

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent of: Chi-Ming Kuo et al.
U.S. Patent No.: 9,774,916 Attorney Docket No.: 52472-0007IP1
Issue Date: September 26, 2017
Appl. Serial No.: 14/591,008
Filing Date: January 7, 2015
Title: INFORMATION CONCENTRATING CENTER CAPABLE
OF MAKING P2P CONNECTIONS WITH REMOTE
CLIENT DEVICES

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. 9,774,916 PURSUANT TO 35 U.S.C. §§311–319, 37 C.F.R. §42**

TABLE OF CONTENTS

I.	REQUIREMENTS FOR IPR—37 C.F.R. §42.104.....	1
A.	Grounds for Standing—37 C.F.R. §42.104(a).....	1
B.	Challenge and Relief Requested—37 C.F.R. §42.104(b)	1
II.	SUMMARY OF THE '916 PATENT	3
A.	Brief Description.....	3
B.	Prosecution of the '916 Patent	6
C.	Effective Filing Date of the Challenged Claims.....	7
III.	LEVEL OF ORDINARY SKILL	8
IV.	CLAIM CONSTRUCTION	9
V.	DETAILED EXPLANATION OF GROUNDS.....	9
A.	GROUND 1A: Lorex Manual in view of Kim941 Would Have Rendered Obvious Claims 1-8, 10, and 16.....	9
1.	<i>Lorex Manual</i>	<i>9</i>
2.	<i>Kim941</i>	<i>11</i>
3.	<i>The Lorex Manual-Kim941 Combination</i>	<i>13</i>
4.	<i>Application to Challenged Claims</i>	<i>17</i>
B.	GROUND 1B: – Lorex Manual in view of Kim941 and Kim517 would have rendered obvious claim 9	38
1.	<i>Kim517</i>	<i>38</i>
2.	<i>The Lorex Manual-Kim941-Kim517 Combination</i>	<i>39</i>
3.	<i>Application to Challenged Claims</i>	<i>41</i>
C.	GROUND 1C: Lorex Manual in view of Kuo would have rendered obvious claims 1-8, 10, and 16	43
1.	<i>Kuo</i>	<i>43</i>
2.	<i>The Lorex Manual-Kuo Combination</i>	<i>45</i>
3.	<i>Application to Challenged Claims</i>	<i>47</i>
D.	GROUND 1D: Lorex Manual in view of Kuo and Kim517 would have rendered obvious claim 9.....	53
E.	GROUND 2A: Lorex Video in view of Galvin and Kuo would have rendered obvious claims 1-8, 10, and 16	54
1.	<i>Lorex Video</i>	<i>54</i>
2.	<i>Galvin</i>	<i>56</i>
3.	<i>Kuo</i>	<i>56</i>
4.	<i>The Lorex Video-Galvin-Kuo Combination</i>	<i>57</i>
5.	<i>Application to Challenged Claims</i>	<i>59</i>

F.	GROUND 2B: Lorex Video in view of Galvin, Kuo, and Kim517 would have rendered obvious claim 9	77
1.	<i>The Lorex Video-Galvin-Kuo-Kim517 Combination</i>	77
2.	<i>Application to Challenged Claims</i>	77
VI.	DISCRETIONARY DENIAL IS NOT JUSTIFIED.....	77
VII.	PAYMENT OF FEES – 37 C.F.R. §42.103.....	80
VIII.	MANDATORY NOTICES UNDER 37 C.F.R §42.8(a)(1).....	80
A.	Real Party-In-Interest Under 37 C.F.R. §42.8(b)(1).....	80
B.	Related Matters Under 37 C.F.R. §42.8(b)(2)	80
C.	Lead And Back-Up Counsel Under 37 C.F.R. §42.8(b)(3).....	80
D.	Service Information	81

LIST OF EXHIBITS

EX1001	U.S. Patent No. 9,774,916 to Kuo et al. (“the ’916 Patent”)
EX1002	Prosecution History of the ’916 Patent (“the Prosecution History”)
EX1003	Declaration and Curriculum Vitae of Vlad Kardashov
EX1004	Prosecution History of U.S. Application Serial No. 13/293,506 (“the ’506 application”)
EX1005	Prosecution History of U.S. Application Serial No. 13/950,282 (“the ’282 application”)
EX1006	File History of U.S. Provisional Application Serial No. 61/924,240 (“the provisional application”)
EX1007	Lorex LH150 ECO4 Series Instruction Manual English Version 1.0 (2013), <i>available at</i> https://www.lorextechnology.com/downloads/security-dvr/LH150-Series/LH150_SERIES_MANUAL_EN_R1_web.pdf (“Lorex Manual”)
EX1008	U.S. Publication No. 2011/0082941 (“Kim941”)
EX1009	U.S. Publication No. 2014/0218517 (“Kim517”)
EX1010	Doherty et al., <i>Wireless Home Networking Simplified</i> (2007) (“Doherty”)
EX1011	U.S. Publication No. US2012/0198040 (“Kuo”)
EX1012	Lorex Technology Inc., “How to set up remote access for DVR using - Lorex Stratus Connectivity” (June 18, 2013), <i>available at</i>

<https://www.youtube.com/watch?v=fMPRi9WFuTM> (“Lorex Video”)

- EX1013 U.S. Publication No. 2012/0113265 (“Galvin”)
- EX1014 RESERVED
- EX1015 Complaint, *ThroughTEK Co. Ltd. v. Reolink Innovation Inc.*, Case No. 1:24-cv-00169 (D. Del.), Feb. 8, 2024
- EX1016 U.S. Publication No. 2007/0300261 (“Barton”)
- EX1017 U.S. Publication No. 2007/0097860 (“Rys”)
- EX1018 Stipulation and Proposed Order to Substitute Party Name, *ThroughTEK Co. Ltd. v. Reolink Innovation Inc.*, Case No. 1:24-cv-00169 (D. Del.), April 13, 2024
- EX1019 Lorex LNR300 netHD Series Instruction Manual English Version 1.0 (2013), *available at* https://www.lorextechnology.com/downloads/security-nvr/LNR300-Series/LNR300_SERIES_MANUAL_EN_R1_web.pdf
- EX1020 Ford et al., Peer-to-Peer Communication Across Network Address Translators, 2005 USENIX Annual Technical Conference, pp. 179-192 (“Ford”)

LISTING OF CLAIMS

<u>Claim Element</u>	<u>Language</u>
[1pre]	An electronic device for concentrating information, comprising:
[1a]	at least one first interface for receiving information from at least one information source;
[1b]	a second interface coupling to the Internet, for establishing a connection with a remote client device through the Internet;
[1c]	a third interface for connecting to a television for viewing said information; and
[1d]	a unique identification (UID) embedded in the electronic device for concentrating information,
[1e]	wherein the electronic device for concentrating information contacts at least one linking server through the Internet to register said embedded unique identification (UID) into the at least one linking server for identifying network addressing information of the electronic device for concentrating information so as to enable the remote client device to establish a P2P connection with the electronic device for concentrating information for viewing said information received by the electronic device for concentrating information;
[1f]	wherein the remote client device contacts the at least one linking server through the Internet according to said unique identification (UID) of the electronic device for concentrating information for establishing a P2P connection between the remote client device and the electronic device for concentrating information via the Internet,
[1g]	wherein at least one portion of the information received by the electronic device for concentrating information is delivered to the remote client device on the P2P connection,

<u>Claim Element</u>	<u>Language</u>
[1h]	wherein the remote client device does not have a unique identification (UID) to register in the at least one linking server for associating connecting information of the remote client device when the remote client device contacts the at least one linking server for establishing the P2P connection.
[2]	The electronic device for concentrating information according to claim 1, wherein the electronic device for concentrating information is a set top box.
[3]	The electronic device for concentrating information according to claim 1, wherein the remote client device is a portable electronic device.
[4]	The electronic device for concentrating information according to claim 1, wherein the remote client device is a mobile phone.
[5]	The electronic device for concentrating information according to claim 1, wherein the remote client device is not registered in the at least one linking server while the P2P connection is being established.
[6]	The electronic device for concentrating information according to claim 5, wherein the at least one linking server transmits hole-punching messages to the electronic device for concentrating information and the remote client device to establish the P2P connection.
[7]	The electronic device for concentrating information according to claim 1, wherein the second interface couples to the Internet through an external routing device or an internal routing device.
[8]	The electronic device for concentrating information according to claim 7, wherein the routing device is an IP router.
[9]	The electronic device for concentrating information according to claim 7, wherein the electronic device for concentrating information is connected to an appliance through the routing device and the remote client device controls the appliance through the electronic device for concentrating information.

<u>Claim Element</u>	<u>Language</u>
[10]	The electronic device for concentrating information according to claim 7, wherein the routing device has a wireless access point for connecting to a portable electronic device so as to deliver the information to the portable electronic device.
[16]	The electronic device for concentrating information according to claim 1, wherein the information is formatted by the electronic device for concentrating information in a way suitable for viewing by the remote client device.

Reolink Innovation Inc. and Shenzhen Reolink Technology Co., Ltd.

(collectively, “Petitioners” or “Reolink”) petition for *Inter Partes* Review (“IPR”) of claims 1-10 and 16 of U.S. Patent 9,774,916 (“the ’916 Patent”).

I. REQUIREMENTS FOR IPR—37 C.F.R. §42.104

A. Grounds for Standing—37 C.F.R. §42.104(a)

Petitioners certify that the ’916 Patent is available for IPR, and Petitioners are not barred or estopped from requesting IPR.

B. Challenge and Relief Requested—37 C.F.R. §42.104(b)

Petitioners request IPR on grounds 1A-2B listed below. An expert declaration from Vlad Kardashov supports each ground. *See* EX1003.

<u>Ground</u>	<u>Claims</u>	<u>Basis for Rejection</u>
1A	1-8, 10, 16	§103 – Obvious based on Lorex Manual (EX1007) in view of Kim941 (EX1008)
1B	9	§103 – Obvious based on Lorex Manual in view of Kim941 and Kim517 (EX1009)
1C	1-8, 10, 16	§103 – Obvious based on Lorex Manual in view of Kuo (EX1011)
1D	9	§103 – Obvious based on Lorex Manual in view of Kuo and Kim517
2A	1-8, 10, 16	§103 – Obvious based on Lorex Video (EX1012) in view of Galvin (EX1013) and Kuo
2B	9	§103 – Obvious based on Lorex Video in view of Galvin, Kuo, and Kim517

Grounds 1A-2B rely on publications that all qualify as prior art under 35

U.S.C. §102 as shown below:

<u>Reference</u>	<u>Prior Art Status</u>
Lorex Manual	§102(a)(1) – published in 2013 ¹
Kim941	§102(a)(1) – published April 7, 2011
Kim517	§102(a)(2) – filed December 13, 2013
Kuo	§102(a)(1) – published August 2, 2012
Lorex Video	§102(a)(1) – published June 18, 2013 ²
Galvin	§102(a)(1) – published May 10, 2012

As detailed below (*infra* § II.C), the '916 Patent is plainly not entitled to the earliest alleged priority date identified on the face of the patent (November 10, 2011), and Patent Owner expressly admitted this fact during prosecution of the '916 Patent. At best, the Challenged Claims are entitled to an effective filing date no earlier than January 7, 2014—the filing date of U.S. Provisional Application

¹ See EX1007, 1 (dated “2013”); EX1003, ¶¶53-60 (sworn testimony confirming public accessibility and dissemination of Lorex Manual by 2013).

² See EX1012 (dated “June 18, 2013”); EX1003, ¶¶53-60 (sworn testimony confirming public accessibility and dissemination of the Lorex Video in June 2013).

No. 61/924,240 (EX1006).³ For that reason, the publications cited in Grounds 1A-2B qualify as prior art.

II. SUMMARY OF THE '916 PATENT

A. Brief Description

The '916 Patent describes techniques for establishing a P2P⁴ connection over the Internet between an information concentrating center (e.g., a set top box)

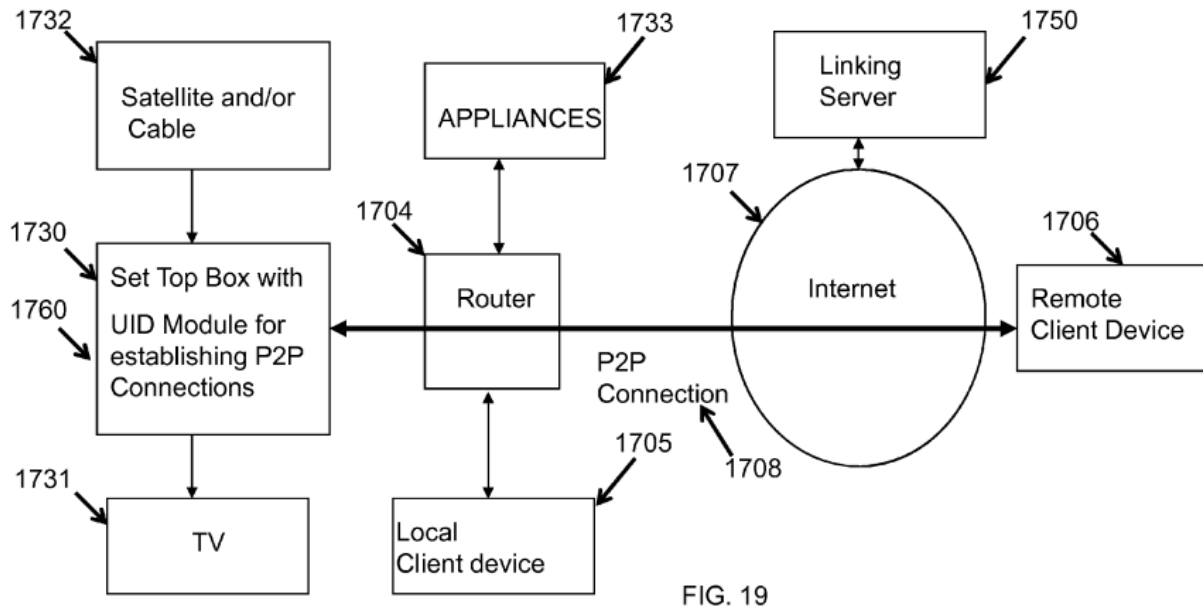
³ Moreover, because the claims recite features that were not described in the '916 Patent's priority applications until at least the January 7, 2014 provisional, the claims should have been examined under the first inventor-to-file provisions of post-AIA § 102. The Patent Owner, however, oddly omitted this fact when filing the application data sheet—contrary to the requirements of 37 C.F.R. § 1.78(d)(6). As such, the application was mistakenly examined under “pre-AIA” provisions. *See* EX1002, 226.

⁴ The '916 Patent uses the term “P2P” as shorthand for “point-to-point.” *See* EX1001, 1:43-54, 12:52. “Point-to-point” is often used interchangeably in the art with “peer-to-peer,” and both are represented by the “P2P” shorthand. The evidence here confirms that the '916 Patent's “point-to-point” connections established over the Internet plainly include conventional “peer-to-peer” connections.

and a client device (e.g., a mobile phone). EX1001, 1:37:53; EX1003, ¶¶28-32.

The information concentrating center has a unique identification (UID) that it registers with a “linking server,” which assists in forming the P2P connection between the information concentrating center and the client device. EX1001, 1:63-67, 13:53-14:57, FIG. 19; EX1003, ¶29. This allows the client, which is not registered in the linking server, to send a request to the linking server with the UID for the information concentrating center so that the linking server can then send “hole punching” messages to both the client and the identified information concentrating center to establish the P2P connection. EX1001, 2:1-11; EX1003, ¶29. The ’916 Patent nonetheless acknowledges “that there are many ways to establish P2P connection ... through the Internet, and [the] present invention is not limited to the ways of establishing the P2P connections.” EX1001, 14:51-57; EX1003, ¶29.

FIG. 19 illustrates the topology of an example network including the remote client device 1706, set top box 1730, and linking server 1750. EX1001, FIG. 19; EX1003, ¶30.



EX1001, FIG. 19.

The specification of the '916 Patent explains that conventional techniques for establishing P2P connections implicated complex protocols such as dynamic domain name system (DDNS), port mapping, and universal plug and play (UPnP). EX1001, 12:19-30; EX1003, ¶31. Purportedly, the “present invention” reduces these complexities through use of a linking server that supports the establishment of a P2P connection between the information concentrating center and the remote client device. EX1001, 12:47-62; EX1003, ¶31. As demonstrated by the grounds in this Petition, however, the use of a “linking server” to establish P2P connections was not new or even innovative before the earliest effective filing date of the '916 Patent (Jan. 7, 2014). Kim941 and Kuo, for example, both confirm that this was a

conventional approach that was well-known in the art before the '916 Patent.

EX1003, ¶32.

B. Prosecution of the '916 Patent

During prosecution, Patent Owner made several admissions relevant to the Challenged Claims when responding to the Examiner's rejections in at least four Office actions. EX1003, ¶¶33-42. For example, regarding the claimed "unique identification (UID)," Patent Owner argued that "the unique identification (UID) is NOT a network address, such as an IP address" but rather is "used for identifying a network address such as an IP address." *Id.*, 217. Patent Owner also contested the Examiner's mapping of a prior art mobile phone to the claimed "information concentrating center," asserting that "a skilled person in the art WOULD NOT think of the wireless device/MOBILE PHONE as an information concentrating center such as a set top box in the first place." *Id.*, 87.

Following several rounds of rejections and responses, the Examiner agreed to allow the claims on June 27, 2017. EX1002, 7-17. The Examiner's notice of allowance included an Examiner's amendment in which the term "information concentrating center" was replaced in the claims with the term "electronic device for concentrating information." *Id.* The Examiner's amendment also added Element [1h] to independent claim 1, which requires that "the remote client device does not have a unique identification (UID) to register in the at least one linking

server for associating connecting information of the remote client device when the remote client device contacts the at least one linking server for establishing the P2P connection.” *Id.*

Notwithstanding these amendments, Grounds 1A-2B of this Petition confirm that the Challenged Claims should not have been allowed. EX1003, ¶42.

C. Effective Filing Date of the Challenged Claims

The ’916 Patent was filed January 7, 2015, and claims priority to a provisional application (EX1006) filed January 7, 2014. *See* EX1001, 1:8-14. Additionally, the ’916 Patent claims to be a “continuation-in-part” of two utility applications: (1) U.S. Serial No. 13/950,282 (EX1005) filed July 25, 2013, and (2) U.S. Serial No. 13/293,506 (EX1004) filed November 10, 2011. Those earlier continuation-in-part parents do not include any teaching from FIGS. 17-19 of the ’916 Patent and are lacking any teaching of several elements recited in Claim 1. EX1003, ¶¶33-34.

To be clear, the Challenged Claims recite multiple limitations that were disclosed no earlier than the January 7, 2014 filing of the provisional application, and are therefore entitled to a priority date no earlier than January 7, 2014. EX1003, ¶34. For example, Elements [1a]-[1c] require that the claimed “electronic device *for concentrating information*” must include three specific types of interfaces—including a “third interface *for connecting to a television for viewing*

said information.” EX1001, 15:7-13. Such a device was absent from the earlier continuation-in-part parent cases, and instead the first (arguable) mention of any electronic device “for concentrating information” that also has an “interface for connecting to a television for viewing said information” was not until FIGS. 1-3 of the provisional application were filed on January 7, 2014. EX1006, FIGS. 1-3; EX1003, ¶¶35-36. This disclosure from FIGS. 1-3 of the provisional application then appeared as FIGS. 17-19 (and in columns 13-14) of the ’916 Patent. EX1001, 12:63-13:41 and 13:53-14:9; EX1003, ¶36.

Significantly, Patent Owner conceded during prosecution that the embodiment in FIG. 19 was relied upon for support of claim 1. To justify support for the amendments to claim 1, Patent Owner specifically pointed to “FIG. 19” and related text of the ’916 Patent—which is found only in the January 7, 2014 provisional (i.e., provisional FIG. 3) and not in the earlier continuation-in-part applications. EX1002, 85, 211, 215, 216; EX1003, ¶¶37-39.

III. LEVEL OF ORDINARY SKILL

A POSITA in the field of the ’916 Patent would have had a bachelor’s degree in electrical engineering and two years of work experience with network and communication technologies. EX1003, ¶¶12-14.

IV. CLAIM CONSTRUCTION

All claim terms should be construed according to the *Phillips* standard.

Phillips v. AWH Corp., 415 F.3d 1303 (Fed. Cir. 2005); 37 C.F.R. §42.100. Here, given the noticeable overlap between the preferred embodiment of the '916 Patent and the prior art/predictable combinations articulated in Grounds 1A-2B, Petitioners submit that no claim elements need a formal construction for purposes of resolving controversies in this proceeding. *Wellman, Inc. v. Eastman Chem. Co.*, 642 F.3d 1355, 1361 (Fed. Cir. 2011); *Google Inc. v. Intellectual Ventures II LLC*, 701 Fed. Appx. 946, 956 (Fed. Cir. 2017) (“do not require construction” for purposes of “resolv[ing] the parties’ patentability arguments”); EX1003, ¶¶43-44.

V. DETAILED EXPLANATION OF GROUNDS

A. GROUND 1A: Lorex Manual in view of Kim941 Would Have Rendered Obvious Claims 1-8, 10, and 16

1. Lorex Manual

Similar to the '916 Patent, Lorex Manual describes techniques for establishing a peer-to-peer (P2P) connection between an information concentrating center (e.g., a digital video recorder (DVR) for a home security system) and a remote client device (e.g., a smartphone, tablet, or PC). EX1007, 57-62, 84-117; EX1003, ¶¶45-49. The P2P connection allows a user to stream video and remotely access additional information from the DVR. EX1003, ¶46. The following

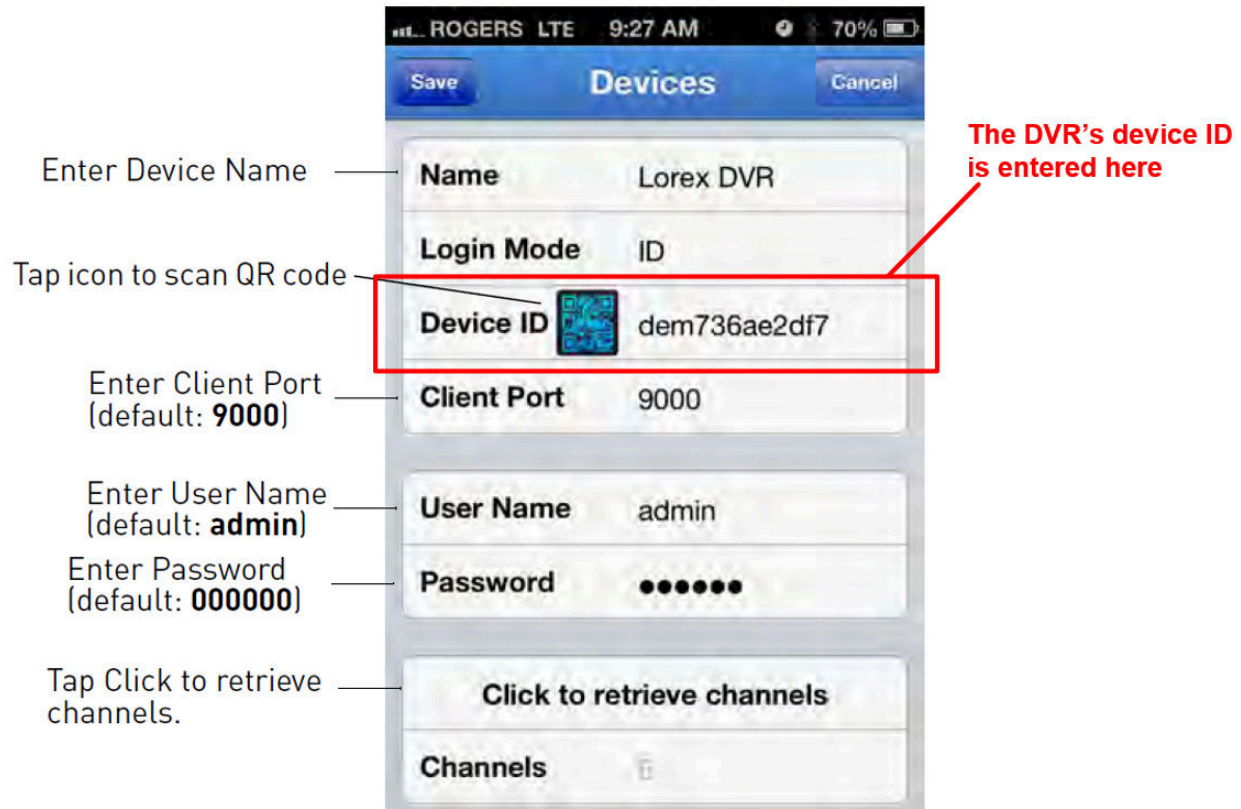
screenshot, for example, shows live video feeds from eight cameras streamed from the DVR to a remote PC over a “P2P” connection:



EX1007, 61.

Lorex Manual explains that the DVR includes a “device ID” that serves as “a unique code that allows your system to handshake with the Lorex servers for connection over the Internet.” EX1007, 58; EX1003, ¶48. The user’s smartphone, tablet, or PC uses the device ID to initiate a process for establishing a direct P2P connection with the DVR. EX1007, 61-62; *see also* 10, 84; EX1003, ¶48. By submitting the device ID and additional login information through a user interface

at the smartphone, tablet, or PC (like that shown below), the smartphone, tablet, or PC can remotely log into the DVR to stream live or recorded video:



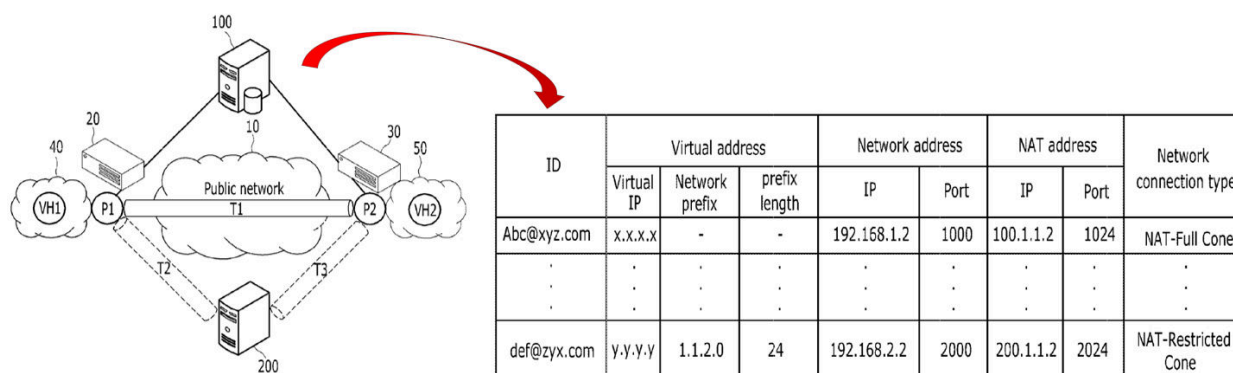
EX1007, 85 (annotated).

2. *Kim941*

Kim941 is like Lorex Manual in that both references describe systems that establish P2P connections between devices. EX1007, 61-62; EX1008, [0018]-[0020]; EX1003, ¶¶61-62. Although Lorex Manual does not expressly disclose many of the back-end details involved in setting up the P2P connection between its DVR and a remote client device (e.g., the smartphone, tablet, or PC), Kim941 describes a conventional process for establishing P2P connections that involve

registering a device's unique ID with a server and configuring the server to use the unique ID to provide each peer with appropriate network address information of the other peer so that the peers can perform hole-punching and establish the P2P connection. EX1003, ¶61.

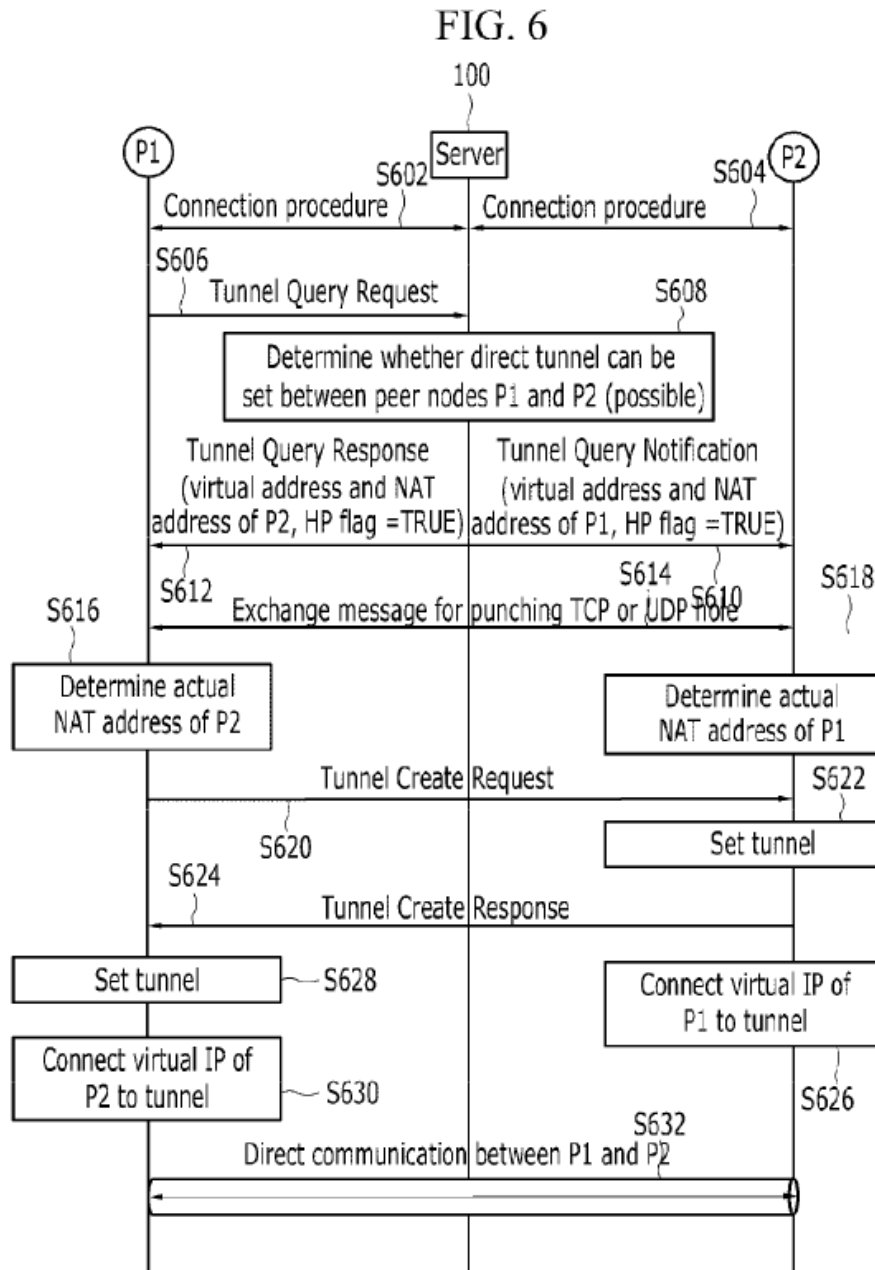
In more detail, Kim941 describes a pair of peer nodes P1 and P2) that register with a server 100 by providing the server 100 with their respective unique IDs and address information (e.g., virtual address, network address, NAT address). EX1008, ¶[0055]; EX1003, ¶61. The server maintains a database of registered peer nodes in which the unique ID for each peer node is mapped to corresponding address information for that node. EX1008, ¶[0055]; EX1003, ¶61.



EX1008, FIGS. 1 and 5 (annotated), [0075].

Once registered, peer nodes maintain a connection to server 100 or later re-connect to server 100 to make themselves available for P2P connections. EX1008, [0078]-[0079], FIG. 6 (“S602”, “S604”); *see also id.*, FIG. 2 (“S210”), [0013], [0055]-[0060], [0080]-[0084], [0122]-[0123]; EX1003, ¶62. FIG. 6 illustrates a

process by which the server 100 performs hole-punching to facilitate the setup of a P2P connection between peer nodes P1 and P2:



EX1008, FIG. 6

3. *The Lorex Manual-Kim941 Combination*

For multiple reasons articulated below, a POSITA would have been motivated to implement Lorex Manual in accordance with Kim941's suggested use of a network server for device registration and hole-punching techniques for establishing P2P connections. EX1003, ¶71. Applying Kim941's teachings to Lorex Manual would have predictably allowed Lorex Manual's DVR to register its unique "device ID" with a network server so that a remote client device (e.g., the user's smartphone, tablet, or PC) can then identify the DVR as the target of a requested P2P connection using the unique ID that has been registered with the server. *Id.*

For instance, consistent with the teachings of Kim941, the remote client device in a predictable Lorex Manual-Kim941 combination would use the DVR's device ID to obtain network address information for the DVR from the network server and the server would then initiate hole-punching to permit the remote client device and DVR to establish a P2P connection with each other. EX1003, ¶72. In the combination, Lorex Manual's DVR would contact Lorex servers in accordance with Kim941's teachings to register its device ID, and the remote client device would subsequently contact the Lorex servers with the DVR's device ID to establish a P2P connection with the DVR. EX1008, [0078]-[0089], FIG. 6; EX1003, ¶72.

Multiple reasons would have prompted a POSITA to implement Lorex Manual in accordance with Kim941's suggested device registration and hole-punching techniques. EX1003, ¶¶71-78.

First, a POSITA would have understood that implementing Lorex Manual's system to include a conventional "network server" that facilitates hole-punching (as suggested by Kim941) would provide an improved and advantageous approach for establishing a P2P connection between the DVR and remote client device when the DVR is located behind a firewall and/or network address translator (NAT) that would otherwise prevent the remote client device from initiating a P2P connection with the DVR (e.g., due to common security policies of firewalls/NATs that block unsolicited inbound communications from devices outside of the DVR's local network). EX1003, ¶74 (corroborated by EX1020); EX1008, [0018]-[0019], [0121].

Second, a POSITA would have been motivated to implement Lorex Manual to include Kim941's suggested use of a network server and hole punching for connecting the remote client device (e.g., the user's smartphone, tablet, or PC) to Lorex Manual's DVR because Kim941's network server can conveniently work with an "existing application" like Lorex Manual's "ECO Stratus" app to advantageously "construct[] a direct communication environment for ... a video

camera.” EX1008, [0123] (“very effective for constructing a service environment such as ... P2P”); EX1003, ¶75.

Third, a POSITA would have implemented Lorex Manual’s system to include a “network server” that uses hole-punching (as suggested by Kim941) to predictably form a “direct communication environment of an IP level” between Lorex Manual’s DVR and the user’s remote client device—and particularly in a manner that renders it “unnecessary for each application service to form a special session,” thereby improving “flexibility” in “operating each service.” EX1008, [0122]; EX1003, ¶76.

Fourth, implementing Lorex Manual’s system to include a network server that uses hole-punching while also using registered “connection type” information from a peer (as suggested by Kim941) would beneficially allow the server to confirm whether a direct tunnel can be formed between the IP camera and user’s/terminal device. EX1008, [0078]-[0083], [0094]-[0099], [0014]-[0018], FIGS. 6, 8; EX1003, ¶77. Indeed, the application of Kim941’s techniques are consistent with and would have furthered Lorex Manual’s goal of establishing a P2P connection between a DVR and a remote client device. EX1008, 62. A POSITA would have appreciated that, in the combination, Kim941’s network server and hole-punching techniques would improve Lorex Manual’s system by ensuring that the DVR and remote client device could establish a P2P connection

in wide range of circumstances such as where the DVR and remote client device are located behind firewalls/NATs and/or where the DVR and remote client devices require either the same or different connection types. EX1008, [0006]-[0007], [0014].; EX1003, ¶77.

Finally, both Lorex Manual and Kim941 are directed to establishing P2P connections between network endpoints (e.g., Lorex Manual's DVR and remote client device), and in this context, a POSITA would have possessed ample skill to successfully implement the combination as described above. EX1003, ¶78. Considering the predictable electrical/network and software components involved in the combination and the relatively advanced state of the art at the time, a POSITA would have reasonably expected success achieving the combination before the earliest effective filing date of the '916 Patent (Jan. 7, 2014). EX1003, ¶78.

4. *Application to Challenged Claims*

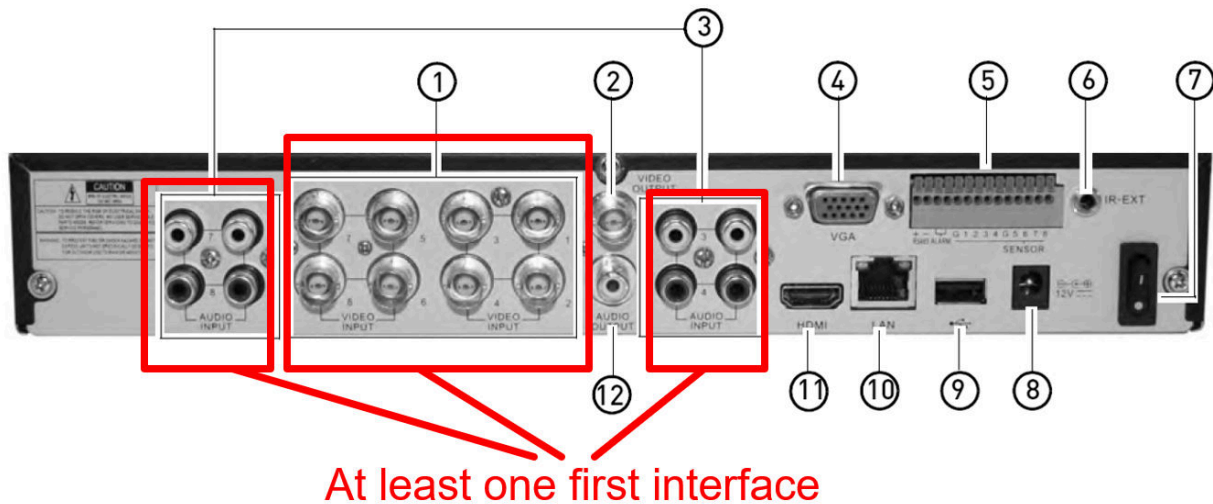
Element [1pre]

Even if the preamble is treated as a limitation (which Petitioners do not concede), the Lorex Manual-Kim941 combination provides the recited “electronic device for concentrating information.” EX1003, ¶¶79-82. For example, Lorex Manual discloses an *electronic device* (e.g., a DVR) that *concentrates information* (e.g., video streams) from one or more cameras of a security system. EX1007, 5;

EX1003, ¶81. Lorex Manual describes both an 8-channel DVR having eight video input ports and a 16-channel DVR having sixteen video inputs ports for receiving respective video streams from up to eight or sixteen connected cameras, respectively. EX1007, 5-6; EX1003, ¶81.

Element [1a]

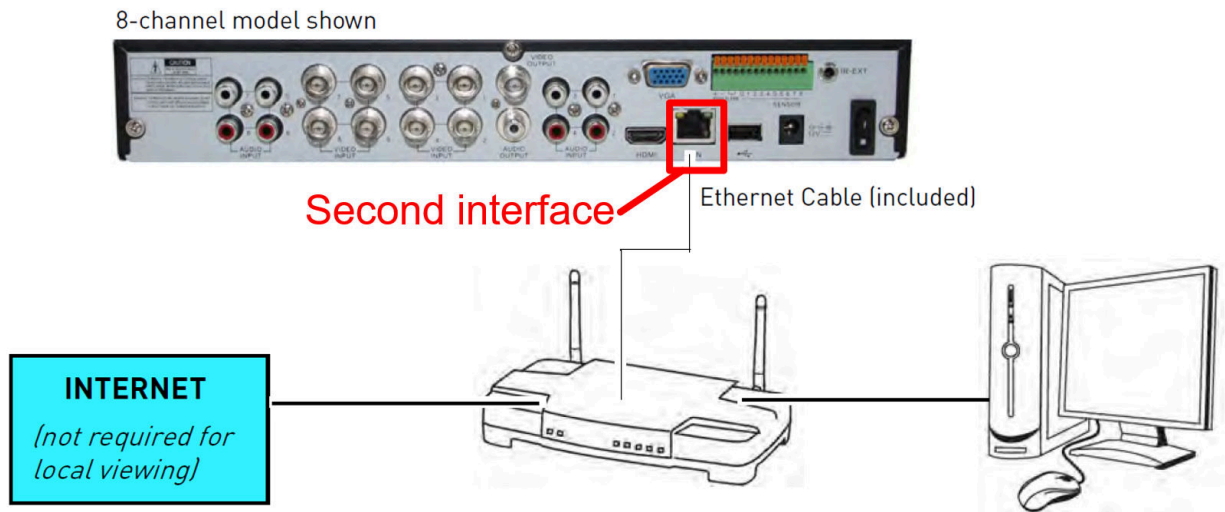
The Lorex Manual-Kim941 combination provides Element [1a]. EX1003, ¶¶83-85. As discussed above (*see* [1pre]), the DVR described in Lorex Manual includes video input ports (***at least one first interface***) configured to connect to up to eight or sixteen video cameras as information sources for video data (***at least one information source***). EX1007, 5 (“1 Video Input; Connect up to 8 BNC cameras”; “3 Audio Input: Connect up to 8 RCA audio-enabled cameras”), 6; EX1003, ¶83. The DVR also includes audio input ports for receiving audio signals from audio-enabled cameras, as another example of the claimed “***at least one first interface***.” EX1007, 5-6; EX1003, ¶83. The video and audio input ports of Lorex Manual’s 8-channel DVR are shown below:



EX1007, 5 (annotated).

Element [1b]

The Lorex Manual-Kim941 combination provides Element [1b]. EX1003, ¶¶86-89. For example, Lorex Manual discloses that the DVR includes a local area network (LAN) port (*a second interface*) that receives one end of an ethernet cable for connecting the DVR to an Internet router. EX1007, 5-6, 7 (“Connect an ethernet cable...to the LAN port...Connect the other end of the ethernet cable to a router on your network.”); EX1003, ¶86. Lorex Manual also teaches that the router connected via the ethernet cable to the LAN port of the DVR connects to the Internet. EX1007, 58; EX1003, ¶84. A network topology of the DVR connected to the Internet and a remote client device (e.g., a smartphone, tablet, or PC) via the router is shown below:



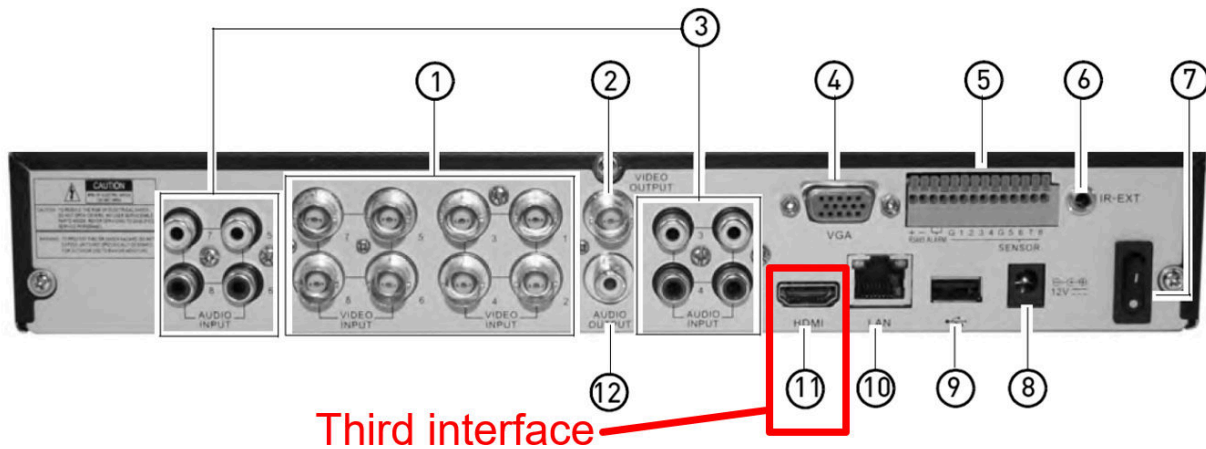
EX1007, 5 (annotated).

Lorex Manual also discloses that a *remote client device* (e.g., a smartphone, tablet, or PC) can connect to the DVR over the Internet to remotely stream video from the cameras connected to the DVR or from video recorded or otherwise stored on the DVR. EX1007, 84 (“You can remotely view camera streams from your DVR on compatible mobile phones and tablets.”), 5, 7, 58; EX1003, ¶87. Lorex Manual explains that this remote connection is achieved by connecting the LAN port (*second interface*) of the DVR to an Internet router using an Ethernet cable. EX1007, 84; EX1003, ¶87.

Element [1c]

The Lorex Manual-Kim941 combination would have rendered obvious Element [1c]. EX1003, ¶¶90-92. The DVR of Lorex Manual includes a high-definition multimedia interface (HDMI) port for connecting to a *television* for

viewing *information* that is concentrated by the DVR. EX1007, 5, 8; EX1003, ¶90. Specifically, Lorex Manual discloses that an HDMI cable can connect the HDMI port of the DVR to a *television*. EX1007, 5, 8 (“Connect the included HDMI cable from the HDMI port to the TV or monitor.”); EX1003, ¶90. The third interface of Lorex Manual’s DVR is illustrated below.



EX1007, 5 (annotated).

Lorex Manual also discloses that the *television* connected to the *third interface* (e.g., HDMI port) of the DVR can display *information* (i.e., video data) concentrated by the DVR. EX1007, 15; EX1003, ¶91. For example, Lorex Manual describes a remote control that can control an interface displayed by the television to play back video recordings. EX1007, 15 (“Press 0 three times to show the mouse cursor on the BNC monitor or the monitor connected with HDMI... In Playback Mode, press to play video.”); EX1003, ¶91. Consequently, Lorex Manual discloses that the DVR includes a *third interface* (i.e., HDMI port) for connecting

to a *television* for viewing *information* (i.e., video) concentrated by the DVR.

EX1007, 5, 8, 15; EX1003, ¶91.

Element [1d]

The Lorex Manual-Kim941 combination provides Element [1d]. EX1003, ¶¶93-96. The *electronic device* (e.g., DVR) of Lorex Manual includes a “device ID.” EX1007, 58-60, 85, 93; EX1003, ¶93. Lorex Manual explains that this device ID is a “unique code” that represents a *unique identification (UID)* of the DVR. EX1007, 58; EX1003, ¶93.

The device ID of the DVR is physically *embedded* in the DVR by a label attached to a housing of the DVR. EX1007, 58; EX1003, ¶94. This label contains the device ID printed in standard characters and encoded in a quick-response (QR) code. EX1007, 85; EX1003, ¶94.

In addition to its physical embedding via the label affixed to the DVR housing, the device ID is digitally *embedded* in the DVR that allows other devices to connect with the DVR over the Internet using the device ID. EX1007, 58; EX1003, ¶95. Kim941 likewise discloses that a peer node can include an ID that is digitally *embedded* in the peer node. EX1008, [0056]; EX1003, ¶95. Kim941 explains that this ID is unique and “distinguishes” the peer node. EX1008, [0056]; EX1003, ¶95. Further, in the predictable Lorex Manual-Kim941 combination, the device ID is embedded in the peer node to permit the peer node to register with a

conventional hole-punching server using the device ID. *Supra*, §V.A.3; EX1003, ¶95.

Element [1e]

The teachings of Lorex Manual in view of Kim941 would have rendered obvious Element [1e]. EX1003, ¶¶ 97-101. To start, Lorex Manual describes a cloud connectivity service – referred to as “Lorex Stratus Connectivity” – that allows a ***remote client device*** (e.g., a computer, tablet, or mobile device) to connect to the DVR over the Internet. EX1007, 10; EX1003, ¶97. This cloud connectivity service creates a connection between the ***remote client device*** and the DVR through a “secure handshake” between the ***remote client device*** and Lorex’s Stratus servers. EX1007, 10; EX1003, ¶97. The Stratus servers represent ***at least one linking server*** that are separate from the DVR and the ***remote client device*** and can facilitate an Internet connection (e.g., a “link”) between the DVR and the ***remote client device***. EX1007, 10; EX1003, ¶97.

Lorex Manual explicitly discloses that the connection between the ***remote client device*** and the DVR can be a peer-to-peer (P2P) connection. EX1007, 62; EX1003, ¶98. When a P2P connection is established, the ***remote client device*** can display information (e.g., video) streaming directly from the DVR to the ***remote client device***. EX1007, 62; EX1003, ¶98. Lorex Manual distinguishes this direct P2P connection from a relay (RLY) connection in which the ***remote client device***

receives information from the DVR through the Lorex servers and indicates that the relay connection is “only used when a direct connection cannot be made between the DVR and the computer. EX1007, 62, 87-90; EX1003, ¶98.

Lorex Manual explains that the *remote client device* (e.g., a computer, tablet, or mobile device) uses the *unique identification (UID)* (e.g., device ID) of the DVR to perform a secure handshake with the Stratus servers to establish a connection with the DVR over the Internet. EX1007, 10, 57-59; EX1003, ¶99. Lorex Manual’s *remote client device* performs this secure handshake with the Stratus servers using a message that includes the device ID of the DVR. EX1007, 59, 85, 93; EX1003, ¶99.

To the extent Lorex Manual does not expressly disclose that the DVR contacts the Stratus servers to register the device ID, these operations would have been predictably provided by the Lorex Manual-Kim941 combination. EX1003, ¶100; *supra*, §V.A.3. Kim941, for example, expressly describes a peer node that contacts a linking server 100 to register a unique ID with the server. EX1008, [0055] (“in order to register information such as an ID and a password to the server 100, the peer node P1 transmits a registration request message including an ID and a password to the server 100.”), [0056]-[0060], FIG. 2; *supra*, §V.A.2; EX1003, ¶100. This allows server 100 to facilitate hole punching and the establishment of a P2P connection between the peer node and another peer node

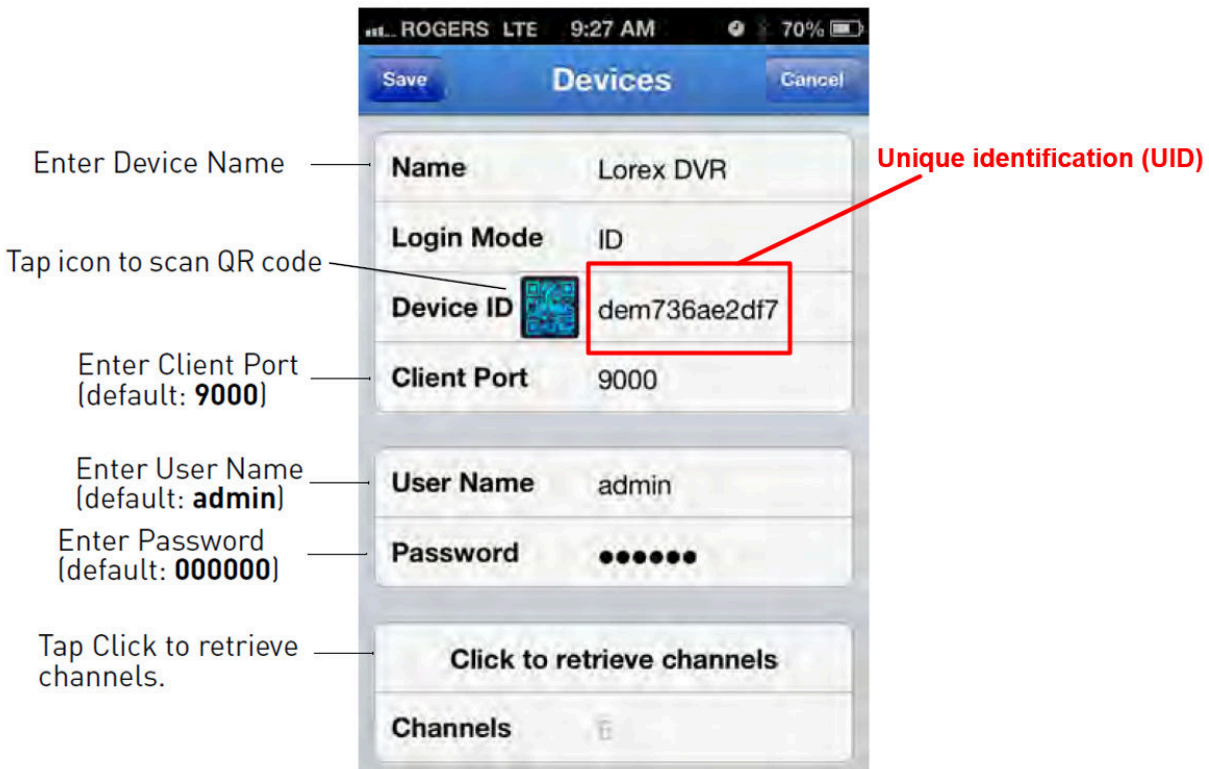
based on the unique ID. EX1008, [0081]; *see also id.*, [0078]-[0089], FIG. 6; EX1003, ¶100. In the combination, Lorex Manual's DVR would predictably contact the Stratus servers (*at least one linking server*) to register its embedded "device ID" consistent with Kim941's teachings. *Supra*, §V.A.3; EX1003, ¶100.

Element [1f]

The teachings of Lorex Manual in view of Kim941 would have rendered Element [1f] obvious.⁵ EX1003, ¶¶102-104. Lorex Manual discloses that a *remote client device* (e.g., smartphone, tablet, or PC) can use the *unique identification* (e.g., the "device ID") of the DVR to identify a particular DVR as the target for a P2P connection. EX1007, 58-59, 61, 62, 85; EX1003, ¶102. An example login page from an iPhone in the Lorex Manual is illustrated below, which includes the

⁵ Petitioners note that Element [1f]—as well as [1h], [3], [4], [5], [6], [8] and [10]—are recitations of intended use that do not further define the structure of the "electronic device for concentrating information" as recited in the preamble. The features recited in these claim elements therefore are not entitled to patentable weight and do not contribute to the patentability of any Challenged Claim. The prior art combinations applied in the grounds of this Petition nonetheless provide these features and confirm that the Challenged Claims would have been obvious even if these claim features were given patentable weight (which they should not).

device ID of the DVR obtained by scanning a QR code on the DVR using the iPhone's built-in camera:



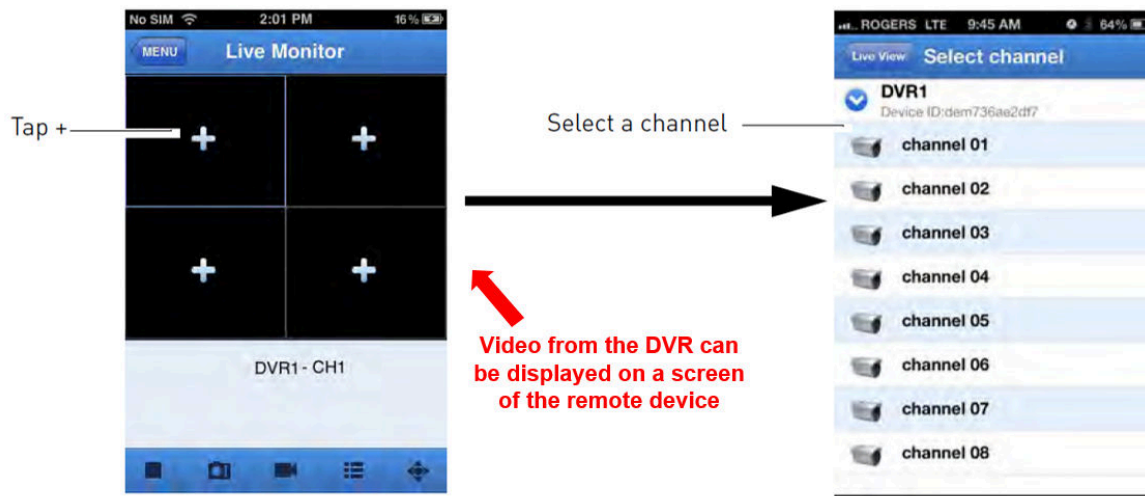
EX1007, 59 (annotated).

Kim941 further describes conventional techniques for a remote client device to contact at least one linking server through the Internet according to a unique identification of another device to establish a P2P connection between the remote client device and the other device via the Internet. *Supra*, §V.A.2; EX1003, ¶103. For example, Kim941 discloses that “in order to perform direct communication with the peer node P2, the peer node P1 performs a process of setting a tunnel with the peer node P2.” EX1008, [0080]. “In order to set a tunnel for performing direct

communication with the peer node P2, the peer node P1 transmits a tunnel query request message to the server 100 (S606)” that “includes an ID of the peer node P2.” *Id.*, [0081]; *see also id.*, [0082]-[0089], FIG. 6. For the reasons articulated above, it would have been obvious to apply Kim941’s suggested techniques for establishing a P2P connection to the system described by Lorex Manual. *Supra*, §V.A.3. In the Lorex Manual-Kim-971 combination, the remote client device (e.g., smartphone, tablet, or PC) would predictably contact the Lorex Servers (e.g., *at least one linking server*) to initiate a P2P connection with the DVR by sending a tunnel query request message that includes the DVR’s unique device ID consistent with the teachings of Kim941. EX1003, ¶103.

Element [1g]

The Lorex Manual-Kim941 combination provides Element [1g]. EX1003, ¶¶105-107. Lorex Manual expressly teaches that the *remote client device* (e.g., smartphone, tablet, or PC) receives *information* (e.g., video streams) from the *electronic device for concentrating information* (e.g., DVR). EX1007, 84 (“You can remotely view camera streams from your DVR on compatible mobile phones and tablets.”), 86-87; EX1003, ¶105. For example, Lorex Manual shows how a user of the remote client device can navigate a user interface of a mobile device to view live video from each of eight video channels:



EX1007, 86-87 (annotated).

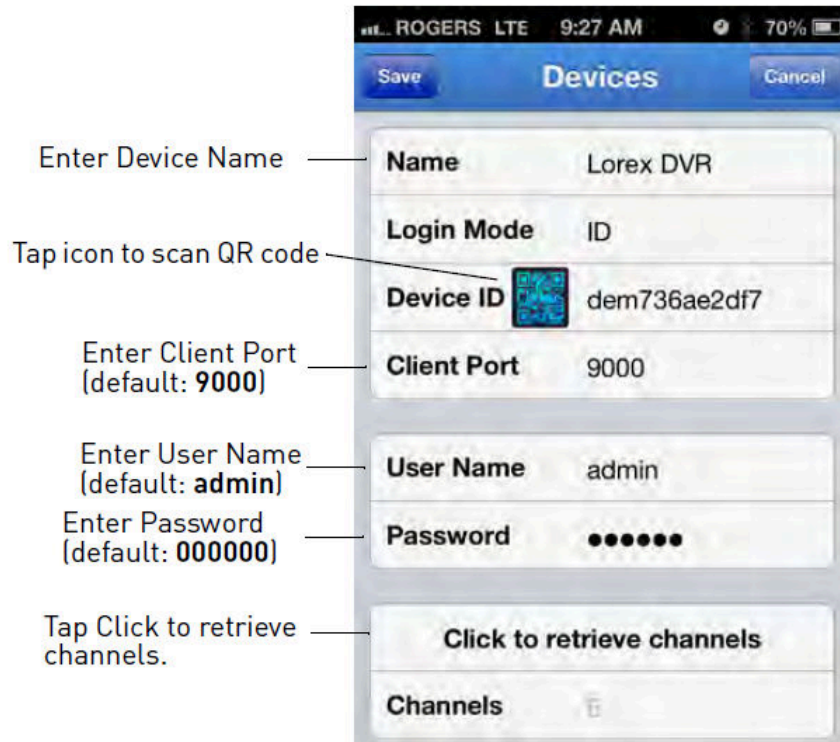
As described above in connection with Element [1a], these eight video channels represent the different video inputs to the eight input ports on the DVR. EX1007, 5, 86-87; EX1003 ¶106. The remote client device receives this data from the DVR over the P2P connection established between the remote client device and the DVR. EX1007, 10, 61, 62; EX1003 ¶106. Consequently, Lorex Manual discloses that at least a portion of the video data received by the DVR is delivered to the remote client device via a P2P connection. EX1003 ¶106.

Element [1h]

The teachings of Lorex Manual in view of Kim941 would have rendered Element [1h] obvious. EX1003 ¶¶108-113. For example, Lorex Manual teaches that a remote client device can use the DVR's device ID and other information corresponding to the DVR to perform a secure handshake with Lorex servers and

establish a P2P connection with the DVR. EX1007, 61, 62, 84-85; EX1003 ¶108.

Lorex Manual shows a user interface screen containing information used to perform the secure handshake:



EX1007, 85.

According to the Lorex Manual, the mobile device initiates a request to connect with the DVR by entering the device ID of the DVR, the client port of the DVR, and a username and password associated with the DVR. EX1007, 85; EX1003, ¶109.

To the extent that Lorex Manual does not expressly disclose that the mobile device does not have a UID to register with the Lorex servers when the remote

client device contacts the servers to connect, such conventional features would have been obvious to a POSITA when considering the teachings of Kim941. EX1003, ¶110. Kim941 teaches that peer nodes (e.g., P1 and P2) **pre-register** their IDs with a server before one of the peer nodes contacts the server for establishing a P2P connection. EX1008, [0055] (“in order to register information such as an ID and a password to the server 100, the peer node P1 transmits a registration request message including an ID and a password to the server.”), [0056]-[0060], FIG. 2; EX1003 ¶110.

Later, when one of the peers (e.g., P1) contacts the server 100 to establish a P2P connection with another peer (e.g., P2),⁶ the first peer **does not** have a unique ID to register in the server 100. EX1003 ¶111. As an initial matter, a POSITA would have understood and it would have been obvious that there is no need for the first peer to register with the server merely to request a P2P connection with the second peer since the server need only look-up registered information (e.g., the ID and network address(es)) of the second peer—not the first peer—to perform hole-

⁶ Note that Element [1h] recites an intended use of the remote client device (not any structure of the claimed “electronic device” in the preamble) *at this later time frame*—“when the remote client device contacts the at least one linking server for establishing the P2P connection.”

punching and follow the process shown in FIG. 6. *Id.* Moreover, Kim941 expressly contemplates that peers register with the server in advance such that the first peer does ***not*** provide its unique ID for registration again when it ***later*** contacts the server 100 to establish the P2P connection. EX1008, [0079]-[0087], FIG. 6; *see* FIGS. 5 (showing peers pre-registered with server 100) and 7. Indeed, Kim941 expressly discloses that the first peer’s “tunnel query request message” includes the unique ID of the second peer rather than that of the first peer to identify the second peer as the device to which the first peer requests to connect. EX1008, [0081], FIG. 6.

For the reasons articulated above in §V.A.3, it would have been obvious to apply Kim941’s procedures for registration and establishing a P2P connection to the system described in Lorex Manual. In this combination, Lorex’s remote client device would predictably not include its own device ID for registration when contacting the Lorex Stratus servers to establish a P2P connection with the DVR. EX1003, ¶112.

Claim [2]

Lorex Manual describes a DVR, which constitutes an “***electronic device for concentrating information***” for the reasons addressed above with respect to Element [1pre]. *Supra*, Element [1pre]; EX1003 ¶¶114-117. A POSITA also would have known that a DVR like that described in the Lorex Manual is a type of “set

top box” that can sit atop a television or other viewing device, for example. Indeed, the evidence here confirms that DVRs were a conventional category of set top boxes by the relatively late Critical Date of the ’916 Patent (Jan. 7, 2014). EX1003, ¶115 (citing EX1016, [0003] (“Because DVRs are usually box-like in shape, and are often found sitting on top of the television sets to which they are connected, DVRs typically are included in the broad category of devices now called ‘set-top boxes.’”) and EX1017, [0049] (“set top box[] ... capabilities can include digital video recorder (DVR) capabilities”)); *see also* EX1019 (describing a prior art NVR set-top box).

Claim [3]

Lorex Manual discloses that the *remote client device* can be a *portable electronic* device such as a smartphone or tablet computer. EX1007, 10, 84 (“Mobile Apps: Accessing your DVR Using a Mobile Device”); EX1003, ¶¶118-120.



EX1007, 87 (annotated).

Claim [4]

Lorex Manual discloses that the *remote client device* can be a *mobile phone*. EX1007, 10, 84 (“You can remotely view camera streams from your DVR on compatible mobile phones ...”); EX1003, ¶¶121-123.

Claim [5]

Supra, Element [1h]. EX1003, ¶¶124-125.

Claim [6]

Kim941 describes a linking server (e.g., server 100) that transmits hole-punching messages to the peer nodes—which predictably include the DVR (*electronic device*) and phone, tablet, or PC (*remote client device*) in the Lorex

Manual-Kim941 combination—to establish the P2P connection. EX1008, [0082]-[0083], FIG. 6; EX1003, ¶¶126-127.

Claim [7]

Lorex Manual discloses that the DVR (*electronic device for concentrating information*) connects to an *external routing device* via an ethernet cable connected to the LAN port (*second interface*) of the DVR. EX1007, 7 (“Connect an ethernet cable (included) to the LAN port on the rear panel of the DVR. Connect the other end of the ethernet cable to a router on your network.”), 57, 84; EX1003, ¶¶129-132. Lorex Manual discloses that connecting the DVR to a router represents “step 1 of 3” of “connecting to your DVR over the Internet.” EX1007, 57-58; EX1003, ¶131.

Claim [8]

Lorex Manual discloses that the DVR connects to the Internet via a “router,” as discussed above in connection with Claim [7]. EX1007, 57-58; EX1003, ¶¶133-136. Lorex Manual explicitly shows that the router connects to the Internet, which is a network that uses IP protocols. EX1007, 58. Lorex Manual further describes that the remote client device connects to the DVR can connect to the Internet using

the DVR's IP address⁷ – while the DVR is connected to the Internet via the router.

EX1007, 120; EX1003, ¶134. In this context, a POSITA would have understood Lorex Manual to mean that the “router” is an IP router as claimed. EX1003, ¶134.

Claim [10]

Lorex Manual discloses that the DVR can connect to the Internet and a local area network (LAN) through a router. EX1007, 58, 119-122; EX1003, ¶¶137-140.

The router depicted in Lorex Manual includes a pair of antennas, which a POSITA would have understood to mean that the router has a wireless access point.

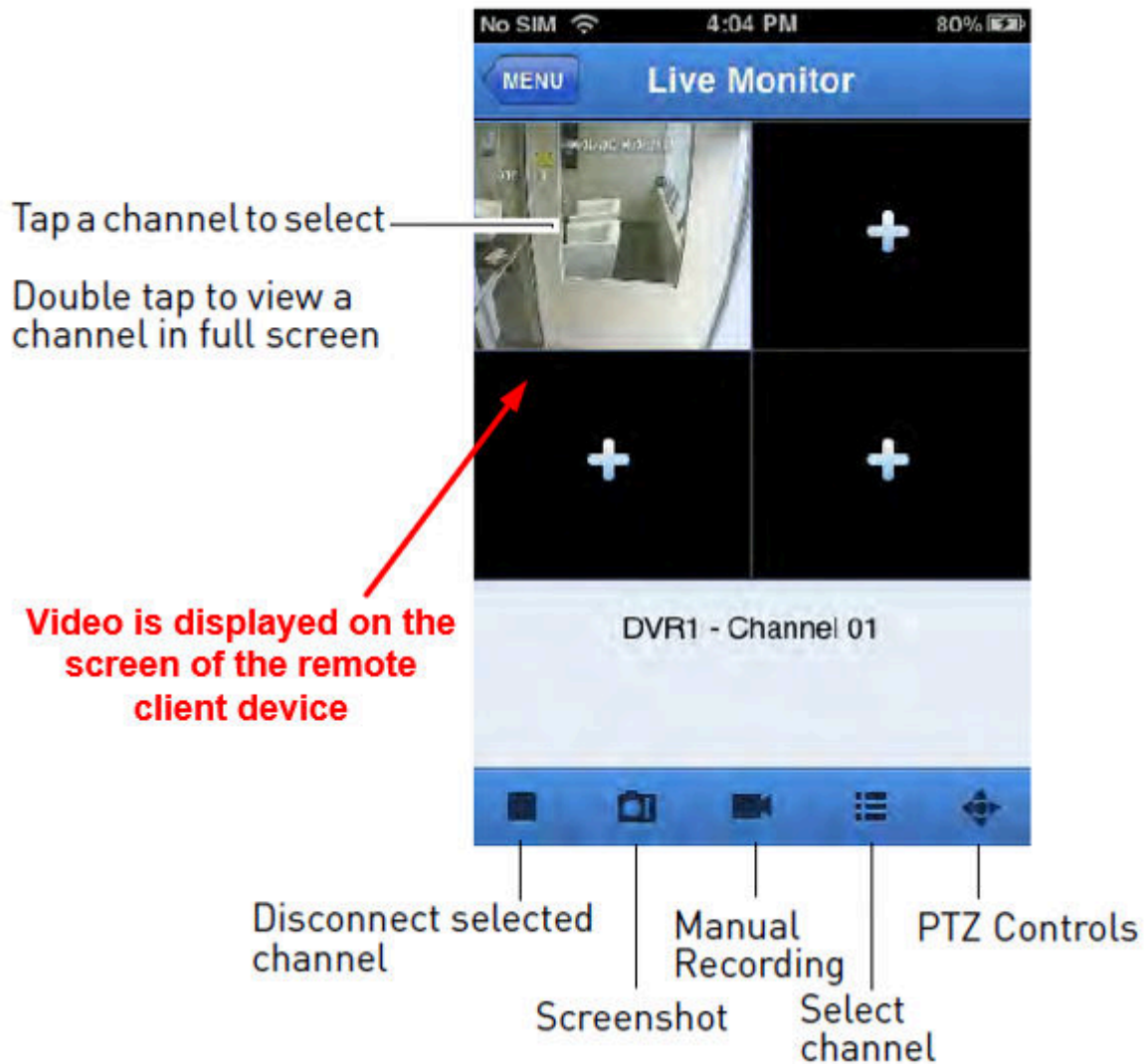
EX1007, 58 and 112 (depicting router with antennas); EX1003 ¶138. Lorex Manual also teaches that the user can connect a client device such as a PC or MAC to the DVR in a LAN, through the router, to deliver information from the DVR (e.g., live or recorded video streams) to the client. EX1007, 119 (“You can connect to your DVR through Internet Explorer through the local area network (LAN).”), 120-122. By the late timeframe of the '916 Patent (Jan. 7, 2014), a POSITA would have known that a conventional class of PC was a notebook or laptop computer

⁷ An IP address is “not required” to connect to the DVR. EX1007, 119; EX1003, ¶134. However, the fact that remote devices are able to connect to the DVR using an IP address in at least some examples means that the router connecting the DVR to the Internet is an “IP router.” EX1003, ¶134.

(portable electronic device). EX1003 ¶139. At a minimum, it would have been obvious to use a notebook or laptop PC for connecting to the DVR as described in Lorex Manual because notebook/laptop computers were a popular PC at the time and because they offered the convenience of mobility and a small form factor to users. EX1003 ¶139.

Claim [16]

As described above in connection with Element [1g], Lorex Manual discloses how the *remote client device* (e.g., smartphone, tablet, or PC) can display video data from the *electronic device for concentrating information* (e.g., DVR), and the remote client device can receive this video data directly from the DVR over a P2P connection. EX1007, 10, 84-87; EX1003 ¶¶141-143. Lorex Manual discloses that a screen of the remote client device displays the video from the DVR in a way that is suitable for viewing at the remote client device:



EX1007, 87 (annotated).

Since the video from the DVR is displayed on the screen of the mobile device, Lorex Manual's DVR must format the video data in a way that allows the mobile device to display the video on the screen so that a user can view the video. EX1007, 87; EX1003, ¶142. For example, Lorex Manual discloses that the DVR can support a range of recording resolutions, the recording resolution selected by a

user. EX1007, 38 (“The DVR restarts and asks you to confirm the new resolution. Click Yes to confirm or No to revert to the old resolution.”); EX1003, ¶142.

Because the DVR sets the recording resolution, the DVR *formats* video data received from security cameras to match the user-selected resolution in a way that is suitable for displaying the video on the *remote client device*. EX1003, ¶142.

B. GROUND 1B: – Lorex Manual in view of Kim941 and Kim517 would have rendered obvious claim 9

1. *Kim517*

Kim517 describes “a home network system, and particularly, [a] home monitoring method and apparatus using electrical appliances and cameras.” EX1009, [0003]; EX1003, ¶¶63-64. “A home network system refers to a system that connects home devices installed in a house through a wired or wireless network so as to control the home devices.” EX1009, [0005]. “An advanced home network system integrates home devices through a Home Gateway (HGW or H-GW) and connects the home devices to an external common data network, for example, an Internet Protocol (IP) network (that is, the Internet), so as to provide more various Internet-based services.” *Id.* FIG. 5 (reproduced below) depicts an example home network implemented in accordance with Kim517’s techniques, including a home gateway 510 wired or wirelessly connected to home devices 512a, 512b, 514, and 516. *Id.*, [0018], [0038]-[0047], [0056], [0059]-[0068]; *see*

also id., FIGS. 1-4 (and associated text). A user can use his or her mobile terminal 532 to remotely control the home devices 512a, 512b, 514 over the Internet 520 and through the home gateway 510:

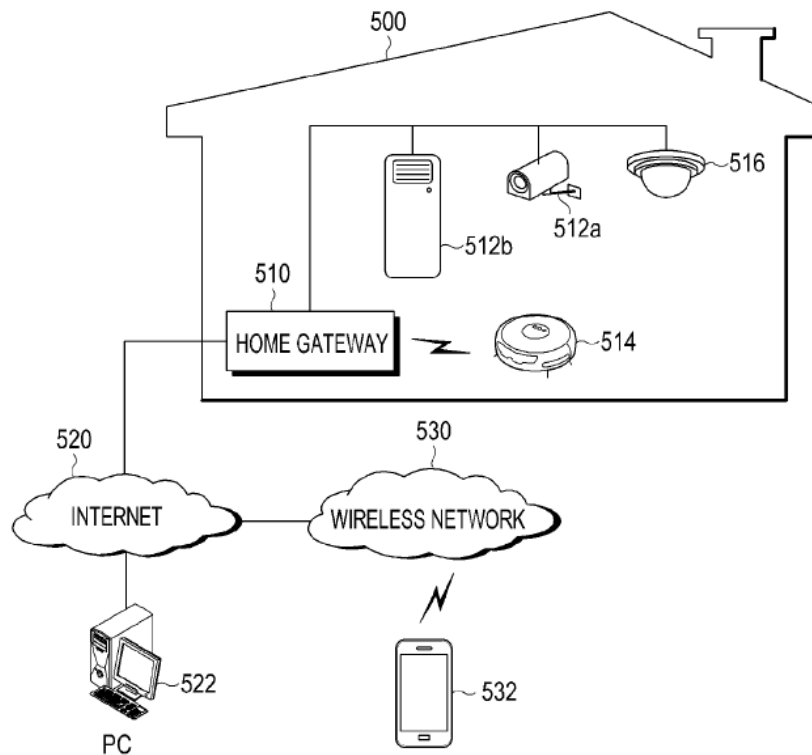


FIG.5

EX1009, FIG. 5.

See also id., [0039]-[0040], [0067]-[0068], [0162]-[0169], FIGS. 18, 19A-19B.

2. The Lorex Manual-Kim941-Kim517 Combination

Lorex Manual describes how a user can remotely control pan-tilt-zoom (PTZ) cameras connected to the DVR through an interface of a remote client device (e.g., the smartphone, tablet, or PC). EX1007, 66, 77-78, 88-89, 96, 106-

108. According to Lorex Manual, PTZ cameras must be physically connected to the DVR through an RS485 port on the rear of the DVR. *Id.*, 106. Lorex Manual does not describe PTZ cameras or other controllable appliances connected to the DVR through a wireless connection, and relatedly, does not expressly disclose a remote client device configured to control through the DVR an appliance that is wirelessly connected to the DVR. EX1003, ¶144. These features were nonetheless well known before the '916 Patent as demonstrated by Kim517 (*see supra*, §V.B.1) and multiple reasons would have prompted a POSITA to apply Kim517's suggestion for remotely controlling a PTZ camera or other appliance wirelessly connected to a home gateway like Lorex Manual's DVR before the earliest effective filing date of the '916 Patent (Jan. 7, 2014). EX1003, ¶145. Indeed, a POSITA would have implemented Lorex Manual's DVR according to Kim517's suggestion for wirelessly connecting remotely controllable appliances (e.g., PTZ cameras) **(1)** to expand the capabilities of the DVR and to increase the number and types of devices to which the DVR could connect, thereby growing the market for the DVR and increasing user satisfaction, **(2)** to simplify the ability to connect certain cameras and other appliances to the DVR without the need to deal with routing wires between the DVR and the appliances, **(3)** to allow the DVR to connect to such appliances over longer distances that would be impractical or difficult to connect by wire, and **(4)** to advantageously permit a user to issue

commands to and control the appliances through a remote client device, thereby increasing the usefulness of the appliances to the user even when the user is not at home (or other premises of the DVR and the connected appliances). EX1003, ¶¶144-149.

A POSITA would have reasonably expected success implementing the combination, especially as Lorex Manual and Kim517 describe similar systems for connecting home devices or appliances (e.g., cameras) to an information concentrating device (e.g., a DVR or home gateway) and for controlling the devices through a remote device. EX1003, ¶149.

3. *Application to Challenged Claims*

Claim [9]

Lorex Manual describes techniques for remotely controlling pan-tilt-zoom (PTZ) cameras connected to a DVR through an interface of a remote client device (e.g., smartphone, tablet, or PC). EX1007, 66, 77-78, 88-89, 96, 106-108; EX1003, ¶¶150-154. Further, for the reasons described in detail above, a POSITA would have found it obvious to implement Lorex Manual's DVR according to Kim517's suggestion enable the DVR to wirelessly connect to remotely controllable home devices or appliances (e.g., PTZ cameras). *Supra*, §§V.B.1-2; EX1003, ¶151. The DVR in the resulting combination would have predictably provided the additional features recited in claim 9. EX1003, ¶151.

Kim517 discloses a home gateway that, like Lorex Manual's DVR, provides an electronic device for concentrating information. EX1009, [0005], [0039]-[0040], FIGS. 1-2, 5. In the combination, the DVR would predictably include the capability of Kim517's home gateway to communicate with a home device (*appliance*) through a wireless connection. *Id.*, [0040] ("home devices 110 may be capable of performing communication with the home gateway 110 according to a ... wireless communication scheme"), [0045], [0047], FIG. 3. For example, Kim517 teaches that the home device (*appliance*) includes a communication module that allows it to communicate with the home gateway over a wireless LAN. *Id.*, [0073], FIG. 6. Kim517 also teaches that communication over a wireless LAN involves communication with a wireless access point, which is conventionally included in a router like that disclosed in Lorex Manual. EX1009, [0056]; EX1007, 58 (depicting a router with a pair of antennas indicative of wireless communication capability); EX1003, ¶152; *see also id.*, EX1009, [0047], FIG. 3. The combination would predictably involve Lorex Manual's DVR connecting to an appliance (e.g., a PTZ camera) through the router. EX1003, ¶152.

Consistent with Kim517's teachings, the remote client device (e.g., smartphone, tablet, or PC) in the predictable Lorex Manual-Kim941-Kim517 combination would also control the appliance (e.g., PTZ camera) through the

DVR. EX1007, 66, 77-78, 88-89, 96, 106-108; EX1009, [0067]-[0068], [0121], [0040]-[0042], FIGS. 5, 18, 19A-19B; *supra*, §V.B.1; EX1003, ¶153.

C. GROUND 1C: Lorex Manual in view of Kuo would have rendered obvious claims 1-8, 10, and 16

1. *Kuo*

Kuo is a publication of an earlier-filed patent application by a subset of co-inventors named on the '916 Patent. *Compare* EX1001 *with* EX1011. The '916 Patent specification expressly refers to Kuo (i.e., U.S. Application Serial No. 13/293,506) multiple times for additional detail on aspects of the subject matter described and claimed in the '916 Patent. EX1011, 14:18-22 (“Please note that all the descriptions, in U.S. patent application Ser. No[.] 13/293,506 ... can be integrated in whole or in part with the information concentrating center for establishing a P2P connection with a remote client device[] ...”), 13:42-52, 14:10-16. Indeed, FIGS. 1-11 of Kuo are identical to those same figures in the '916 Patent. EX1003, ¶¶65-69.

Like the '916 Patent and Lorex Manual, Kuo describes techniques for establishing P2P connections between devices by hole punching. EX1007, 10;

EX1011, ¶[0029]; EX1003, ¶66. In Kuo, a “remote device”⁸ registers its serial number with a “linking server.” EX1011, ¶[0055]; EX1003, ¶66. The linking server maintains a list of serial numbers corresponding to respective remote devices:

TABLE 1

the mapping relationship between the remote devices and the linking server groups			
	Codes of Linking Servers	Serial Numbers of Remote Devices	Notes
Service Provider A	Ser 01	D01, D02, D03,	Ser 01: Shanghai
	Ser 02	D04, D05	Ser 02: Tokyo
	Ser 03		Ser 03: Los Angeles
	Ser 04	D06, D07, D08,	Ser 04: New York
	Ser 05	D09	Ser 05: Berlin
Service Provider B	Ser 11	D11, D12, D13,	Ser 11: Paris
	Ser 12	D14	Ser 12: Cairo

EX1011, ¶[0033], TABLE 1 (annotated).

⁸ Remote devices include “security apparatuses” and “home electric appliances.”

EX1011, [0039]; EX1003, ¶66.

Kuo explains that a “proximal device”⁹ can request a connection with a remote device registered in the linking server. EX1011, ¶[0038]; EX1003, ¶68. In response to receiving a connection request, Kuo’s linking server performs hole punching to establish a P2P connection between the remote device and the proximal device. EX1011, ¶[0038]; EX1003, ¶68. Kuo expressly discloses that the remote devices are registered in the linking server, but proximal devices do not register because they simply use an API to identify a linking server or address for the particular remote device to which the proximal device requests to connect. EX1011, ¶¶[0010]-[0012] (“As long as a proximal device has API supported by the administration server, the user can request the administration server to find out the linking address.”), [0029]-[0039], FIGS. 3, 10-11; EX1003, ¶68.

2. *The Lorex Manual-Kuo Combination*

Lorex Manual describes a cloud service—i.e., “Lorex Stratus”—that facilitates the establishment of a P2P connection between a DVR and a remote client device (e.g., a smartphone, tablet, or PC). EX1007, 10, 57, 62; *supra*, § V.A.1. Lorex Manual does not, however, describe many details as to how the P2P

⁹ Proximal devices include “mobile phones” and “computers.” EX1008, ¶[0039]; EX1003, ¶68.

connection is established after the client device requests to login to the service and connect to the DVR. Kuo nonetheless describes a conventional solution that would have been obvious to apply to Lorex Manual to achieve its goals of establishing a P2P connection between the DVR and remote client device. Multiple reasons would have prompted a POSITA to implement Lorex Manual in accordance with Kuo's suggestions for establishing a P2P connection using device registration, identification, and hole-punching techniques before the alleged invention of the '916 Patent. EX1003, ¶¶155-159.

First, a POSITA would have understood that implementing Lorex Manual's system to include a linking server that registers a device ID (e.g., the unique "Device ID" or serial number of Lorex's DVR) based on Kuo's suggestions would predictably provide a simple and secure way for the user's remote client device (e.g., smartphone, tablet, or PC) to connect with the DVR. EX1003, ¶156. Kuo explains that the linking server enhanced security over conventional P2P connection techniques because device ID or serial number registration obviates a need to share IP addresses for the remote device. EX1011, ¶¶[0007], [0039]; EX1003, ¶156.

Second, as discussed above (*supra*, § V.A.3), a POSITA would have been prompted to apply Kuo's hole-punching techniques to Lorex Manual because hole-punching was a well-known and popular solution for establishing P2P connections

between devices, even in situations where the endpoints are located behind firewalls or network address translators (NATs) that would otherwise block direct communication between the endpoints. EX1003, ¶157.

Third, a POSITA would have implemented Lorex Manual's system in accordance with Kuo's techniques for establishing P2P connections to provide a simple method for the remote client device (referred to as the "proximal device" in Kuo) to locate an appropriate linking server where the DVR (corresponding to the "remote device in Kuo) is registered and from which a hole-punching process can be initiated to form the P2P connection. EX1011, ¶¶[0010]-[0012], [0029]-[0039], FIGS. 3, 10-11; EX1003, ¶158.

Considering the predictable electrical/network and software components involved in the combination and the relatively advanced state of the art at the time, a POSITA would have reasonably expected success achieving the combination before the earliest effective filing date of the '916 Patent (January 7, 2014). EX1003, ¶159.

3. *Application to Challenged Claims*

Elements [1pre]-[1d]

See supra, Ground 1A (§V.A.4) at Elements [1pre]-[1d].¹⁰ EX1003, ¶¶160-162.

Element [1e]

Lorex Manual discloses a ***remote client device*** (e.g., a computer, tablet, or mobile device) that uses a ***unique identification (UID)*** (e.g., device ID) of a DVR (***electronic device for concentrating information***) to perform a secure handshake with Lorex Stratus servers and establish a connection with the DVR over the Internet. EX1007, 10, 57, 59, 85, 93; *supra*, §V.A.4 (Element [1e]); EX1003, ¶¶163-167.

To the extent Lorex Manual does not expressly disclose that the DVR contacts the at least one linking server to register the device ID, such features would have been obvious and provided in the Lorex Manual-Kuo combination. EX1003, ¶163; *supra*, §V.C.2. Kuo, for example, discloses a “remote device” (analogous to the DVR in Lorex Manual or the electronic device for concentrating information in the ’916 Patent) that contacts a linking server through the Internet to register a unique identification (e.g., a serial number) into the linking server for

¹⁰ For purposes of Ground 1C, Petitioner relies on Lorex Manual’s disclosure for Element [1d] and not the additional disclosure from Kim941 cited in Ground 1A. EX1003, ¶162.

identifying network addressing information of the device so as to enable a proximal device (analogous to the remote client device such as a phone or PC in Lorex Manual and the '916 Patent) to establish a P2P connection with the remote device. EX1011, [0037] (“remote device sends a piece of device-registering information to the linking server” such that “the linking server learns the IP and information necessary for communicating with the remote device”) & FIG. 10, [0038]-[0039] (describing process for establishing a P2P connection & FIG. 11; *see also id.*, [0007]-[0012], [0024]-[0027], FIGS. 1-3; EX1003, ¶164. For the reasons expressly articulated above (*supra*, §V.C.2), a POSITA would have found it obvious to combine Lorex Manual and Kuo such that Lorex Manual’s DVR would contact a linking server through the Internet to register its unique Device ID consistent with Kuo’s suggested techniques. EX1003, ¶166.

Element [1f]

As described above in connection with the analysis of Element [1f] in Ground 1A (*supra*, §V.A.4), Lorex Manual discloses a ***remote client device*** (e.g., a computer, tablet, or mobile device) that uses a ***unique identification (UID)*** (e.g., device ID) of a DVR (***electronic device for concentrating information***) to perform a secure handshake with Lorex Stratus servers and establish a connection with the DVR over the Internet. EX1007, 10, 57, 59, 85, 93; EX1003, ¶¶168-170.

To the extent Lorex Manual does not explicitly disclose details of the client device's contact with a linking server as claimed in [1f], these features would have been obvious in view of Kuo. EX1003, ¶169. For instance, Kuo discloses a "proximal device" (analogous to the remote client device such as a phone or PC in Lorex Manual and the '916 Patent) that contacts a linking server to establish a P2P connection with a "remote device" (analogous to the DVR in Lorex Manual or the electronic device for concentrating information in the '916 Patent). EX1011, [0038] & FIG. 11, [0037], [0039], FIG. 10; *see also id.*, [0007]-[0012], [0024]-[0027], FIGS. 1-3; EX1003, ¶169. The proximal device uses an identifier for the targeted remote device, which can be a serial number as described in Kuo or a Device ID as described in Lorex Manual. EX1011, [0034], [0037]-[0039], Table 1; EX1007, 58-60, 85; EX1003, ¶169. For the reasons expressly articulated above (*supra*, §V.C.2), a POSITA would have found it obvious to combine Lorex Manual and Kuo such that Lorex Manual's remote client device (e.g., smartphone, tablet, or PC) would contact a linking server through the Internet according to the Device ID of the DVR to establish a P2P connection with the DVR. EX1003, ¶169.

Element [1g]

Lorex Manual expressly teaches that at least a portion of the video data received by the DVR is delivered to the remote client device on the P2P

connection. *Supra*, §V.A.4 (Element [1g]); EX1007, 5, 61, 62, 84-87; EX1003, ¶¶171-172.

Element [1h]

As discussed above in connection with Element [1f], Kuo discloses a “proximal device” (analogous to the remote client device such as a phone or PC in Lorex Manual and the ’916 Patent) that contacts a linking server to establish a P2P connection with a “remote device” (analogous to the DVR in Lorex Manual or the electronic device for concentrating information in the ’916 Patent). EX1011, [0038]-[0039], FIG. 11; *supra*, Element [1f]; EX1003, ¶¶173-176. In Kuo, the proximal device does not have a unique identification to register in the linking server when it contacts the linking server for establishing the P2P connection. EX1003, ¶173. In fact, the proximal device is not registered in the linking server when the P2P connection is established at all. *Id.*

That the proximal device is not registered in the linking server when contacting the linking server to establish the P2P connection or when the P2P connection is established when have been evident to a POSITA reviewing Kuo, at least because Kuo’s linking servers are configured to maintain registration information for the remote devices (not the proximal devices) and because Kuo defines an API that allows a proximal device to contact a linking server to connect with a remote device based merely on information about the linking server that the

proximal device obtains from an administration server. EX1011, [0008] (“the remote device registering the information thereof in the linking server”), [0009]-[0012], [0032]-[0034], [0037]-[0039], FIGS. 10-11; EX1003, ¶174. Kuo is clear that “the proximal device can merely use the administration server to find out a linking server that a specified remote device registers, neither needing a fixed IP nor remembering the IP addresses or domain names of the linking servers. *As long as proximal device has API supported by the administration server, the user can request the administration server to find out the linking address.*” *Id.*, [0012], [0039] (“all automatically executed by API”). Kuo’s API thus obviates any need for the proximal device to register with the linking server. *Id.*, EX1003, ¶174. Noticeably, Kuo’s approach is identically described in the ’916 Patent and the specification of the ’916 Patent expressly refers to Kuo (U.S. Serial No. 13/293,506) as providing the registration and connection procedures implemented by the disclosed devices. *Cf.* EX1001, 8:54-9:15, 13:42-52, 14:10-23.

For the reasons expressly articulated above (*supra*, §V.C.2), a POSITA would have found it obvious to combine Lorex Manual and Kuo such that Lorex Manual’s remote client device (e.g., smartphone, tablet, or PC) would not have had and would not register a unique ID for associating connecting information of the remote client device when contacting the linking server for establishing the P2P connection or while the P2P connection is being established. EX1003, ¶175.

Claim [5]

Supra, Element [1h]. EX1003, ¶¶183-184.

Claim [6]

Kuo discloses, and the Lorex Manual-Kuo combination provides, that the linking server transmits hole-punching messages to establish a P2P connection to both endpoints of the connection, which would include the remote client device (e.g., smartphone, tablet, or PC) and the DVR of Lorex Manual in the combination described above. EX1011, [0029] (“The linking server group A (20)...sends hole-punching information 960 and hole-punching information 961 to the proximal device 4 and the remote device A (31) so as to establish a point-to-point link 97 between the proximal device 4 and the specified remote device A (31).”), [0038], FIG. 11; *supra*, §V.C.2; EX1003, ¶¶185-186.

Claims [2], [3], [4], [7], [8], [10], and [16]

The Lorex Manual-Kuo combination would have rendered obvious Claims [2], [3], [4], [7], [8], [10], and [16] for at least the reasons described above in connection with the Lorex Manual-Kim941 combination (*see* Ground 1A, Elements [3], [4], [7], [8], [10], and [16]); EX1003, ¶¶177-182, 187-194.

**D. GROUND 1D: Lorex Manual in view of Kuo and Kim517
would have rendered obvious claim 9**

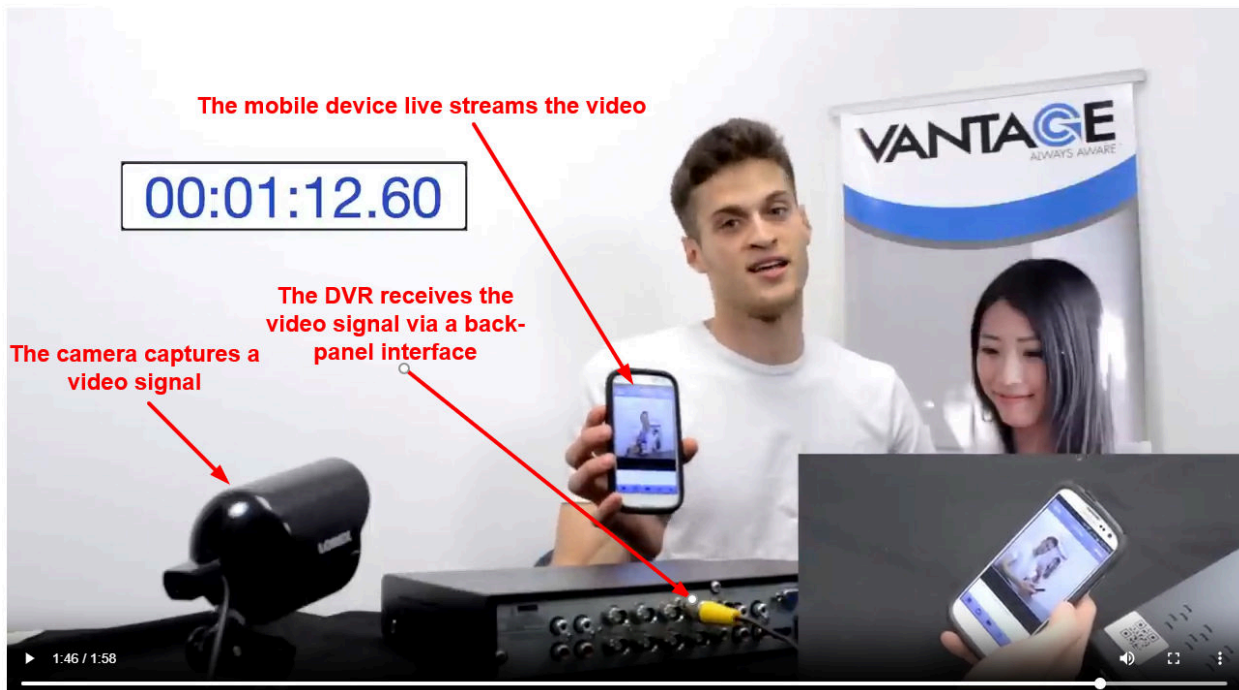
Claim [9]

A POSITA would have found it obvious and would have been motivated to further modify the Lorex Manual-Kuo combination in view of Kim 517 for substantially the same reasons discussed above in Ground 1B. *Supra*, § V.B.2. The resulting combination likewise would have provided Claim 9 for at least the reasons described above in Ground 1B. *Supra*, § V.B.3, Claim 9; EX1003, ¶¶195-196.

E. GROUND 2A: Lorex Video in view of Galvin and Kuo would have rendered obvious claims 1-8, 10, and 16

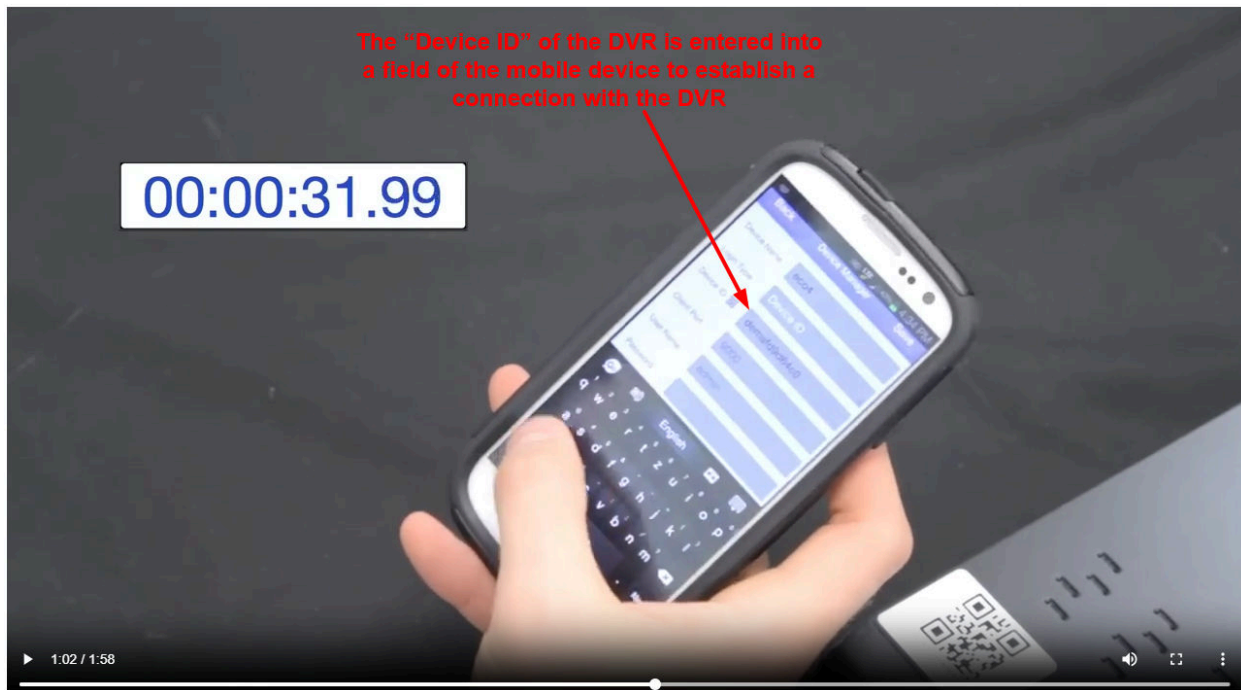
1. *Lorex Video*

Lorex Video is a video published on YouTube that illustrates a process for connecting a mobile device (i.e., an Android smartphone) to a DVR using Lorex's connectivity solutions similar to those described in Lorex Manual. EX1012; EX1003, ¶¶50-52. The connection enables live streaming of video from the DVR to the mobile device:



EX1012, 1:46 (annotated).

Lorex Video demonstrates how the mobile device can be used to initiate a process of establishing a connection with the DVR by entering the DVR's "device ID" into a field of a user interface displayed on the mobile device. EX1012, 1:03-1:58; EX1003, ¶51. For example, the device ID can be obtained by scanning a QR code affixed to the DVR to autofill the user interface field. EX1012, 0:56-1:03; EX1003, ¶51.



EX1012, 1:02 (annotated).

2. *Galvin*

Like Lorex Video, Galvin discloses a video recorder that receives video streams from security cameras. EX1013, [0057]; EX1003, ¶70. Galvin's video recorder has ports for connecting to security cameras and at least one port for connecting to a video display monitor (e.g., television). EX1013, [0067], FIGS. 4-5; EX1003, ¶70. Galvin teaches that the video recorder can output video from at least one of the security cameras for display by the video display monitor. EX1013, [0108]; EX1003, ¶70.

3. *Kuo*

Supra, §V.C.1. EX1003, ¶¶65-69.

4. *The Lorex Video-Galvin-Kuo Combination*

Lorex Video describes a process for connecting a DVR and a remote client device (e.g., a smartphone) to enable live video streaming. EX1012, 0:15-1:58; *supra*, §V.E.1; EX1003, ¶197. Lorex Video, however, does not explicitly many details about how the connection is established after the mobile device requests to login to the service and connect to the DVR. Kuo nonetheless describes a conventional solution that would have been obvious to apply to Lorex Video to achieve its goals of establishing a direct connection between the DVR and mobile device. Multiple reasons would have prompted a POSITA to implement Lorex Video in accordance with Kuo's suggestions for establishing a P2P connection using device registration, identification, and hole-punching techniques to achieve known benefits. EX1003, ¶¶197-201.

First, a POSITA would have understood that implementing Lorex Video's system to include a linking server that registers a device ID (e.g., a unique "Device ID" or serial number of Lorex's DVR) based on Kuo's suggestions would predictably provide a simple and secure way for the mobile device to connect with the DVR. EX1003, ¶198. Kuo explains that the linking server enhanced security over conventional P2P connection techniques because device ID or serial number registration obviates a need to share IP addresses for the remote device. EX1011,

¶¶[0007], [0039] (“the remote device and the linking server needn’t directly disclose the IPs and domain names thereof”); EX1003, ¶198.

Second, as discussed above (*supra*, § V.C.1), a POSITA would have been prompted to apply Kuo’s hole-punching techniques to Lorex Video because hole-punching was a well-known and popular solution for establishing P2P connections between devices, even in situations where the endpoints are located behind firewalls or network address translators (NATs) that would otherwise block direct communication between the endpoints. EX1003, ¶199.

Third, a POSITA would have implemented Lorex Video’s system in accordance with Kuo’s techniques for establishing P2P connections to provide a simple method for the remote client device (referred to as the “proximal device” in Kuo) to locate an appropriate linking server where the DVR (corresponding to the “remote device in Kuo) is registered and from which a hole-punching process can be initiated to form the P2P connection. EX1011, ¶¶[0010]-[0012] (“As long as a proximal device has API supported by the administration server, the user can request the administration server to find out the linking address.”), [0029]-[0039], FIGS. 3, 10-11; EX1003, ¶¶200-201.

Furthermore, Lorex Video describes the DVR as including a back panel with ports that can connect to a router and a camera, but Lorex Video does not describe a port for connecting the DVR to a television. EX1012, 0:33-0:40; *Supra*, §V.E.1;

EX1003, ¶202. Galvin nonetheless describes a conventional solution that would have been obvious to apply to Lorex Video's DVR to supply this television connection port. EX1013, [0057], [0067], FIGS. 4-5; supra, §V.E.2; EX1003, ¶202. A POSITA would have been prompted to implement Lorex Video to include a display output port in accordance with Galvin's suggestion to enable connection of the DVR to a television or other screen through which a user would be able to view video from one or more cameras connected to the DVR. EX1003, ¶202. A POSITA also would have sought to include a display output port on Lorex Video's DVR to allow a user to view and interact with DVR configuration/menu screens locally even without a mobile device, which would have been convenient to many users. EX1003, ¶202.

Considering the predictable electrical/network and software components involved in the combination and the relatively advanced state of the art at the time, a POSITA would have reasonably expected success achieving the Lorex Video-Galvin-Kuo combination before the earliest effective filing date of the '916 Patent (January 7, 2014). EX1003, ¶202.

5. *Application to Challenged Claims*

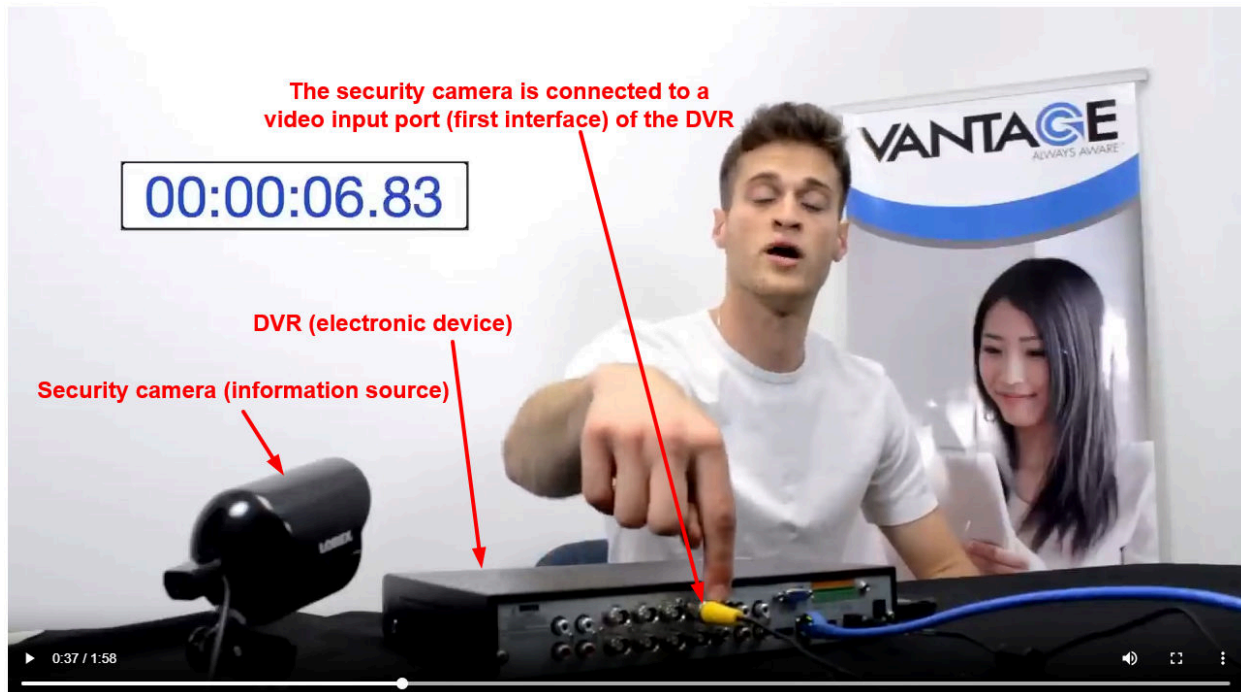
Element [1pre]

Even if the preamble is treated as a limitation (which Petitioners do not concede, the Lorex Video-Galvin-Kuo combination provides the recited

“electronic device for concentrating information.” EX1003, ¶205. Lorex Video discloses an *electronic device* (i.e., a DVR) that *concentrates information* (i.e., video data) from security cameras connected to the DVR. EX1012, 0:01-0:38; EX1003, ¶¶203-207. For example, a security camera can be connected to an input port on the back panel of the DVR so that the DVR receives a video signal from the security camera. EX1012, 0:01-0:38; EX1003, ¶206.

Element [1a]

The Lorex Video-Galvin-Kuo combination provides Element [1a]. EX1003, ¶¶208-210. As previously discussed (*see* [1pre]), Lorex Video’s DVR includes video input ports that can connect to security cameras to receive video signals from the security cameras. EX1012, 0:01-0:38; EX1003, ¶208. The video input port of Lorex Video’s DVR and a security camera connected to the video input port are shown below:



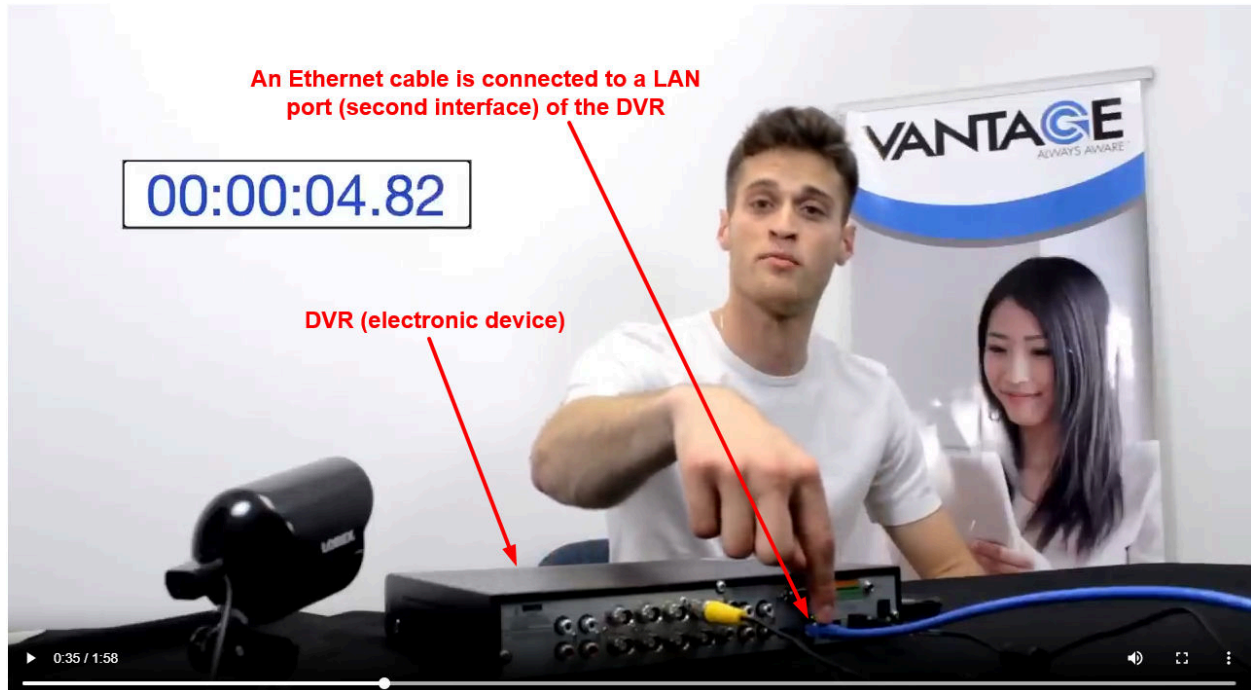
EX1012, 0:37 (annotated).

The security camera provides an *information source* that generates *information* including a video signal. EX1003, ¶209. In Lorex Video, the presenter points directly at a video input port of the DVR and proclaims that “I have one camera set up.” EX1012, 0:36-0:39; EX1003, ¶209. One security camera is visible as the presenter points at the video input port. EX1012, 0:36-0:39; EX1003, ¶209. Consequently, Lorex Video’s DVR includes *at least one first interface* for receiving *information* from *at least one information source*. EX1003, ¶209.

Element [1b]

The Lorex Video-Galvin-Kuo combination provides Element [1b]. EX1003, ¶¶[211]-[214]. For example, Lorex Video explains that the DVR includes a local

area network (LAN) port for connecting the DVR to a router using an Ethernet cable. EX1012, 0:01-0:38; EX1003, ¶211. The Ethernet port of Lorex Video's DVR is illustrated below with an Ethernet cable connected to the Ethernet port, the Ethernet cable extending off-screen:



EX1012, 0:35 (annotated).

While pointing at the LAN port of the DVR, the presenter of Lorex Video proclaims that the DVR “is connected to my router using an Ethernet [cable].” EX1012, 0:35-0:39; EX1003, ¶212. Ethernet is a family of computer networking technologies and standards that was well-known for providing Internet connections in LANs and wide area networks (WANs). EX1003, ¶212 (citing EX1010, 27, 91-

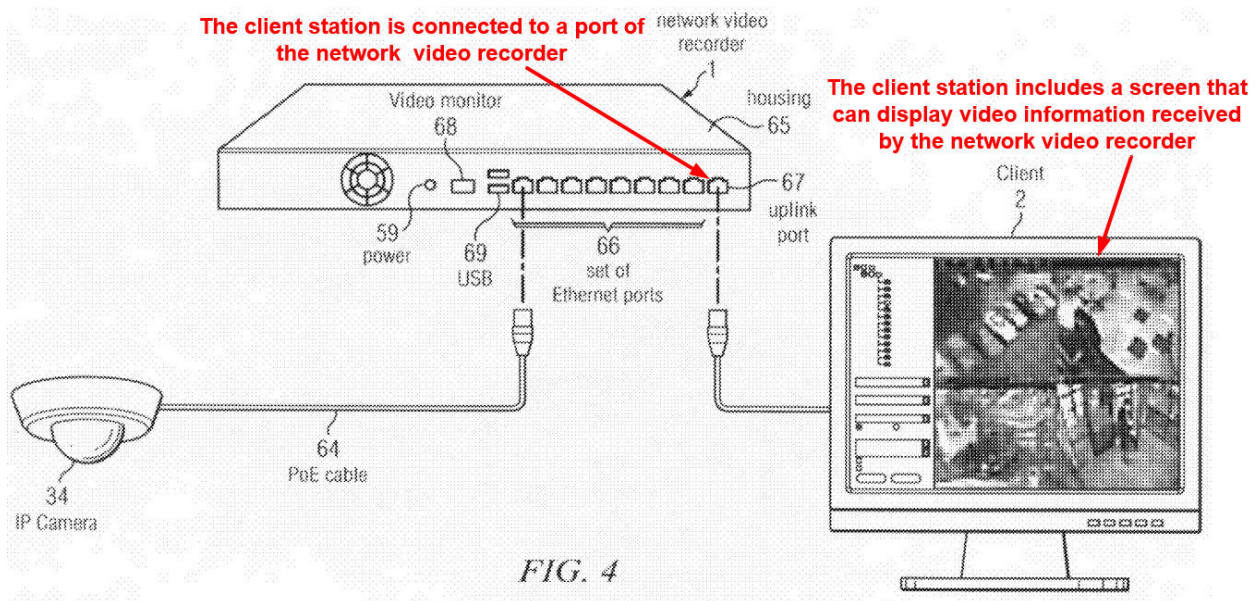
92). Additionally, “routers” are network devices that were well-known for relaying network traffic over the Internet. *Id.*

As Lorex Video explicitly discloses that the DVR is connected to a router using an Ethernet cable, a POSITA would have understood Lorex Video as teaching that the DVR is coupled to the Internet via a port that connects to the Ethernet cable. EX1003, ¶213. As described above (*see* §V.I.1), Lorex Video describes a connection method by which a remote client device (i.e., mobile device) can connect to the DVR over the Internet to receive video data from the DVR. EX1012, 0:35-0:39; EX1003, ¶213. Consequently, a connection can be established between the DVR and a mobile device via the *second interface* (i.e., LAN port) of the DVR, which connects the DVR to the Internet via a router and an Ethernet cable. EX1003, ¶213.

Element [1c]

The Lorex Video-Galvin-Kuo combination provides Element [1c]. EX1003, ¶¶215-218. In Lorex Video, a DVR is presented with a wide selection of ports located on a back panel of the DVR including the *first interface* (i.e., video input port) and the *second interface* (i.e., LAN port) discussed above. EX1012, 0:01-0:39; EX1003, ¶215. To the extent that the presenter of Lorex Video does not expressly identify a *third interface* for connecting to a *television*, such interfaces were well-known interfaces on DVRs and related technology. EX1003, ¶215.

For example, Galvin discloses a system including a network video recorder that, much like the Lorex Video's DVR, can receive video data from security cameras. EX1013, [0057]; EX1003, ¶216. Galvin discloses that the video recorder includes a set of ports – with at least one of these ports being connected to a camera and at least one of these ports being connected to an IP client station that includes a television screen for viewing video data. EX1013, [0067]; EX1003, ¶216. FIG. 4 of Galvin illustrates the network video recorder connected to the camera and connected to the IP client station:



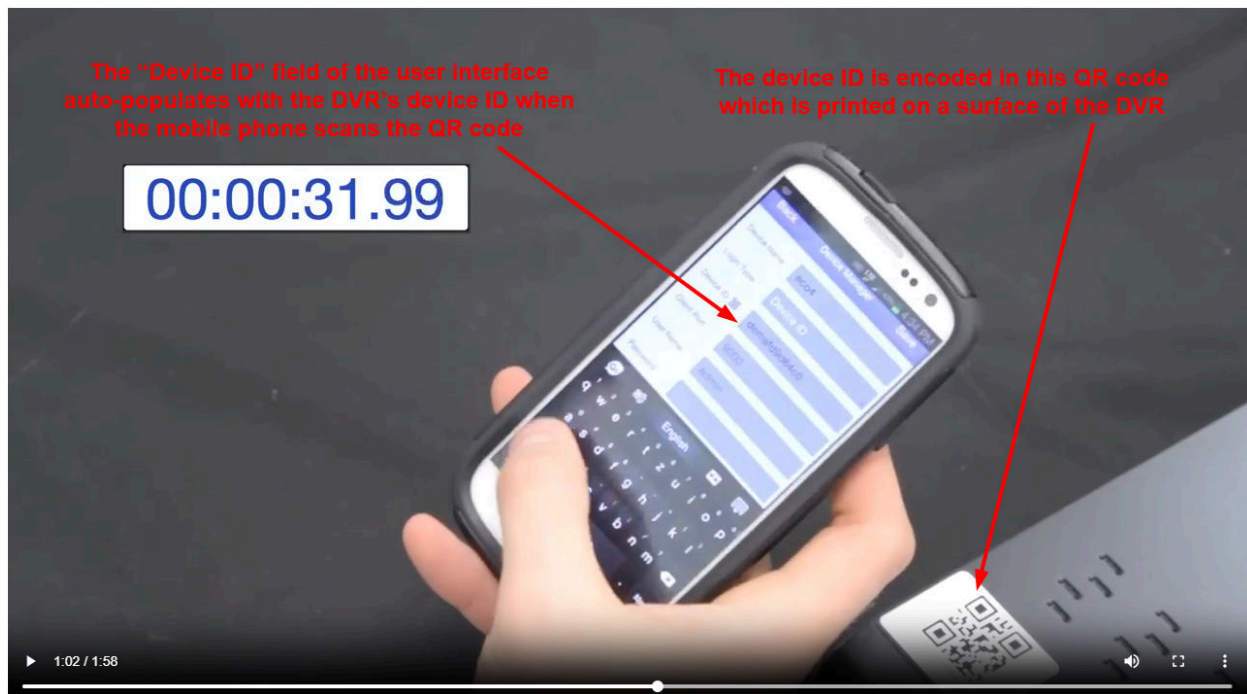
EX1013, [0067], FIG. 4 (annotated).

As illustrated above, Galvin's IP client station includes a television screen that can display video data received by the network video recorder, which is connected to the IP client station via an interface (i.e., uplink port 67). EX1013,

[0067], FIG. 4; EX1003, ¶217. For at least the reasons discussed above (*see* §V.E.4), it would have been obvious for a POSITA to implement Lorex Video's DVR in accordance with Galvin's suggestions such that the DVR would include an interface for connecting to a device including a screen that can display information (i.e., video) received by the DVR. EX1003, ¶217. Consequently, the Lorex Video-Galvin-Kuo combination discloses an *electronic device* (i.e., DVR) that includes a *third interface* for connecting to a television for viewing video data collected by cameras. EX1003, ¶217.

Element [1d]

The Lorex Video-Galvin-Kuo combination provides Element [1d]. EX1003, ¶¶219-221. As described above (*see* §V.I.1), Lorex Video describes a method for entering the "device ID" of a DVR into a user interface of a mobile device to establish a connection between the mobile device and the DVR. . EX1012, 0:38-1:58; EX1003, ¶219. This device ID represents a *unique identification (UID)* of the DVR and allows the mobile device to connect specifically to the DVR to receive video collected by cameras that supply the video to the DVR. EX1003, ¶219.



EX1012, 1:02 (annotated).

The QR code containing the DVR's device ID is affixed to the upper panel of the DVR and is both physically and digitally "*embedded*" in the DVR. EX1003, ¶220.

Element [1e]

The Lorex Video-Galvin-Kuo combination provides Element [1e]. EX1003, ¶¶222-226. Lorex Video discloses a *remote client device* (e.g., a mobile device) that uses a *unique identification (UID)* (e.g., device ID) of a DVR (*electronic device for concentrating information*) to establish a connection with the DVR over the Internet. EX1012, 0:38-1:58; EX1003, ¶222. To the extent Lorex Video does not expressly disclose that the DVR contacts the at least one linking server to

register the device ID, such features would have been obvious and provided in the Lorex Video-Galvin-Kuo combination. EX1003, ¶222; *supra*, §V.E.4.

Kuo, for example, discloses a “remote device” (analogous to the DVR in Lorex Video or the electronic device for concentrating information in the ’916 Patent) that contacts a linking server through the Internet to register a unique identification (e.g., a serial number) into the linking server for identifying network addressing information of the device so as to enable a proximal device (analogous to the mobile phone in Lorex Video and remote client device in the ’916 Patent) to establish a P2P connection with the remote device. EX1011, [0037], FIG. 10, [0038]-[0039] (P2P connection), FIG. 11; *see also id.*, [0007]-[0012], [0024]-[0027], FIGS. 1-3; EX1003, ¶223. For the reasons expressly articulated above (*supra*, §V.E.4), a POSITA would have found it obvious to combine Lorex Video and Kuo such that Lorex Video’s DVR would contact a linking server through the Internet to register its unique Device ID consistent with Kuo’s suggested techniques. EX1003, ¶223.

Element [1f]

The Lorex Video-Galvin-Kuo combination provides Element [1f]. EX1003, ¶¶227-229. Lorex Video shows that the ***remote client device*** (e.g., a mobile device) uses the ***unique identification (UID)*** (e.g., device ID) of a DVR (***electronic device for concentrating information***) to establish a connection with the DVR over the

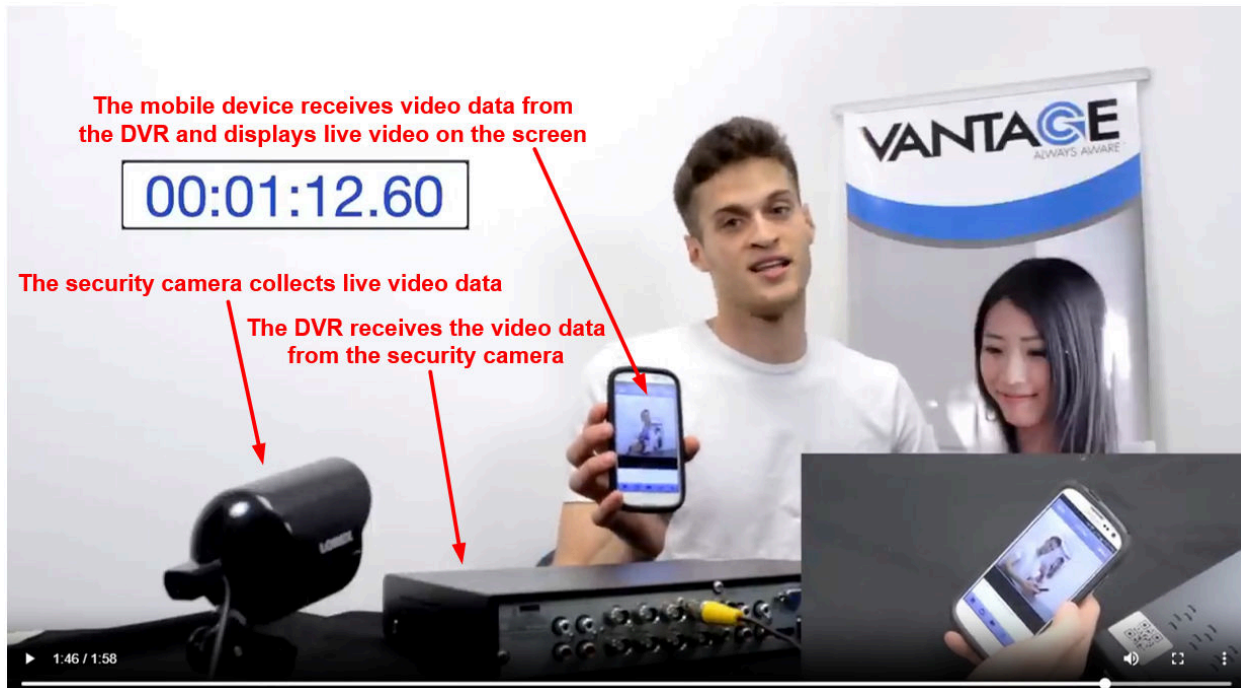
Internet. EX1012, 0:38-1:58; EX1003, ¶227. As discussed above in connection with Element [1d], the DVR's device ID can be entered into an information field on a user interface of an application running on the mobile device. EX1012, 0:59-1:05; EX1003, ¶227. Once the DVR's device ID is entered, the mobile device can submit the device ID to establish a connection with the DVR. EX1012, 0:59-1:36; EX1003, ¶227.

To the extent Lorex Video does not explicitly disclose details of the client device's contact with a linking server as claimed in [1f], these features would have been obvious in view of Kuo. EX1003, ¶228. For instance, Kuo discloses a "proximal device" (analogous to the remote client device such as a mobile phone in Lorex Video and the '916 Patent) that contacts a linking server to establish a P2P connection with a "remote device" (analogous to the DVR in Lorex Video or the electronic device for concentrating information in the '916 Patent). EX1011, [0038] ("asks the linking server to establish a link") & FIG. 11, [0037], [0039], FIG. 10; *see also id.*, [0007]-[0012], [0024]-[0027], FIGS. 1-3; EX1003, ¶228. The proximal device uses an identifier for the targeted remote device, which can be a serial number as described in Kuo or a Device ID as described in Lorex Video. EX1011, [0034], [0037]-[0039], Table 1; EX1007, 58-60, 85. EX1003, ¶228. For the reasons expressly articulated above (*supra*, §V.E.4), a POSITA would have found it obvious to combine Lorex Video and Kuo such that Lorex Video's *remote*

client device (e.g., mobile phone) would contact a linking server through the Internet according to the Device ID of the DVR to establish a P2P connection with the DVR. EX1003, ¶228.

Element [1g]

The Lorex Video-Galvin-Kuo combination provides Element [1g]. EX1003, ¶¶230-233. As described above (*see* [1a]), the DVR receives *information* (e.g., a video signal) from an *information source* (e.g., a security camera) connected to an *interface* on a back panel of the DVR. EX1012, 0:36-0:39; EX1003, ¶230. When the *remote client device* (e.g., a mobile device) of Lorex Video establishes a connection with the DVR by entering the DVR's device ID, the mobile device can receive *information* including video data collected by the DVR and display this video data on a screen. EX1012, 0:38-1:58; EX1003, ¶230. As illustrated below, Lorex Video's mobile device displays live video from the camera that is connected to the DVR. EX1012, 1:46; EX1003, ¶230.



EX1012, 1:46 (annotated).

Since Lorex Video's mobile device displays video data collected by a camera connected to the rear panel of the DVR, at least a portion of the video information received by the DVR is delivered to the mobile device over the connection. EX1012, 0:55-1:58; EX1003, ¶231.

As described above, Lorex Video shows that a mobile device can connect to a DVR and receive information from the DVR simply by entering the DVR's device ID and other information corresponding to the DVR, but Lorex Video does not expressly refer to this link as a "P2P connection." EX1012, 0:55-1:58; EX1003, ¶232. However, Kuo discloses a similar method for using a proximal device to contact a linking server to establish a connection with a remote device,

the linking server establishing the connection using hole punching to enable “point-to-point transmission” – well known characteristics of P2P connections. EX1011, [0024], [0038]; EX1003, ¶232. Kuo discloses that the proximal device can be a mobile phone and the remote device can be a surveillance camera, so it would be obvious for a POSITA to implement the connection method of Lorex Video with the P2P connection method of Kuo so that Lorex Video’s mobile device receives video data from the DVR over a **P2P connection**. EX1011, [0039]; EX1003, ¶232.

Element [1h]

As discussed above in connection with Element [1f], Kuo discloses a “proximal device” (analogous to the remote client device such as a mobile phone in Lorex Video and the ’916 Patent) that contacts a linking server to establish a P2P connection with a “remote device” (analogous to the DVR in Lorex Video or the electronic device for concentrating information in the ’916 Patent). EX1011, [0038]-[0039], FIG. 11; *supra*, Element [1f]; EX1003, ¶¶234-237. In Kuo, the proximal device does not have a unique identification to register in the linking server when it contacts the linking server for establishing the P2P connection. EX1003, ¶234. In fact, the proximal device is not registered in the linking server when the P2P connection is established at all. *Id.*

That the proximal device is not registered in the linking server when contacting the linking server to establish the P2P connection or when the P2P connection is established when have been evident to a POSITA reviewing Kuo, at least because Kuo's linking servers are configured to maintain registration information for the remote devices (not the proximal devices) and because Kuo defines an API that allows a proximal device to contact a linking server to connect with a remote device based merely on information about the linking server that the proximal device obtains from an administration server. EX1011, [0008] ("the remote device registering the information thereof in the linking server"), [0009]-[0012], [0032]-[0034], [0037]-[0039], FIGS. 10-11; EX1003, ¶235. Kuo is clear that "the proximal device can merely use the administration server to find out a linking server that a specified remote device registers, neither needing a fixed IP nor remembering the IP addresses or domain names of the linking servers. *As long as proximal device has API supported by the administration server, the user can request the administration server to find out the linking address.*" *Id.*, [0012], [0039] ("all automatically executed by API"). Kuo's API thus obviates any need for the proximal device to register with the linking server. *Id.*, EX1003, ¶235. Noticeably, Kuo's approach is identically described in the '916 Patent and the specification of the '916 Patent expressly refers to Kuo (U.S. Serial No.

13/293,506) as providing the registration and connection procedures implemented by the disclosed devices. *Cf.* EX1001, 8:54-9:15, 13:42-52, 14:10-23.

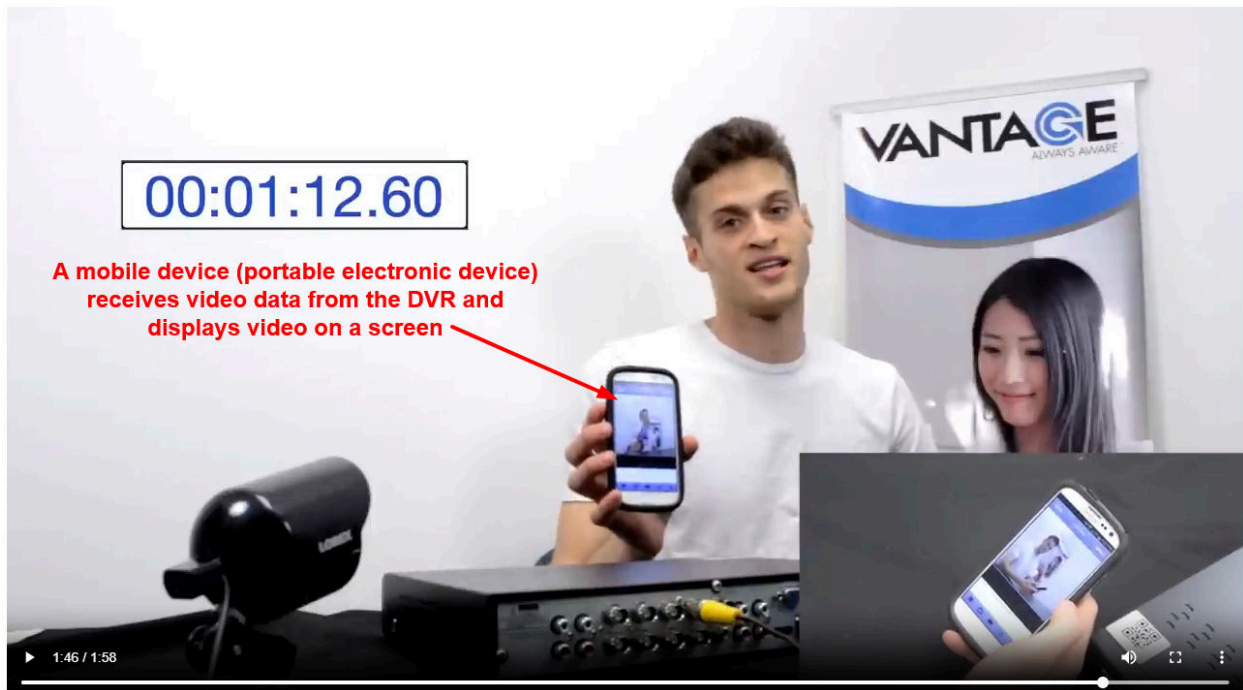
For the reasons expressly articulated above (*supra*, §V.E.4), a POSITA would have found it obvious to combine Lorex Video and Kuo such that Lorex Video's remote client device (e.g., smartphone, tablet, or PC) would not have had and would not register a unique ID for associating connecting information of the remote client device when contacting the linking server for establishing the P2P connection or while the P2P connection is being established. EX1003, ¶236.

Claim [2]

Lorex Video depicts a DVR in the form of a set top box. *Supra*, Element [1pre]; Ground 1A at [2]; EX1012; 0:01-0:38; EX1003, ¶¶238-239 (citing EX1016, [0003] and EX1017, [0049]).

Claim [3]

Lorex Video discloses the ***remote client device*** as an Android smartphone, which is a ***portable electronic device***. EX1012, 0:45-1:42 (“Use my Android phone...automatically we have live streaming right to my phone”); EX1003, ¶¶241-243.



EX1012, 1:46 (annotated).

Claim [4]

Lorex Video discloses the *remote client device* as an Android smartphone, which is a *mobile phone*. EX1012, 0:45-1:42 (“Use my Android phone...automatically we have live streaming right to my phone”); EX1012, 0:45-1:42; EX1003, ¶¶245-246.

Claim [5]

Supra, Element [1h]. EX1003, ¶¶247-249.

Claim [6]

Kuo discloses, and the Lorex Video-Galvin-Kuo combination provides, that the linking server transmits hole-punching messages to establish a P2P connection

to both endpoints of the connection, which would include the mobile device and the DVR of Lorex Video in the combination described above. EX1011, [0029] (“The linking server group A (20)...sends hole-punching information 960 and hole-punching information 961 to the proximal device 4 and the remote device A (31) so as to establish a point-to-point link 97 between the proximal device 4 and the specified remote device A (31).”), [0038], FIG. 11; *supra*, §V.E.4; EX1003, ¶¶250-252.

Claim [7]

For the reasons addressed above with respect to Element [1b], Lorex Video discloses that the second interface couples to the Internet through an external routing device. *Supra*, [1b]; EX1012, 0:35-0:39 (the DVR “is connected to my router using an Ethernet [cable]”); EX1003, ¶¶253-255.

Claim [8]

Claim 8 merely adds an intended use of the “routing device” and does not further define the claimed “electronic device for concentrating information.” The additional features recited in claim 8 are therefore not entitled to patentable weight. Even if it were, it would have been obvious to a POSITA to implement Lorex Video’s router as an IP router given the ubiquitous use of IP routers before the alleged invention and to achieve known benefits of IP routers (e.g., to connect the

DVR to the Internet or other IP networks). EX1012, 0:35-0:39 (the DVR “is connected to my router using an Ethernet [cable]”); EX1003, ¶¶256-257.

Claim [10]

Claim 10 merely adds an intended use of the “routing device” and does not further define the claimed “electronic device for concentrating information.” The additional features recited in claim 10 are therefore not entitled to patentable weight. Lorex Video’s DVR nonetheless would have been capable of connecting to such a “routing device” as claimed since the additional features in claim 10 would not have interfered with the functions of the DVR. EX1012, 0:35-0:39 (the DVR “is connected to my router using an Ethernet [cable]”); EX1003, ¶¶258-259.

Claim [16]

As described above in connection with Element [1g], Lorex Video’s mobile device can display video data from a DVR and the mobile device receives this video data directly from the DVR over a P2P connection. EX1012, 0:38-1:58; EX1003, ¶¶260-262. Lorex Video confirms that the video streamed from the DVR is formatted so that the video is suitable for viewing. EX1012, 1:46; EX1003, ¶261. This is evident at least because video from Lorex Video’s DVR is displayed on the screen of the mobile device, indicating that the DVR has streamed the video in a format that allows the mobile device to display the video on the screen. EX1003, ¶261.

F. GROUND 2B: Lorex Video in view of Galvin, Kuo, and Kim517 would have rendered obvious claim 9

1. *The Lorex Video-Galvin-Kuo-Kim517 Combination*

A POSITA would have found it obvious and would have been motivated to further modify the Lorex Video-Galvin-Kuo combination based on Kim517's suggestion for remotely controlling a PTZ camera or other appliance wirelessly connected to a home gateway like Lorex Video's DVR for substantially the same reasons as those discussed above in Ground 1B. *Supra*, § V.B.2; EX1003, ¶263.

2. *Application to Challenged Claims*

Claim [9]

The Lorex Video-Galvin-Kuo- Kim517 combination would have rendered Claim [9] obvious for at least the reasons described above in connection with the analysis of Claim [9] in Ground 1B. *Supra*, § V.B.3, Claim [9]; EX1003, ¶¶264-265.

VI. DISCRETIONARY DENIAL IS NOT JUSTIFIED

A. The Petition's New Prior Art and Errors Made During Prosecution Warrant Institution—35 U.S.C. § 325(d)

This Petition does not present a situation where “the same or substantially the same prior art or arguments” were previously presented. 35 U.S.C. § 325(d); *Advanced Bionics, LLC v. MED-EL Elektromedizinische Geräte GmbH*, IPR2019-01469, Paper 6 (Feb. 13, 2020). Indeed, there is no indication from the file history that Lorex Manual, Kim941, Kim517, Lorex Video, and Galvin were previously

presented to the Office during prosecution of the '916 Patent. Nor does the file history reveal consideration by the Examiner of any of the prior art combinations from Grounds 1A-2B of this Petition. And while the '916 Patent allegedly claims priority to Kuo, Patent Owner never alerted the Examiner to the fact that the claims recite features that were not disclosed in Kuo or otherwise before the Jan. 7, 2014 provisional application (EX1006). Patent Owner failed to identify Kuo as prior art during prosecution of the '916 Patent, and the record contains no indication that the Examiner appreciated that Kuo qualified as prior art to the Challenged Claims. Simply put, none of Grounds 1A-2B were addressed during prosecution.

B. The *Fintiv* Factors Weigh in Favor of Institution—35 U.S.C. § 314(a)

Essentially all of the *Fintiv* factors weigh against exercising discretionary denial. The related litigation in the District of Delaware (1:24-cv-00169) is in its infancy.

Factor 1—No motion to stay has been filed. This factor is neutral.

Factor 2—Even though Patent Owner filed its Complaint (EX1015) against Reolink on February 8, 2024, Reolink's initial motion to dismiss is still pending and no Answer to the Complaint has been filed. No scheduling order/trial date has been established. The Board's final decision will surely precede the not-yet-scheduled jury trial in the Delaware proceeding. Additionally, the current median-

time-to trial in Delaware is 38.0 months—indicating a jury trial date long after any final decision in this IPR. See https://www.uscourts.gov/sites/default/files/fcms_na_distprofile1231.2023_0.pdf, 14. Factor 2 weighs heavily against exercising discretion to deny.

Factor 3—Neither Patent Owner nor Reolink has invested in *Markman* briefing, substantive fact discovery, expert discovery, summary judgment motions, or pre-trial preparations. Reolink diligently filed this Petition *before* receiving preliminary infringement contentions from Patent Owner and even *before* submitting an Answer to the initial Complaint. As such, the investment “in the []lawsuit, particularly as related to any validity issues, has not been substantial.” *Illumina, Inc. v. Ravgen, Inc.*, IPR2021-01271, Paper 12, 27 (January 26, 2022). Factor 3 weighs heavily against exercising discretion to deny.

Factor 4—Reolink diligently filed this Petition *before* receiving preliminary infringement contentions from Patent Owner, so it follows that there are no invalidity contentions in the Reolink litigation at this time. For this reason, the overlap of issues cannot be fully assessed, and Patent Owner cannot point to any evidence to the contrary. Factor 4 is neutral.

Factor 5—Petitioners are the defendants in the Reolink lawsuit. EX1015, EX1018. Because the Board’s final decision here will likely precede the date for

Reolink’s jury trial “by many months,” this factor “weighs against discretionary denial.” *Illumina*, at 30.

Factor 6—The merits of this Petition are compelling as demonstrated by Grounds 1A-2B above. Factor 6 weighs heavily in favor of institution.

VII. PAYMENT OF FEES – 37 C.F.R. §42.103

Reolink authorizes the Patent and Trademark Office to charge Deposit Account No. 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)

Reolink Innovation Inc. and Shenzhen Reolink Technology Co., Ltd. (“Reolink”) are the Petitioners and real parties-in-interest. No other party had access or control over this Petition, and no other party provided funding for this Petition.

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

Petitioners are not aware of any disclaimers, reexamination certificates, or other petitions for IPR of the ’916 Patent. The ’916 Patent is the subject of civil action captioned *ThroughTEK Co. Ltd. v. Reolink Innovation Inc.*, Case No. 1:24-cv-00169 (D. Del.), Document 1 (Complaint), February 8, 2024. *See* EX1015.

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

Reolink provides the following designation of counsel.

<u>Lead Counsel</u>	<u>Backup Counsel</u>
Michael Hawkins, Reg. No. 57,867 Fish & Richardson P.C. 60 South Sixth Street Minneapolis, MN 55402 Tel: 202-783-5070 Fax: 877-769-7945 Email: IPR52472-0007IP1@fr.com	Nicholas Stephens, Reg. No. 74,320 Cameron Ubel, Reg. No. 77,081 John Phillips, Reg. No. 35,322 Joseph Bauer, Reg. No. 81,218 Fish & Richardson P.C. 60 South Sixth Street Minneapolis, MN 55402 Tel: 202-783-5070 Fax: 877-769-7945 IPR52472-0007IP1@fr.com

D. Service Information

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

Petitioner consents to electronic service by email at IPR52472-0007IP1@fr.com.

Respectfully submitted,

Dated: July 19, 2024

/Michael T. Hawkins/
Michael Hawkins, Reg. No. 57,867
Nicholas Stephens, Reg. No. 74,320
Cameron Ubel, Reg. No. 77,081
John Phillips, Reg. No. 35,322
Joseph Bauer, Reg. No. 81,218
Fish & Richardson P.C.
60 South Sixth Street
Minneapolis, MN 55402
T: 202-783-5070
F: 877-769-7945

(Control No. IPR2024-01192)

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 13,815 words, which is less than the 14,000 allowed under 37 CFR §42.24.

Dated: July 19, 2024

/Michael T. Hawkins/
Michael Hawkins, Reg. No. 57,867
Nicholas Stephens, Reg. No. 74,320
Cameron Ubel, Reg. No. 77,081
John Phillips, Reg. No. 35,322
Joseph Bauer, Reg. No. 81,218
Fish & Richardson P.C.
60 South Sixth Street
Minneapolis, MN 55402
T: 202-783-5070
F: 877-769-7945

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 July 19, 2024, 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:

Litron Patent and Trademark Office
11F, No.287, Sec. 3, Nanjing E. Rd.
Songshan District
Taipei City - 10595
TAIWAN

/Crena Pacheco/

Crena Pacheco
Fish & Richardson P.C.
60 South Sixth Street, Suite 3200
Minneapolis, MN 55402
pacheco@fr.com