.*” See 2:24-27.

To address this problem, the '592 Patent discloses that the content server (DSCT) should verify that the client-receiver (e.g.: laptop, PDA, etc.) is entitled, or authorized, to receive the requested content. See 21:46-60. When a subscriber requests to receive a service instance, the DSCT determines whether the client receiver is “entitled” to the selected service. See 3:29-32; 21:46-49. The DSCT therefore checks entitlement prior to transmitting the requested content to the remote device. Such entitlement checks can be implemented using encryption schemes such as “*secure sockets layer (SSL) protocol, Digital Transmission Content Protection (DTCP), Content Protection for Recordable Media (CPRM), and transport layer security (TLS) protocol.*” See 20:20-40.

In addition to determining that a client-receiver is entitled to receive the requested content, the DSCT checks whether or not the content is accessible within

the local storage. *See* 21:51-60. If the content is locally stored, the DSCT sends the content to the remote client-receiver device. Alternatively, when the content is not locally available, the DSCT sends a request to the headend at the central distribution systems/providers (cable or satellite TV) for the requested content (service instance). *See* 10:56-61; 21:61-63.

D. SUMMARY OF PROSECUTION HISTORY OF THE ‘592 PATENT

The prosecution history of the ‘592 Patent is summarized below. *See* Ex. 1008. On December 31, 2007, the examiner issued a non-final rejection of all claims as being anticipated by U.S. Patent No. 6,157,719 to Wasilewski et al. (“Wasilewski”). Applicant’s attempts to argue around Wasilewski were unsuccessful, and the Examiner issued a final rejection of all claims based on Wasilewski. *See* Ex. 1008 at 292 (Final Office Action, dated 07/07/2008).

In response to the final rejection, Applicant amended the independent claims to include the limitation that a “communications device” be in a local network with the remote client devices and that these devices be located at a subscriber’s premises. *See* Ex. 1008 at 272-279 (October 7, 2008 Response to Final Office Action, p.2-9).

It was only after the amendment to include multiple devices on a local network within the home that the Examiner was found the claims allowable over Wasilewski. *See* Ex. 1008 at 17 (November 13, 2008, Notice of Allowance at 2).

E. PROPOSED CLAIM CONSTRUCTION

Petitioner's proposed constructions and supporting evidence for construed claim terms are set forth below pursuant to the broadest reasonable interpretation standard under 37 C.F.R. §§ 42.100(b) and 42.104(b)(3). Petitioner's proposed claim constructions below are offered only to comply with 37 C.F.R. § 42.100(b) and for the sole purpose of this petition, and thus do not necessarily reflect appropriate claim constructions to be used in litigation and other proceedings where a different claim construction standard applies. The proposed claim constructions are not binding upon Petitioner beyond this *inter partes* review.

1. "Service Instance"

The '592 Patent discloses a subscriber network system that offers certain services to its subscribers. These services include, but are not limited to Internet services, telephone services and potentially hundreds of program and selection services. *See* 4:34-37. The '592 Patent describes a service instance as "*an installment of an audio or visual or audio/visual program that can be broadcast to all of subscribers of a conditional access system, a portion of subscribers or to an individual subscriber.*" *See* 4:37-41; 1:40-47. The '592 Patent further states that a service instance includes "*regular programming, special programming such as pay-per-view, and subscriber requested services such as personal television.*" *See*

4:41-44; 1:40-47. Based on the specification support, Petitioner’s proposed construction of the term “service instance” is “a program or service.”

2. “Communications Device”

The term “communications device” does not appear anywhere in the ‘592 specification or the originally filed claims. Indeed, “communication device” was added by amendment, six years after the ‘592 Patent’s filing date, to independent claims 1, 6 and 12 in order to overcome a final rejection in light of the Wasilewski reference. *See* Ex. 1008 at 272-279 (October 7, 2008 Response to Final Office Action). The specification, however, does disclose a digital subscriber communication terminal (DSCT) that manages a home network and provides services to remote clients coupled to the home network. *See* 3:4-6. The DSCT is shown in Figures 1 and 3 and described in detail in Col. 15, line 30 through Col. 29, line 50. Based on the above intrinsic evidence, and affording the term its broadest reasonable interpretation, Petitioner’s proposed construction of “communications device” is “a terminal for distributing service instances in a local network.”

3. “Remote Client Devices”

The term “remote client devices” suffers from the same flaw as “communications device” in that the term is not used in the ‘592 patent specification and was first introduced into the claims during prosecution. *See* Ex.

1008 at 272-279 (October 7, 2008 Response to Final Office Action). The closest reference to “remote client devices” in the specification is the client-receiver. The client receiver is illustrated in Figures 1 and 9 and is described as a device remotely coupled to the DSCT within a home network. *See* 9:50-65. The ‘592

5 Patent defines a client-receiver as “*any smart appliance including, but not limited to, a laptop computer, a computer, a personal digital assistant (PDA), VCR, another DSCT, or television, or the like, adapted to receive information or a service instance from the subscriber network system.*” *See* 10: 2-7; 1:51-56. Based on the intrinsic evidence, Petitioner’s proposed construction of “remote client
10 devices” is “a smart appliance configured to receive service instances.”

4. “Entitled to receive”

The ‘592 Patent states “*an entitlement agent is an entity that provides the subscribers of the DBDS [Digital Broadcast Delivery System] with entitlements for services and content associated with the entitlement agent and an entitlement is the
15 authority to access a service.*” *See* 4:19-24. Based on this definition, Petitioner’s proposed construction of the term “entitled to receive” is “has authority to access.”

5. “Subscriber Premises”

The ‘592 Patent states that “*[I]n one preferred embodiment, a digital subscriber communication terminal (DSCT), which is located at a subscriber’s
20 premises, receives services from the headend of a subscriber television system*”

(STS).” See 3:1-4. The specification goes on to describe that “[t]he DSCT manages a local area network (LAN) at the subscriber’s premises and provides services to client-receivers coupled to the LAN.” See 3:4-6. These descriptions do not limit the term “premises” to a subscriber’s residence. Instead, the description

5 ties the “premises” to the location of the subscriber whether the subscriber is an individual, a company or another entity. As such, Petitioner’s proposed construction for “subscriber’s premises” is “the location of the subscriber.”

6. “Subscriber”

The ‘592 Patent does not provide an explicit definition of a subscriber.

10 The ‘592 Patent, however, describes in detail methods for making multimedia and other content (i.e., service instances) available to those who pay. See 22:30-33. Based on these disclosures, Petitioner’s proposes construing “subscriber as “an individual or entity who pays for the authority to access.”

7. “Format protocol”

15 The phrase “format protocol” is not defined in the specification nor is the phrase a term of art. The Institute of Electrical and Electronics Engineers (“IEEE”) Dictionary (1988) defines “format” as “the general order in which information appears on the input medium.” See Ex. 1010. The IEEE Dictionary further defines “protocol” as “a formal set of conventions governing the format and

20 relative timing of message exchange between two communication terminals.”

Blending these definitions in light of the teachings in the ‘592 Patent to achieve the broadest reasonable interpretation, Petitioner proposes construing the phrase “format protocol” as “a set of rules governing the analog or digital representation of communication signals.”

8. “Accessible”

The ‘592 Patent does not provide an explicit definition of the term “accessible.” However, the specification and explicit claim language provides context for this term. Figure 5 shows and its corresponding description states that “if the selected service instance is currently not accessible at the DSCT 110, in step 508, the DSCT 110 sends a request for the service instance to the headend 102.” See 21:61-63; Fig. 5. Further, independent claim 6 explicitly requires that “if the requested service instance is accessible, transmitting the service instance . . . to the remote client device; and if the requested service instance is NOT accessible, sending a request . . . to a headend for the requested service instance.” See Claim 6. Based on the disclosure and claim language, Petitioner’s proposed construction of the term “accessible” is “available without having to send a request for the content to the headend.”

V. THERE IS A REASONABLE LIKELIHOOD THAT AT LEAST ONE CLAIM OF THE ‘592 PATENT IS UNPATENTABLE

A. IDENTIFICATION OF THE REFERENCES AS PRIOR ART

Pursuant to Rules 42.22(a)(1) and 42.104(b)(1)-(2), Petitioner challenges claims 1-20 of the '592 Patent and requests that each challenged claim be cancelled. Petitioner relies upon the previously listed Payton, Hicks, Safadi, Egli and Putterman references (*See* section IV of this Petition).

5 As described below in detail, the prior art, alone or in combination, clearly discloses residential entertainment systems having a video server (communication device) that stores and transmits content (service instances) received from various service providers such as satellite TV, cable TV or the Internet, to other remote devices within a subscriber's home or premises. The prior art also shows that it
10 was well-known for remote devices within a home entertainment network to send requests for content to the video server and for the video server to determine whether the remote device was entitled to receive the requested content. It was also well known in the prior art for video servers to check local availability of the content wherein if the content was accessible, the video servers would send the
15 content to the requesting device, and if the content was not accessible, the video server would send a request for the content to the headend at the satellite or cable provider. As explained in detail below, these prior art references make clear that the residential entertainment systems and methods disclosed in the '592 Patent were well known in the prior art long before May 2002.

20 **B. SUMMARY OF INVALIDITY POSITIONS**

A matrix showing the challenged claims and the applicable prior art reference(s) is provided as Exhibit 1009 to this petition.

C. DIFFERENT INVALIDITY POSITIONS AGAINST EACH CLAIM ARE INDEPENDENT, DISTINCTIVE AND NOT REDUNDANT

5 This petition uses only two references, (1) Payton and (2) Hicks, to form independent and distinctive invalidity positions against independent claims 1, 6 and 12 and several dependent claims and further combines these references as two primary references with three additional references, (3) Safadi, (4) Egli and (5) Putterman, to reject the remaining claims. These references are selected because of
10 their distinctive teachings that cover different technical aspects of the ‘592 Patent and provide the Office and the public with a fuller view of the prior art landscape prior to the filing of the ‘592 patent.

 These references do not constitute cumulative teaching. Payton primarily discloses the use of a content server in a home served by a satellite broadcast
15 network. As was well known, a satellite broadcast network typically lacked a communication channel from a subscriber premise to the headend. Hicks, on the other hand, primarily discloses cable network embodiments of the home content server in which reverse channel communication between the home server and the cable headend is available.

20 To facilitate “just, speedy and inexpensive resolution” in the spirit of 35 C.F.R. § 42.1(b), Petitioner made due diligence in minimizing both the number of

references, out of myriad highly relevant prior art references uncovered by
Petitioner, and the number of invalidity positions against the lengthy and
ambiguous claims 1-20. The requirements of the speedy and inexpensive resolution
are duly met by this Petition.

5 Rule 35 C.F.R. § 42.1(b) also requires the just resolution of the
unpatentability issues. In this consideration, Petitioner respectfully reminds of the
Office that the absence of full and proper prior art references during the original
examination of the '592 Patent is the chief reason that led to the issuance of invalid
claims 1-20 being asserted in patent litigation. Claims 1-20 fail to meet the
10 statutory requirements on multiple grounds for multiple reasons and from different
aspects of the prior art teaching. This Petition is a remedial measure for correcting
the mistake in the original examination and is necessitated by Patent Owner's
improper enforcement of the invalid claims. Petitioner respectfully submits that all
proposed invalidity positions be fully adopted due to the need for just resolution of
15 the unpatentability issues.

VI. DETAILED EXPLANATION OF THE GROUNDS FOR UNPATENTABILITY

A. ANTICIPATION

20 **1. Claims 1-2, 6-8, 12-13, and 17-20 are Unpatentable Under
35 U.S.C. § 102(b) as Being Anticipated by Payton**

Claims 1-2, 6-8, 12-13, and 18-20 of the '592 Patent are unpatentable under 35 U.S.C. § 102(b) as being anticipated by Payton. *See* Ex. 1002. Payton published on August 4, 1998 more than one year before the May 24, 2002 priority date and thus qualifies as prior art under 35 U.S.C. § 102(b). Payton discloses

5 techniques for providing audio/video content (“digital items” or “items”) to subscribers by predictively caching content from a recommended list of items at a local server. *See* Abstract. The content is downloaded to a local video server from a central distribution server over a cable, fiber, or satellite network to reduce network bandwidth requirements. *See* Abstract, Fig. 2. The system in Payton

10 determines which content would likely be desired by the subscriber, referred to as “recommended items,” and downloads the recommended content to local storage during off-peak hours. *See* 4:34-38. Alternatively, the subscriber may make a specific request for content that is not on the “recommended items” list, and that content will also be downloaded and stored in the local storage device. *See* 2:67-

15 3:2. The local video server is connected with multiple client playback devices within a local home network. *See* Fig. 8. Requests for video content are initiated from the client playback devices, e.g., by using a control device 64 such as a remote or a keyboard. *See* 6:20-31. The local video server determines if the requested item is stored locally and sends the content for decryption,

20 decompression, and display if the content is in local storage. Otherwise, the server

requests the content to be downloaded from the central distribution server via the cable, fiber, or satellite network. *See* 7:13-20, Fig. 3b. Before content can be viewed on a client playback device, the system will determine if the subscriber is entitled, or authorized, to view the requested content. *See* 4:64-66. Verifying authorization of a client device is especially important for the disclosed embodiment where an apartment building has a single video server supplying content to client devices in each apartment. *See* 9:64-10:8. In the apartment embodiment, each client device may be associated with a distinct subscriber, and only the paying subscriber(s) will be authorized to receive and view the content.

See 4:64-66.

Claim 1(a) - Method of transmitting service instance from communication device to remote device. As shown in Figures 2 and 8, Payton's delivery system is configured to deliver requested digital items including video and audio to a subscriber's playback device 32 in response to a subscriber's request. *See* 4:51-58.

Payton's local server 28 (Fig. 2) or video server 176 (Fig. 8) is the claimed communication device, the subscriber playback devices 32 and CD-Rom Writer 65 are the claimed remote devices, and the digital items are the claimed service instances. Figure 8 further depicts implementing the delivery system over a local network at a subscriber's premises as shown by the video server 176 being connected over a local cable or wireless line 178 to multiple playback devices 32.

See 9:62-10:8 Payton's local server is at a subscriber premise: *"For example, a video server configuration may be used to service multiple televisions within a single home or to service all the residents in an apartment complex."* See 9:64-67; Ex. 1007, Perkins Decl., ¶¶ 51-57.

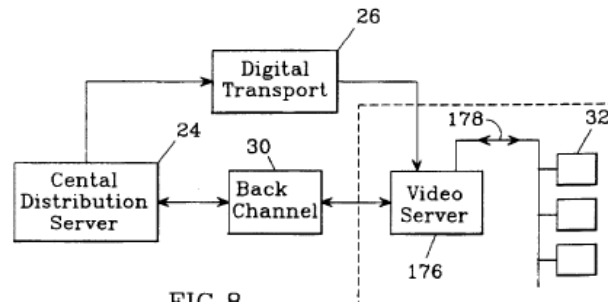


FIG. 8

Claim 1(b) - Receiving and storing a service instance...from a headend. As shown in Figures 2 and 8, a local video server located at the subscriber's premises receives content from the central distribution server 24 over a digital transport network. See 5:55-57. One of ordinary skill in the art would have understood that the central distribution server is located at the headend. See Ex. 1007, Perkins Decl., ¶¶ 58-60. The local video server 176 stores video content from the central distribution server 24: *"Each subscriber has a local server that downloads recommended and specifically requested items and stores them in a local storage device."* See 2:67-3:2. Additionally, Figure 5 shows that digital content is received and stored in the local storage of the video server before being transferred to a playback device. See Fig. 5; 8:11-25; 4:66-5:1.

Claim 1(c) - Receiving a request for stored service instance from remote device. As shown in Figure 3b at step 74, a subscriber sends a request to the local server using the “On-Demand Request.” The “On-Demand Request” is submitted by the subscriber using a remote control or keyboard to request digital content from the video server. *See* 6:20-23. Payton further discloses that “[i]n response to a subscriber’s request, the delivery system 22 delivers the requested item to the subscriber’s playback device 32 such as a television, audio system or computer.” *See* 4:51-54 (emphasis added); Ex. 1007, Perkins Decl., ¶¶ 61-62.

Claim 1(d) - Determining if the remote client device is entitled. As construed above, the phrase “entitled to receive” means “authority to access.” Payton determines whether a playback device has authority to access digital content stored at the local server and states that “the digital items are preferably encrypted so that **downloaded items cannot be accessed without first being paid for.**” *See* 4:64-66 (emphasis added). Moreover, the entire specification in Payton is based on the concept of “subscribers” to digital content service. One of ordinary skill in the art would have understood that only subscribers would be able to access content from the local video server of a particular service provider. *See* Ex. 1007, Perkins Decl., ¶¶ 66-68.

One mechanism used by Payton to prevent unauthorized use of the content is encryption of the digital content. *See* 4:64-66. Figure 3b at 77 and Figure 5 at 132

show that the content from the local video server must be decrypted and decompressed before it is displayed at the playback device. If the content is not decrypted, it will not be viewable to the subscriber. One of ordinary skill in the art would have understood that only subscribers who are authorized to view the

5 content will be able to decrypt the content. *See* Ex. 1007, Perkins Decl., ¶ 66.

Moreover, the fact that Payton requires that its content be encrypted makes clear that not just anyone has authority to access the stored content. Rather, Payton teaches that the local server must determine whether the digital content has been paid for prior to a subscriber being authorized to access (or entitled to receive) the
10 requested content. *See* 4:64-66. Additional teachings by Payton regarding determining entitlement can also be found in Payton's embodiments describing use of the video server in a hotel or apartment complex environment. *See* Ex. 1007, Perkins Decl., ¶ 68.

Claim 1(e) - If entitled, transmitting the requested service instance to the

15 remote client device. Payton states that "*the delivery system 22 delivers the requested item to the subscriber's playback device 32 such as a television, audio system or computer.*" *See* 4:51-54. Payton further states that "*when a subscriber makes an on-demand request (step 74), the local server 28 polls the local storage 56 (step 75) to determine whether the requested item is stored locally (step 76). If*
20 *it is stored locally, the item is sent to the decryption and decompression processor*

(step 77) 60 and then routed to the subscriber.” See 7:13-16; Ex. 1007, Perkins Decl., ¶ 69. Finally, Figures 3b and 5 show that the content is decrypted and decompressed prior to sending to the remote client device. See 7:13-18; 8:17-21.

One of ordinary skill in the art would have understood that in Payton’s subscriber-based network, transmission of content to the requesting device would be in response to determining that the playback device has authority to access the content. See Ex. 1007, Perkins Decl., ¶ 70.

Claim 1	Payton
[A] A method of transmitting service instances to a remote client device in a local network, including a communications device and one or more of said remote client devices, at a subscriber premises, comprising the steps of:	4:7-11; 4:45-60; 9:62-10:8; Figs. 2, 8.
[B] receiving a service instance at the communications device of the subscriber premises from a headend, wherein the service instance is stored in memory of the communications device;	2:67-3:2; 4:45-49; 4:55-57; 5:55-57; 6:11-17; 8:11-25; 10:5-8; Figs. 2, 5, 8.
[C] receiving a request at the communications device for the stored service instance from the remote client device;	5:36-39; 6:26-33; 6:51-53; 7:13-16; 10:3-9; Figs. 2, 3b, 8.
[D] determining whether the remote client device is entitled to receive the requested stored service instance; and	4:64-66; 7:13-18; Figs. 3b, 5.
[E] responsive to determining the remote client device is entitled to receive the requested stored service instance, transmitting the requested service instance from the communications device to the remote client device.	4:51-54; 6:11-19; 7:13-18; 8:17-21; 10:3-11; Figs. 3b, 5.

Claim 2 - Transmit the service instance in the proper format for the playback

device. Payton discloses that the local video server can provide digital content to a

variety of device types, which includes displays such as a standard television and a computer monitor. *See* 6:20-25. Payton further teaches that “*Techniques for converting digitally formatted and encrypted signals into standard video and audio signals are well known in the art.*” *See* 6:17-19. In addition to teaching the well-known conversion of compressed and encrypted signals into standard video and audio, Payton’s local video server distinguishes between a T.V. and a CD ROM audio writer as potential playback devices because the former requires both video and audio signals, but the latter only requires audio. *See* 6:18-25. Additionally, the content is transported to the client devices over a wired or wireless network, which would necessarily require support for different network protocol formats. *See* 10:3-5; Ex. 1007, Perkins Decl., ¶ 135. One of ordinary skill in the art would have recognized displaying on a T.V., a computer monitor, and a CD-ROM writer will each require a different format of the digital content, and that the conversion would be performed by the video server. Ex. 1007, Perkins Decl., ¶ 136.

Claim 2	Payton
[A] The method of claim 1, further comprising the steps of: determining a device type for the remote client device;	6:17-25; 8:17-21, 10:3-5.
[B] using the device type of the remote client device to determine a format protocol for the requested service instance; and	6:17-25; 8:17-21, 10:3-5.
[C] reformatting the requested service instance prior to transmitting the requested service instance.	6:17-25; 8:17-21, 10:3-5.

Claim 6(a) - Method of transmitting service instances from communication device to remote device. Claim 6(a) is identical to claim 1(a). The arguments presented for claim 1(a) apply here with equal force. As such, Payton discloses claim 6(a) for at least the reasons stated above.

5 Claim 6(b) - Receiving a request for stored service instance from a remote device. Claim 6(b) is identical to claim 1(c). The arguments presented for claim 1(c) apply here with equal force. As such, Payton discloses claim 6(b) for at least the reasons stated above. *See* Ex. 1007, Perkins Decl., ¶ 74.

10 Claim 6(c) - Determining if the remote client device is entitled. This limitation is identical to limitation 1(d). As described above with respect to 1(d) and incorporated herein, Payton discloses both (1) granting access only to paying subscribers and (2) using encryption as a means to prevent unauthorized use. *See* 4:64-66, 7:13-18, Fig. 3b, and Ex. 1007, Perkins Decl., ¶ 75.

15 Claim 6(d) - Determining Whether Service Instance Is Accessible. As described in Figure 3b, Payton determines accessibility of a requested service when the local video server “*polls the local storage 56 (step 75) to determine whether the requested item is stored locally (step 76).*” *See* 7:13-16. Additionally, Payton teaches “[w]hen one of the subscribers requests an item, the video server either retrieves it from the local storage or requests it from the central distribution

server.” See 10:5-8, Ex. 1007, Perkins Decl., ¶ 79. Determining whether a service instance is accessible as required by claim 6(d) is disclosed by Payton.

Claim 6(e) - If accessible, transmitting service instance to remote device. In

Figure 3b, if the local video server determines that the content is stored locally,

5 “the item is sent to the decryption and decompression processor (step 77) 60 and then routed to the subscriber.” See 7:16-18. Payton further teaches “[i]n response to a subscriber’s request, the delivery system 22 delivers the requested item to the subscriber’s playback device 32 such as a television, audio system or computer.”

See 4:51-54, Ex. 1007, Perkins Decl., ¶ 80. As such, Payton discloses transmitting

10 content to the subscriber upon determining that it is accessible.

Claim 6(f) - If not accessible, request service instance from headend. In

Figure 3b, Payton teaches having the local server transmit a request to the central distribution server (headend) when the requested content item is not locally

available: Payton states “[i]f the item is not immediately available, the local server

15 sends the request over the back channel to the central distribution server, which places the request in the queue for on-demand broadcast. As soon as the item is received locally, it is sent to a local playback device.” See 3:27-33, 7:18-20, Ex.

1007, Perkins Decl., ¶ 82. In light of the above, Payton discloses claim 6(f).

Claim 6	Payton
[A] A method of transmitting service instances to a remote client device in a local network, including a	4:7-11; 4:45-60; 9:62-10:8; Figs. 2, 8.

communications device and one or more of said remote client devices, at a subscriber premises, comprising the steps of:	
[B] receiving a request at the communications device of the subscriber premises for a service instance from the remote client device;	5:36-39; 6:26-33; 6:51-53; 7:13-16; 10:3-9; Figs. 2, 3b, 8.
[C] determining whether the remote client device is entitled to receive the requested service instance;	4:64-66; 7:13-18; Figs. 3b, 5.
[D] responsive to determining the remote client device is entitled to receive the requested service instance, determining whether the requested service instance is accessible within the communications device;	3:25-27; 7:13-16; 10:3-8; Fig. 3b.
[E] if the requested service instance is accessible, transmitting the service instance from the communications device to the remote client device; and	7:13-18; 8:17-21; 10:3-11; Fig. 3b.
[F] if the requested service instance is not accessible, sending a request from the communications device to a headend for the requested service instance, wherein upon receipt of the service instance at the communications device, transmitting the service instance from the communications device to the remote client device.	3:25-33; 6:11-17; 7:13-20; 10:3-11; Fig. 3b.

Claim 7 - Storing the service instance before transmitting to the client.

Payton's Figure 5 shows that received content is stored in the local storage before transmitting it to the playback device. *See* Fig. 5, 6:11-17. Payton also

5 states "*If it is, the filter determines whether the pause control is on (step 128), and if so routes the item to the local storage 56 (step 130). Once the pause control is released, the item is transferred to the decryption and decompression processor 60 (step 132) and then routed to the playback device 32 or CD ROM writer 65 (step 134).*" *See* 8:15-21 (emphasis added), Ex. 1007, Perkins Decl., ¶¶137-138.

Claim 7	Payton
The method of claim 6, further comprising the step of, prior to transmitting the service instance to the remote client device, storing the received service instance in memory of the communications device.	6:11-17; 8:11-25; Fig. 5.

Claim 8 - Transmit the service instance in the proper format for the playback device. This limitation is identical to claim 2, but depends from claim 6 instead of claim 1. As described above with respect to claim 2, Payton discloses that the

5 local video server can provide the digital content to a variety of device types, including a standard television, a computer monitor, and a CD-ROM writer. *See* 6:17-19, 6:18-25, 10:3-5, and Ex. 1007, Perkins Decl., ¶ 140.

Claim 8	Payton
[A] The method of claim 6, further comprising the steps of: determining a device type for the remote client device;	6:17-25; 8:17-21; 10:3-5.
[B] using the device type of the remote client device to determine a format protocol for the requested service instance; and	6:17-25; 8:17-21; 10:3-5.
[C] reformatting the requested service instance prior to transmitting the requested service instance.	6:17-25; 8:17-21; 10:3-5.

Looking now at independent claim 12, there is only one substantive

10 difference between independent claim 1 and independent claim 12. That is, claim 12 requires that the communication device work with multiple connected client devices. As shown below, Payton teaches that its video server can support multiple client devices.

Claim 12 (a) - Method of transmitting service instances from communication device to remote device. Claim 12(a) is identical to claim 1(a). The arguments presented for claim 1(a) apply here. As such, Payton discloses claim 12(a) for at least the reasons stated above.

5 Claim 12(b) - Receiving a first request for stored service instance from first remote device. Claim 12(b) is identical to claim 6(b). The arguments present for claim 6(b) also apply here. As such, Payton discloses claim 12(b) for at least the reasons stated above.

10 Claim 12(c) - Determining if the remote client device is entitled. This limitation is identical to limitation 1(d). As described above with respect to 1(d) and incorporated herein, Payton discloses both (1) granting access only to paying subscribers and (2) using encryption as a means to prevent unauthorized use. *See* 4:64-66, 7:13-18, Fig. 3b, and Ex. 1007, Perkins Decl., ¶ 84.

15 Claim 12(d) - If entitled, transmitting service instance to first requester. This limitation is identical to claim 1(e). The arguments presented for claim 1(e) are fully incorporated herein. As such, Payton discloses claim 12(d) for at least the reasons stated above.

20 Claim 12(e) - Receiving a second request for a service instance. Claim 12(e) is identical to claim 6(b). The arguments presented for claim 6(b) apply to claim 12(e). Payton also discloses that the local video server can receive requests from a

plurality of subscriber playback devices. Specifically, Payton states “[f]or example, a video server configuration may be used to service multiple televisions within a single home or to service all of the residents in an apartment complex...When one of the subscribers requests an item, the video server either
5 retrieves it from the local storage or requests it from the central distribution server.” See 9:64-10:8, Ex. 1007, Perkins Decl., ¶ 85.

Claim 12(f) - Determining if the remote client device is entitled. This limitation is identical to limitation 1(d). As described above with respect to 1(d), Payton discloses both (1) granting access only to paying subscribers and (2) using
10 encryption as a means to prevent unauthorized use. See 4:64-66, 7:13-18, Fig. 3b, and Ex. 1007, Perkins Decl., ¶ 84.

Claim 12(g) - If entitled, transmitting service instance to second requester. This limitation is largely identical to claim 1(e). The arguments present for claim 1(e) also apply to claim 12(g). Moreover, Payton further teaches transmitting
15 digital content from an on-demand request to a second playback device based on the local availability of the requested multimedia item. Payton teaches: “When one of the subscribers requests an item, the **video server either retrieves it from the local storage** or requests it from the central distribution server.” See 10:5-8.

Additionally, Payton discloses checking local storage to see if the content is
20 available and “[i]f it is stored locally, the item is sent to the decryption and

decompression processor (step 77) 60 and then routed to the subscriber.” See

7:13-18, Ex. 1007, Perkins Decl., ¶¶ 69-70.

Claim 12	Payton
[A] A method of transmitting service instances to a plurality of remote client devices in a local network, including a communications device, at a subscriber premises, comprising the steps of:	4:7-11; 4:45-60; 9:62-10:8; Figs. 2, 8.
[B] receiving a first request for a service instance at the communications device of the subscriber premises from a first remote client device;	5:36-39; 6:26-33; 6:51-53; 7:13-16; 10:3-9; Figs. 2, 3b, 8.
[C] determining whether the first remote client device is entitled to receive the requested service instance;	4:64-66; 7:13-18; Figs. 3b, 5.
[D] responsive to determining the first remote client device is entitled to receive the requested service instance, transmitting the requested service instance from the communications device to the first remote client device;	4:51-54; 6:11-19; 7:13-18; 8:17-21; 10:3-11; Figs. 3b, 5.
[E] receiving a second request for the service instance at the communications device from a second remote client device in the local network;	5:36-39; 6:26-33; 6:51-53; 7:13-16; 10:3-9; Figs. 2, 3b, 8.
[F] determining whether the second remote client device is entitled to receive the requested service instance; and	4:64-66; 7:13-18; Figs. 3b, 5.
[G] responsive to determining the second remote client device is entitled to receive the requested service instance, transmitting the requested service instance from the communications device to the second remote client device based upon local availability of the requested service instance within the communications device.	3:25-27; 4:51-54; 6:11-19; 7:13-18; 8:17-21; 10:3-11; Figs. 3b, 5.

Claim 13 - Transmit the service instance in the proper format for the

- 5 playback device. This limitation is identical to claim 2, but depends from claim 12 instead of claim 1. As described above with respect to claim 2, Payton discloses that the local video server can provide the digital content to a variety of device

types, including a standard television, a computer monitor, and a CD-ROM writer.

See 6:17-19, 6:18-25, 10:3-5, and Ex. 1007, Perkins Decl., ¶ 136.

Claim 13	Payton
[A] The method of claim 12, further comprising the steps of: determining a device type for each of the first and second remote client devices;	6:17-25; 8:17-21, 10:3-5.
[B] using the device type of the first and second remote client devices to determine a format protocol for the requested service instance; and	6:17-25; 8:17-21, 10:3-5.
[C] reformatting the requested service instance prior to transmitting the requested service instance.	6:17-25; 8:17-21, 10:3-5.

Claim 17. With respect to Claim 17, Payton discloses that “*the device type*
5 *information from each of the first and second remote devices may require a same*
encryption scheme or a different encryption scheme” at least because Payton
discloses the use of a same encryption scheme for all subscribers.

Claim 17	Payton
The method of claim 16, wherein the device type information from each of the first and second remote devices may require a same encryption scheme or a different encryption scheme.	4:17-27.

Claim 18(a) - Determining Whether Service Instance Is Accessible. This
10 limitation is nearly identical to limitation 6(d). As described above with respect to
claim 6(d), Payton discloses determining if the requested content is available at the

local server before transmitting any content to the playback device. *See* 7:13-16, 10:5-8, Ex. 1007, Perkins Decl., ¶¶ 76-79.

Claim 18(b) - If not accessible, request service instance from headend. This limitation is nearly identical to limitation 6(f). As described above with respect to claim 6(f), Payton discloses forwarding the on-demand request for content to the central distribution server (headend) and subsequently transmitting the content to the playback device from the local server upon receipt. *See* 3:27-33, 7:18-20, Ex. 1007, Perkins Decl., ¶ 82.

Claim 18	Payton
[A] The method of claim 12, further comprising the steps of: prior to transmitting the requested service instance to the first remote client device, determining whether the requested service instance is accessible within the communications device; and	3:25-27; 7:13-16; 10:3-8; Fig. 3b.
[B] if the requested service instance is not accessible, sending a request to a headend for the requested service instance, wherein upon receipt of the service instance, transmitting the service instance from the communications device to the first remote client device.	3:25-33; 6:11-17; 7:13-20; 10:3-8; Fig. 3b.

Claim 19 - Service instance is accessible if locally stored. The local video server checks for the requested content in its local memory and transmit the requested content to the playback device if available (Figure 3b). Specifically, Payton states “[a]s shown in FIG. 3b, when a subscriber makes an on-demand request (step 74), the local server 28 polls the local storage 56 (step 75) to determine whether the requested item is stored locally (step 76). If it is stored

locally, the item is sent to the decryption and decompression processor (step 77)

60 and then routed to the subscriber.” See 7:13-20, Ex. 1007, Perkins Decl., ¶ 147.

Claim 19	Payton
The method of claim 18, wherein the requested service instance is accessible if the service instance is stored in memory of the communications device.	7:13-20; Fig. 3b.

Claim 20 - Storing the service instance before transmitting to the client.

- 5 This claim is nearly identical to claim 7. As described above with respect to claim 7, Payton discloses storing the digital content at the local video server (communication device) before transmitting it to the playback device (remote device). *See* 6:11-17, 8:15-21, Fig. 5, Ex. 1007, Perkins Decl., ¶¶ 138, 149.

Claim 20	Payton
The method of claim 18, further comprising the step of, prior to transmitting the service instance to the first remote client device, storing the received service instance in memory of the communications device.	6:11-17; 8:11-25; Fig. 5.

10 **2. Claims 1-4, 6-10, 12-15 and 17-20 Are Unpatentable Under 35 U.S.C. § 102(e) As Being Anticipated By Hicks.**

- Claims 1-4, 6-10, 12-15 and 17-20 of the ‘592 Patent are unpatentable under 35 U.S.C. § 102(e) as being anticipated by Hicks. *See* Ex. 1003. Hicks was filed on
- 15 December 28, 2000, which predates the May 24, 2002 filing date of the ‘592

Patent. Hicks published on December 23, 2004 and issued on April 13, 2010.

Hicks therefore qualifies as prior art under 35 U.S.C. § 102(e).

Hicks discloses a home entertainment system for distributing multimedia content to remote devices within a home. *See* 1:5-7. Hicks' recognizes that with
5 the increasing popularity of multimedia serves, consumers are likely to have multiple set-top boxes within their homes. *See* 1:62-67, 2:1-7. However, enhanced digital set top boxes offering more sophisticated service such as web access, video on demand, and interactive TV are expensive. *See* 1:62-63. It is therefore likely that only one set-top box per home will offer these enhanced
10 services. *See* 2:1-3. To this end, Hicks discloses a digital residential entertainment system that provides remote devices with access to multimedia content and services on the enhanced set top box over an in-home data network. *See* 2:14-22, 3:10-14, 5:55-59.

The residential entertainment system in Hicks makes available multimedia
15 services from the enhanced set top box to other devices by automatically downloading selections of multimedia content from a service provider to a residential-based mass storage device so other devices in the home can access the content. *See* 2:14-22, 3:10-14, 5:49-54. Upon a user accessing the locally stored multimedia from remote devices, a multimedia usage report is sent to multimedia-
20 on-demand service provider for billing. *See* 2:18-20 In this way, locally stored

multimedia content can be automatically updated with downloads of new content in addition to making the stored content available to multiple subscriber devices in a residential network.

Looking now at Hicks' residential entertainment system in detail, Hicks
5 discloses an in-home server called a "broadband media gateway" (BMG). *See* 3:50-54, Fig. 1. The BMG receives video, audio and other forms of multimedia content from a variety of networks such as digital broadcast satellite, digital cable and terrestrial television networks. *See* 3:55:58. The BMG also transmits multimedia content to a variety of remote information appliances, e.g., digital thin
10 client set-top box (TC STB), an audio system, a wireless MP3 player, etc. *See* 4:7-10. For protecting access to the content, the BMG uses conditional access (CA) techniques such as DTCP and smartcard based systems from NagraCard or NDS and then transmits content in the encrypted format across the residential network. . *See* 4:17-27, 9:22-32. The BMG includes a mass storage device on which
15 multimedia content is stored in encrypted format. *See* 4:17-18, 14:44-45, 13:1-23.

The BMG thus allows access to content based on the type of multimedia content item requested by the subscriber as follows: (1) when a subscriber requests live content that is being broadcast on a network, the BMG tunes to the selected broadcast channel and streams the corresponding stream to the TC STB. *See* 4:55-
20 61. (2) For pre-scheduled pay-per-view, the subscriber tunes to the content at a

scheduled time. *See* 1:56-61. (3) For real-time on-demand pay-per-view, the BMG provides access to encrypted content using smartcard-based conditional access technology. *See* 10:60-67. (4) And for media-on-demand content that has been downloaded and stored in the local storage, the BMG provides access using a copy protection or a conditional access scheme. *See* 13:25-42. (5) Finally, the BMG also provides access to content such as web pages, e-mail, etc., using the residential gateway module that has a broadband data connection. *See* 4:53-54.

Claim 1(a) - Method of transmitting service instance from communication device to remote device. As shown in Hicks' Figure 1, the BMG 100 operates as a content server and receives video, audio or other forms of multimedia from a variety of content providers 10, 20, 21 (e.g., satellite TV, digital cable TV, Internet sources) and transmit the multimedia to remote information appliances 40, 50 (e.g., thin client STBs, wireless electronic devices, MP3 players) all of which are connected together by a local area network. *See* 3:26-27, 4:8-12, 8:5-16. The BMG is the claimed communication device. *See* 3:50-58. The information appliances are the claimed remote client devices. *See* 4:8-12, 8:5-16. And, the multimedia content are the claimed service instances. *See* 3:60-65. Finally, Hicks states that “[m]ultimedia content that is stored on the BMG can be accessed from any of the information appliances on the broadband home network.” *See* 4:34-37, *see also* 3:10-14, 3:25-46, 4:34-37, Ex. 1007, Perkins Decl., ¶¶ 87-89.

Claim 1(b) - Receiving and storing a service instance...from a headend. As

shown in Figure 1, Hick's residential entertainment system includes a BMG (100) that receives video, audio and other multimedia content from a variety of transmission sources including satellite TV (20/21) and broadcast TV (10/11). *See* 3:55-59, 6:18-34. Hicks also states that "*a tuner/demodulator 102 can be coupled to a CATV system (e.g., a head-end of a CATV) via a communications link 32 (e.g., a coaxial cable).*" *See* 6:18-34. One of ordinary skill in the art would have understood that direct digital broadcast satellite TV systems and digital cable TV systems use headends to distribute content to their subscribers. Ex. 1007, Perkins Decl., ¶¶ 90-92.

Upon receiving the multimedia content from any one of these sources, the BMG stores the media in its mass storage device (Figure 1, 103) that includes "*a hard disk drive, a magnetic storage device, an optical storage device*" for storing multimedia information for subsequent playback. *See* 5:14-17, 7:7-15, Ex. 1007, Perkins Decl., ¶¶ 90-92. Hicks also states that "*multimedia content downloading can be accomplished using a broadband data service, such as ADSL, a satellite direct multicast/broadcast service, a cable television service, a digital cable television service . . .*" *See* 13:6-12.

Claim 1(c) - Receiving a request for stored service instance from remote

device. According to Hicks, "*the thin client digital STB communicates with the*

BMG requesting that the media content be delivered to the digital STB.” See 4:58-61, 5:6-12 (emphasis added). In this way, the BMG (communication device) receives a request for multimedia (service instance) from an information application (remote client devices) as recited in claim 1(c).

5 Claim 1(d) - Determining if the remote client device is entitled. Hicks clearly recognizes the importance of protecting proprietary digital content transmitted within a home entertainment system. Indeed, Hicks states that “*[e]ncryption of multimedia content can ensure that proprietary and/or copy-righted materials is protected as it is transmitted across the residential broadband*
10 *data network.*” See 4:17-27 (emphasis added). Petitioner construes the phrase “entitled to receive” to mean “authority to access.” Hicks discloses that remote clients obtain authority to access requested multimedia in a number of ways.

First, Hicks discloses incorporating various conditional access (CA) techniques into the residential entertainment system. Hicks specifically states

15 “*[c]onditional access systems (“CAS”) using smartcard technology, such as those manufactured by NagraCard S.A. of Cheseaux, Switzerland and NDS Group PLC of United Kingdom, can be integrated into the entertainment system.*” See 4:17-27.

Conditional access systems ensure that only authorized subscribers view a particular program or content which is typically transmitted in encrypted form. See

20 Ex. 1007, Perkins Decl., ¶¶ 95-108. Based on this disclosure in Hicks, one of

ordinary skill in the art would have understood that the BMG could determine whether the requesting device is authorized to receive the content. *See* Ex. 1007, Perkins Decl., ¶ 101.

Second, Hicks discloses using various “*encryption/copy protection protocols*” that combine licensing and technical elements to determine whether a remote client has authority to access particular content. Indeed, Hicks identifies a number of protection protocol standards. Hicks states “[i]n an embodiment, information signals can be encrypted and/or decrypted by cipher/decipher logic 168. Cipher/decipher logic 168 can decrypt and/or encrypt information signals according to encryption/copy protection protocols such as ... DTCP (Digital Transmission Content Protection), and so forth” *See* 9:16-36. The DTCP protocol defines steps taken to determine whether sink devices (information appliances) are authorized to access requested content from the source device (BMG). *See* Ex. 1007, Perkins Decl., ¶ 107. Importantly, the DTCP standard has been available for licensing since the late 1990s. *See* Ex. 1007, Perkins Decl., ¶ 97. Based on Hicks’ disclosure of DTCP, one of ordinary skill in the art would have understood that DTCP can be used to determine whether a requesting device is authorized to access multimedia content as required by claim 1(d). *See* Ex. 1007, Perkins Decl., ¶¶ 98-101.

Finally, Hicks' disclosure of encryption/decryption logic at the BMG and the thin-client indicates that not just any device has access to the stored content and that the BMG must determine whether the requesting device is allowed to receive the media item. *See* Figure 2 (168), Figure 3 (320); 9:23-27, 11:25-33. *See* Ex. 1007, Perkins Decl., ¶¶ 104-107.

In sum, Hicks' disclosure of classical conditional access, DTCP licensing standard and encryption/decryption capabilities are all possibilities for determining whether a remote device is authorized to access requested content from the BMG and therefore anticipates claim 1(d).

Claim 1(e) - If entitled, transmitting the requested service instance to the remote client device. As described above, Hicks discloses numerous ways of implementing conditional access protection within a residential entertainment system. Hicks also describes using DTCP to determine if the remote information appliance is entitled to receive the multimedia. *See* 9:16-36. One of ordinary skill in the art would have understood that, when using conditional access techniques or DTCP, the multimedia (or service instance) will only be transmitted to the remote device upon determination that the remote device has the proper authority to access. *See* Ex. 1007, Perkins Decl., ¶¶ 109-111.

Furthermore, Hicks states that “[u]pon receiving multimedia content, the BMG can transmit the multimedia content through the Ethernet switch over the

twisted pair data network to an information appliance (e.g. a thin-client digital set top box, an audio system, a wireless MP3 player, or a wireless electronic device), store the multimedia content for future access or transmit and store coincidentally (e.g. simultaneously).” See 4:8-14. As such, when the residential entertainment

5 system in Hicks determines that the remote device is authorized to access the requested content, the requested content is transmitted to the device as required by claim 1(e).

Claim 1	Hicks
[A] A method of transmitting service instances to a remote client device in a local network, including a communications device and one or more of said remote client devices, at a subscriber premises, comprising the steps of:	3:10-14; 3:26-47; 3:48-65; 4:7-14; 4:49-54; 5:55-59, 7:47-55; 8:7-13; 17:24-30; Fig. 1 (and corresponding description).
[B] receiving a service instance at the communications device of the subscriber premises from a headend, wherein the service instance is stored in memory of the communications device;	1:12-18; 1:46-50; 2:23-27; 3:55-65; 4:3-18; 4:28-37; 6:18-34; 7:8-15; 8:7-16; 12:66 - 13:4; 13:6-13, Fig. 1 (and corresponding description).
[C] receiving a request at the communications device for the stored service instance from the remote client device;	4:55-61; 15:23-25; 14:44-55; 5:6-12; 4:34-37.
[D] determining whether the remote client device is entitled to receive the requested stored service instance; and	4:17-27; 9:8-36; 10:58-67; 14:33-38; 11:25-29.

[E] responsive to determining the remote client device is entitled to receive the requested stored service instance, transmitting the requested service instance from the communications device to the remote client device.	3:55-65; 4:34-37; 9:22-36; Fig. 3; 11:1-2; 11:25-33; 4:7-14; 14:46-55; 13:29-36; 4:58-67.
--	---

Hicks also anticipates independent claim 6 as set forth below and as described in detail in the corresponding claim chart.

Claim 6(a) - Method of transmitting service instance from communication device to remote device. Claim 6(a) is identical to claim 1(a). The arguments

5 present for claim 1(a) also apply to claim 6(a). As such, Hicks discloses claim 6(a) for at least the reasons stated above.

Claim 6(b) - Receiving a request for stored service instance from remote device. Hicks states that “*after the consumer makes a selection, the thin-client*

digital STB communicates with the BMG requesting that the digital multimedia
10 *content be delivered to the digital STB.” See 4:58-61, 4:34-37, 5:6-12, Ex. 1007, Perkins Decl., ¶¶ 113-114. Therein, the BMG (communication device) receives a request (service instance) from thin client digital STB over the in-home broadband work as required by claim 6(b).*

Claim 6(c) - Determining if the remote client device is entitled. This

15 limitation is identical to claim 1(d). As described above with respect to claim 1(d), Hicks discloses both (1) traditional CA techniques such as smart cards and subscriber management systems and (2) security technology licensing standards

such as DTCP as ways for determining whether the remote information appliances have the authority to access the requested content. *See* 4:23-27; 9:22-36, 10:58-67, and Ex. 1007, Perkins Decl., ¶¶ 115-121.

Claim 6(d) - Determining Whether Service Instance Is Accessible Within the

5 Communication Device. Hicks discloses two ways in which the BMG makes content available for viewing. When requested content is locally stored (e.g., top-40 lineup downloaded by MODD), the BMG/MODD sends the content to the playback device upon request. *See* 14:51-54. When content is not locally stored but is broadcast video content (e.g., over a CATV system or a DBS TV system),
10 the BMG tunes a demodulator/tuner to the requested channel and streams to the requesting playback device. *See* 4:55-65. The use of two different techniques, one for content stored locally (accessible within) and the other for content not stored locally but available on a broadcast channel, inherently required “determining whether service instances is accessible within the communication device” as
15 required by claim 6(d).

As a specific example, Hicks discloses two different ways in which pay-per-view services can be made available within its residential entertainment system: (1) by local storage of movies for on-demand pay-per-view access via the MODD and MODSP and (2) by viewing real-time pay-per-view transmissions. *See* 1:53-55,
20 10:63-65. As such, one of ordinary skill in the art would have understood that the

BMG determines whether the requested pay-per-view content resides on the BMG's mass storage or whether it needs to be retrieved from the content provider/source. *See* Ex. 1007, Perkins Decl., ¶¶ 122-125.

Claim 6(e) - If accessible, transmitting service instance to remote device.

5 Hicks states that the “*BMG can also store that television program on mass storage device so that a user can view the television program at a later time on one or more information appliances (e.g., televisions and/or computer).*” *See* 8:12-16. Hicks further teaches that “*after the consumer selects a movie for viewing, the BMG would begin streaming the selected movie out to the thin-client STB/TV for*
10 *viewing.*” *See* 5:34-37, Ex. 1007, Perkins Decl., ¶ 126. Therefore, Hicks discloses transmitting the requested multimedia item from the BMG to the remote information appliance if the requested multimedia item is accessible from the local storage as required by claim 6(e).

Claim 6(f) - If not accessible, request service instance from headend. Hicks
15 discloses the operation of a pay-per-view system in which a user can subscribe to the pay-per-view service offered by a media-on-demand service provider (MODSP). *See* 13:30-32. If the requested pay-per-view content is not locally available on the BGM, one of ordinary skill in the art would have understood that the BGM would retrieve the content using real-time delivery capabilities of the
20 service provider's pay-per-view service. *See* Ex. 1007, Perkins Decl., ¶ 127.

Hicks further discloses that, upon receiving the content, the BGM forwards the requested content to the remote information appliance. Specifically, Hicks states

“[u]pon receiving multimedia content, the BMG can transmit the multimedia content to an information appliance (e.g. a thin-client digital set top box, an audio system, a wireless MP3 player, or a wireless electronic device), store the multimedia content for future access or transmit and store coincidentally (e.g. simultaneously).” See 4:8-14.

Claim 6	Hicks
[A] A method of transmitting service instances to a remote client device in a local network, including a communications device and one or more of said remote client devices, at a subscriber premises, comprising the steps of:	See claim 1[A].
[B] receiving a request at the communications device of the subscriber premises for a service instance from the remote client device;	See claim 1[C].
[C] determining whether the remote client device is entitled to receive the requested service instance;	See claim 1[D].
[D] responsive to determining the remote client device is entitled to receive the requested service instance, determining whether the requested service instance is accessible within the communications device;	See claim 1[E].
[E] if the requested service instance is accessible, transmitting the service instance from the communications device to the remote client device; and	4:34-37; 8:12-16; 13:49-52; 14:4-10; 14:21-33; 5:34-37; 5:10-12.

[F] if the requested service instance is not accessible, sending a request from the communications device to a headend for the requested service instance, wherein upon receipt of the service instance at the communications device, transmitting the service instance from the communications device to the remote client device.	1:53-61; 10:63-67; 13:4-24; 13:29-42; 15:26-29; 17:17-23; 2:36-41; 4:49-61; 7:1-6 ; 4:7-16; Fig. 4; 4:61-67.
---	--

Hicks also anticipates independent claim 12. Claim 12 is almost identical to independent claim 1. The only difference between the two claims is that claim 12 recites a communication device receiving requests for service items from at least two remote devices. Hicks discloses that “*a user at any appliance through a Web-based graphical user interface can instruct the processor to record any broadcast program onto the mass storage for subsequent viewing and/or listening from a multiplicity of appliances.*” See 17:1-21. Hicks further states that “[*m*]ultimedia content that is stored on the BMG can be accessed **from any of the information appliances on the broadband home network.**” See 4:34-37 (emphasis added).

Finally, Figure 1 illustrates that Hicks’ system supports a plurality of devices on the residential local network connected to the BMG. See Figure 1 (40/300, 50, 60, 70, 80), Ex. 1007, Perkins Decl., ¶¶ 128-132.

These descriptions make clear that Hicks’s system receives, manages and responds to content requests from multiple remote devices as required by claim 12.

Claim 12 (a) - Method of transmitting service instance from communication device to remote device. Claim 12(a) is identical to claim 1(a). The arguments

present for claim 1(a). As such, Hicks discloses claim 12(a) for at least the reasons stated above.

Claim 12(b) - Receiving a first request for stored service instance from first remote device. Claim 12(b) is identical to claim 6(b). The arguments present for
5 claim 6(b) also apply to claim 12(b). As such, Hicks discloses claim 12(b) for at least the reasons stated above.

Claim 12(c) - Determining if the remote client device is entitled. This limitation is identical to claim 1(d). As described above with respect to claim 1(d) and incorporated herein, Hicks discloses both (1) traditional CA techniques such as
10 smart cards and subscriber management systems and (2) security technology licensing standards such as DTCP as ways for determining whether the remote information appliances have the authority to access the requested content. *See* 4:23-27; 9:22-36, 10:58-67, and Ex. 1007, Perkins Decl., ¶¶ 95-108.

Claim 12(d) - If entitled, transmitting service instance to first requester.
15 This limitation is identical to claim 1(e). The arguments present for claim 1(e) are fully incorporated herein. As such, Hicks discloses claim 12(d) for at least the reasons stated above.

Claim 12(e) - Receiving a second request for a service instance. Claim 12(e) is identical to claim 6(b). The arguments present for claim 6(b) also apply to claim
20 12(e). As set forth above, Hicks discloses that the BGM can receive multiple

requests from a plurality of remote information appliances. Specifically, Hicks states “a user at any appliance through a Web-based graphical user interface can instruct the processor to record any broadcast program onto the mass storage for subsequent viewing and/or listening from a multiplicity of appliances.” See 17:1-

5 21, Ex. 1007, Perkins Decl., ¶¶ 113-114. As such, Hicks discloses claim 12(e).

Claim 12(f) - Determining if the remote client device is entitled. This

limitation is identical to claim 1(d). As described above with respect to claim 1(d),

Hicks discloses both (1) traditional CA techniques such as smart cards and

subscriber management systems and (2) security technology licensing standards

10 such as DTCP as ways for determining whether the remote information appliances

have the authority to access the requested content. See 4:23-27; 9:22-36, 10:58-67,

and Ex. 1007, Perkins Decl., ¶¶ 95-111.

Claim 12(e) - If entitled, transmitting service instance to second requester.

This limitation is largely identical to claim 1(e). The arguments presented for

15 claim 1(e) also apply to claim 12(e). Moreover, Hicks further teaches transmitting

a multimedia request to a second information appliance based on the local

availability of the requested multimedia item. Hicks teaches that content

downloaded to MODD and locally stored and made available to the subscriber

upon request, whereas live content can be made available by tuning the tuner to the

selected channel thereby disclosing that transmission is based on local availability.

See 15:44-59, 4:55-67, Ex. 1007, Perkins Decl., ¶¶ 109-111.

Claim 12	Hicks
[A] A method of transmitting service instances to a plurality of remote client devices in a local network, including a communications device, at a subscriber premises, comprising the steps of:	2:14-17; 3:10-14.
[B] receiving a first request for a service instance at the communications device of the subscriber premises from a first remote client device;	14:51-53; 4:34-37; 4:55-61.
[C] determining whether the first remote client device is entitled to receive the requested service instance;	4:17-27; 11:25-29.
[D] responsive to determining the first remote client device is entitled to receive the requested service instance, transmitting the requested service instance from the communications device to the first remote client device;	4:58-67; 5:18-20; 13:30-32.
[E] receiving a second request for the service instance at the communications device from a second remote client device in the local network;	8:48-52; 3:10-14; 14:51-53; 4:34-37; 4:55-61.
[F] determining whether the second remote client device is entitled to receive the requested service instance; and	4:17-27; 11:25-29.
[G] responsive to determining the second remote client device is entitled to receive the requested service instance, transmitting the requested service instance from the communications device to the second remote client device based upon local availability of the requested service instance within the communications device.	4:58-67; 5:18-20; 13:30-32.

Claims 2, 8, 13. With respect to dependent claims 2, 8 and 13, Hicks

discloses operating a variety of information appliances such as thin-client set-top

5 boxes, audio systems, and wireless MP3 players in the residential broadband

network. *See* Fig. 1, 4:8-11. Hicks also discloses that two different types of conditional access systems or different copy protection encryptions schemes could be integrated in the residential entertainment system. *See* 4:4:23-28, 9:16-36. One of skill in the art would have understood that the BMG would “determin[e] a device type for the remote client device” so that the BMG can “us[e] the device type of the remote client device to determine a format protocol for the requested service instance” (e.g., use the correct conditional access format or digital program format) for delivering content. *See* Ex. 1007, Perkins Decl., ¶¶ 152-155. Hicks also teaches “*reformatting the requested service instance prior to transmitting the requested service instance*” because encrypted content must be re-formatted to suit the format of the conditional access smart technology prior to being used by a requesting device.

Claims 2, 8 and 13	Hicks
[A] The method of claim 1, further comprising the steps of: determining a device type for the remote client device;	7:47-53; 9:11-14.
[B] using the device type of the remote client device to determine a format protocol for the requested service instance; and	7:47-53; 9:11-14.
[C] reformatting the requested service instance prior to transmitting the requested service instance.	7:47-53; 9:11-14.

Claims 3, 9, 14. With respect to claims 3, 9 and 14, Hicks discloses the use of DTCP to encrypt information or multimedia signals. *See* 9:16-36. DTCP’s message exchange includes a “device capabilities” message in which the receiver

device provides information about its decryption capabilities to the source device. *See* Ex. 1007, Perkins Decl., ¶¶ 156-158. Hicks also discloses the use of different types of conditional access systems in the residential entertainment system. *See* 4:4:23-28. Both DTCP copy protection and smartcard technology provide content protection in which encryption is performed prior to transmission. *See* Ex. 1007, Perkins Decl., ¶¶ 96-111. Therefore, Hicks reads on the claim limitation “prior to transmitting the requested service instance, encrypting the requested service instance.”

Claims 3, 9 and 14	Hicks
[A] The method of claim 1, further comprising the steps of: determining an encryption scheme for the requested service instance based on the remote client device; and	4:21-27.
[B] prior to transmitting the requested service instance, encrypting the requested service instance.	9:23-36.

Claims 4, 10, 15. With respect to claims 4, 10 and 15, Hicks discloses the use of DTCP for content protection. *See* 9:30-33. One of ordinary skill would have understood that DTCP uses (and thus Hicks inherently discloses) a “device capabilities” mask by which a remote client device communicates encryption capabilities to the source device. *See* Ex. 1007, Perkins Decl., ¶¶ 159-160. This feature of DTCP reads on claim 4, 10 and 15 which requires “receiving a message along with the request from the remote client device, the message having device

type information regarding the remote client device.” Furthermore, per DTCP, devices that do not support any additional cryptographic features are assumed to only support a 56-bit baseline cipher. *See* Ex. 1007, Perkins Decl., ¶ 160.

Therefore, the disclosure of DTCP in Hicks teaches “determining from the device

5 type information the encryption scheme for encryption of the requested service instance” as recited in dependent claims 4, 10 and 15.

Claims 4, 10 and 15	Hicks
[A] The method of claim 3, further comprising the steps of: receiving a message along with the request from the remote client device, the message having device type information regarding the remote client device; and	9:31-32.
[B] determining from the device type information the encryption scheme for encryption of the requested service instance.	9:31-32.

Claim 17. With respect to Claim 17, Hicks discloses that “*the device type information from each of the first and second remote devices may require a same encryption scheme or a different encryption scheme*” because Hicks discloses that

10 playback devices of multiple subscribers are served by the same video server 176.

Only two possibilities inherently exist for the video server 176 to provide content access to subscribers - either to use the same encryption scheme or to use different encryption schemes.

Claim 17	Hicks
The method of claim 16, wherein the device type information from each of the first and second remote devices may require a same encryption scheme or a different	4:17-27.

encryption scheme.	
--------------------	--

Claim 18(a) - Determining whether service instance is accessible. This limitation is nearly identical to limitation 6(d). As described above with respect to claim 6(d), Hicks discloses determining if the requested content is available at the local server before transmitting any content to the playback device. *See* 14:51-54, 4:55-65, 1:53-55, Ex. 1007, Perkins Decl., ¶ 127.

Claim 18(b) - If not accessible, request service instance from headend. This limitation is nearly identical to limitation 6(f). As described above with respect to claim 6(f), Hicks discloses forwarding the on-demand request for content to the central distribution server (headend) and subsequently transmitting the content to the playback device from the local server upon receipt. *See* 13:30-32, 4:8-14, Ex. 1007, Perkins Decl., ¶ 127.

Claim 18	Hicks
[A] The method of claim 12, further comprising the steps of: prior to transmitting the requested service instance to the first remote client device, determining whether the requested service instance is accessible within the communications device; and	14:51-54; 4:55-65; 1:53-55.
[B] if the requested service instance is not accessible, sending a request to a headend for the requested service instance, wherein upon receipt of the service instance, transmitting the service instance from the communications device to the first remote client device.	13:30-32; 4:8-14.

Claim 19. With respect to Claim 19, Hicks discloses that “the requested service instance is accessible if the service instance is stored in memory of the communication device.” Because Hicks’ MODD can download top ten movie rentals and store them locally and make them available for the user to watch on one of the multiple devices. *See* 13:43-58, Ex. 1007, Perkins Decl., ¶¶ 179-180.

Claim 19	Hicks
The method of claim 18, wherein the requested service instance is accessible if the service instance is stored in memory of the communications device.	4:34-37; 5:10-12.

Claims 7, 20 - Storing the service instance before transmitting to the client.

Hicks discloses storing the digital content (movies, TV programs, etc.) at the MODD (communication device) before transmitting it to the playback device (remote device). *See* 6:11-17, 8:15-21, Fig. 5, Ex. 1007, Perkins Decl., ¶ 162.

Claim 7	Hicks
The method of claim 6, further comprising the step of, prior to transmitting the service instance to the remote client device, storing the received service instance in memory of the communications device.	2:23-26; 4:17- 18; 5:1-3; 12:66 - 13:4; 13:6-3.

Claim 20 recites claim limitation identical to claim 7 and is anticipated by

Hicks for the same reasons as in claim 7.

Claim 20	Hicks
The method of claim 18, further comprising the step of, prior to transmitting the service instance to the first remote client device, storing the received service instance in memory of the communications device.	2:23-26; 4:17-18; 5:1-3; 12:66 - 13:4; 13:6-13.

B. OBVIOUSNESS

1. Claims 2, 8 and 13 Are Unpatentable Under 35 U.S.C. § 103(a) over Hicks and Egli

An overview of Hicks has been provided previously. Egli relates to media

5 delivery from a server to client devices. *See* Ex. 1005 “Egli”, Abstract. Egli provides for a technique that provides on-the-fly media reformatting with advanced client detection to enable the delivery of an appropriate and best possible incarnation of a provider’s media to a connected device. *See* Egli ¶ [0014].

Hicks and Egli both relate to providing multimedia content to a wide range
10 of information appliances connected to a server. Therefore, one of skill in the art would have readily combined Egli’s on-the-fly media reformatting technique with the BMG of Hicks to enable the delivery of an appropriate and best possible incarnation of a provider’s media to a connected device. *See* Egli, ¶ [0014], Ex. 1007, Perkins Decl., ¶¶ 184-189.

15 Claim 2, 8 and 13. With respect to dependent claims 2, 8 and 13, Egli teaches on-the-fly media reformatting technique. *See* Egli ¶ [0014]. A device type of the client is identified based on an HTTP request received from the client. *See* Egli ¶ [0029]. Some examples of device capability include screen resolution, whether or not an image is to be rotated, etc. *See* Egli ¶ [0069]. The source media
20 is reformatted according to those capabilities. *See* Egli ¶ [0029]. The transformed

media content is then returned to the client device. *See* Egli ¶ [0034], Ex. 1007 Perkins Decl., ¶¶ 184-189.

Claims 2, 8 and 13	Egli
[A] The method of claim 1, further comprising the steps of: determining a device type for the remote client device;	[0029].
[B] using the device type of the remote client device to determine a format protocol for the requested service instance; and	[0014], [0069].
[C] reformatting the requested service instance prior to transmitting the requested service instance.	[0014], [0029].

2. Claims 3-5, 9-11 and 14-16 Are Unpatentable Under 35 U.S.C. § 103(a) over Hicks and Safadi

5 An overview of Hicks has been provided previously. Safadi describes a Personal Versatile Recorder (PVR) that functions as a caching and distribution gateway that provides the integrated capacity to store, replay, retrieve, and distribute content.” *See* Ex. 1004 “Safadi” ¶ [0023], [0032]. Safadi further discloses that “it is an object of the present invention to provide an apparatus and

10 method that affords a Multiple System Operator, the Internet Service Provider, or the content provider, (hereinafter referred to as the system operator) the ability to limit the unauthorized distribution and reproduction of content transferred by the system operator over a delivery network to a user of the system.” *See* Safadi ¶ [0012], [0022].

15 Both Hicks and Safadi disclose the use of DTCP copy protection scheme for encrypting content. As such, one of skill in the art could have readily combined

Safadi's content encryption technique with Hicks' BMG. *See* Ex. 1007, Perkins Decl., ¶¶ 190-192.

Claims 3, 9, 14. Hicks' disclosure of each and every limitation of Claims 3, 9 and 14 has been described previously.

Claims 3, 9 and 14	Hicks
[A] The method of claim 1, further comprising the steps of: determining an encryption scheme for the requested service instance based on the remote client device; and	4:21-27.
[B] prior to transmitting the requested service instance, encrypting the requested service instance.	9:23-36.

5 Claims 4, 10, 15. In addition to Hicks as applied to claims 3, 9 and 14, Safadi discloses "The secure transfer of the content from the Personal Versatile Recorder (10) to a receiver/playback device (30) is established using a standard protocol. This protocol may include, but is not limited to, the Secure Sockets Layer (SSL) protocol." *See* Safadi ¶ [0022], [0028]. The receiver playback devices
10 can be PCs, handheld computers, cellphones, MP3 players, etc. *See* Safadi ¶ [0022], [0026]. One of ordinary skill in the art would have understood that Safadi's PVR, once it knows the device type, picks the appropriate encryption scheme (SSL, no encryption, etc.) for that device type. "This content is transported from the Personal Versatile Recorder (10) to the receiver/playback device (30).
15 The content is transferred either as an encrypted stream or an unencrypted stream." *See Safadi* ¶ [0022], [0025], Ex. 1007, Perkins Decl., ¶¶ 193-197.

Claims 4, 10 and 15	Safadi
[A] The method of claim 3, further comprising the steps of: receiving a message along with the request from the remote client device, the message having device type information regarding the remote client device; and	[0022], [0025], [0026]
[B] determining from the device type information the encryption scheme for encryption of the requested service instance.	[0022], [0025], [0026]

Claim 5, 11 and 16. With respect to claims 5, 11 and 16, Safadi further

discloses that “a system operator compares the identifier (of a requesting device) against a nationally known revocation list of prohibited devices...If identifier is not on the revocation list and has not been previously associated with any other set-top terminal, the identifier is then registered and associated with the Personal Versatile Recorder (10). The system operator sends an acknowledgement to the Personal Versatile Recorder (10) indicating the association of the Personal Versatile Recorder (10) with the receiver/playback device (30). But if the identifier is on the revocation list, then the association of the Personal Versatile Recorder (10) with the receiver/playback device (30) is denied and the system operator sends a negative acknowledgement to the Personal Versatile Recorder (10). Upon receipt of this negative acknowledgement, the Personal Versatile Recorder (10) terminates the transfer request.” *See* Safadi ¶ [0022], [0039]. One of ordinary skill in the art would have understood that the headend control would include telling the PVR not just whether to allow the transfer, but which encryption scheme to use if the transfer is allowed. *See* Ex. 1007, Perkins Decl., ¶¶ 198-201. Safadi’s use of

DTCP standard, which also uses a revocation list, further demonstrates the teaching of headend based determination of encryption by Safadi. *See* Ex. 1007, Perkins Decl., ¶ 195.

Claims 5, 11 and 16	Safadi
[A] The method of claim 3, further comprising the steps of: receiving a message along with the request from the remote client device, the message having device type information regarding the remote client device;	[0022], [0039]
[B] transmitting a second message to the headend, the second message having the device type information included therein, wherein the headend determines the encryption scheme using at least the device type information.	[0022], [0039]

3. Claim 6 is Unpatentable Under 35 U.S.C. § 103(a) over Hicks and Putterman

As previously discussed, Hicks discloses each and every step of claim 6.

Claim 6 recites an availability determination step (“*determining whether the requested service instance is available within the communication device*”) that is performed responsive to an entitlement determination step (“*determining the remote client device is entitled to receive the requested service instance.*”)

There is nothing in the ‘592 Patent indicating that the specific order of the steps is important, non-obvious or produces unexpected results. In fact, the sequence of these steps, or implementing them in parallel, would have been an implementation choice to one of skill in the art, producing the same intended result of controlling access to content. *See* Ex. 1007, Perkins Decl., ¶¶ 220-223.

The claim steps are further obvious in view of Putterman. *See* Ex. 1006 “Putterman”. In analogous art, Putterman discloses a home media network (title, Fig. 2), in which a user can access content stored in an in-home set-top box 220 (Fig. 2). In one content access method, (Putterman, Fig. 10, ¶¶ [0057], [0058]) the sequence of step includes checking whether the requesting user is authorized to receive the media (step 1030), and if authorized, in step 1040, using a storage module to search for the requested media object. One of skill in the art would have combined Putterman with Hicks as an implementation choice to produce the predictable result that content access is controlled only to a user who is entitled to watch it. Ex. 1007, Perkins Decl., ¶¶ 220-223.

VII. CONCLUSION

In light of the above prior art, there is a reasonable likelihood that Petitioner will prevail in its challenge of patentability for claims 1-20 of the ‘592 Patent. It is respectfully requested that a trial for Inter Partes Review of the ‘592 Patent be instituted and claims 1-20 be rejected and canceled.

Dated: June 4, 2013

PERKINS COIE LLP
11988 El Camino Real, Suite 200
San Diego, CA 92130
(858) 720-5700

Respectfully submitted,

/Amy E. Simpson/

Amy E. Simpson, Reg. No. 54,688
Bing Ai, Reg. No. 43,312
Nicholas T. Bauz, Reg. No. 41,604

Attorneys for Petitioner OpenTV, Inc.

CERTIFICATE OF SERVICE

The undersigned hereby certifies that a true copy of the foregoing
PETITION FOR *INTER PARTES* REVIEW OF U.S. PATENT NO. 7,505,592 B2
and supporting materials (Exhibits 1001-1010 and Power of Attorney) have been
served in its entirety this 4th day of June, 2013, by EXPRESS MAIL® on the
Patent Owner at the official correspondence address for the attorney of record for
the '592 Patent shown in USPTO PAIR and the attorneys of record for Plaintiff in
the concurrent litigation matter:

SCIENTIFIC-ATLANTA, INC.
Intellectual Property Department
5030 Sugarloaf Parkway
Room 4.3.518
Lawrenceville, Georgia 30044

Edward R. Reines
Sonal N. Mehta
J. Jason Lang
WEIL, GOTSHAL & MANGES LLP
Silicon Valley Office
201 Redwood Shores Parkway
Redwood Shores, California 94065

/Amy E. Simpson/
Amy E. Simpson, Reg. No. 54,688
Bing Ai, Reg. No. 43,312
Nicholas T. Bauz, Reg. No. 41,604

Attorneys for OpenTV, Inc.