

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

In re Patent of: Sekiguchi et al.  
U.S. Patent No.: 8,230,101 Attorney Docket No. 50095-0245IP1  
Issue Date: July 24, 2012  
Appl. Serial No.: 12/527,777  
Filing Date: September 2, 2009  
Title: SERVER DEVICE FOR MEDIA, METHOD FOR  
CONTROLLING SERVER FOR MEDIA, AND PROGRAM

**Mail Stop Patent Board**

Patent Trial and Appeal Board  
U.S. Patent and Trademark Office  
P.O. Box 1450  
Alexandria, VA 22313-1450

**PETITION FOR *INTER PARTES* REVIEW OF UNITED STATES PATENT  
NO. 8,230,101 PURSUANT TO 35 U.S.C. §§ 311–319, 37 C.F.R. § 42**

**TABLE OF CONTENTS**

I.	Standing .....	1
II.	The '101 Patent.....	1
	A. Brief Description.....	1
	B. Prosecution History.....	4
	C. Priority Date.....	4
III.	Level of Ordinary Skill.....	5
IV.	Claim Construction.....	5
V.	The Challenged Claims are Unpatentable .....	5
	A. Ground 1A: Lamkin.....	6
	1. Lamkin (APPLE-1004) .....	6
	2. Analysis .....	7
	B. Ground 1B: Lamkin-Fiechter.....	40
	1. Fiechter (APPLE-1006).....	40
	2. Lamkin-Fiechter Combination .....	42
	3. Analysis .....	45
	C. Ground 1C: Lamkin-Ito .....	48
	1. Ito (APPLE-1012) .....	48
	2. Lamkin-Ito Combination.....	49
	3. Analysis .....	52
	D. Ground 2A: Franke .....	54
	1. Franke (APPLE-1005).....	54
	2. Analysis .....	55
	E. Ground 2B: Franke-Fiechter .....	83
	1. Franke-Fiechter Combination .....	83
	2. Analysis .....	85
	F. Ground 2C: Franke-Ito.....	89
	1. Franke-Ito Combination .....	89
	2. Analysis .....	91
VI.	INSTITUTION SHOULD NOT BE DENIED ON DISCRETION.....	93
VII.	Conclusion and Fees—37 C.F.R. §42.103 .....	93
VIII.	MANDATORY NOTICES UNDER 37 C.F.R. § 42.8(a)(1).....	94
	A. Real Party-In-Interest Under 37 C.F.R. § 42.8(b)(1).....	94
	B. Related Matters Under 37 C.F.R. § 42.8(b)(2).....	94
	C. Lead And Back-Up Counsel Under 37 C.F.R. § 42.8(b)(3).....	94
	D. Service Information .....	95

**LIST OF EXHIBITS**

APPLE-1001	U.S. Patent No. 8,230,101
APPLE-1002	U.S. Patent No. 8,230,101 File History
APPLE-1003	Declaration of Dr. Erez Zadok
APPLE-1004	U.S. Patent Publication No. 2006/0161635 to Lamkin et al. ("Lamkin")
APPLE-1005	U.S. Patent Publication No. 2003/0195924 to Franke et al. ("Franke")
APPLE-1006	U.S. Patent No. 7,219,123 to Fiechter et al. ("Fiechter")
APPLE-1007	U.S. Patent Publication No. 2004/0006606 to Marotta et al. ("Marotta")
APPLE-1008	U.S. Patent Publication No. 2002/0184457 to Yuasa et al. ("Yuasa")
APPLE-1009	U.S. Patent Publication No. 2008/0104219 to Kageyama et al. ("Kageyama")
APPLE-1010	U.S. Patent Publication No. 2006/0184972 to Rafey et al. ("Rafey")
APPLE-1011	U.S. Patent Publication No. 2007/0238471 to Bae et al. ("Bae")
APPLE-1012	International Patent Publication No. WO2006/073040 to Ito et al. with certified English translation ("Ito")
APPLE-1013	U.S. Patent Publication No. 2002/0099952 to Lambert, et. al. ("Lambert")

- APPLE-1014 U.S. Patent Publication No. 2002/0010819 to Dye (“Dye”)
- APPLE-1015 U.S. Patent Publication No. 2004/0220926 to Lamkin (“Lamkin ’926”)
- APPLE-1016 U.S. Patent Publication No. 2005/0281185 to Kawasaki (“Kawasaki”)
- APPLE-1017 Microsoft Computer Dictionary, 5<sup>th</sup> ed., 2002, excerpts (“Microsoft Computer Dictionary”)
- APPLE-1018 Abraham Silberschatz and Peter B. Galvin, *Operating Systems Concepts*, 4th Edition, 1994, Addison-Wesley Publishing, excerpts (“Silberschatz”)
- APPLE-1019 Andrew S. Tanenbaum, *Computer Networks*, 2nd ed., 1988, excerpts (Tanenbaum)
- APPLE-1020 W. Richard Stevens, *TCP/IP Illustrated Volume 1, The Protocols*, 1994, excerpts (Stevens)
- APPLE-1021 William R. Cheswick & Steven M. Bellovin, *Firewalls and Internet Security, Repelling the Wily Hacker*, 1994, excerpts (Cheswick)
- APPLE-1022 U.S. Patent No. 6,687,846 to Adrangi et al. (“Adrangi”)
- APPLE-1023 U.S. Patent No. 6,487,663 to Jaisimha et al. (“Jaisimha”)
- APPLE-1024 U.S. Patent No. 6,732,365 to Belknap et al. (“Belknap”)
- APPLE-1025 U.S. Patent Publication No. 2008/0060081 to Van Den Heuvel (“VDH”)
- APPLE-1026 Digital Living Network Alliance (DLNA), *Overview and Vision*, White Paper, June 2004 (“DLNA Overview”)

- APPLE-1027 UPNP Forum Version 1.0 Approved Standard,  
*MediaServer:2 Device Template Version 1.01*, Document  
Version 1.00, May 31, 2006 (“UPnP MediaServer”)
- APPLE-1028-1100 RESERVED
- APPLE-1101 Complaint for Patent Infringement (August 20, 2024), Case  
No. 2-24-CV-00687 (EDTX), Document 1
- APPLE-1102 Appendix E-3 to Complaint for Patent Infringement – Claim  
Chart for U.S. Patent No. 8,230,101 Against Apple HomeKit  
Secure Video Products
- APPLE-1103 Appendix E-2 to Complaint for Patent Infringement – Claim  
Chart for U.S. Patent No. 8,230,101 Against Products with  
HTTP Live Streaming (HLS)
- APPLE-1104 Appendix E-1 to Complaint for Patent Infringement – Claim  
Chart for U.S. Patent No. 8,230,101 Against Apple Products  
with iCloud Storage
- APPLE-1105 Interim Process for PTAB Workload Management,  
Memorandum dated March 26, 2025 downloaded from  
<https://www.uspto.gov/sites/default/files/documents/InterimProcesses-PTABWorkloadMgmt-20250326.pdf>
- APPLE-1106 Patent Trial and Appeal Board (PTAB) Boardside Chat:  
Interim processes relating to institution in AIA proceedings,  
downloaded from  
[https://www.uspto.gov/sites/default/files/documents/boardside\\_chat\\_interim\\_process\\_for\\_aia\\_institution\\_decisions\\_.pdf](https://www.uspto.gov/sites/default/files/documents/boardside_chat_interim_process_for_aia_institution_decisions_.pdf)  
on April 25, 2025

**LISTING OF CLAIMS**

Claim 1	
[1pre]	A server device for media, the server device for media comprising:
[1a-i]	an internal storage device for storing digital contents,
[1a-ii]	wherein the server device for media responds to a data transmission request from a network player by stream-delivering corresponding data in corresponding digital contents from the internal storage device to the network player during connection to a network;
[1b-i]	a transfer control unit adapted to transfer and store part of held digital contents in the internal storage device to a network storage device,
[1b-ii]	wherein the network storage device is connected to the network and is capable of storing data,
[1b-iii]	and wherein said transfer control unit does not transfer, from the internal storage device to the network storage device, the digital contents that cannot be recovered if a network failure occurs during the transferring of the digital contents from the internal storage device to the network storage device;
[1c-i]	a list information transmission unit adapted to respond to a list presentation request for the held digital contents of the server device for media from the network player by transmitting list information to the network player,
[1c-ii]	wherein the list information lists the digital contents left in the internal storage device and the digital contents transferred from the internal storage device to the network storage device and stored in the network storage device,
[1c-iii]	and wherein the list information maintains a tree structure of the digital contents in the internal storage device before transferring the digital contents to the network storage device;

[1d]	a search unit adapted to respond to a data transmission request for the held digital contents from the network player by searching for a location where the held digital contents are currently stored; and
[1e]	a digital contents data transmission processing unit adapted to allow the corresponding data in held digital contents to be stream-delivered from the network storage device to the network player, if the result of search shows the network storage device,
[1f]	wherein the server device for media is a media player.
<b>Claim 2</b>	
[2]	The server device for media according to claim 1, wherein said digital contents data transmission processing unit causes the network storage device to transmit the corresponding data to the server device for media, and then transmits the corresponding data received from the network storage device from the server device for media to the network player.
<b>Claim 3</b>	
[3]	The server device for media according to claim 1, wherein said digital contents data transmission processing unit transmits the corresponding data and information for identifying the network storage device to the network player, and causes the network storage device to directly transmit the corresponding data to the network player.
<b>Claim 4</b>	
[4]	The server device for media according to claim 1, further comprising a return control unit adapted to cause the digital contents corresponding to a predetermined condition among the digital contents which have been transferred to the network storage device to be returned from the network storage device to the internal storage device.

Claim 5	
[5]	The server device for media according to claim 1, wherein said list information transmission unit makes the list information to be transmitted to the network player include information for identifying whether each digital content is currently stored in the internal storage device or the network storage device in the display list of the network player.
Claim 6	
[6pre]	A server device for media, the server device for media comprising:
[6a-i]	an internal storage device for storing digital contents,
[6a-ii]	wherein the server device for media responds to a data transmission request from a network player by stream-delivering corresponding data in corresponding digital contents from the internal storage device to the network player during connection to a network;
[6b-i]	a transfer control unit adapted to transfer and store part of held digital contents in the internal storage device to a network storage device,
[6b-ii]	wherein the network storage device is connected to the network and is capable of storing data,
[6b-iii]	and wherein the digital contents that cannot be recovered if a network failure occurs during the transferring of the digital contents from the internal storage device to the network storage device is transferred after obtaining permission from a user;
[6c-i]	a list information transmission unit adapted to respond to a list presentation request for the held digital contents of the server device for media from the network player by transmitting list information to the network player,
[6c-ii]	wherein the list information lists the digital contents left in the internal storage device and the digital contents transferred from the internal storage device to the network storage device and stored in the network storage device,

[6c-iii]	and wherein the list information maintains a tree structure of the digital contents in the internal storage device before transferring the digital contents to the network storage device;
[6d]	a search unit adapted to respond to a data transmission request for the held digital contents from the network player by searching for a location where the held digital contents are currently stored; and
[6e]	a digital contents data transmission processing unit adapted to allow the corresponding data in held digital contents to be stream-delivered from the network storage device to the network player, if the result of search shows the network storage device,
[6f]	wherein the server device for media is a media player.
<b>Claim 7</b>	
[7pre]	A method for controlling a server device for media which is equipped with an internal storage device for storing digital contents, the method comprising the steps of:
[7a]	responding to a data transmission request from a network player by stream-delivering corresponding data in corresponding digital contents from the internal storage device to the network player during connection to a network;
[7b]	transferring and storing part of held digital contents in the internal storage device to a network storage device, wherein the network storage device is connected to the network and is capable of storing data, and wherein the digital contents that cannot be recovered if a network failure occurs during the transferring of the digital contents are not transferred from the internal storage device to the network storage device;

[7c]	responding to a list presentation request for the held digital contents of the server device for media from the network player by transmitting list information to the network player, wherein the list information lists the digital contents left in the internal storage device and the digital contents transferred from the internal storage device to the network storage device and stored in the network storage device, and wherein the list information maintains a tree structure of the digital contents in the internal storage device before transferring the digital contents to the network storage device;
[7d]	responding to a data transmission request for the held digital contents from the network player by searching for a location where the held digital contents are currently stored; and
[7e]	allowing the corresponding data in held digital contents to be stream-delivered from the network storage device to the network player, if the result of search shows the network storage device,
[7f]	wherein the service device for media is a media player.
<b>Claim 8</b>	
[8]	The server device for media according to claim 6, wherein said digital contents data transmission processing unit causes the network storage device to transmit the corresponding data to the server device for media, and then transmits the corresponding data received from the network storage device from the server device for media to the network player.
<b>Claim 9</b>	
[9]	The server device for media according to claim 6, wherein said digital contents data transmission processing unit transmits the corresponding data and information for identifying the network storage device to the network player, and causes the network storage device to directly transmit the corresponding data to the network player.

<b>Claim 10</b>	
[10]	The server device for media according to claim 6, further comprising a return control unit adapted to cause the digital contents corresponding to a predetermined condition among the digital contents which have been transferred to the network storage device to be returned from the network storage device to the internal storage device.
<b>Claim 11</b>	
[11]	The server device for media according to claim 6, wherein said list information transmission unit makes the list information to be transmitted to the network player include information for identifying whether each digital content is currently stored in the internal storage device or the network storage device in the display list of the network player.
<b>Claim 12</b>	
[12pre]	A method for controlling a server device for media which is equipped with an internal storage device for storing digital contents, the method comprising the steps of:
[12a]	responding to a data transmission request from a network player by stream-delivering corresponding data in corresponding digital contents from the internal storage device to the network player during connection to a network;
[12b]	transferring and storing part of held digital contents in the internal storage device to a network storage device, wherein the network storage device is connected to the network and is capable of storing data, and wherein the digital contents that cannot be recovered if a network failure occurs during the transferring of the digital contents from the internal storage device to the network storage device is transferred after obtaining permission from a user;

[12c]	responding to a list presentation request for the held digital contents of the server device for media from the network player by transmitting list information to the network player, wherein the list information lists the digital contents left in the internal storage device and the digital contents transferred from the internal storage device to the network storage device and stored in the network storage device, and wherein the list information maintains a tree structure of the digital contents in the internal storage device before transferring the digital contents to the network storage device;
[12d]	responding to a data transmission request for the held digital contents from the network player by searching for a location where the held digital contents are currently stored; and
[12e]	allowing the corresponding data in held digital contents to be stream-delivered from the network storage device to the network player, if the result of search shows the network storage device,
[12f]	wherein the server device for media is a media player.

Apple Inc. (“Apple”) petitions for IPR of claims 1-12 (“Challenged Claims”) of U.S. Patent No. 8,230,101 (“’101 patent”).

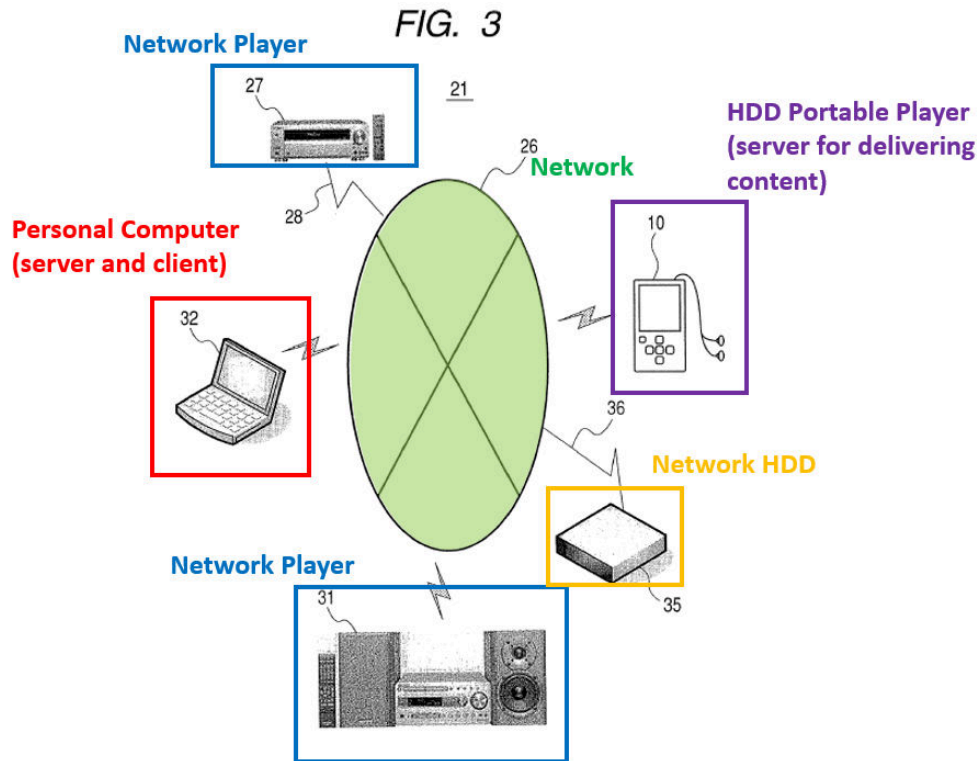
## **I. STANDING**

Apple certifies the ’101 patent is available for IPR. This petition is being filed within one year of service of a complaint *Advanced Coding Technologies LLC v. Apple Inc.*, 2-24-cv-00687 (EDTX), filed August 20, 2024. APPLE-1101. Apple is not barred or estopped from challenging the Challenged Claims on the below-identified grounds.

## **II. THE ’101 PATENT**

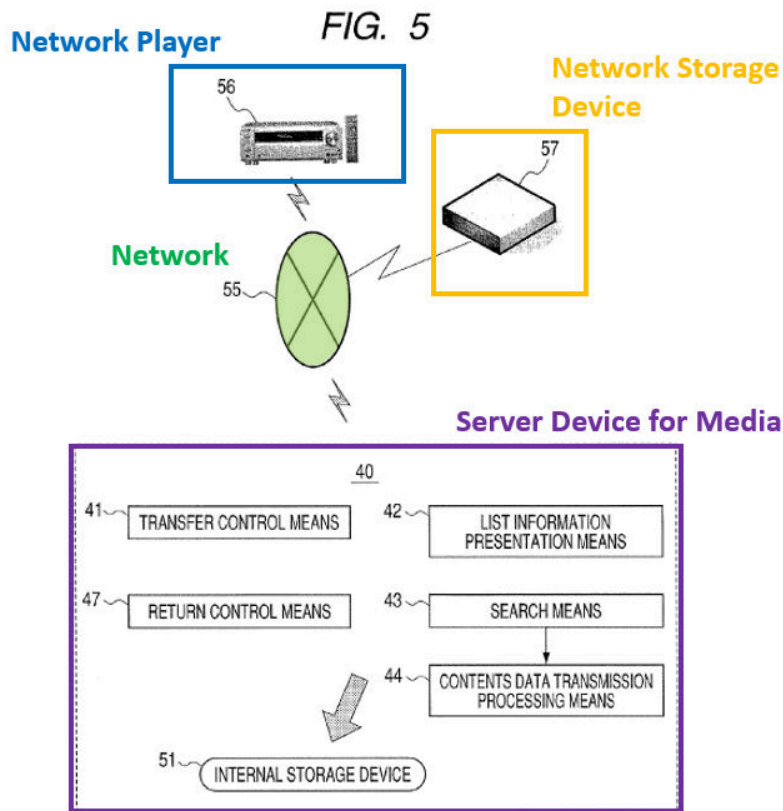
### **A. Brief Description**

The ’101 patent discusses “a server device for media such as an HDD portable player” and “controlling a server for media... capable of smoothly dealing with [] large amounts of digital contents.” APPLE-1001, 1:7-12, 1:51-53, 3:52-55, 4:17-37, FIG. 3.



**APPLE-1001, FIG. 3 (annotated)**

The '101 patent describes a server device that stores digital contents to a network storage device. *Id.*, 6:9-16. The server device 40 “responds to [a] data transmission request from the network player 56 by stream-delivering the corresponding data of the corresponding digital contents from the internal storage device 51 to the network player 56.” *Id.*



**APPLE-1001, FIG. 5 (annotated)**

“The server device for media 40 has transfer control means 41, list information presentation means 42, search means 43, and contents data transmission processing means 44” which allow the server device to store contents to the network storage device, present a list of available content to the network player, determine a location of desired content in internal storage of the server device or in the network storage device, and transmit the desired content to the network player. *Id.*, 6:17-7:12.

## **B. Prosecution History**

During prosecution, the independent claims and various dependent claims were rejected as obvious over US2006/0184972 (APPLE-1010, “Rafey”) and US2007/0238471 (APPLE-1011, “Bae”). Dependent claims 6-7, directed to scenarios where some digital contents would be unrecoverable in a network failure, were rejected as obvious over Rafey, Bae, and US7,219,129 (APPLE-1006, “Fiechter”). APPLE-1002, 169-188. Applicant responded by amending the independent claims to specify “the list information maintains a tree structure of the digital contents” but did not include amendments or arguments responsive to the rejections of dependent claims 6-7. APPLE-1002, 85-88, 89-92.

In a subsequent Action, the Office inexplicably omitted an earlier art rejection of claims 6-7 (from the 11/16/2011 Office Action) without Applicant traversing the rejection or offering amendment relating to those claims. APPLE-1002, 62-78. Applicant then exploited the Office’s omission by incorporating the subject matter of claims 6-7 into pending and new independent claims to obtain allowance. APPLE-1002, 46-56.

However, as illustrated herein, the features of claims 6 and 7, respectively, were well-known by the Critical Date.

## **C. Priority Date**

The ’101 patent was filed as a national stage application of

PCT/JP2007/054603, filed March 2, 2007 (“Critical Date”). APPLE-1001, 1.

Apple does not concede the claimed priority date is correct but nonetheless applies art predating it.

### **III. LEVEL OF ORDINARY SKILL**

The range of qualifications for a POSITA would have included a bachelor’s degree in computer engineering or a comparable field and about 2-3 years of professional experience working with networking and data storage architectures. APPLE-1003, ¶¶44-46. Additional years of experience could substitute for an advanced-level degree (and vice versa). *Id.*

### **IV. CLAIM CONSTRUCTION**

The claim interpretations on which this Petition depends are incorporated in and apparent from the prior art mapping analysis below. *Infra*, §V. While, presently, no claim terms need be construed to resolve issues of controversy raised by this Petition, *see Wellman, Inc. v. Eastman Chem. Co.*, 642 F.3d 1355, 1361 (Fed. Cir. 2011), Apple reserves the right to address and respond to any construction advanced by Patent Owner or the Board.

### **V. THE CHALLENGED CLAIMS ARE UNPATENTABLE**

Apple requests IPR of the Challenged Claims on the following grounds for which Dr. Zadok’s Declaration provides additional explanation. APPLE-1003, ¶¶1-573.

Ground	Claims	Basis - §103
<b>1A</b>	1-12	Lamkin
<b>1B</b>	1-12	Lamkin-Fiechter
<b>1C</b>	1-5, 7-11	Lamkin-Ito
<b>2A</b>	1-12	Franke
<b>2B</b>	1-12	Franke-Fiechter
<b>2C</b>	1-5, 7-11	Franke-Ito

Each reference pre-dates the Critical Date and qualifies as prior art.

Reference	Filing Date	Publication Date	Prior Art
<b>Lamkin</b>	12/16/2005	07/20/2006	§§102(a), (e)
<b>Fiechter</b>	11/21/2000	05/17/2007	§102(e)
<b>Ito</b>	12/12/2005	07/13/2006	§102(a)
<b>Franke</b>	04/15/2002	10/16/2003	§§102(a)-(b), (e)

**A. Ground 1A: Lamkin**

**1. Lamkin (APPLE-1004)**

Lamkin describes a “network media service [for] managing media content over a network.” APPLE-1004, [0002]-[0003]; APPLE-1003, ¶¶197-201.

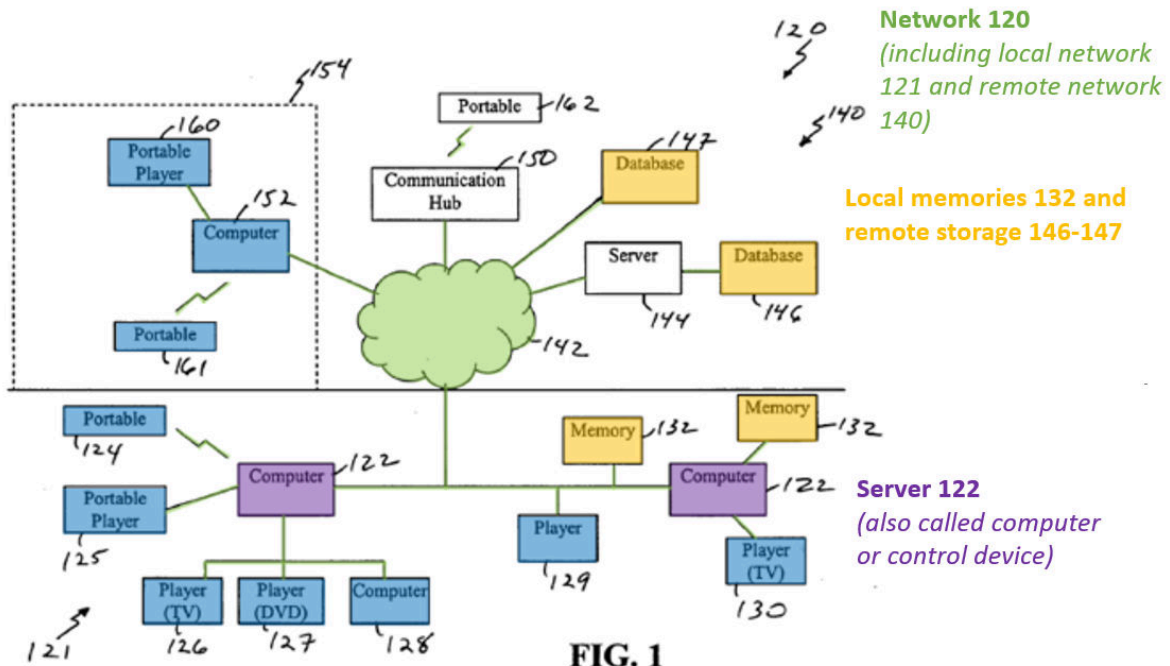


FIG. 1

APPLE-1004, FIG. 1.

Lamkin describes a network 120 in which “[t]he one or more local servers, computers or other control devices 122 provide control over the local network 121 and/or remote network 140, communicate with the client devices 124-130 and storage or other memory 132 (e.g., database, network attached storage (NAS), and other such storage) that store content.” APPLE-1004, [0049].

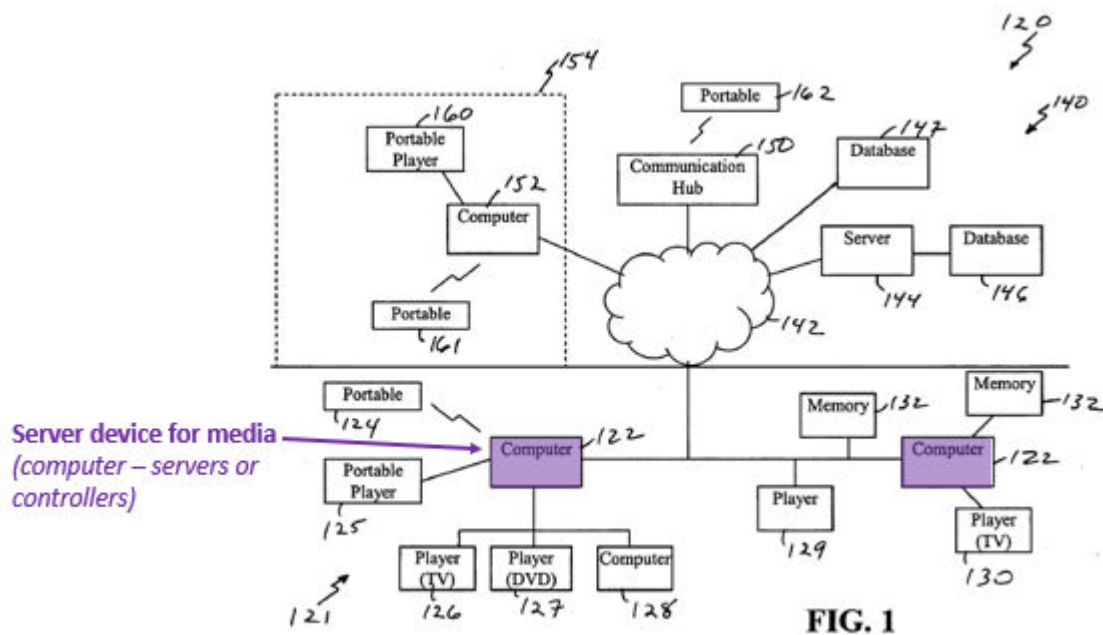
## 2. Analysis

### (a) Claim 1

[1pre]

To the extent the preamble is considered limiting, Lamkin discloses [1pre].

APPLE-1003, ¶¶214-220. Lamkin describes “**one or more local servers, computers or other devices 122**”<sup>1</sup> which “provide control over the local network 121 and/or remote network 140, communicate with the client devices 124-130 and storage or other memory 132 ... that store content.” APPLE-1004, [0049], [0050], [0002], [0052]; APPLE-1003, ¶¶216-217.



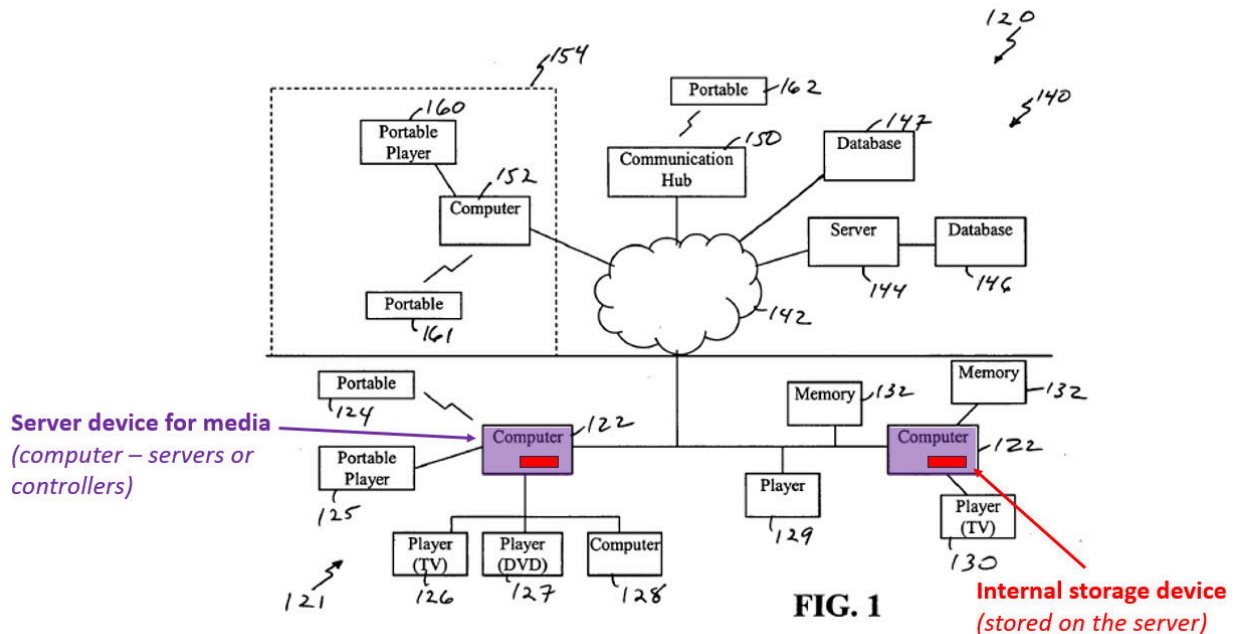
APPLE-1004, FIG. 1 (annotated)

The content stored on the server includes “**multimedia content** including but not limited to video content, audio content, image content, picture content, graphics content” (“server device for media”). *Id.*, [0049]; APPLE-1003, ¶218.

<sup>1</sup> All emphasis added unless otherwise indicated.

[1a-i]

Lamkin discloses [1a-i]. APPLE-1003, ¶¶221. Lamkin describes that server may store content internally (i.e., in an internal storage of the server.) APPLE-1004, [0050] (“content ... **stored in the servers 122**”), [0052] (“stored on the one or more servers 122”), [0078] (“one of the servers 122 can be designated ... **to store content**”), [0077]; APPLE-1003, ¶¶221-228.

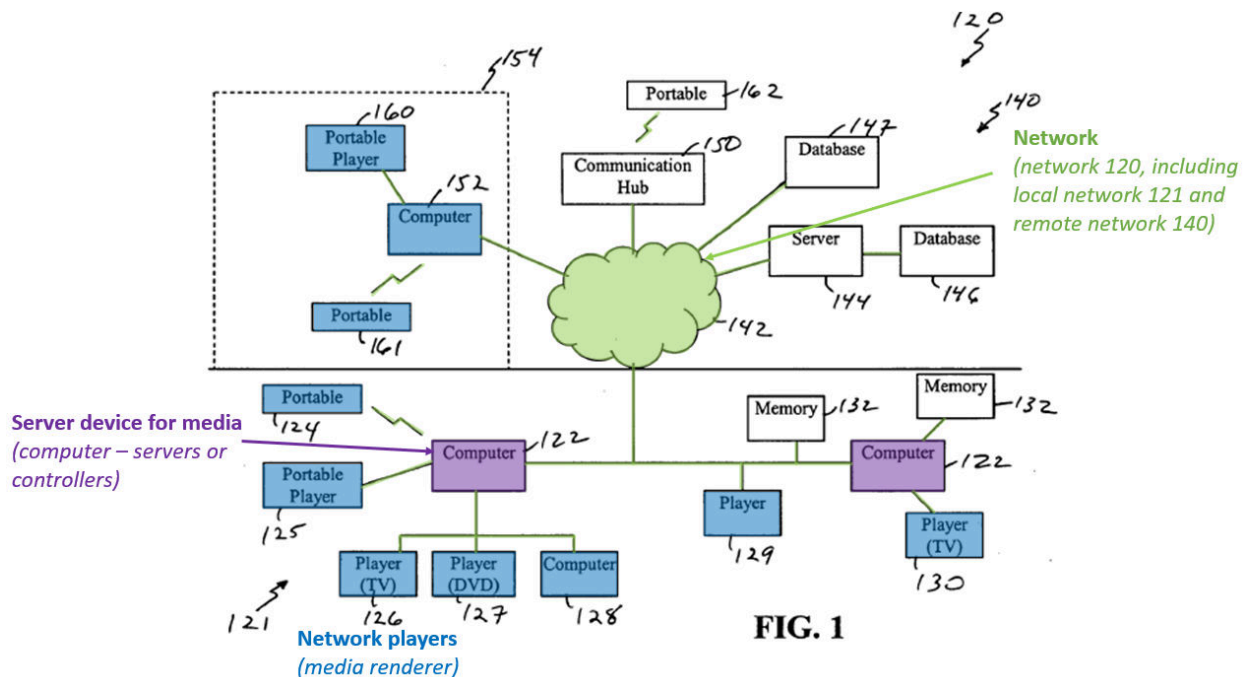


APPLE-1004, FIG. 1 (annotated); APPLE-1003, ¶201

A POSITA would have understood that it was well-known that computers (such as server 122) have internal storage including RAM (volatile storage) and hard disks (non-volatile storage) for storing digital contents and would have understood that Lamkin’s servers include such internal storage. APPLE-1003, ¶¶222-226 (citing APPLE-1013, [0033]; APPLE-1014, [0044]-[0046]).

[1a-ii]

Lamkin discloses [1a-ii]. APPLE-1003, ¶¶229-237. Lamkin describes that server (“server device”) distributes contents (“stream-delivering”) to a client device (“network player”) on the network, such as network players 124-128, 152, and 160-161. APPLE-1004, [0049] (“network allows communication of content ... between components of the network”), [0013] (describing FIG. 2 shows “pulling of content from a media server 22 to a client device”), [0058] (describing FIG. 3 shows “pushing of content between a media server 122 to a client device”), FIGS. 1-3, 27; APPLE-1003, ¶¶230-231.



APPLE-1004, FIG. 1 (annotated)

Lamkin further describes that server (“server device”) receives a request for content from the client device (“responds to a data transmission request from a

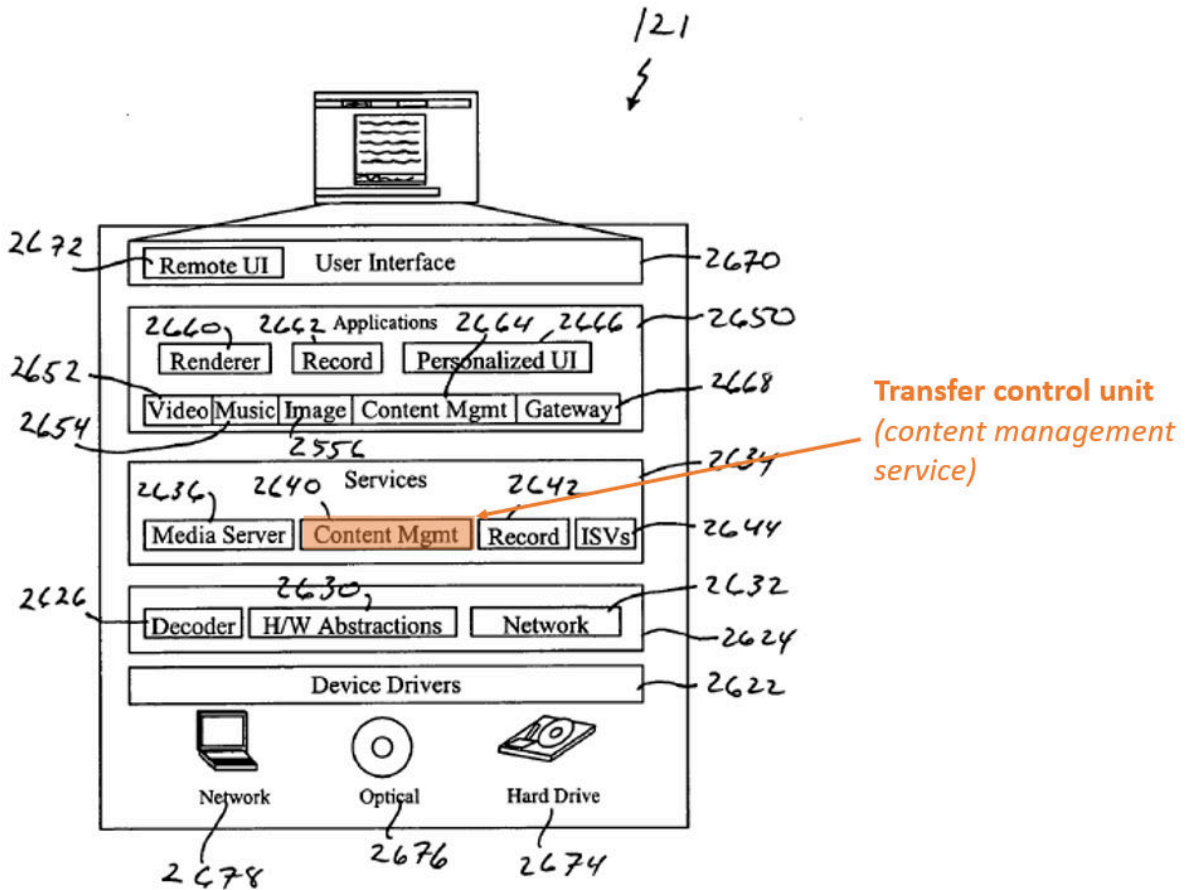
network player”) and provides requested content (“delivering corresponding data in corresponding digital contents from the internal storage device”) to the user at the client device (“network player”). APPLE-1004, [0064] (“Content can be distributed through the network 120 ... for many reasons, such as ... user **or client device demands**”), [0241] (“media server ... **provides media on request**”), [0286], [0056] (“a user interface [that] **allows the user to select the content to be pulled to the client device**”); APPLE-1003, ¶¶230-233. Lamkin describes that “a user 224 initiates and/or controls the push scheme from the media server 122, and [in response] content is delivered to the media renderer.” APPLE-1004, [0058], [0078], [0083], [0230]-[0231], [0241]; APPLE-1003, ¶¶232-233 (citing APPLE-1008, [0111] (“reproduce content upon receipt of a user operation”)).

Lamkin describes that the transfer of content from the server to the client device can occur via stream-delivery (“stream-delivering”) over the network (“during connection to a network”), for example, through “real time streaming protocol (RTSP) streaming.” APPLE-1004, [0160], [0055]; *see id.*, [0056] (“selected content is pulled over the network 120”), [0231]; APPLE-1003, ¶¶234-235.

***[1b-i]***

Lamkin discloses [1b-i]. APPLE-1003, ¶¶238-248. Although the bounds of the term “transfer control unit” are unclear, Lamkin discloses a “content

management service” formed as an agent or bot that is adapted to perform the same functions as the claimed “transfer control unit.” *Compare* APPLE-1004, [0220] (“content management can be implemented in part through one or more agents and/or bots from which services are requested and the agent performs the task”), *with* APPLE-1001, 3:5-9 (“The program ... causes a computer to function as each means of the above-described server device”), 6:28-40; *see* APPLE-1004, [0217]-[0220], [0127], [0166], FIG. 26; APPLE-1003, ¶¶239-242 (explaining that an agent/bot is computer-implemented software for performing a task). A POSITA would have understood that Lamkin’s content management service transfers and stores digital content as described below. APPLE-1003, ¶¶241-246.



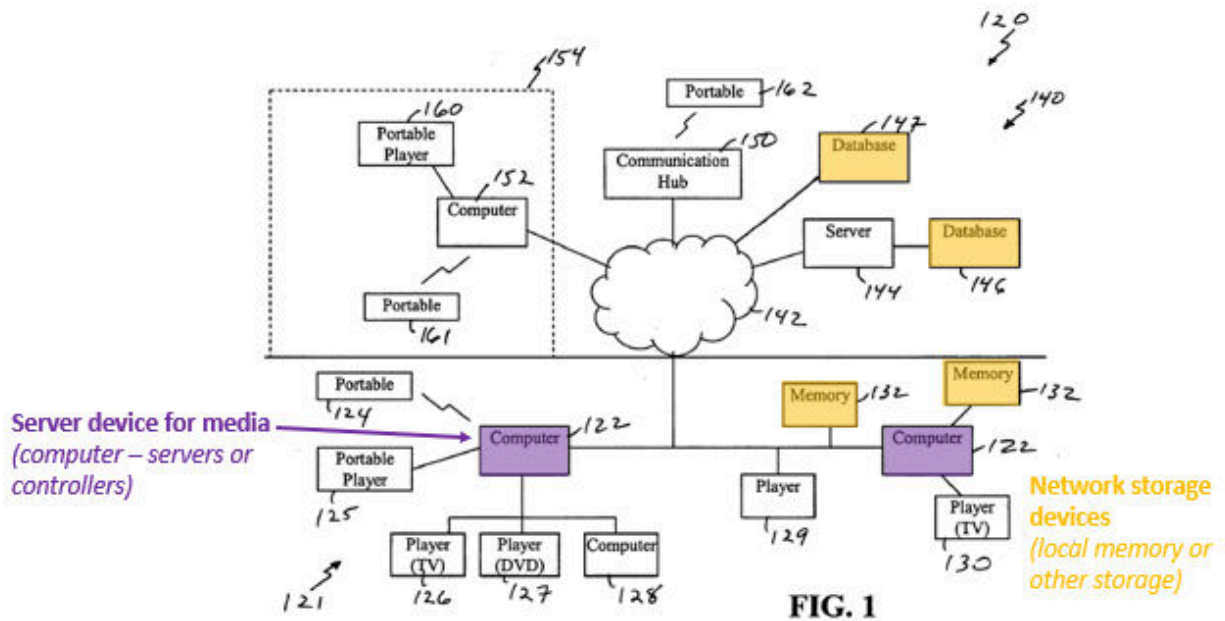
**FIG. 26**

**APPLE-1004, FIG. 26 (annotated)**

Lamkin describes that the content management service (“transfer control unit”) transfers content (“digital contents”) from storage on the server (“internal storage device”) to be stored in other memory 132/remote storage 146-147 (“network storage device”) to optimize storage and access to content. *See* APPLE-1004, [0077] (“**content is transferred and/or stored to one or more storage locations** for centralization, such as on the server, **in the local storage 132, remote storage 146-147, or other such storage**”), [0049]-[0051], [0064]-[0065]

(describing “content distribution models” including “embodiments [that] centralize content and/or provide an automation of file management and transfers allowing for a substantially centralized data model”), [0072], [0141]; APPLE-1003, ¶¶243-246.

Lamkin’s content management service 2640 (“transfer control unit”) and related application 2666 distributes content over the network for storage. *See* APPLE-1004, [0220] (“**content management service 2640** at least in part **performs active management of the content and/or files on the network**, distributes content over the network, tracks content on the network, **initiates archiving of content ...**”), [0049] (“one or more local servers ... communicate with the client devices 124-130 and storage or other memory 132 (e.g., database, network attached storage (NAS), and other such storage) that store content.”), [0082] (“**storing, recording and/or archiving**”), FIG. 26; APPLE-1003, ¶¶245-246. “The **management of the content can move content from being stored on local client devices 124-130 and/or servers 122 to local storage devices 132, and/or to remote storage 146-147.**” APPLE-1004, [0141], [0144]-[0146], [0219]-[0220].



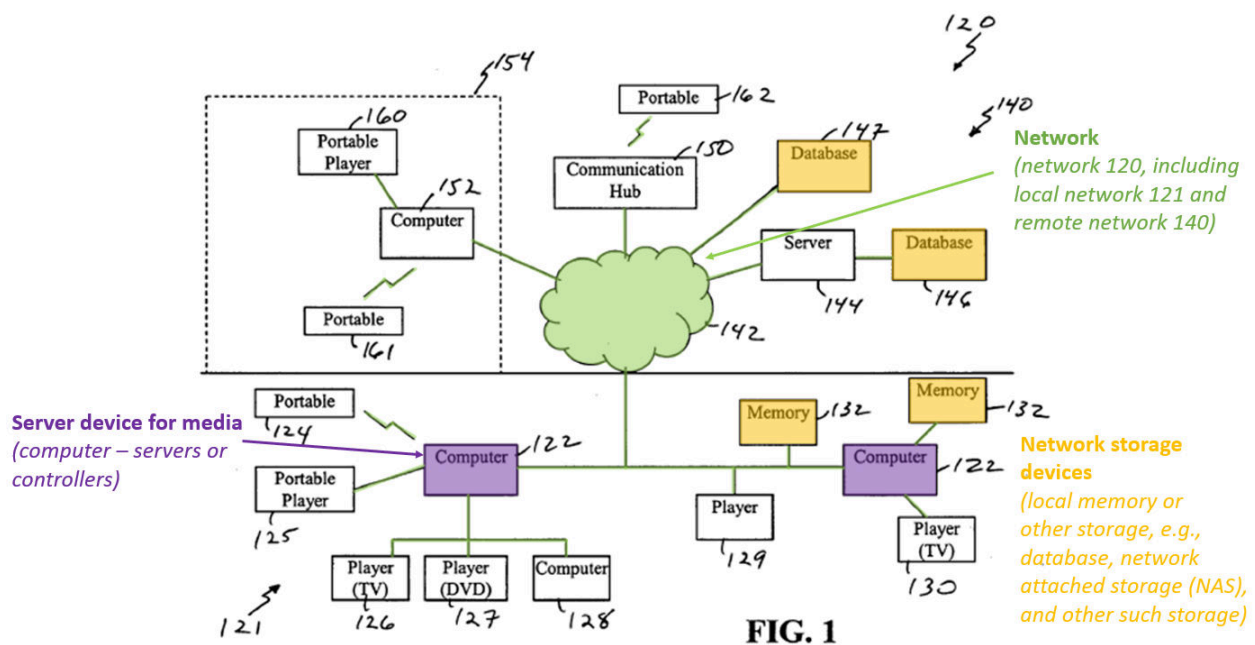
**APPLE-1004, FIG. 1 (Annotated)**

Lamkin further describes that some content is maintained on storage of the server while other content is transferred to other local or remote servers (“transfer and store part of held digital contents”). APPLE-1004, [0078] (“the tiered structure can maintain some content at a local server readily available to the server for distribution to client devices, some content at a local storage 132 to be locally accessed and retrieved, and other content remotely stored”); APPLE-1003, ¶246.

**[1b-ii]**

Lamkin discloses [1b-ii]. APPLE-1003, ¶¶249-254. Lamkin describes that other memory 132 or remote storage 146-147 (“network storage devices”) are part of the network 120 (“connected to the network”) and that these components are able to store content (“capable of storing data”). APPLE-1004, [0002], [0049]

(“one or more local servers ... provide control **over the local network 121** and/or remote network 140, communicate with the client devices 124-130 and **storage or other memory 132 ... that store content**”), [0051] (“**remote network 140** further includes ... **storage devices or databases 144-145**”), [0052], [0069]; APPLE-1003, ¶¶250-252.



APPLE-1004, FIG. 1 (annotated)

*[1b-iii]*

Lamkin renders obvious [1b-iii]. APPLE-1003, ¶¶255-267. Lamkin describes that, in some situations, Lamkin’s system does not transfer certain contents having properties that increase risk of loss of the content during transfer – e.g., large file size or copyright protections. APPLE-1004, 1004, [0074], [0127], [0220]; APPLE-1003, ¶¶256-257.

Lamkin describes that, when a size of content to be stored exceeds a threshold, it is not transferred in some embodiments. APPLE-1004, [0074] (“determine whether the size or amount of new content exceeds a content threshold”), [0127], [0220], FIG. 4; APPLE-1003, ¶¶258-260. A POSITA would have understood that content having a large file size will take longer to transfer and is more likely to be only partially transferred if a network interruption causes failure of the transfer, especially in view of Lamkin’s description of transferring content in segments. APPLE-1003, ¶¶258-260 (citing APPLE-1004, [0082], [0160], [0105]). Accordingly, a POSITA would have understood that Lamkin renders obvious not transferring from the server to the local/remote storage, digital contents that have a large file size requiring transfer of a large number of segments, because they are more likely to be unrecoverable if a network failure occurs during the transfer. APPLE-1003, ¶¶258-260.

Additionally or alternatively, Lamkin describes that digital rights management (“DRM”) considerations alter whether content is transferred within the system, including preventing the transfer of some protected content.<sup>2</sup> APPLE-

---

<sup>2</sup> The claims do not require that the unrecoverability of digital contents be related to DRM status and none of the claims mention “DRM.” Nonetheless, we provide

1004, [0067] (“some content may be content protected and thus unable to be distributed ... without further authorization”), [0055], [0075]-[0076], [0114]-[0117], [0006], [0123], [0173], [0237], FIG. 8; APPLE-1003, ¶¶261-264. A POSITA would have understood from Lamkin’s description of DRM considerations, that in situations where a system intends to transfer protected content, the protected content is not transferred, and further, from Lamkin’s discussion of overriding the restriction on transfer with user authorization, that the content protections prevent unlimited copying. APPLE-1004, [0067], [0107] (“When ... the content is not to be further distributed, the process 720 terminates”); APPLE-1003, ¶¶262-264. Indeed, Lamkin’s description that “some protected files ... are not allowed to be stored locally for later playback” and are thus not transferred is consistent with Patent Owner’s infringement contentions mapping [1b-iii] to protected content that cannot be locally cached according to regional DRM policy. *Compare* APPLE-1004, [0055], *with* APPLE-1104, 5-8; APPLE-1103, 8-12.

Because Lamkin describes monitoring network failures and includes mechanisms for mitigating network failure effects on user experience, a POSITA

---

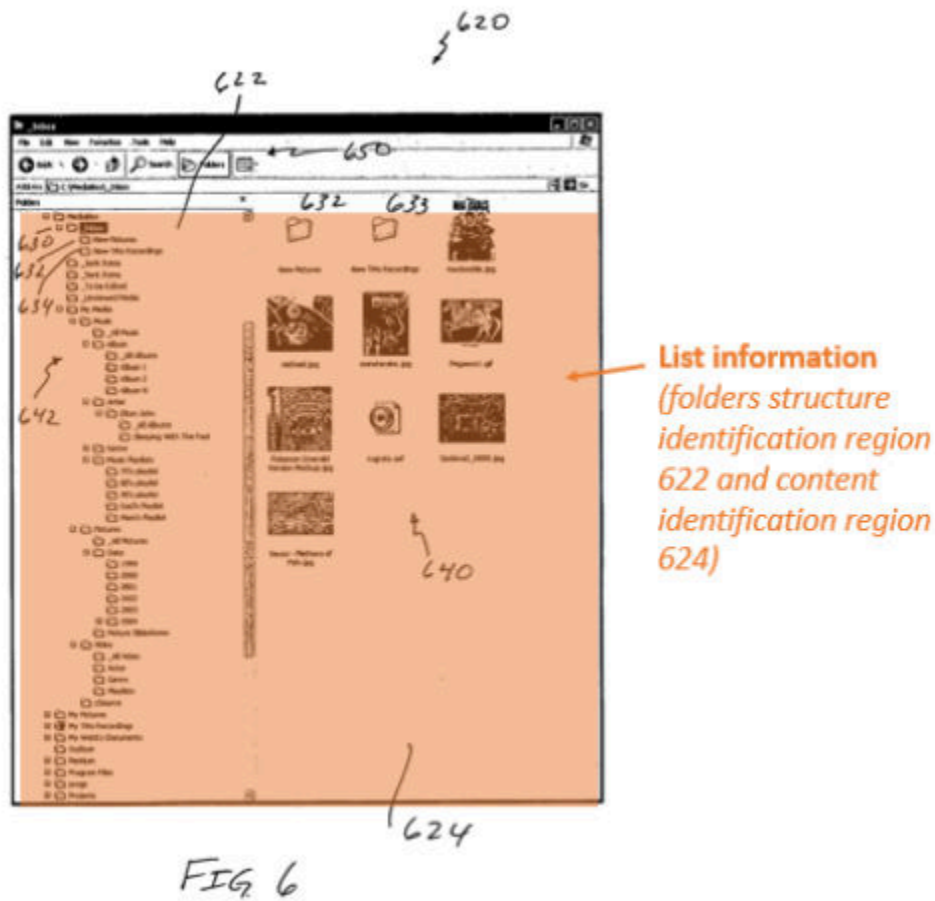
an alternative mapping based on Lamkin’s disclosure of not transferring content with protected status.

would have understood Lamkin’s discussion of not transmitting content having a large files size or DRM protection dictating a file cannot be copied as disclosing not transferring “from the internal storage device to the network storage device, the digital contents that cannot be recovered if a network failure occurs during the transferring of the digital contents from the internal storage device to the network storage device.” APPLE-1003, ¶¶256-266; APPLE-1004, [0240], [0082], [0105], [0254], [0290]. Lamkin’s description of failure monitoring would have indicated to a POSITA that Lamkin’s system is configured to detect and address potential network issues as they arise – including not transferring content that is at risk of being lost if there is a network failure during transfer. APPLE-1003, ¶265.

*[1c-i]*

Lamkin discloses [1c-i]. APPLE-1003, ¶¶268-275. Although the bounds of the term “list information transmission unit” are unclear, Lamkin discloses “content directory service” formed as a database and software and adapted to perform the same functions as the claimed “list information transmission unit.” *Compare* APPLE-1004, [0054] (“[a] content directory service (CDS) of a device can be used to identify and/or **display the available files and/or associated metadata**”), [0084], *with* APPLE-1001, 3:5-9, 3:31-40; *see* APPLE-1004, [0083], [0236], FIGS. 26, 28; APPLE-1003, ¶¶268-271 (explaining that a CDS includes software for displaying database contents in a user interface).

Lamkin describes that a CDS (“list information transmission unit”) identifies a list of available files (“list information”) to a user in response to a user request to access a list of available content on a user display (“respond to a list presentation request for the held digital contents”) and provides the list to the user device (“transmitting list information to the network player”). APPLE-1004, [0054], [0087] (“**a listing of one or more content that can potentially be distributed over the local network 121 and/or remote network 140**”), [0266] (“database can create the structure **upon the request of multiple clients**”), [0296] (“user has... the option to **browse the live server as necessary**”), [0088], [0068], [0077], [0262], FIGS. 5-6, 8, 27, 31; APPLE-1003, ¶¶272-273 (explaining that a user accessing the media inbox of FIG. 6 is a request to view the list of content).



**APPLE-1004, FIG. 6 (annotated)**

Lamkin's FIG. 6 shows a "media in-box" that "can identify content and in some implementations present the content according to an organized structure, similar to a file structure" ("list information [transmitted to] to the network player"). APPLE-1004, [0095], FIG. 6. As another example, Lamkin's FIG. 31 shows a user interface view of a content directory list ("transmitting list information to the network player") provided by the content directory service ("list information transmission unit"). APPLE-1004, [0265], [0263] ("network-enabled

devices query the server 122 by using the support provided by the CDS”). As Lamkin describes, a user request to present the list results in transmission and display of the list of held contents on the user interface. APPLE-1004, [0056], [0262]-[0264], APPLE-1003, ¶¶270-274.

*[1c-ii]*

Lamkin discloses [1c-ii]. APPLE-1003, ¶¶276-281. Lamkin describes that the CDS list (“list information”) includes “an aggregated content view that allows users to find content independent of the device” and can include “**[a]n aggregated database of the servers**” (“lists digital contents left in the internal storage device”) and other devices storing content (“digital contents transferred from the internal storage device to the network storage device and stored in the network storage device”). APPLE-1004, [0303], [0068]; APPLE-1003, ¶277. Lamkin describes that “listing 522 includes **a listing of one or more content that can potentially be distributed over the local network 121 and/or remote network 140.**” *Id.*, [0087], [0113], [0204]-[0205], [0266]-[0268]; APPLE-1003, ¶¶278-279.

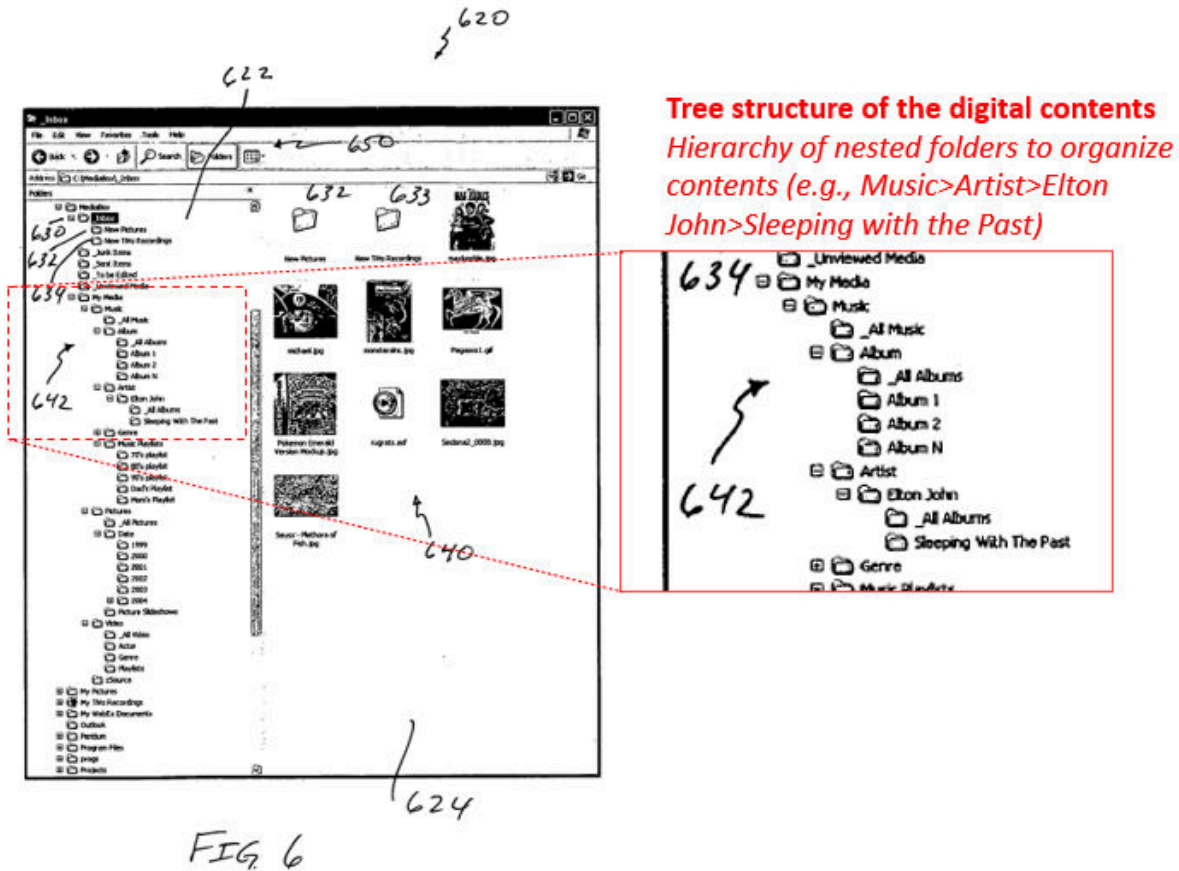
As content is added to the system, the CDS is updated to include the content and “**whether the new content is centralized and/or where the content is stored and/or centralized,**” such that the list of available content includes content whether stored in the server or in the local memory or remote storage. APPLE-1004, [0077], [0128] (“An aggregated database of the servers 122, local client

devices 124-130, local storage devices 132”). With this information, Lamkin’s server, and in particular the CDS (“list information transmission unit”), is able to provide a full list (“list information”) of all available contents to the user, including content stored in the server (“digital contents left in the internal storage device”) and content transferred from the server to the local or remote memories (“digital contents transferred from the internal storage device to the network storage device and stored in the network storage device”). *Id.*, [0077], [0087], APPLE-1003, ¶¶277-280.

***[1c-iii]***

Lamkin discloses [1c-iii]. APPLE-1003, ¶¶282-290. Lamkin describes that the CDS (“list information transmission unit”) provides a content directory list (“list information”) that “provides a hierarchy of the content available to client devices” structured as a hierarchical file system including folders and sub-folders (“maintains a tree structure of the digital contents”). APPLE-1004, [0264], [0232] (“Content is described in content items and containers that include ... available metadata and other information”), [0071]; APPLE-1003, ¶¶283-288. Lamkin describes multiple directory structures, but that it is common to “utilize[e] the date of the files **to form a tree structure** based on year, month, date.” APPLE-1004, [0264], [0095] (“folder structure identification region identifies **an in-box folder 630 and within that in-box folder sub-folders 632-633** can further be identified

[and the] sub-folders can further categorize or separate the content”), [0087]-  
[0088].



APPLE-1004, FIG. 6 (annotated, inset added)

A POSITA would have understood that a “tree structure” refers to a database that uses a hierarchical system to organize content using nested folders and subfolders to categorize like data, and further that Lamkin’s CDS with hierarchical directory as shown in FIG. 6, as a content directory having a tree structure (“maintains a tree structure of the digital contents”). APPLE-1009, [0084] (“a tree structure containing a plurality of containers arranged in hierarchical levels”),

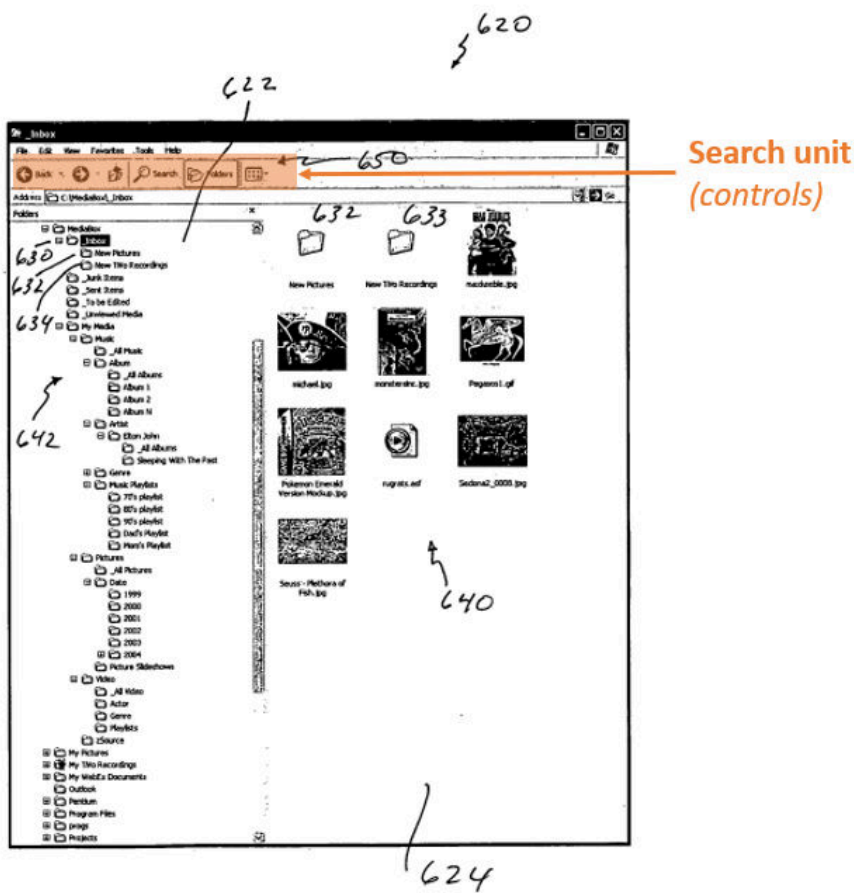
[0009], [0105]-[0109], FIGS. 4A-C, 6-7; APPLE-1004, [0264]-[0272] . APPLE-1003, ¶¶285-287.

As content is added to the system, “a log file, database listing, CDS or other tracking is updated identifying the new content, whether the new content is centralized **and/or where the content is stored and/or centralized,**” such that the hierarchical directory of available content to be displayed to the user is updated to include contents regardless of where they are stored in the internal memory of the server or in remote storage and local memories (“maintains a tree structure of digital contents in the internal storage device before transferring the digital contents to the network storage device”). APPLE-1004, [0077], [0124] (“an aggregated content view that allows users to find content independent of the device”); APPLE-1003, ¶¶285-288.

*[1d]*

Lamkin discloses [1d]. APPLE-1003, ¶¶291-299. Although the bounds of the term “search unit” are unclear, Lamkin discloses that the server provides an interface for a user to search available content including using “controls 650” adapted to perform the same functions as the claimed “search unit,” for example, by using a universal locator to identify a location of requested content. *Compare* APPLE-1004, [0097] (“controls 650 can allow the user to perform searches for content, navigation through other folders and/or storage systems”), [0131], *with*

APPLE-1001, 3:5-9, 6:41-48; *see* APPLE-1004, [0131], FIGS. 6, 28; APPLE-1015, [0201] (describing a content search engine which “searches various levels [of storage] for content”); APPLE-1003, ¶¶292-295 (explaining that controls are typically implemented as software algorithms for searching within a server database).



**APPLE-1004, FIG. 6 (annotated)**

Lamkin describes that controls 650 (“search unit”) allow the user to perform searches to browse for and select desired content, including content at the live

server. APPLE-1004, [0124] (“servers 122 of the local network allow users to locate content through displays of content and/or file structures, searching, and other such access”), [0097], [0296]; APPLE-1003, ¶¶295-296. To the extent that Lamkin does not explicitly detail that the controls 650 enable a search within and on the server, a POSITA would have appreciated that such search methodology was well-known and conventional and would have further understood that Lamkin’s server is capable of searching for a location of requested content based on Lamkin’s description of providing requested content to a user. APPLE-1003, ¶¶295-297; APPLE-1004, [0296] (“user has... the option to **browse the live server as necessary**”).

Lamkin’s CDS displays available content across multiple storages/devices to the user regardless of the content location, and can further locate requested content to transmit to the user. APPLE-1004, [0124], [0303]; *infra* §V.A.2.a.[1e]. When searching for content in the aggregated view, a user can select desired content (“data transmission request for the held digital contents from the network player”) without knowing where the content is stored. *Id.*, [0124] (“[the] user does not need to know which device contains the content, but simply what content they are looking for”); APPLE-1003, ¶¶295-298.

After a user selects content, the server controls (“search unit”) uses a locator to identify a storage device containing the content (“searching for a location where

the held digital contents are currently stored”) requested by the user device.

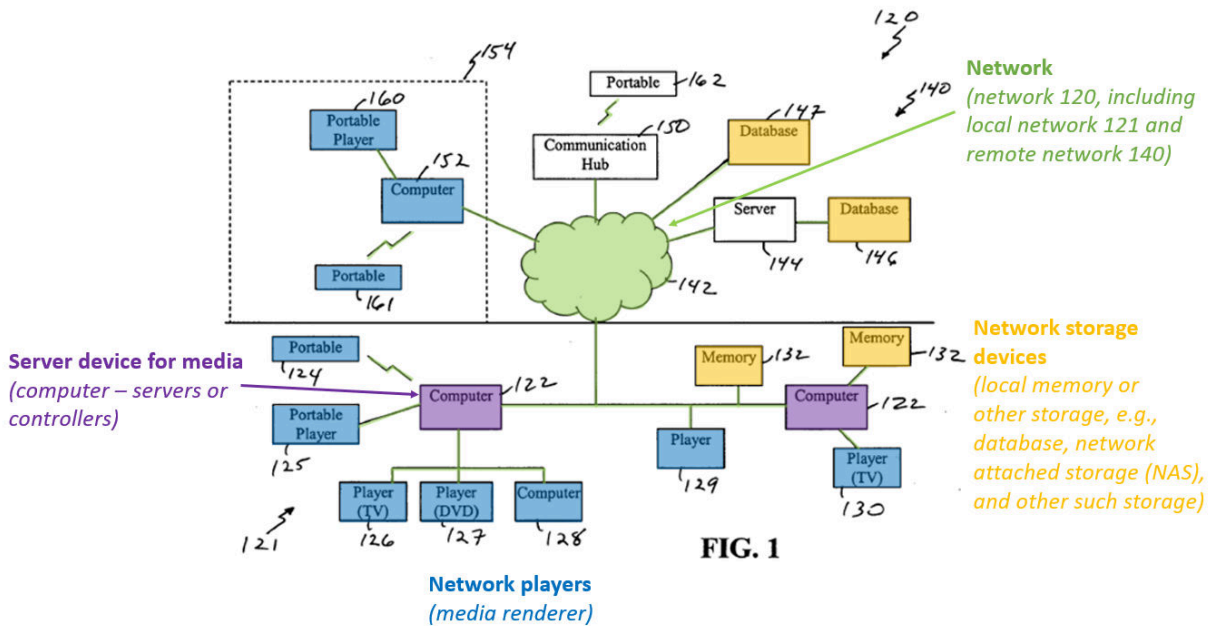
APPLE-1004, [0131] (“**some metadata can include a universal locator [that can be utilized in the aggregate view to, in part, access and/or locate content, ... [so that when] a user attempts to access content through the aggregate view, the universal locator can be utilized to direct the user to and/or retrieve the content**”), [0131]; APPLE-1003, ¶¶293-298 (citing APPLE-1015, [0201] (describing a content search engine which “**searches various levels for content**”). In this way, after a user has selected content, “desired content is searched for and located” by the controls (“search unit”). APPLE-1004, [0236].

*[1e]*

Lamkin discloses [1e]. APPLE-1003, ¶¶300-307. Although the bounds of the term “digital contents data transmission processing unit” are unclear, Lamkin discloses an “AV transport service” instantiated as an AV transport algorithm that is adapted to perform the same functions as the claimed unit. *Compare* APPLE-1004, [0236] (“control algorithm 2820 for an AV architecture”), *with* APPLE-1001, 3:5-9, 7:28-55; *see* APPLE-1004, [0235]-[0236], FIGS. 26, 28; APPLE-1003, ¶¶301-304 (explaining that AV transport service performs its functions using a control algorithm).

Lamkin describes that an AV transport service of the content management service (“digital contents data transmission processing unit”) controls transport of

content streams to the client devices (“adapted to allow the corresponding data in held digital contents to be stream-delivered from the network storage device to the network player”). APPLE-1004, [0220] (“content management service ... distributes content over the network”), [0235] (“AV transport service 2734 and 2744 enable control over the transport of audio, video and/or other content streams”), [0236] (“AV transport service 2734 initiates and controls the transfer of the located content”), [0083] (“Upon receiving a request for the content ... the content is forwarded to the requester”), [0078], [0141], [0213], [0286]; APPLE-1003, ¶¶302, 305-306. A POSITA would have understood that, if the search described in [1d] for a storage location of desired content shows the content to be located in the local memory 132 or remote database 146-147 (“if the result of search shows the network storage device”), Lamkin’s AV transport provides the content to the client device, based on Lamkin’s description of the aggregated view of contents accessible to the user. APPLE-1004, [0303], [0068], [0087], [0113], [0204]-[0205], [0266]-[0268]; APPLE-1003, ¶¶302-305 (explaining that content located in any accessible storage of the system is provided to the client device by the AV transport service); *supra* §V.A.2.a.[1d].



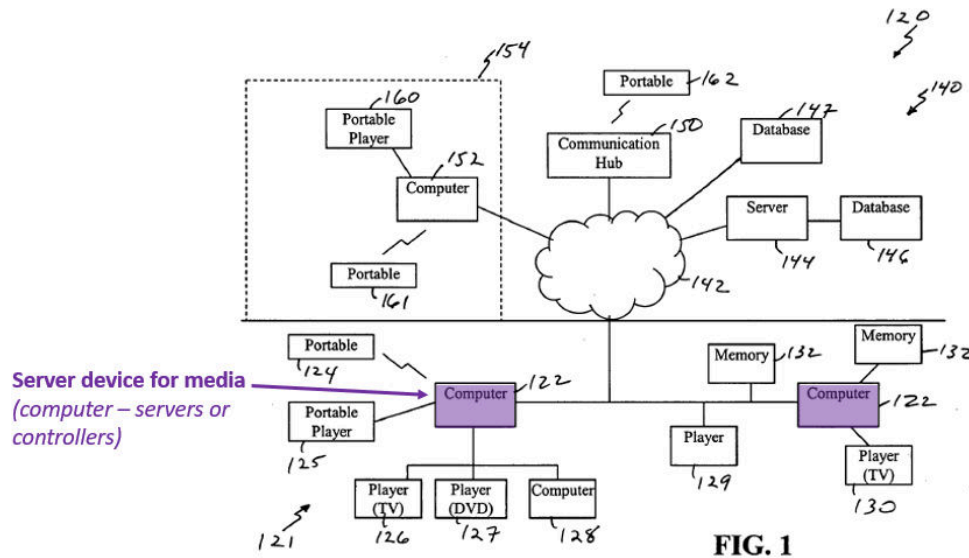
**APPLE-1004, FIG. 1 (annotated)**

Further, the requested content is delivered to the user device by streaming (“allow the corresponding data in held digital contents to be stream-delivered from the network storage device to the network player”). APPLE-1004, [0160] (“real time streaming protocol (RTSP) streaming”), [0128], [0220], [0231], [0241]; APPLE-1003, ¶305.

**[1f]**

Lamkin discloses [1f]. APPLE-1003, ¶¶308-313. Lamkin describes that the server can “include **computers, DVD players, CD players,** and other such relevant devices.” APPLE-1004, [0241]; APPLE-1003, ¶309. A POSITA would have understood that such devices are “media players” because content (such as music) can be “played” by a user directly on these devices. APPLE-1003, ¶¶310-

311; compare APPLE-1004, [0241], with APPLE-1001, 1:7-8 (“server device for media such as an HDD portable player”), 4:32-37 (“listening to the held music pieces of the HDD portable player 10 through the headphones 12 is referred to as ‘self-playback’”).



**APPLE-1004, FIG. 1 (annotated)**

**(b) Claim 2**

Lamkin discloses [2]. APPLE-1003, ¶¶324-329. Lamkin describes that the AV transport (“said digital contents data transmission processing unit”) transfers content from local memories or remote storage to the server (“causes the network storage device to transmit the corresponding data to the server device for media”), and further transfers the content to a client device (“and then transmits the corresponding data received from the network storage device from the server

device for media to the network player”). APPLE-1004, [0049] (“[t]he one or more **local servers, computers or other control devices 122 ... communicate with the client devices 124-130 and storage or other memory 132**”), [0050] (“one or more servers or controllers 122 ... **provide and/or coordinate access to content [such that the] client devices receive and/or access some content through the servers 122.**”), [0241] (“media server stores, **retrieves and provides** media on request”), [0052], [0078]-[0079], [0141], FIG. 34; APPLE-1003, ¶¶325-326. Lamkin accordingly describes that, when requested content is located in remote storage, the content is first transferred to the server before being distributed to the client device. APPLE-1004, [0275] (“request of this file from a user and/or client device is typically received causing the server to first download the file ... then transfer this file to the client device”); APPLE-1003, ¶¶236-238.

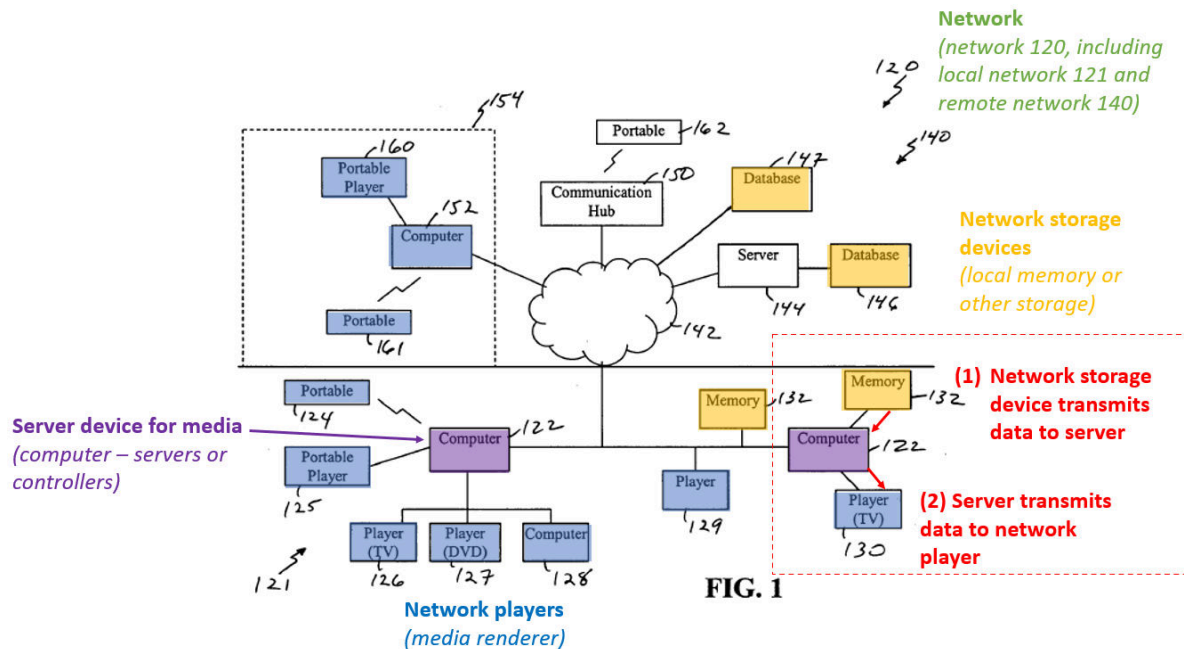


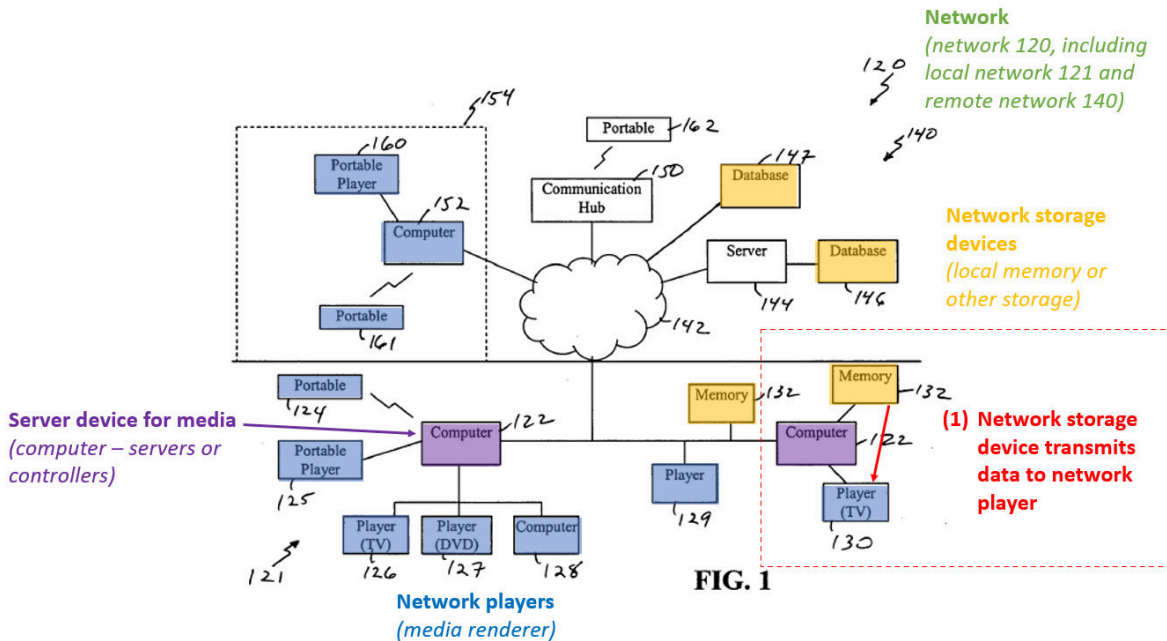
FIG. 1

APPLE-1004, FIG. 1 (annotated)

(c) Claim 3

Lamkin discloses [3]. APPLE-1003, ¶¶330-337. As described in [1e] and [5], Lamkin describes that the location of the requested data (“information for identifying the network storage device”) can be made known to the user device (“transmits the corresponding data and information for identifying the network storage device to the network player”), and, in some situations, the local memory or remote storage can provide content directly to a client device (“causes the network storage device to directly transmit the corresponding data to the network player”). APPLE-1004, [0286] (“playback device that generally pulls content from a server 122 and/or storage 132”), [0205] (“content user interface can list or identify content available through the network, and in some embodiments, **further**

identify the device on which content is stored”), [0113], [0204] (“displays ... available content accessible over the local and/or extended networks”), [0056]; APPLE-1003, ¶¶331-332. Accordingly, Lamkin describes that requested content can be provided to a user either from the internal storage of the server (“server device”) or from the storage 132 (“network storage device”). Compare APPLE-1004, [0286] (“a playback device that generally pulls content from ... storage 132.”), with APPLE-1001, 7:50-65; APPLE-1003, ¶333.



APPLE-1004, FIG. 1 (annotated)

(d) Claim 4

Lamkin discloses [4]. APPLE-1003, ¶¶338-351. Although the bounds of the term “return control unit” are unclear, Lamkin discloses that the AV transport is adapted to perform the same functions as the claimed “return control unit.”

*Compare* APPLE-1004, [0236] (“control algorithm 2820 for an AV architecture”), *with* APPLE-1001, 3:5-9, 7:66-8:4; *see* APPLE-1004, [0049]-[0052]; APPLE-1003, ¶¶339-344 (explaining that the AV architecture control algorithm transfers content from remote storage to the server). Alternatively, or additionally, Lamkin discloses that the content management service transfers content between storage devices based on predicted use, also performing the same functions as the claimed “return control unit.” *Compare* APPLE-1004, [0064], [0046], *with* APPLE-1001, 3:5-9, 7:66-8:4; APPLE-1003, ¶¶348-349.

As described above in [1e] and [2], Lamkin describes that requested content is transferred from the local memory or remote storage to the server (“cause the digital contents... to be returned from the network storage device to the internal storage device”) by the AV transport (“return control unit”) in response to a user request (“digital contents corresponding to a predetermined condition”), after originally being archived to the local memory or remote storage from the server (“digital contents corresponding to a predetermined condition among the digital contents which have been transferred to the network storage device”). *Supra* §§V.A.2.a.[1e], [2]; APPLE-1004, [0049]-[0052], [0078]-[0079], [0083], [0128], [0141], [0220], [0231]-[0236], [0241]; APPLE-1003, ¶¶340-347. Being requested by a user is a predetermined condition of the digital contents. *See e.g.*, APPLE-1001, 8:5-10 (describing that predetermined conditions can include “the digital

contents which have recently been subjected to the self-playback” or “network playback”); APPLE-1003, ¶347.

Additionally or alternatively, Lamkin describes that content predicted to be requested by a user is transferred within the network so as to anticipate user needs. APPLE-1004, [0079] (“utilize the **local server storage to maintain the most used and/or most current content on the network**”), [0064] (“**Content can be distributed through the network 120 [to accommodate] anticipated or predicted use of the content**”), [0133], [0141]-[0144], [0146], [0238]; APPLE-1003, ¶¶348-349. Accordingly, content predicted to be used (“digital contents corresponding to a predetermined condition”) is moved from storage in local memory or remote storage to the server (“among the digital contents which have been transferred to the network storage device to be returned from the network storage device to the internal storage device”) based on the predetermined condition of being predicted to be accessed by the user. APPLE-1003, ¶¶348-349; APPLE-1004, [0078] (“maintain some content at a local server readily available to the server for distribution to client devices, some content at a local storage 132 to be locally accessed and retrieved, and other content remotely stored”), [0080], [0103] (“server 122 initiates the distribution of content based on a predicted distribution scheme”), [0146].

**(e) Claim 5**

Lamkin discloses [5]. APPLE-1003, ¶¶352-357. Lamkin describes that a CDS (“list information transmission unit”) provides a list (“list information”) to the user at the client device (“to be transmitted to the network player”) that includes an indicated storage location of content (“include information for identifying whether each digital content is currently stored in the internal storage device or the network storage device in the display list of the network player”). APPLE-1004, [0205] (“content user interface can ... **further identify the device on which content is stored**”), [0077] (“[a] CDS or other tracking **is updated identifying the new content, [and] where the content is stored and/or centralized**”), [0085] (“collections may consist of the **metadata and/or pointers to the files on another device** across the local network 121”), [0199], [0087], [0113], [0204]; APPLE-1003, ¶¶353-355.

**(f) Claim 6**

***[6pre]-[6b-ii]***

*Supra* §§V.A.2.a.[1pre]-[1b-ii]. APPLE-1003, ¶314.

***[6b-iii]***

Lamkin renders obvious [6b-iii]. APPLE-1003, ¶¶315-323. Lamkin describes a system that accounts for possible network failures during transfer of contents, including by not transferring certain protected contents. *Supra*

§V.A.2.a.[1b-iii]; APPLE-1003, ¶¶316-318.

Lamkin also describes situations in which a user is presented with options to provide instructions to the system in response to some event, such as a potential network failure. APPLE-1004, [0253] (“warnings [are] presented to define what the system is waiting for ... allowing the user to make an informed decision to continue to wait or to cancel the current operation”), [0254] (“provide a visual indication when a client device has been lost [and in some cases a] network device status/control panel can be presented”), [0292] (“warnings are present[ed] ... to allow the user to continue to wait or to cancel the current operation”), [0293], [0316] (“agent interface... informs the user when additional information is needed”); APPLE-1003, ¶318.

Lamkin further describes that, in some situations, protected content that could not otherwise be transferred requires user authorization to transfer. APPLE-1004, [0067] (“some content may be content protected and thus **unable to be distributed or properly distributed without further authorization**”), [0052], [0055], [0092]-[0093], [0173], [0191]-[0196]; APPLE-1003, ¶¶320-321. A POSITA would have appreciated that such content is at risk of being unrecoverable in the case of a network failure, at least because the protected content could not be played by a user device without also receiving additional authorization. APPLE-1003, ¶321. A POSITA would have understood, based on Lamkin’s disclosure,

that requiring authorization prior to transferring content that could not be successfully transferred or accessed upon transfer without authorization provides the claimed “digital contents ... transferred after obtaining permission from a user” because, were the content to be transferred without authorization, it would not be readable by a client device (in the event of network failure or otherwise) and the protected content is thus an example of “digital contents that cannot be recovered if a network failure occurs during the transferring of the digital contents from the internal storage device to the network storage device.” APPLE-1003, ¶321 (citing APPLE-1004, [0318] (“a user obtains the necessary rights to that content (for personal use and some specific number of copies/backups)”).

**[6c-i]-[6f]**

*Supra* §§V.A.2.a.[1c-i]-[1f]. APPLE-1003, ¶314.

**(g) Claim 7**

**[7pre]-[7f]**

As described above, Lamkin provides a server device for media and provides various components that operate to perform various functions of the server device, as well as a method for controlling the server device. *Supra* §§V.A.2.a.[1pre]-[1f]; APPLE-1003, ¶¶214-312; APPLE-1004, [0005] (“methods for distributing content.”), [0006]-[0009], [0054]-[0057], [0085]-[0086], FIGS. 4, 7-8, 10.

**(h) Claims 8-11**

*Supra* §§V.A.2.b.[2]-V.A.2.e.[5]. APPLE-1003, ¶¶324-357.

**(i) Claim 12**

***[12pre]-[12a]***

*Supra* §§V.A.2.a.[1pre]-[1a-ii]. APPLE-1003, ¶¶214-237.

***[12b]***

*Supra* §§V.A.2.a.[1b-i]-[1b-ii], V.A.2.f.[6b-iii]. APPLE-1003, ¶¶238-254,  
315-323.

***[12c]-[12f]***

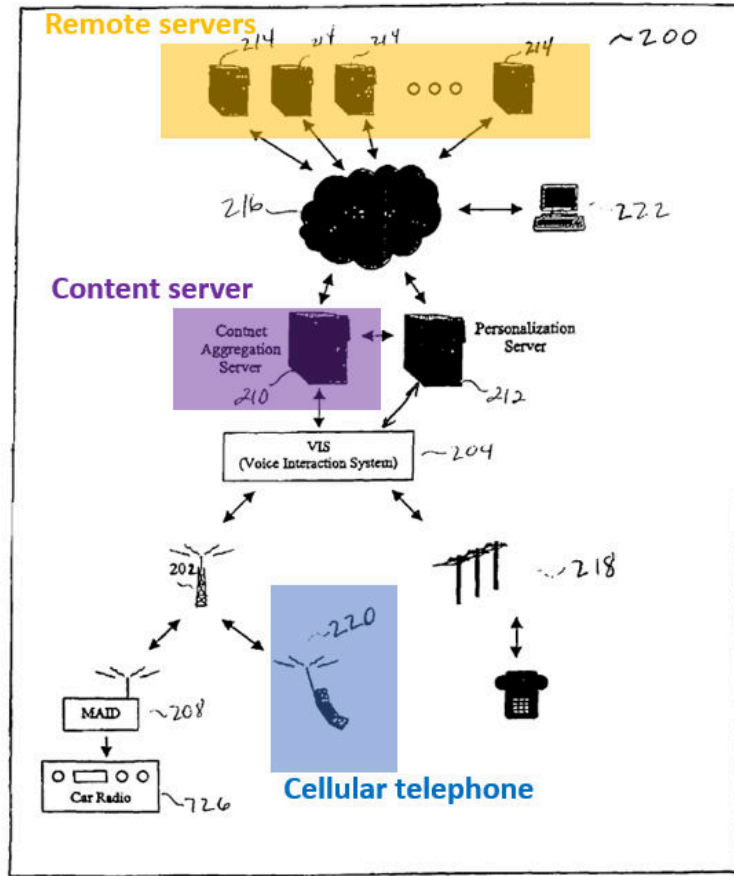
*Supra* §§V.A.2.a.[1c-i]-[1f]. APPLE-1003, ¶¶268-313.

**B. Ground 1B: Lamkin-Fiechter**

**1. Fiechter (APPLE-1006)**

Fiechter describes a “network browser system” that includes a user device (e.g., cellular telephone system 220) that receives user commands and transmits the commands to content server 210 which executes the command, including providing requested information from servers 210, 212, and 214. *Id.*, 5:46-57, 5:61-64, 7:52-66, FIGS. 2, 9.

FIGURE 2



APPLE-1006, FIG. 2

Fiechter describes that “mobile audio device 904 [e.g., user device 220] includes capability to detect and compensate for data transmission errors in wireless communication network 906,” including detecting the device is in an area “where there is a high incidence of data loss due to propagation errors.” *Id.*, 17:50-59.

For example, “[w]hen mobile audio device 904 is likely to experience a data loss rate that is higher than a pre-selected value, one of several options may be

taken including informing the user of the likelihood of errors or gaps in the information, asking the user if they would prefer to wait for the information until transmission of the data will be more reliable, or buffering a greater than normal amount of information to be able to continue uninterrupted output until the connection is re-established.” *Id.*, 17:62-18:3, 12:41-45.

## 2. Lamkin-Fiechter Combination

As described above, Lamkin renders obvious [1b-iii] and [6b-iii]. *Supra* §§V.A.2.a[1b-iii], V.A.2.f.[6b-iii], V.A.2.g.[7b], V.A.2.i.[12b]; APPLE-1003, ¶¶255-267, 315-323. To the extent one argues that Lamkin does not provide sufficient details related to these limitations, Lamkin-Fiechter renders obvious [1b-iii] and [6b-iii].

In Lamkin-Fiechter, a system, per Lamkin, is implemented to address issues arising from potential network failures interrupting transfer of contents and rendering the contents unrecoverable and inaccessible by a user by not transferring content when network failure is likely and by providing a user with an option to proceed with the transfer, per Fiechter. APPLE-1004, [0067], [0074]-[0076], [0082], [0105], [0182], [0245], [0253]-[0254], [0290]-[0293]; APPLE-1006, 17:62-18:3; APPLE-1003, ¶¶358-371.

A POSITA would have been motivated to pursue the combination for multiple reasons.

First, Lamkin's discussion of system monitoring of connectivity issues and impacts on transfer of content would have motivated a POSITA to look to references like Fiechter that also describe multimedia communication of audio and video and provide additional details for addressing increased likelihood of transfer failure. APPLE-1004, [0082], [0105], [0245], [0254], [0290]; APPLE-1006, 17:50-59; APPLE-1003, ¶¶373-374. Both Fiechter and Lamkin are concerned with systems where a device attempts to transfer media data over a network where communication is not always reliable, which a POSITA would have understood to be true of most networks. APPLE-1003, ¶¶360-362. Fiechter offers additional details for how systems can respond when transfer of data is expected to be unreliable; a POSITA would have been motivated to implement a system, per Lamkin, with these additional details from Fiechter in such situations. APPLE-1003, ¶¶362.

Second, a POSITA would have appreciated that Fiechter's solutions of halting the content transfer and providing a user with options for proceeding are similar to the mechanisms Lamkin describes: not transferring data (e.g., when the data has too large of a file-size, or when data is protected) and transferring data with authorization (e.g., when protected data may be transferred with further authorization). APPLE-1004, [0055], [0067], [0074]-[0076], [0107], [0114]-[0117], [0123], [0173], [0237], FIGS. 4, 8; APPLE-1006, 17:50-18:3; APPLE-

1003, ¶¶375-376. A POSITA would have been motivated to implement additional user options of stopping the transfer and waiting for improved connectivity or proceeding with the transfer, per Fiechter, in view of Lamkin's description of user authorization of a transfer.

Third, a POSITA would have understood that presenting a user with options of waiting or proceeding with the transfer—when a network is likely to be unreliable—optimizes system performance. APPLE-1006, 17:62-18:3; APPLE-1003, ¶377. For example, presenting a user with options for proceeding allows a user to make informed decisions about the importance of particular transfers; to decide that they would rather cancel a scheduled transfer or archive, for example, to save battery life or bandwidth of a device or to prioritize other actions; or to reschedule such a transfer at a later, more desirable time, possibly when the network is more reliable. APPLE-1003, ¶377.

Fourth, a POSITA would have understood that providing mechanisms for addressing elevated network failure and data loss risks improve the user experience of interacting with the system, per Fiechter, whether in a home environment or on a mobile device. APPLE-1004, [0003], [0130], [0151] [0312], [0323], FIG. 1, 34; APPLE-1006, 2:9-14, 3:10-14, FIGS. 2, 8-9; APPLE-1003, ¶378.

Fifth, a POSITA would have understood that the combination of known elements according to known methods would have yielded predictable results, as

each element performs a similar function combined as it does separately. APPLE-1003, ¶¶379-380. Lamkin's system includes mechanisms for addressing network issues by not transferring content or presenting user options to proceed with transferring. *Supra* §V.A.2.a[1b-iii], V.A.2.f.[6b-iii]; APPLE-1003, ¶380. Fiechter's additional details for halting transfer of content and providing options to a user do not alter Lamkin's system's performance. APPLE-1003, ¶380.

Sixth, combining Lamkin-Fiechter would have been well within a POSITA's skill because mechanisms for monitoring network failures and methods for preparing for such failures by preventing a transfer or providing options to a user were well-known by the Critical Date, as Fiechter teaches. APPLE-1003, ¶381; APPLE-1006, 17:62-18:3. Accordingly, a POSITA would have had a reasonable expectation of success in doing so for the reasons explained above, and because methods for responding to potential network failure during data transfer were well known to a POSITA by the Critical Date. APPLE-1003, ¶¶372-382.

### **3. Analysis**

#### **(a) Claim 1**

##### ***[1pre]-[1b-ii]***

*Supra* §§V.A.2.a.[1pre]-[1b-ii]. APPLE-1003, ¶¶215-254.

##### ***[1b-iii]***

Lamkin-Fiechter renders obvious [1b-iii]. APPLE-1003, ¶¶364-367. As

described above, Lamkin describes a system that accounts for network connectivity issues, as well as content transfer methods in which content is not archived from the server to the remote/local storage if particular conditions are met. *Supra* §V.A.2.a.[1b-iii]. In combination with Fiechter, content is not transferred from the server to the remote/local storage when the system detects an increased likelihood of network failure that would result in transfer failure (“said transfer control unit does not transfer, from the internal storage device to the network storage device, the digital contents that cannot be recovered if a network failure occurs during the transferring of the digital contents from the internal storage device to the network storage device”). *Supra* §V.B.2; APPLE-1003, ¶¶363-365. For example, where network characteristics increase likelihood of data loss during transfer, Lamkin-Fiechter does not transfer content from the server to the local/remote storage when the content has a large file size and/or where data protections on the content make transfer impossible or problematic. APPLE-1004, [0067], [0074]-[0076], [0082], [0105], [0182], [0245], [0253]-[0254], [0290]-[0293]; APPLE-1006, 17:62-18:3; APPLE-1003, ¶¶365-366.

***[1c-i]-[1f]***

*Supra* §§V.A.2.a.[1c-i]-[1f]. APPLE-1003, ¶¶268-313.

**(b) Claims 2-5 and 8-11**

*Supra* §§V.A.2.b.[2]-V.A.2.e.[5], §§V.A.2.h.[8]-[11]. APPLE-1003, ¶¶358-

359.

(c) **Claim 6**

**[6pre]-[6b-ii]**

*Supra* §§V.A.2.a.[1pre]-[1b-ii]. APPLE-1003, ¶¶215-254.

**[6b-iii]**

Lamkin-Fiechter renders obvious [6b-iii]. APPLE-1003, ¶¶368-371. As described above, in Lamkin-Fiechter, content is transferred from the server to the remote/local storage only after obtaining permission from a user when the system detects an increased likelihood of network failure resulting in a failure of a transfer (“digital contents that cannot be recovered if a network failure occurs during the transferring of the digital contents from the internal storage device to the network storage device is transferred after obtaining permission from a user”). *Supra* §V.B.2; APPLE-1003, ¶¶363, 369. For example, where network characteristics make data loss during transfer more likely, Lamkin-Fiechter presents network conditions and presents an option to the user to proceed with transferring the contents. APPLE-1004, [0067], [0253]-[0254] [0292]-[0293]; APPLE-1006, 17:62-18:3 (“**asking the user** if they would prefer to wait for the information until transmission of the data will be more reliable”); APPLE-1003, ¶¶369-370.

**[6c-i]-[6f]**

*Supra* §§V.A.2.a.[1c-i]-[1f]. APPLE-1003, ¶¶268-313.

**(d) Claim 7**

***[7pre]-[7a]***

*Supra* §§V.A.2.a.[1pre]-[1a-ii]. APPLE-1003, ¶¶215-237.

***[7b]***

*Supra* §§V.A.2.a.[1b-i]-[1b-ii] and §V.B.3.a.[1b-iii]. APPLE-1003, ¶¶238-254, 364-367.

***[7c]-[7f]***

*Supra* §§V.A.2.a.[1c-i]-[1f]. APPLE-1003, ¶¶268-313.

**(e) Claim 12**

***[12pre]-[12a]***

*Supra* §§V.A.2.a.[1pre]-[1a-ii]. APPLE-1003, ¶¶215-237.

***[12b]***

*Supra* §§V.A.2.a.[1b-i]-[1b-ii] and §V.B.3.c.[6b-iii]. APPLE-1003, ¶¶238-254, 368-371.

***[12c]-[12f]***

*Supra* §§V.A.2.a.[1c-i]-[1f]. APPLE-1003, ¶¶268-313.

**C. Ground 1C: Lamkin-Ito**

**1. Ito (APPLE-1012)**

Ito describes a backup system includes a backup device and a recording and playback device which includes storage means and “content transmitting means for ... transmitting the read out content o[f the storage means] to the backup device.”

APPLE-1012, [0007], [0001]. Ito describes that, in some cases, content is lost “due to mishandling or failure” including “a failure of the recording and playback device or the network to which the recording and playback device is connected.” *Id.*, [0008].

Ito explains that, in some cases, copy control information related to digital content “indicates that copying is allowed only once (Copy Once).” *Id.*, [0002]. Ito describes that, for such copy-protected content, if the information associated with the content “indicates that backup is prohibited, [then] the transmission is terminated.” *Id.*, [0252]; *see id.* (“If the backup process indicates permission to generate backup information corresponding to the encrypted content to be backed up, the encrypted content is sent to the backup device”).

## **2. Lamkin-Ito Combination**

As described above, Lamkin renders obvious [1b-iii]. *Supra* §§V.A.2.a.[1b-iii] and V.A.2.g.[7b]; APPLE-1003, ¶¶255-267. To the extent it is argued that Lamkin does not provide sufficient details related to these limitations, Lamkin-Ito renders obvious [1b-iii] and [7b].

In Lamkin-Ito, a system, per Lamkin, is implemented to anticipate network failure issues during content transfer and to not transfer content to the remote/local storage, per Ito. APPLE-1004, [0067], [0074]-[0076], [0082], [0105], [0182], [0245], [0253]-[0254], [0290]-[0293]; APPLE-1012, [0001]-[0008], [0252];

APPLE-1003, ¶¶383-387.

Like Lamkin, Ito describes a system for backing up digital content in a network, including copyright-restricted content. *Compare* APPLE-1012, [0001] (“generating a backup of digital content while taking copyright protection of digital content into consideration”), *with* APPLE-1004, [0050] (“content can be received from the client devices and stored in the servers 122 and/or storage 132”), [0107] (“in determining whether the content can be distributed, the network may determine whether the content is protected”), [0237], Fig. 4; APPLE-1003, ¶¶385-387. Lamkin and Ito are both concerned about network reliability during transfer, and a POSITA would have looked to the additional details per Ito about terminating a transfer to prevent content loss due to failure. APPLE-1012, [0001]-[0008], [0252]; APPLE-1004, [0047]-[0052]; APPLE-1003, ¶¶386-391 (explaining that Ito’s determination of whether to proceed with a backup anticipates network failure issues specific to protected content).

A POSITA would have been motivated to pursue the combination for multiple reasons.

First, Lamkin’s discussion of network issues during content archiving attempts would have motivated a POSITA to look to references like Ito that provide further details for anticipating network failure issues for particular content and not transmitting that content. APPLE-1004, [0082], [0105], [0245], [0254],

[0290]; APPLE-1012, [0001]-[0008], [0252]; APPLE-1003, ¶¶393-394.

Second, a POSITA would have appreciated that Ito's described termination of content transfer where content would be lost in the case of a network failure is similar to mechanisms Lamkin describes including not transferring data with too large a file-size, or when data is protected. APPLE-1004, [0055], [0067], [0074]-[0076], [0107], [0114]-[0117], [0123], [0173], [0237], FIGS. 4, 8; APPLE-1012, [0001]-[0008], [0252]; APPLE-1003, ¶¶395-397. A POSITA would have been motivated to implement a policy of not transferring such protected (or other) content likely to be lost in the case of network failure, per Ito, to prevent content loss. APPLE-1003, ¶¶396-397.

Third, a POSITA would have understood that anticipating transfer failures resulting from network issues improves user experience with the system, per Ito. APPLE-1004, [0078], [0142], [0326], [0003]; APPLE-1012, [0252]-[0253]; APPLE-1003, ¶398.

Fourth, a POSITA would have understood that the combination of known elements according to known methods would have yielded predictable results, as each element performs a similar function combined as it does separately. APPLE-1003, ¶399. Lamkin's system already includes mechanisms for addressing network issues by not transmitting the content. *Supra* §V.A.2.a.[1b-iii]; APPLE-1003, ¶¶255-267. Ito's additional details about anticipating network failure issues

for certain content types and terminating backup of such content does not alter Lamkin's system's performance. APPLE-1003, ¶399.

Fifth, combining Lamkin-Ito would have been well within a POSITA's skill because mechanisms for anticipating content loss due to network failure and preventing transfer were well-known by the Critical Date, as Ito teaches. APPLE-1003, ¶400; APPLE-1012, [0001]-[0008], [0252]-[0253]. Accordingly, a POSITA would have had a reasonable expectation of success in making the combination for the reasons explained above, and because methods for responding to increased likelihood of network failures during data transfer were well known to a POSITA by the Critical Date. APPLE-1003, ¶¶392-401.

### **3. Analysis**

#### **(a) Claim 1**

##### ***[1pre]-[1b-ii]***

*Supra* §§V.A.2.a.[1pre]-[1b-ii]. APPLE-1003, ¶¶215-254.

##### ***[1b-iii]***

Lamkin-Ito renders obvious [1b-iii]. APPLE-1003, ¶¶385-391. As described above, in Lamkin-Ito, where content is protected and cannot be backed up to guard against network failure (“digital contents that cannot be recovered if a network failure occurs during the transferring of the digital contents from the internal storage device to the network storage device”) the content transfer to the

backup is terminated (“said transfer control unit does not transfer, from the internal storage device to the network storage device”). *Supra* §V.C.2; APPLE-1003, ¶¶389-390. For example, in Lamkin-Ito, transfer of protected content that would be lost in the case of a network failure during transfer is terminated. APPLE-1004, [0067], [0074]-[0076], [0082], [0105], [0182], [0245], [0253]-[0254], [0290]-[0293]; APPLE-1012, [0001]-[0008], [0252]-[0253]; APPLE-1003, ¶¶389-390.

**[1c]-[1f]**

*Supra* §§V.A.2.a.[1c-i]-[1f]. APPLE-1003, ¶¶268-313.

**(b) Claim 7**

**[7pre]-[7a]**

*Supra* §§V.A.2.a.[1pre]-[1a]. APPLE-1003, ¶¶215-237.

**[7b]**

*Supra* §§V.A.2.a.[1b-i]-[1b-ii] and §V.C.3.a.[1b-iii]. APPLE-1003, ¶¶238-254, 388-391.

**[7c]-[7f]**

*Supra* §§V.A.2.a.[1c-i]-[1f]. APPLE-1003, ¶¶268-313.

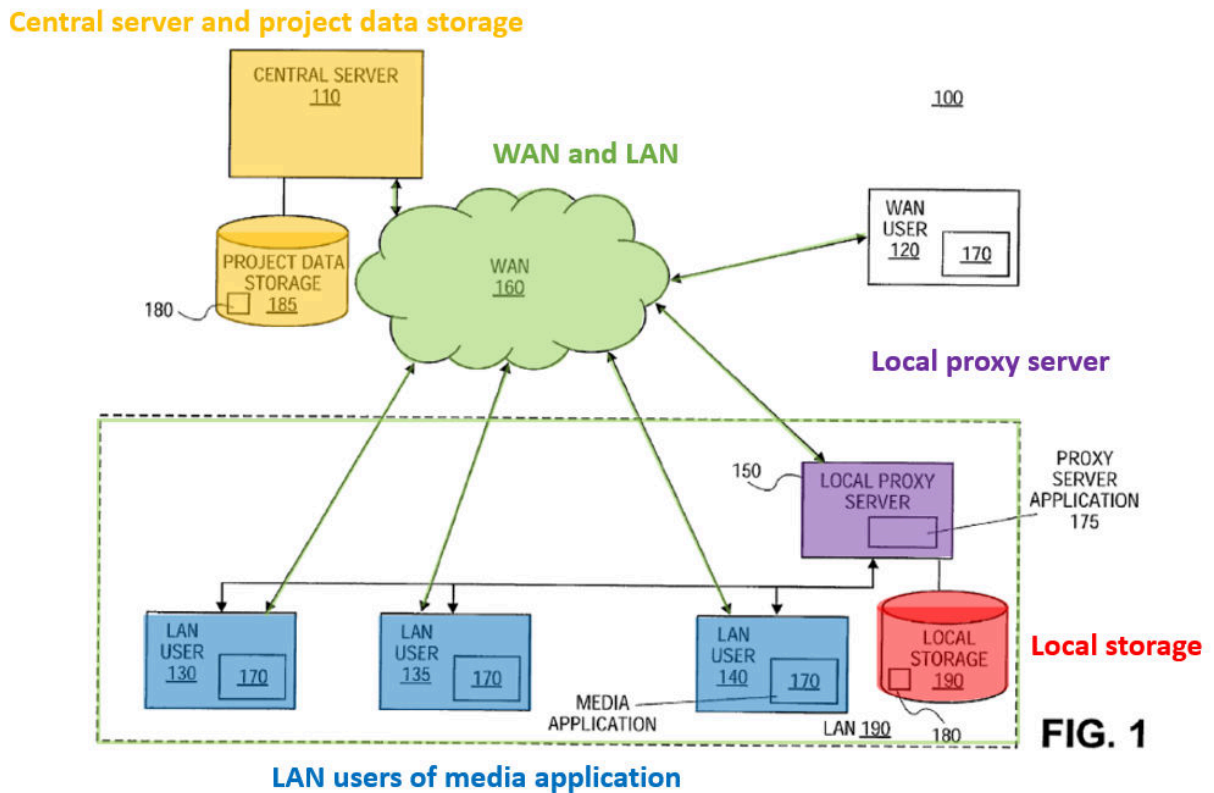
**(c) Claims 2-5 and 8-11**

*Supra* §§V.A.2.b.[2]-V.D.2.e.[5], §§V.D.2.h.[8]-[11]. APPLE-1003, ¶¶383-384.

**D. Ground 2A: Franke**

**1. Franke (APPLE-1005)**

Franke describes a data sharing system that uses “a local proxy server to process media data for local area users” in an extended network in which “LAN users 130-140 ... [are] coupled to a local proxy server 150 [which] acts as intermediary between central server 110 and LAN users 130-140.” APPLE-1005, [0002], [0030], [0032]-[0034], FIG. 1; APPLE-1003, ¶¶202-211.



**APPLE-1005, FIG. 1 (annotated)**

“LAN users 130-140, when posting media data, can store media data on local proxy server 150 [which] can then store the media data for the users

on central server 110 as media data 180.” APPLE-1005, [0037], [0009], [0028], [0042]-[0045]. Franke’s “local proxy server 150 can copy or download media data or object being stored on central server 110 [such that] LAN users 130-140 can copy project data being stored on central server 110 from local proxy server 150.” *Id.*, [0042].

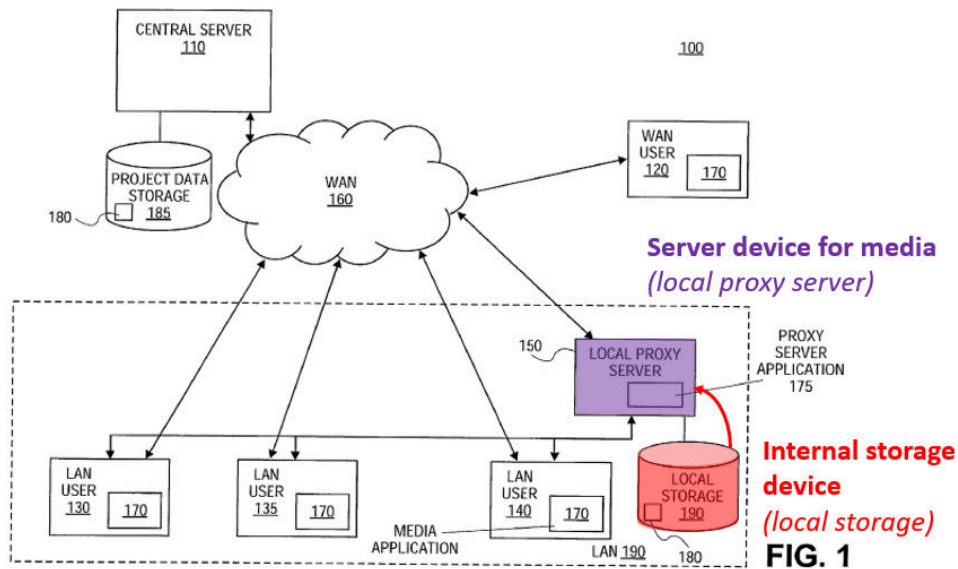
Franke’s proxy server includes a server application, which handles requests to store media data on central server and to deliver media data to LAN users 130-140. *Id.*, [0047]. “To download project data [users] can request project data from central server 110 directly [or] can also request project data from local proxy server 150,” and, “[i]f local proxy server 150 does not contain the requested project data, local proxy server 150 can request it from central server 110 and then distribute it to LAN users 130-140.” *Id.*, [0053], [0054].

## 2. Analysis

### (a) Claim 1

*[1pre]*

To the extent the preamble is considered limiting, Franke discloses [1pre]. APPLE-1003, ¶¶402-407. Franke describes that “users can post or store [] data, e.g., **media data**, on the **local proxy server**” (“server device for media”). APPLE-1005, [Abstract], [0028], [0030]; APPLE-1003, ¶¶403-405.



APPLE-1005, FIG. 1 (annotated); APPLE-1003, ¶404

[1a-i]

Franke discloses [1a-i]. APPLE-1003, ¶¶408-414. Franke describes that the local proxy server (“server device”) contains storage devices (“internal storage”) for storing media data (“for storing digital contents”). APPLE-1005, [0045] (“**storage devices contained within server 150** may operate as a shared stor[age] device”), [0056]-[0059], FIG. 2; APPLE-1003, ¶409.

Franke describes that users can “store...data, e.g., **media data, on the local proxy server,**” and that the “[l]ocal proxy server **150** can store project data (e.g., **media data 180**) in local storage 190... as one or more data files.” APPLE-1005, [Abstract], [0043]-[0044]. The local storage 190 may be any of a variety of “appropriate shared storage systems or devices” or “[a]lternatively, **storage**

devices contained within local proxy server 150 may operate as a shared stor[age] device” *Id.*, [0045], FIG. 2; APPLE-1003, ¶¶409-411.

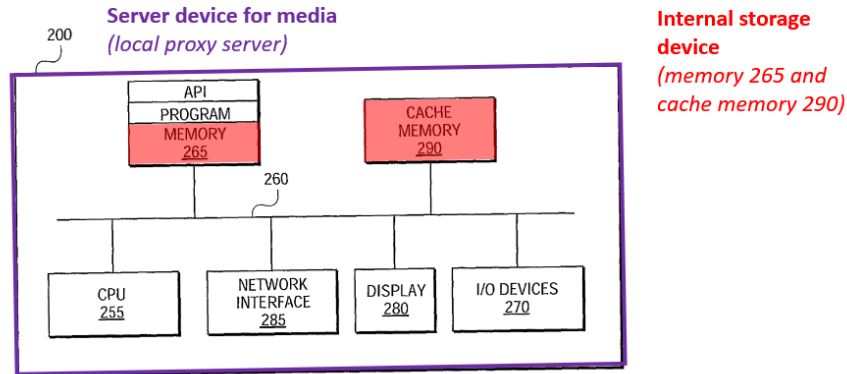


FIG. 2

APPLE-1005, FIG. 2 (annotated)

Franke’s local proxy server (“server device”) includes “memory 265 and cache memory 290” (“internal storage device”) which “may store media data (or data files) for storing or downloading to and from central server 110” (“for storing digital contents”). *Id.*, [0057], [0056]-[0059], FIG. 2; APPLE-1003, ¶412.

**[1a-ii]**

Franke discloses [1a-ii]. APPLE-1003, ¶¶415-421. Franke describes that the “[l]ocal proxy server 150” (“server device”) can “**handle requests for media data or object data from LAN users 130-140...from local storage**” (“respond to a data transmission request from a network player”) by “**transfer[ring]... data files to LAN users 130-140**” (by delivering corresponding data in corresponding

digital contents... to the network player”). APPLE-1005, [0047], [0028] (“Local area users can post or store data, e.g., media data, on the local proxy server ... for the data to be accessed locally”), [0042] (“LAN users 130-140 can copy project data being stored on central server 110 **from local proxy server 150**”), [0064], [0045]-[0046], [0098]; APPLE-1003, ¶¶416-417.

Franke describes that the “[s]erver application can maintain storage of media data ... in local storage 190 as one or more data files” (“data in corresponding digital contents”) which can be delivered to LAN users 130-140. APPLE-1005, [0047]; APPLE-1003, ¶¶416-418. Further, Franke describes that “a streaming process can be implemented to download segments of the requested media data” over a network (“stream-delivering corresponding data in corresponding digital contents from the internal storage device to the network player”). APPLE-1005, [0103], [0008],[0109]; APPLE-1003, ¶419.

***[1b-i]***

Franke discloses [1b-i]. APPLE-1003, ¶¶422-431. Although the bounds of the term “transfer control unit” are unclear, Franke discloses a “[s]erver application 175 [which] can be software operating within local proxy server 150” that is

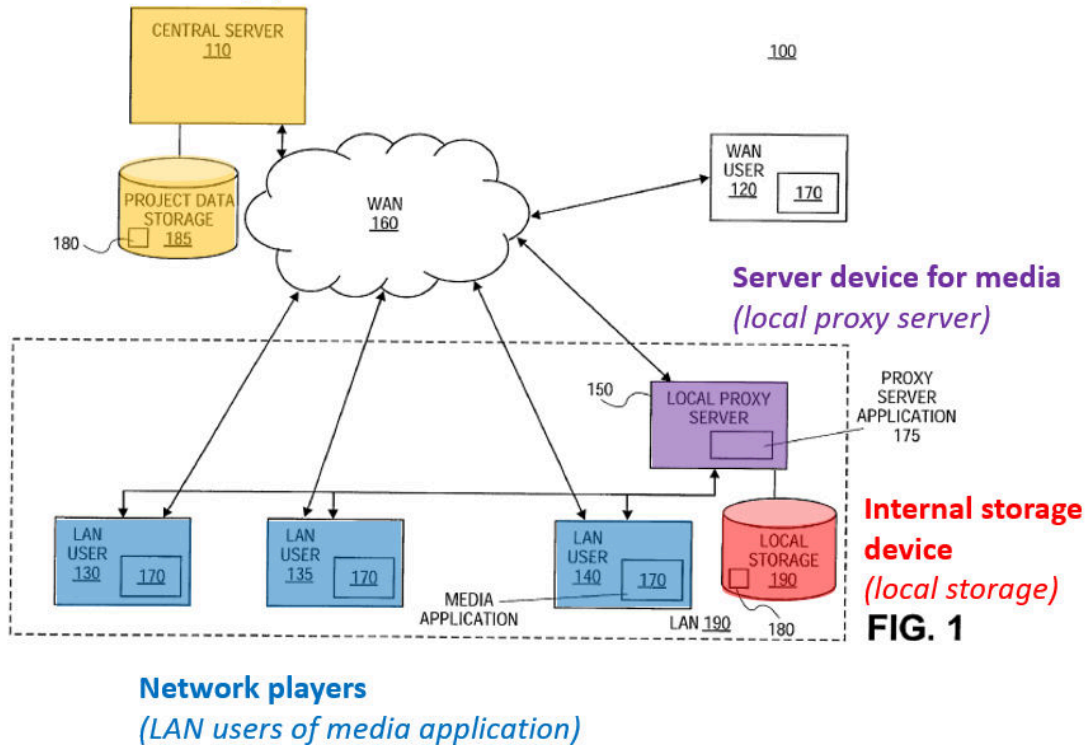
adapted to perform the same functions as the claimed “transfer control unit.”<sup>3</sup>

*Compare* APPLE-1005, [0047] (“Local proxy server 150 includes a server application 175, which can ... store media data or object on central server 110 for the LAN users 130-140”), [0059], *with* APPLE-1001, 3:5-9, 6:28-40; *see* APPLE-1005, [0073], [0080], [0117], [Abstract]; APPLE-1003, ¶¶423-426 (explaining that computer software transfers and stores data files).

---

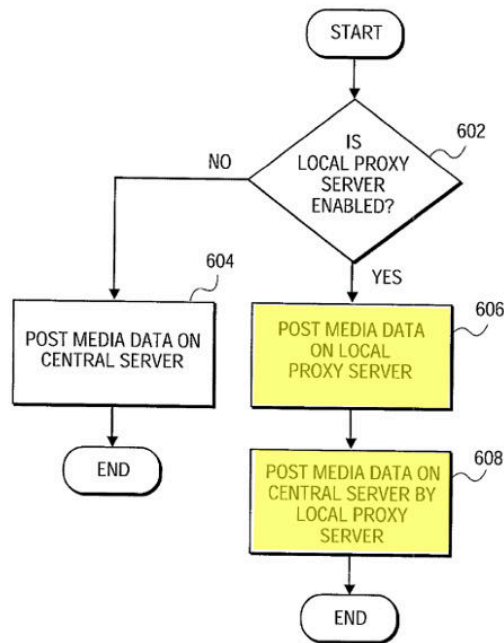
<sup>3</sup> The ’101 patent does not identify particular algorithms or software for performing the functions of the “transfer control unit” and other claimed “units.” *See* APPLE-1001, 3:5-9. As will be further described below, Franke’s server application performs each of the claimed functions of the claimed “units.” Dr. Zadok explains that an application may include software and algorithms that perform a variety of tasks, and that Franke’s server application’s performance of the claimed functions is consistent with ’101 patent’s description that a computer is caused to perform the functions. APPLE-1003, ¶426.

**Network storage device**  
(central server and storage)



**APPLE-1005, FIG. 1 (annotated)**

For example, Franke’s server application (“transfer control unit”) is used to “forward or store the project data from the users on central server 110” (“adapted to transfer and store part of held digital contents in the internal storage device to a network storage device”). APPLE-1005, [0042], [0028], [0047], [0073], [0080]; APPLE-1003, ¶¶427-429. “[M]edia data is stored on the local proxy server and stored on the central server by the local proxy server.” *Id.*, [0008], [0028], [0037], [0008].



**FIG. 6**

**APPLE-1005, FIG. 6 (annotated)**

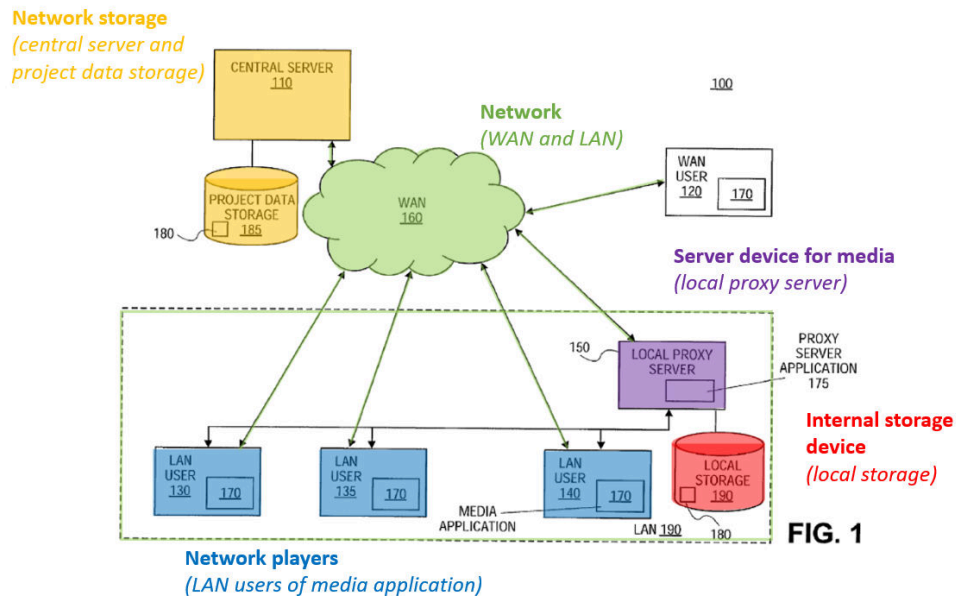
Franke is aware that files may not be fully transferred or stored, describing that “if requested project data has not been completely stored or posted central server 110, central server 110 can send status updates to the users or devices connected via WAN 160.” APPLE-1005, [0036]. A POSITA would have understood that computers transfer data in a piecemeal fashion and not all at once – thus, until all data is transferred, *only a part of the data* is transferred. APPLE-1003, ¶¶423-425.

Moreover, Franke discloses segmenting (large) data files and transmitting them piecemeal (“transfer and store part of held digital contents”). APPLE-1005,

[0109] (“a streaming process can be implemented to download segments of the requested media data as soon as the segments become available on central server 110”). APPLE-1003, ¶424 (explaining that segmenting of files applies to transfers as well as downloads). A POSITA would have known that when data is transmitted one segment at a time, that (a) only part of the full data has been transmitted until all of it has and (b) that it made little sense not to store the parts that had been received already (e.g., because there is always more room on larger hard disks than in main memory). APPLE-1003, ¶¶423-425.

*[1b-ii]*

Franke discloses [1b-ii]. APPLE-1003, ¶¶422-436. Franke describes that the central server (“network storage device”) is connected to the network via the WAN and includes storage for storing media data (“is connected to the network and is capable of storing data”). APPLE-1005, [0008] (“users are interconnected via a first network and connected to a second network [where the] **second network includes a central server** and the first network includes a selectively enabled local proxy server”), [0033], [0036]; APPLE-1003, ¶¶433-435.



**APPLE-1005, FIG. 1 (annotated)**

As illustrated in FIG. 1, Franke describes that “**central server 110 is shown connected to WAN 160** outside of LAN 190 [or alternatively] **can be located within LAN 190**” (“network storage device is connected to the network”).

APPLE-1005, [0036]; APPLE-1003, ¶434. Additionally, Franke describes that “[a]ttached to central server 110 is a storage device (“project data storage 185”) **storing project data** including media data (“media data 180”)” (“network storage device ... capable of storing data”). APPLE-1005, [0034]; APPLE-1003, ¶434.

**[1b-iii]**

Franke discloses [1b-iii]. APPLE-1003, ¶¶437-446.

Franke describes that, “media data is stored on the local proxy server and stored on the central server by the local proxy server if the local proxy server is

enabled.” APPLE-1005, [0009], [0051] (“if enabled, local proxy server 150 stores project data ... on central server 110”); APPLE-1003, ¶438. A POSITA would have understood that when the local proxy server is not enabled, the local proxy server does not store media data on the central server (“transfer control unit does not transfer, from the internal storage device to the network storage device, the digital contents that cannot be recovered if a network failure occurs during the transferring of the digital contents from the internal storage device to the network storage device”). APPLE-1003, ¶¶438-441; *see* APPLE-1005, [0078], [0051], [0078]-[0080], [0115]. Franke’s description of the local proxy server only storing data to the central server when it is enabled, and not storing media data to the central server when not enabled is consistent with Patent Owner’s infringement contentions mapping this limitation to not transferring recorded data when there is a power loss or loss of connectivity. APPLE-1003, ¶¶442-445 (explaining that the proxy server being not enabled is similar to a loss of connectivity); APPLE-1102, 15; *see* APPLE-1005, [0094] (describing indication of incomplete transfers of media data from the local proxy server to the central server using completions signals), [0096], [0103], [0108], [0036].

***[1c-i]***

Franke discloses [1c-i]. APPLE-1003, ¶¶447-454. Although the bounds of the term “list information transmission unit” are unclear, Franke describes that

“[s]erver application” is adapted to perform the same functions as the claimed “list information transmission unit.” *Compare* APPLE-1005, [0047] (“Local proxy server 150 includes a **server application 175**, which can **communicate with media application 170 to handle requests for media data or object data from LAN users**”), [0047] (“Proxy server application 175 can be used to **identify, organize, and reference data files**”), *with* APPLE-1001, 3:5-9, 3:31-40; *see* APPLE-1005, [0038], [0047]-[0049], [0059], [0117]; APPLE-1003, ¶¶448-451 (explaining that computer software functions to display an available file list).

Franke describes a user interface that allows a user to view assigned projects and select media data from a displayed set of projects or sessions (“respond to a list presentation request for the held digital contents of the server device for media from the network player by transmitting list information to the network player”). APPLE-1005, [0049] (“**identify, organize, and reference posted media data 180 for LAN users 130-140**”), [0070] (“**API 193 may provide interfaces** (e.g., as shown in FIGS. 11-14) ... **to display media data**”), [0112] (“user interface 1110 depicts a local proxy server... **dialog interface [including] a plurality of inputs 1115 through 1150** allowing a user to configure settings for posting or downloading media data”), [0113] (“**window 1140 can display sessions or projects assigned to the user**”), FIG. 11; APPLE-1003, ¶¶452-453.

Inputs 1120-1135  
allow user to  
request display of  
indicated sessions

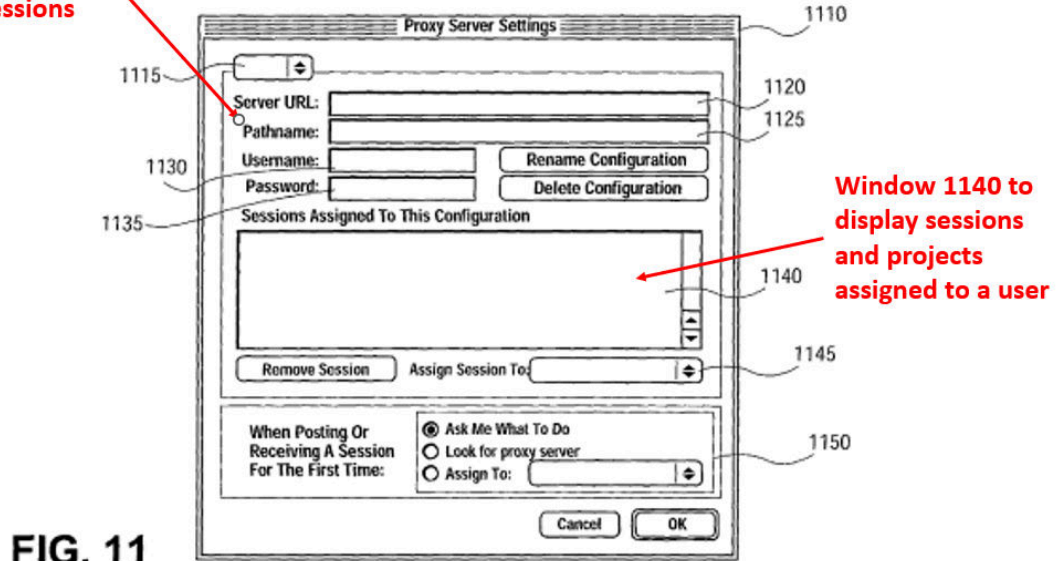


FIG. 11

APPLE-1005, FIG. 11 (annotated)

[1c-ii]

Franke renders obvious [1c-ii]. APPLE-1003, ¶¶455-460. As described above, Franke describes that a user interface allows a user to request to view assigned projects (“list information”) including information about whether the project is completely transferred to the central server or is downloadable from the proxy server (“lists the digital contents left in the internal storage device and the digital contents transferred from the internal storage device to the network storage device and stored in the network storage device”). *Supra*, §V.D.2.a.[1c-i]; APPLE-1005, [0042], [0049], [0112]-[0113], FIG. 11; APPLE-1003, ¶¶447-460.

Franke describes that users request project data from the local proxy server, and, “[i]f local proxy server 150 does not contain the requested project data, local proxy server 150 can request it from central server 110 and then distribute it to LAN users 130-140.” APPLE-1005, [0053]. A POSITA would have understood that the project list displayed by the server application in the user interface includes contents stored in the local proxy server (“digital contents left in the internal storage device”) as well as contents transferred from the local proxy server to the central server (“digital contents transferred from the internal storage device to the network storage device and stored in the network storage device”) based on Franke’s description of users requesting content that is stored on the local proxy server *or* in the central server. *Id.*, [0053], [0048]-[0049], [0070], Fig. 10; APPLE-1003, ¶¶456-459.

**[1c-iii]**

Franke renders obvious [1c-iii]. APPLE-1003, ¶¶461-468. Franke describes that in some instances, “a standard filing system ... is used to organize and store the media data” in a folder structure. APPLE-1005, [0084]; *see id.*, [0083] (“folders ... to store common media data”); APPLE-1003, ¶¶462-463. A POSITA would have understood that a “tree structure” refers to a database that uses a hierarchical system to organize content using nested folders and subfolders to categorize like data. APPLE-1009, [0084] (“a tree structure containing a plurality

of containers arranged in hierarchical levels”); APPLE-1003, ¶464. Franke provides “an exemplary folder hierarchy” with folders that illustrate an example of a tree structure of the list information. APPLE-1005, [0084]-[0092]; APPLE-1003, ¶¶463-465.

[0085] Parent Directory (root directory on the local proxy server)  
[0086] Project1 (folder)  
    [0087] Aaron1-123456789123-datafile1.doc (file)  
    [0088] Mike1-894576890532-datafile1.doc (file)  
[0089] Project2 (folder)  
    [0090] Aaron1-72384732874-picture.jpg (file)  
    [0091] Mike1-77773234234-mynotes.txt (file)  
[0092] Project3 (folder) . . .

**APPLE-1005, “exemplary folder hierarchy” of paras. [0085]-[0092]**

A POSITA would have recognized that the hierarchy of nested folders described and illustrated by Franke is a “tree structure of the digital contents” because such database structures were well-known hierarchical content organizing systems by the Critical Date, and Franke’s description and depiction of the data directory illustrates the use of hierarchically nested folders. APPLE-1003, ¶¶464-465 (citing APPLE-1009, [0084], FIGS. 4A-C, 6-7).

As discussed above, the project sessions provided to the user allow a user to select projects stored in the proxy server or on the central server. *Supra*

§V.C.2.a.[1c-i]; APPLE-1003, ¶¶447-454. Additionally, Franke describes that organization of newly received media data into the folder hierarchy of the local proxy server (“list information maintains a tree structure of the digital contents in the internal storage device”) occurs when media is posted to the server to be displayed to the user regardless of where the media is located in the system (“before transferring the digital contents to the network storage device”). APPLE-1005, [0099], FIGS. 6-7; APPLE-1009, [0006]-[0009]; APPLE-1003, ¶¶463-467. Accordingly, a POSITA would have understood that the hierarchical tree structure the proxy server uses to store project media data reflects “a tree structure of the digital contents in the internal storage device before transferring the digital contents to the network storage device.” APPLE-1003, ¶¶462-467.

***[1d]***

Franke renders obvious [1d]. APPLE-1003, ¶¶469-476. Although the bounds of the term “search unit” are unclear, Franke discloses that “[p]roxy server application 175 can determine the location of data files” and is adapted to perform the same functions as the claimed “search unit.” *Compare* APPLE-1005, [0048], [0047], [0059], [0117], FIG. 2, *with* APPLE-1001, 3:5-9, 6:41-48; APPLE-1003, ¶¶470-472 (explaining that computer software determines requested content location).

Franke describes that the proxy server (including server application)

(“search unit”) makes a check for a location of content requested by a user device (“adapted to respond to a data transmission request for the held digital contents from the network player”) to determine whether the requested content is available in the proxy server or ready to be downloaded from the central server (“by searching for a location where the held digital contents are currently stored”). APPLE-1005, [0098] (“LAN user is requesting media data to be downloaded”), [0099] (“A check is then made to determine if the media data ... is stored on local proxy server”), [0047], [0054], [0070], [0094]; FIGS. 8-10; APPLE-1003, ¶¶473-474.

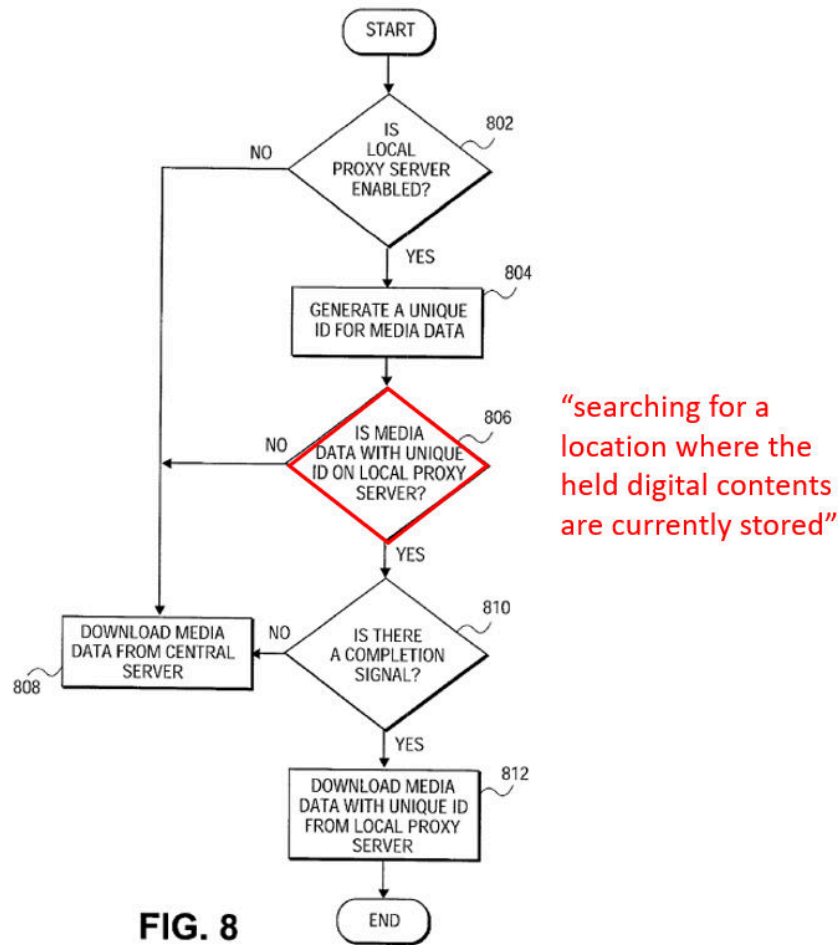


FIG. 8

APPLE-1005, FIG. 8 (annotated)

Alternatively or additionally, Franke describes that an API 193 “may determine whether posted media data 180 is stored on local proxy server 150” or if the “API 193 determines that the media data is not stored on local proxy server 150, API 193 may download posted media data 180 from central server 110.” APPLE-105, [0070]; APPLE-1003, ¶474. Franke makes clear that the API (and the proxy server application) search for the location of requested contents in the local proxy server or central server. APPLE-1005, [0070]; APPLE-1003, ¶¶470-

475. It would have been obvious to a POSITA that the same determination of requested media data location described by Franke with regard to the API 193 would also be a function of the proxy server application and/or API of the local proxy server based on Franke's similar description of the location determination function of the server application and API. APPLE-1005, [0099], [0059], [0070]; APPLE-1003, ¶¶473-475.

*[1e]*

Franke discloses [1e]. APPLE-1003, ¶¶477-486. Although the bounds of the term “digital contents data transmission processing unit” are unclear, Franke discloses that “server application” is adapted to perform the same functions as the claimed unit. *Compare* APPLE-1005, [0047] (“Proxy server application 175 may also be used to **transfer such data files to LAN users**”), [0054] (“if, e.g., media data 180 is not stored in local storage 190, local proxy server 150 can **request the data from central server 110** ”), *with* APPLE-1001, 3:5-9, 7:28-55; *see* APPLE-1005, [0042]-[0048], [0053]-[0054], [0103], [0117]; APPLE-1003, ¶¶478-480 (explaining that computer software performs transfer functions). A POSITA would have recognized from Franke's discussion that if requested media data is not stored in the local storage, then the requested media data must be stored remotely in the central server, and that such data is allowed by the server application to be transmitted to the user. APPLE-1005, [0047]; APPLE-1003, ¶¶478-483.

Franke describes that in downloading requested media data to a LAN user, a check is “made to determine if the media data having the unique ID is stored on local proxy server” and “[i]f no media data having the unique ID is stored on local proxy server 150,” (“if the result of search shows the network storage device”) then, the proxy server application (“digital contents data transmission processing unit adapted to allow”) proceeds so that “the media data is downloaded from central server 110” and presented to the user (“corresponding data in held digital contents to be stream-delivered from the network storage device to the network player”). APPLE-1005, [0099], [0054], [0052], FIGS. 8-10. Alternatively, Franke describes that when the data is located on the central server, the media data is downloaded from the central server to the user. APPLE-1005, [0048], [0053], [0099], [0107]- [0109], FIGS. 8-10; APPLE-1003, ¶¶478-485.

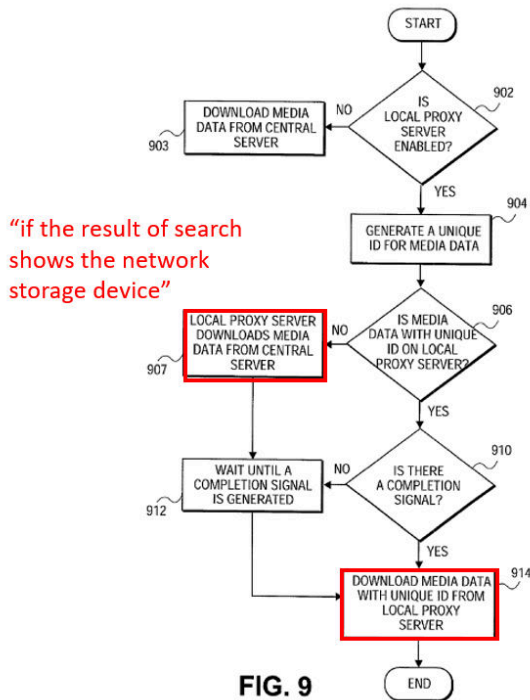


FIG. 9

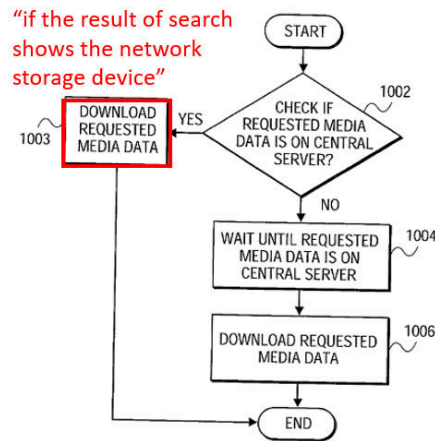


FIG. 10

**APPLE-1005, FIGS. 9 (left) and 10 (right) (annotated)**

Further, Franke describes that the media data is delivered to users by a streaming process. APPLE-1005, [0103] (“a streaming process can be implemented to download segments of the requested media data”), [0109]; APPLE-1003, ¶484.

*[1f]*

Franke discloses [1f]. APPLE-1003, ¶¶487-491. Franke describes that the local proxy server is a computing system, such as a personal computer. APPLE-1005, [0044], [0032]; APPLE-1003, ¶488. A POSITA would have recognized that a personal computer is a media player, because media can be “played” by a user directly from the personal computer, for example, by playing music through

headphones connected to the personal computer or viewing media content on a screen of the computer. APPLE-1003, ¶489.

**(b) Claim 2**

Franke discloses [2]. APPLE-1003, ¶¶502-508. As described above, Franke describes that, in at least some cases, the server application (“digital contents data transmission processing unit”) downloads the media data from the central server to the local proxy server (“causes the network storage device to transmit the corresponding data to the server device for media”) and then distributes the requested media data to the LAN users (“and then transmits the corresponding data received from the network storage device from the server device for media to the network player”). APPLE-1005, [0054] (“if, e.g., media data 180 is not stored in local storage 190, local proxy server 150 can request the data from central server 110 to make it accessible to LAN users 130-140”), [0047], [0064], [0068]-[0070], FIG. 9; *supra* §V.D.2.a.[1.e]; APPLE-1003, ¶¶503-507.

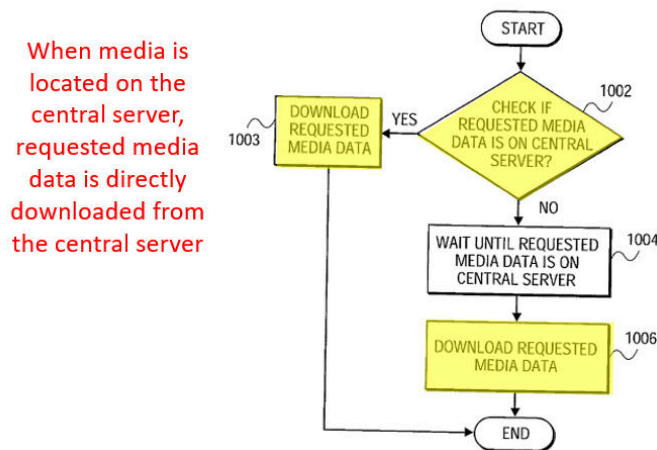
**(c) Claim 3**

Franke discloses [3]. APPLE-1003, ¶¶509-515. As described above, Franke describes that in some cases, the server application (“digital contents data transmission processing unit”) identifies the location of the requested content to the media application (“transmits the corresponding data and information for identifying the network storage device to the network player”) and the content is

downloaded to the user directly from the central server (“causes the network storage device to directly transmit the corresponding data to the network player”).

APPLE-1005, [0036] (“**Central server 110 can also handle download requests of project data from LAN users**”), [0070] (“**API 193 may download posted media data 180 from central server 110**”), [0033]-[0035], [0053], [0099], [0108];

APPLE-1003, ¶¶506-514.



**FIG. 10**

**APPLE-1005, FIG. 10 (annotated)**

**(d) Claim 4**

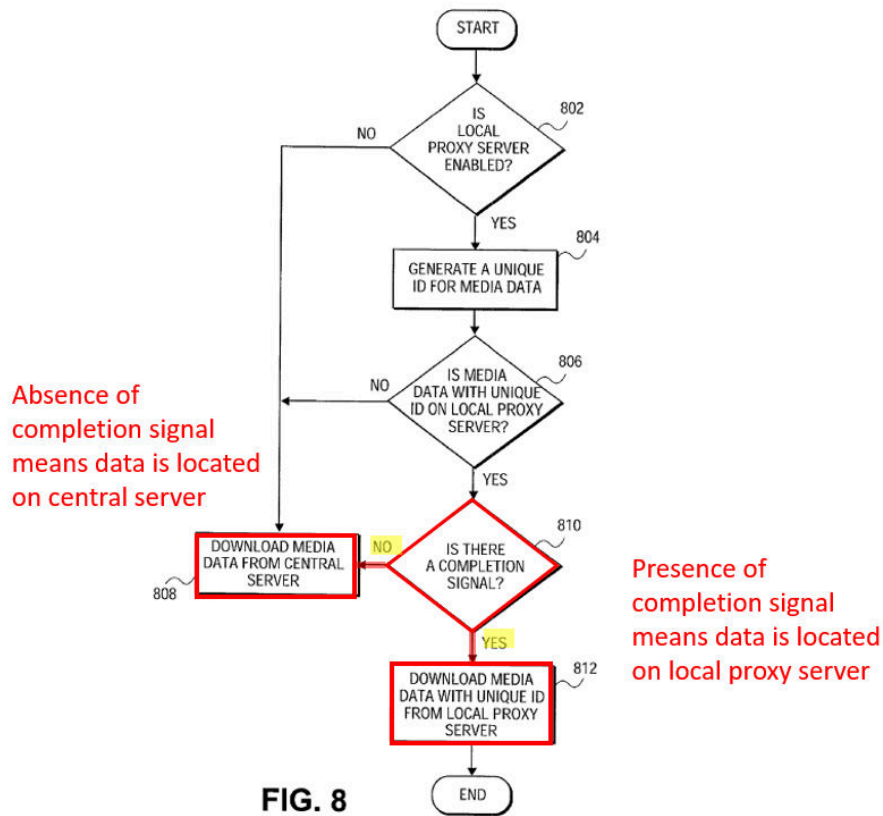
Franke discloses [4]. APPLE-1003, ¶¶516-523. Although the bounds of the term “return control unit” are unclear, Franke discloses that the server application downloads requested data from the central server to the proxy server for distribution to LAN users and thus is adapted to perform the same functions as the

claimed “return control unit.” *Compare* APPLE-1005, [0072] (“Local proxy server 150 can ... act as an intermediary between central server 110 and LAN users”), [0054] (“local proxy server 150 can request the data from central server 110 to make it accessible to LAN users”), *with* APPLE-1001, 3:5-9, 7:66-8:4; *see* APPLE-1005, [0049]-[0054], [0074], [0081], [0117], FIG. 9; APPLE-1003, ¶¶517-519 (explaining that computer applications transfer stored content between storage devices).

As described above in [1e] and [2], Franke describes that requested content stored in the central server (“digital contents corresponding to a predetermined condition among the digital contents which have been transferred to the network storage device”) is transferred from the central server to the proxy server (“cause the digital contents... to be returned from the network storage device to the internal storage device”) by the server application (“return control unit”) in response to a user request for content (“digital contents corresponding to a predetermined condition”). *Supra* §§V.D.2.a.[1e], V.D.2.b.[2]; APPLE-1005, [0047], [0053]-[0054], [0064], [0068]-[0070], FIG. 9; APPLE-1003, ¶¶518-520. Being requested by a user is a predetermined condition of the digital contents. *See e.g.*, APPLE-1001, 8:5-10 (predetermined conditions include “digital contents which have recently been subjected to the self-playback” or “network playback”); APPLE-1003, ¶¶520-521.

**(e) Claim 5**

Franke renders obvious [5]. APPLE-1003, ¶¶524-530. Franke describes that the server application (“list information transmission unit”) provides the list of projects in the user interface (“makes the list information to be transmitted to the network player... in the display list of the network player”) with the unique ID corresponding to the media data and a completion signal indicating whether the data has been completely stored in the local proxy server (“include information for identifying whether each digital content is currently stored in the internal storage device or the network storage device”). APPLE-1005, [0093]-[0096], [0099], [0103]-[0105]; APPLE-1003, ¶¶525-526.



**APPLE-1005, FIG. 8 (annotated)**

Franke describes that “[a]fter the media data is completely posted on local proxy server 150, a completion signal is generated ... [which] notifies other LAN users 130-140 that the media data has been completely posted or stored on the local proxy server.” APPLE-1005, [0093]. The completion signal (or absence thereof) for a project is presented to the user, so that “a user can avoid downloading an incomplete copy of media data.” *Id.*, [0094] (also describing other ways for determining if content is stored on the proxy server); APPLE-1003, ¶¶527-528. Franke describes that presence of a completion signal indicates that the data is located in and can be downloaded from the proxy server, while an absence

of the completion signal indicates the data is not completely stored in the proxy server and “the media data is downloaded from central server 110.” APPLE-1005, [0099]; APPLE-1003, ¶528. A POSITA would have understood from Franke’s disclosure that the project data completion signal displayed to the user is information for identifying whether each digital content is currently stored in the internal storage device or the network storage device in the display list of the network player. APPLE-1003, ¶¶526-529.

**(f) Claim 6**

***[6pre]-[6b-ii]***

*Supra* §§V.D.2.a.[1pre]-[1b-ii]. APPLE-1003, ¶¶403-436.

***[6b-iii]***

Franke renders obvious [6b-iii]. APPLE-1003, ¶¶493-501. Franke describes that users are presented with various options and information related to the storage and download of content, including selection of an “ask me what to do” option. APPLE-1005, [0113], [0112], [0113], [0115]; APPLE-1003, ¶¶494-495. It would have been obvious to a POSITA that Franke’s concern with network connection of the proxy server would have been equally applicable to the central server because Franke describes that the system is aware of the download and upload status of content to the servers, and that the user would have been kept informed of options for proceeding. APPLE-1005, [0108] (“If the requested media data is not on

central server 110, the user waits until the requested data is on central server 110”), [0036], [0094]-[0096], [0103]-[0104], [0109]; APPLE-1003, ¶¶494-495.

It would have been obvious to a POSITA that if the network between the proxy server and central server were in a state in which digital contents could not be recovered if a network failure occurs (e.g., if the central server is not available on the network) (“digital contents that cannot be recovered if a network failure occurs during the transferring of the digital contents from the internal storage device to the network storage device”) the user is presented with options, including an “Ask me what to do” option and options for proceeding with the storage of the data to the central server (“is transferred after obtaining permission from a user”). APPLE-1005, [0108]-[0115], [0345] (“authentication”), [0049] (“password protection”), [0112] (“User interface 1110 includes a plurality of inputs”), [0005]; APPLE-1003, ¶¶496-499. Franke’s description of the local proxy server only storing data to the central server when it is enabled, and not storing media data to the central server when not enabled is consistent with Patent Owner’s infringement contentions mapping “digital contents that cannot be recovered if a network failure occurs” as recited in [1b-iii] to content that would be transferred during a power loss or loss of connectivity. APPLE-1003, ¶¶497-498 (explaining that the proxy/central server being not enabled is similar to a loss of connectivity); APPLE-1102, 15; *see* APPLE-1005, [0094], [0096], [0103], [0108], [0036].

**[6c-i]-[6f]**

*Supra* §§V.D.2.a.[1c-i]-[1f]. APPLE-1003, ¶¶447-491.

**(g) Claim 7**

**[7pre]-[7f]**

As described above, Franke provides a proxy server for media data storage and a server application that performs functions of the server, as well as a method for controlling the proxy server. *Supra* §V.D.2.a.[1pre]-[1f]; APPLE-1003, ¶¶402-491; APPLE-1005, [0002] (“methods ... using a local proxy server to process media data for local area users.”), [0007]-[0011], [0042]-[0049], [0054], [0072], [0099], [0112]-[0113], FIG. 11.

**(h) Claims 8-11**

*Supra* §§V.D.2.b.[2]-V.D.2.e.[5]. APPLE-1003, ¶¶502-530.

**(i) Claim 12**

**[12pre]-[12a]**

*Supra* §§V.D.2.a.[1pre]-[1a-ii]. APPLE-1003, ¶¶403-421.

**[12b]**

*Supra* §§V.D.2.a.[1b-i]-[1b-ii], V.D.f.[6b-iii]. APPLE-1003, ¶¶422-436, 493-501.

**[12c]-[12f]**

*Supra* §§V.D.2.a.[1c-i]-[1f]. APPLE-1003, ¶¶447-491.

**E. Ground 2B: Franke-Fiechter**

**1. Franke-Fiechter Combination**

As described above, Franke renders obvious [1b-iii] and [6b-iii]. *Supra* §§V.D.2.a.[1b-iii], V.D.2.f.[6b-iii], V.D.2.g.[7b], V.D.2.i.[12b]; APPLE-1003, ¶¶437-446, 493-501. To the extent it is argued that Franke does not provide sufficient details related to these limitations, Franke-Fiechter renders obvious [1b-iii] and [6b-iii].

In Franke-Fiechter, a system, per Franke, is implemented to not transfer content when network failure rendering content unrecoverable is likely and to provide a user with options to proceed with the transfer, per Fiechter. APPLE-1005, [0112]-[0115]; APPLE-1006, 17:62-18:3; APPLE-1003, ¶¶531-543.

A POSITA would have been motivated to pursue the combination for multiple reasons.

First, Franke's discussion of network failures and connectivity issues would have motivated a POSITA to look to references like Fiechter that provide additional details for dealing with increased failure likelihood. APPLE-1005, [0005] (discussing bandwidth/connectivity issues impacting server function); APPLE-1006, 17:50-59; APPLE-1003, ¶¶545-546.

Second, a POSITA would have appreciated that Fiechter's solutions of halting content transfer and providing a user with options for proceeding are

similar to Franke's description of not transferring content to the central server when the proxy server is not enabled and instead providing options to the user. APPLE-1005, [0078], [0051], [0078]-[0080], [0115]; APPLE-1006, 17:50-18:3; APPLE-1003, ¶¶547-548. A POSITA would have been motivated to implement additional user options to stop the transfer, wait for improved conditions, or proceed with the transfer, per Fiechter, in view of Franke's description of providing information to the user. APPLE-1003, ¶¶547-548.

Third, a POSITA would have understood that presenting a user with options of waiting or proceeding with the transfer—when a network is likely to be unreliable—optimizes system performance. APPLE-1006, 17:62-18:3; APPLE-1003, ¶549. A user presented with options can make decisions about the importance of particular transfers; decide to cancel a scheduled transfer; or reschedule a transfer. APPLE-1003, ¶549.

Fourth, a POSITA would have understood that providing mechanisms for addressing elevated network failure and data loss risks improve the user experience of interacting with the networked system, per Fiechter, through various personal devices. APPLE-1005, [0005], [0028], [0032], [0036], [0053]-[0054], [0058], [0115]; APPLE-1006, 2:9-14, 3:10-14, FIG. 2, 8-9; APPLE-1003, ¶550.

Fifth, a POSITA would have understood that the combination of known elements according to known methods would have yielded predictable results, as

each element performs a similar function combined as it does separately. APPLE-1003, ¶551. Franke's system already includes mechanisms for addressing situations where content cannot be transferred by not transmitting the content or by presenting options to a user. *Supra* §§V.D.2.a.[1b-iii], V.D.2.f.[6b-iii]; *see e.g.*, APPLE-1005, [0036], [0094]-[0096], [0103]-[0108]; APPLE-1003, ¶552.

Fiechter's additional details regarding halting content transfer and providing options to a user do not alter Franke's system's performance. APPLE-1003, ¶552.

Sixth, combining Franke-Fiechter would have been well within a POSITA's skill because mechanisms for responding to network failures by preventing a transfer or providing options to a user were well-known by the Critical Date, as Fiechter teaches. APPLE-1003, ¶553; APPLE-1006, 17:62-18:3. Accordingly, a POSITA would have had a reasonable expectation of success in doing so for the reasons explained above, and because methods for responding to increased likelihood of network failures during data transfer were well known to a POSITA by the Critical Date. APPLE-1003, ¶¶544-554.

## **2. Analysis**

### **(a) Claim 1**

*[1pre]-[1b-ii]*

*Supra* §§V.D.2.a.[1pre]-[1b-ii]. APPLE-1003, ¶¶403-436.

***[1b-iii]***

Franke-Fiechter renders obvious [1b-iii]. APPLE-1003, ¶¶533-538. As described above, Franke describes monitoring a connection status of the proxy and central servers and transfer status of content being stored in the central server by the proxy server, including preventing transfer of contents when the servers are not enabled to receive content. *Supra* §V.D.2.a.[1b-iii]; APPLE-1003, ¶¶437-446. In combination with Fiechter, content is not transferred from the proxy server to the central server when the system detects that network failure (i.e., failure of the connection between the proxy and central servers) is likely or happening (“said transfer control unit does not transfer, from the internal storage device to the network storage device, the digital contents that cannot be recovered if a network failure occurs during the transferring of the digital contents from the internal storage device to the network storage device”). *Compare* APPLE-1005, [0094]-[0096], [0103]-[0108], [0036], and APPLE-1006, 17:62-18:3, with APPLE-1102, 15 (Patent Owner’s infringement contentions mapping “digital contents that cannot be recovered if a network failure occurs” to content that would be transferred during a power loss or loss of connectivity); *supra* §V.E.1; APPLE-1003, ¶¶536-537. For example, where characteristics of the network make data loss during transfer more likely, Franke-Fiechter does not transfer content from the proxy server to the central server. APPLE-1005, [0005], [0078], [0051], [0078]-[0080],

[0115]; APPLE-1006, 17:62-18:3; APPLE-1003, ¶¶536-537.

**[1c-i]-[1f]**

*Supra* §§V.D.2.a.[1c-i]-[1f]. APPLE-1003, ¶¶447-491.

**(b) Claims 2-5 and 8-11**

*Supra* §§V.D.2.b.[2]-V.D.2.e.[5], §§V.D.2.h.[8]-[11]. APPLE-1003, ¶¶502-530.

**(c) Claim 6**

**[6pre]-[6b-ii]**

*Supra* §§V.D.2.a.[1pre]-[1b-ii]. APPLE-1003, ¶¶403-436.

**[6b-iii]**

Franke-Fiechter renders obvious [6b-iii]. APPLE-1003, ¶¶539-543. As described above, Franke describes reporting a transfer status and options to a user including when transfer is not complete. *Supra* §V.D.2.f.[6b-iii]. In combination with Fiechter, content is transferred from the proxy server to the central server after presenting options to a user and receiving instructions to proceed with the transfer when failure to fully transfer content is anticipated or detected (“digital contents that cannot be recovered if a network failure occurs during the transferring of the digital contents from the internal storage device to the network storage device is transferred after obtaining permission from a user”). *Supra* §V.E.1; APPLE-1005, [0094]-[0096], [0103]-[0108], [0036]; APPLE-1102, 15;

APPLE-1003, ¶¶540-541, 443-444 (explaining that the proxy/central server being not enabled is similar to a loss of connectivity). For example, where characteristics of the network make data loss during transfer more likely, Franke-Fiechter provides network condition and transfer information and further presents the user with options including proceeding with transferring the contents to the central server. APPLE-1005, [0108]-[0115], [0345], [0049], [0112], [0005]; APPLE-1006, 17:62-18:3; APPLE-1003, ¶¶539-542.

**[6c-i]-[6f]**

*Supra* §§V.D.2.a.[1c-i]-[1f]. APPLE-1003, ¶¶447-501.

**(d) Claim 7**

**[7pre]-[7a]**

*Supra* §§V.D.2.a.[1pre]-[1a]. APPLE-1003, ¶¶403-421.

**[7b]**

*Supra* §§V.D.2.a.[1b-i]-[1b-ii] and §V.E.2.a.[1b-iii]. APPLE-1003, ¶¶422-436, 535-538.

**[7c]-[7f]**

*Supra* §§V.D.2.a.[1c-i]-[1f]. APPLE-1003, ¶¶447-491.

**(e) Claim 12**

**[12pre]-[12a]**

*Supra* §§V.D.2.a.[1pre]-[1a]. APPLE-1003, ¶¶403-421.

**[12b]**

*Supra* §§V.D.2.a.[1b-i]-[1b-ii], §V.E.2.c.[6b-iii]. APPLE-1003, ¶¶422-436, 539-543.

**[12c]-[12f]**

*Supra* §§V.D.2.a.[1c-i]-[1f]. APPLE-1003, ¶¶447-491.

**F. Ground 2C: Franke-Ito**

**1. Franke-Ito Combination**

As described above, Franke renders obvious [1b-iii] and [7b]. *Supra* §§V.D.2.a.[1b-iii], V.D.2.g.[7b]; APPLE-1003, ¶¶437-446. To the extent it is argued that Franke does not provide sufficient details related to these limitations, Franke-Ito renders obvious [1b-iii] and [7b].

In Franke-Ito, a system, per Franke, is implemented to anticipate loss of content in the case of network failure during backup by not transferring such content from the proxy server to the central server, per Ito. APPLE-1005, [0112]-[0115]; APPLE-1012, [0001]-[0008], [0252]-[0253]; APPLE-1003, ¶¶555-565.

Franke and Ito both describe networked systems for backing up content, and further are both concerned network reliability during transfer of certain contents. APPLE-1012, [0001]-[0008], [0252]-[0253]; APPLE-1005, [0008], [0030], FIG. 1; APPLE-1003, ¶¶558-559.

A POSITA would have been motivated to pursue the combination for

multiple reasons:

First, Franke's discussion of network and connectivity issues would have motivated a POSITA to look to references like Ito that provide further details for terminating an attempted transfer to prevent content loss due to failure. APPLE-1005, [0005], [0028], [0054]; APPLE-1012, [0001]-[0008], [0252]; APPLE-1003, ¶¶566-567.

Second, a POSITA would have appreciated that Ito's mechanism of terminating transfer of content that would not be recoverable in the case of a network failure is similar to the mechanisms Franke describes for not transferring content from the proxy server to the central server when the proxy server is not enabled (and not transferring when the central server is not enabled, *supra* §V.D.2.a.[1b-iii]). APPLE-1005, [0078], [0051], [0078]-[0080], [0115]; APPLE-1012, [0001]-[0008], [0252]-[0253]; APPLE-1003, ¶568.

Third, a POSITA would have understood that anticipating transfer failures during network issues improves user experience with the system, per Ito. APPLE-1005, [Abstract], [0028], [0094]; APPLE-1012, [0252]-[0253]; APPLE-1003, ¶569.

Fourth, a POSITA would have understood that the combination of known elements according to known methods would have yielded predictable results, as each element performs a similar function combined as it does separately. APPLE-

1003, ¶570. Franke's system already includes mechanisms for addressing situations where content cannot be transferred by not transmitting the content, to prevent accessing incomplete content. *Supra* §V.D.2.a.[1b-iii]; *see e.g.*, APPLE-1005, [0036], [0094]-[0096], [0103]-[0108]; APPLE-1003, ¶¶437-446. Ito's additional details about terminating content backup do not alter Franke's system's performance. APPLE-1003, ¶570.

Fifth, combining Franke-Ito would have been well within a POSITA's skill because mechanisms for anticipating content loss due to network failure by preventing a transfer were well-known by the Critical Date, as Ito teaches. APPLE-1003, ¶571; APPLE-1012, [0001]-[0008], [0252]-[0253]. Accordingly, a POSITA would have had a reasonable expectation of success in doing so for the reasons explained above, and because methods for responding to increased likelihood of network failures during data transfer were well known to a POSITA by the Critical Date. APPLE-1003, ¶¶566-572.

## **2. Analysis**

### **(a) Claim 1**

#### ***[1pre]-[1b-ii]***

*Supra* §§V.D.2.a.[1pre]-[1b-ii]. APPLE-1003, ¶¶403-436.

#### ***[1b-iii]***

Franke-Ito renders obvious [1b-iii]. APPLE-1003, ¶¶557-565. As described

above, Franke-Ito, where content cannot be backed up to the central server to guard against network failure (“digital contents that cannot be recovered if a network failure occurs during the transferring of the digital contents from the internal storage device to the network storage device”) the content transfer to the backup is terminated (“said transfer control unit does not transfer, from the internal storage device to the network storage device”). *Supra* §V.F.1; APPLE-1003, ¶¶561-564. For example, in Franke-Ito, protected content that would be lost in the case of a network failure during transfer to the central server, is not backed up to the central server. APPLE-1005, [0005], [0036], [0051], [0078]-[0080], [0094]-[0096], [0103]-[0109], [0112]-[0115]; APPLE-1012, [0001]-[0008], [0252]-[0253]; APPLE-1003, ¶¶561-564.

***[1c-i]-[1f]***

*Supra* §§V.D.2.a.[1c-i]-[1f]. APPLE-1003, ¶¶447-491.

**(b) Claim 7**

***[7pre]-[7a]***

*Supra* §§V.D.2.a.[1pre]-[1a]. APPLE-1003, ¶¶403-421.

***[7b]***

*Supra* §§V.D.2.a.[1b-i]-[1b-ii] and §V.F.2.a.[1b-iii]. APPLE-1003, ¶¶422-436, 560-565.

*[7c]-[7f]*

*Supra* §§V.D.2.a.[1c-i]-[1f]. APPLE-1003, ¶¶447-491.

**(c) Claims 2-5 and 8-11**

*Supra* §§V.D.2.b.[2]-V.D.2.e.[5], §§V.D.2.h.[8]-[11]. APPLE-1003, ¶¶502-530.

**VI. INSTITUTION SHOULD NOT BE DENIED ON DISCRETION**

Petitioner believes that discretionary denial is unwarranted, and yet, Petitioner intends to utilize the bifurcated briefing process contemplated by the March 26, 2025 Stewart Memorandum to rebut contentions if offered by Patent Owner to the contrary. *See* APPLE-1105; APPLE-1106; Video at <https://uspto.cosocloud.com/p9xpz6s4jn75/>.

**VII. CONCLUSION AND FEES—37 C.F.R. §42.103**

The Challenged Claims are unpatentable. Please charge fees to Deposit Account 06-1050.

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

**A. Real Party-In-Interest Under 37 C.F.R. § 42.8(b)(1)**

Apple Inc. is the petitioner and the real party-in-interest.

**B. Related Matters Under 37 C.F.R. § 42.8(b)(2)**

Petitioner is not aware of any disclaimers, reexamination certificates or petitions for inter partes review for the '101 Patent. The '101 patent is the subject of civil actions including: *Advanced Coding Technologies LLC v. Apple Inc.*, 2-24-cv-00687 (EDTX), August 20, 2024 and *Advanced Coding Technologies LLC v. Google LLC*, 2-24-cv-00353 (EDTX), May 10, 2024.

**C. Lead And Back-Up Counsel Under 37 C.F.R. § 42.8(b)(3)**

Petitioner provides the following designation of counsel.

Lead Counsel	Backup counsel
W. Karl Renner, Reg. No. 41,265 Fish & Richardson P.C. 60 South Sixth Street, Suite 3200 Minneapolis, MN 55402 Tel: 202-783-5070 Fax: 877-769-7945 Email: <a href="mailto:IPR50095-0245IP1@fr.com">IPR50095-0245IP1@fr.com</a>	Jeremy J. Monaldo, Reg. No. 58,680 Jennifer J. Huang, Reg. No. 64,297 Kiersten Batzli, Reg. No. 75,476 Fish & Richardson P.C. 60 South Sixth Street, Suite 3200 Minneapolis, MN 55402 Tel: 202-783-5070 Fax: 877-769-7945 Email: <a href="mailto:IPR50095-0245IP1@fr.com">IPR50095-0245IP1@fr.com</a>

**D. Service Information**

Please address all correspondence and service to the address listed above.

Petitioner consents to electronic service by email at [IPR50095-0245IP1@fr.com](mailto:IPR50095-0245IP1@fr.com).

Respectfully submitted,

Dated June 4, 2025

/Jennifer J. Huang/  
W. Karl Renner, Reg. No. 41,265  
Jeremy J. Monaldo, Reg. No. 58,680  
Jennifer J. Huang, Reg. No. 64,297  
Kiersten Batzli, Reg. No. 75,476  
Fish & Richardson P.C.  
60 South Sixth Street, Suite 3200  
Minneapolis, MN 55402  
T: 202-783-5070  
F: 877-769-7945

(Control No. IPR2025-01103)

*Attorneys for Petitioner*

**CERTIFICATION UNDER 37 CFR § 42.24**

Under the provisions of 37 CFR § 42.24(d), the undersigned hereby certifies that the word count for the foregoing Petition for *Inter Partes* Review totals 13,993 words, which is less than the 14,000 allowed under 37 CFR § 42.24.

Dated June 4, 2025

/Jennifer J. Huang/

W. Karl Renner, Reg. No. 41,265  
Jeremy J. Monaldo, Reg. No. 58,680  
Jennifer J. Huang, Reg. No. 64,297  
Kiersten Batzli, Reg. No. 75,476  
Fish & Richardson P.C.  
60 South Sixth Street, Suite 3200  
Minneapolis, MN 55402  
T: 202-783-5070  
F: 877-769-7945

(Control No. IPR2025-01103)

*Attorneys for Petitioner*

**CERTIFICATE OF SERVICE**

Pursuant to 37 CFR §§ 42.6(e)(4)(i) *et seq.* and 42.105(b), the undersigned certifies that on June 4, 2025, a complete and entire copy of this Petition for *Inter partes* Review, Power of Attorney, and all supporting exhibits were provided via Federal Express, to the Patent Owner by serving the correspondence address of record as follows:

Robinson Intellectual Property Law Office, P.C.  
3975 Fair Ridge Drive  
Suite 20 North  
Fairfax, VA 22033  
(571) 434-6789

/Crena Pacheco/

Crena Pacheco  
Fish & Richardson P.C.  
60 South Sixth Street, Suite 3200  
Minneapolis, MN 55402  
[pacheco@fr.com](mailto:pacheco@fr.com)