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

| | | |
|---|---|---|
| In re Patent of: | Kuo et al. | |
| U.S. Patent No.: | RE47,842 | Attorney Docket No.: 52472-0005IP1 |
| Issue Date: | February 4, 2020 | |
| Appl. Serial No.: | 16/218,841 | |
| Filing Date: | December 13, 2018 | |
| Title: | SYSTEM AND METHOD OF IDENTIFYING NETWORKED DEVICE FOR ESTABLISHING A P2P CONNECTION | |

**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. RE47,842 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 '842 PATENT ..... 3
- **A.** Brief Description ..... 3
- **B.** Prosecution of the '842 Patent ..... 5
- **C.** The '842 Patent Is Entitled to an Effective Filing Date No Earlier Than September 20, 2016 ..... 8

**III.** LEVEL OF ORDINARY SKILL ..... 11

**IV.** CLAIM CONSTRUCTION ..... 11

**V.** DETAILED EXPLANATION OF GROUNDS ..... 12
- **A.** GROUND 1: Lorex Guide in View of Kim Would Have Rendered Obvious Claims 1-3, 6, 10, 12-14, 17, and 18 ..... 12
  - 1. Lorex Guide ..... 12
  - 2. Kim ..... 14
  - 3. The Lorex Guide-Kim Combination ..... 16
  - 4. Application to Challenged Claims ..... 19
    - Element [1.P] ..... 19
    - Element [1.1] ..... 19
    - Element [1.2] ..... 21
    - Element [1.3] ..... 23
    - Element [1.4] ..... 24
    - Element [1.5] ..... 26
    - Element [1.6] ..... 29
    - Element [2] ..... 30
    - Element [3] ..... 31
    - Element [6] ..... 31
    - Element [10] ..... 31
    - Element [12.P] ..... 32
    - Element [12.1] ..... 32
    - Element [12.2] ..... 32

Element [12.3] ..... 33
Element [12.4] ..... 33
Element [12.5] ..... 33
Element [12.6] ..... 34
Element [13] ..... 34
Element [14] ..... 34
Element [17] ..... 35
Element [18] ..... 36

**B.** GROUND 2: Kim in View of Lorex Video Would Have Rendered Obvious Claims 1-3, 6, 10, 12-14, 17, and 18 ..... 37
1. Lorex Video ..... 37
2. The Kim-Lorex Video Combination ..... 38
3. Application to Challenged Claims ..... 40
Element [1.P] ..... 40
Element [1.1] ..... 40
Element [1.2] ..... 42
Element [1.3] ..... 43
Element [1.4] ..... 45
Element [1.5] ..... 46
Element [1.6] ..... 49
Element [2] ..... 50
Element [3] ..... 51
Element [6] ..... 52
Element [10] ..... 53
Element [12.P] ..... 53
Element [12.1] ..... 54
Element [12.2] ..... 54
Element [12.3] ..... 54
Element [12.4] ..... 55
Element [12.5] ..... 55
Element [12.6] ..... 55

Element [13] ..... 56
Element [14] ..... 56
Element [17] ..... 56
Element [18] ..... 57

**C.** GROUND 3: Throughtek-2012 in View of Lorex Video Would Have Rendered Obvious Claims 1-4, 6-19 ..... 57
1. Throughtek-2012 ..... 57
2. The Througtek-2012-Lorex Video Combination ..... 58
3. Application to Challenged Claims ..... 60
Element [1.P] ..... 60
Element [1.1] ..... 60
Element [1.2] ..... 61
Element [1.3] ..... 61
Element [1.4] ..... 62
Element [1.5] ..... 62
Element [1.6] ..... 63
Element [2] ..... 64
Element [3] ..... 64
Element [4] ..... 64
Element [6] ..... 65
Element [7] ..... 65
Element [8] ..... 65
Element [9] ..... 65
Element [10] ..... 66
Element [12.P] ..... 66
Element [12.1] ..... 66
Element [12.2] ..... 67
Element [12.3] ..... 67
Element [12.4] ..... 67
Element [12.5] ..... 67
Element [12.6] ..... 67

Element [13] ..... 67
Element [14] ..... 68
Element [15] ..... 68
Element [16] ..... 68
Element [17] ..... 68
Element [18] ..... 68
Element [19] ..... 68

**VI.** DISCRETIONARY DENIAL IS NOT JUSTIFIED ..... 68
- **A.** The Petition's New Prior Art and Errors Made During Prosecution Warrant Institution—35 U.S.C. § 325(d) ..... 68
- **B.** The Fintiv Factors Weigh in Favor of Institution—35 U.S.C. § 314(a) 69

**VII.** PAYMENT OF FEES—37 C.F.R. §42.103 ..... 73

**VIII.** MANDATORY NOTICES—37 C.F.R §42.8(a)(1) ..... 73
- **A.** Real Party-In-Interest—37 C.F.R. §42.8(b)(1) ..... 73
- **B.** Related Matters—37 C.F.R. §42.8(b)(2) ..... 73
- **C.** Lead And Back-Up Counsel—37 C.F.R. §42.8(b)(3) ..... 74
- **D.** Service Information ..... 74

## LIST OF EXHIBITS

| | |
|---|---|
| EX1001 | Declaration of Harry Bims, Ph.D. |
| EX1002 | U.S. Patent No. RE47,842 ("the '842 patent") |
| EX1003 | Prosecution History of Provisional Application Serial No. 61/812,262 ("the provisional application") |
| EX1004 | Prosecution History of U.S. Patent No. 9,787,498 ("the utility application") |
| EX1005 | Prosecution History of the '842 patent ("the reissue application") |
| EX1006 | Lorex LNC100 Series User's Guide Version 2.0 (2012), *available at* https://www.lorextechnology.com/downloads/ip-cameras/LNC104/LNC100_SERIES_MANUAL_EN_R2_web.pdf ("Lorex Guide") |
| EX1007 | U.S. Publication No. 2011/0082941 ("Kim") |
| EX1008 | Lorex Technology Inc., "How-to Set Up and Connect the NEW Lorex LNC100 Series IP Network Camera" (October 19, 2012), *available at* https://www.youtube.com/watch?v=DPaIWj2f65I ("Lorex Video") |
| EX1009 | Lorex Technology Inc., "How-To Get to Know New Lorex IP Wireless Network Camera" (October 5, 2012), *available at* https://www.youtube.com/watch?v=g9U-xhOk8kQ ("Lorex Unboxing") |
| EX1010 | Lorex Technology Inc., "How to Set up Wireless Network Cameras Using QR codes" (November 23, 2012), *available at* https://www.youtube.com/watch?v=HzJfkqg2VWY ("Lorex QR Codes") |
| EX1011 | Declaration of Vlad Kardashov |

| | |
|---|---|
| EX1012 | [RESERVED] |
| EX1013 | [RESERVED] |
| EX1014 | Korean Patent No. KR100984288B1 |
| EX1015 | Certified English Translation of Korean Patent No. KR100984288B1 ("Park") |
| EX1016 | German Utility Model No. DE202012101164U1 |
| EX1017 | Certified English Translation of German Utility Model No. DE202012101164U1 ("Throughtek-2012") |
| EX1018 | Throughtek Co. Ltd., *CSJ233 P2P IP Camera Plug and View Instant Surveillance* (2011) ("2011 Brochure") |
| EX1019 | *ThroughTEK Co., Ltd. v. Reolink Innovation Inc. et al.*, Case No. 1-23-cv-00218 (DDE), Document 1 (Complaint), February 28, 2023 |
| EX1020 | Ford et al., *Peer-to-Peer Communication Across Network Address Translators*, USENIX Annual Technical Conference, pp. 179-192 (2005) |
| EX1021 | Reolink Technology Co., Ltd., *Reolink Support \| Initial Setup for Reolink Argus Series Cameras via Reolink App* (Aug. 22, 2019), *available at* https://www.youtube.com/watch?v=jn2BhMmKcyg ("Reolink Video") |
| EX1022 | U.S. Publication No. 2014/0013100 ("Menzel") |
| EX1023 | U.S. Publication No. 2012/0287290 ("Jain") |
| EX1024 | Saxena et al., *Secure Device Pairing based on a Visual Channel*, IEEE Symposium on Security and Privacy (2006) ("Saxena") |

| | |
|---|---|
| EX1025 | U.S. Publication No. 2010/0259549 ("Brown") |
| EX1026 | Scott et al., *Using Visual Tags to Bypass Bluetooth Device Discovery*, Mobile Computing & Communications Review, Vol. 1, No. 2 (2005) ("Scott") |
| EX1027 | Eppinger, *TCP Connections for P2P Apps: A Software Approach to Solving the NAT Problem*, Carnegie Mellon University Institute for Software Research International (2005) ("Eppinger") |
| EX1028 | Maier et al., *NAT Hole Punching Revisited*, 36th Annual IEEE Conference on Local Computer Networks (2011) ("Maier") |
| EX1029 | U.S. Publication No. 2008/0313721 ("Corella") |

## LISTING OF CLAIMS

| Claim Element | Language |
|---|---|
| [1.P] | A system to identify a networked device for establishing a point-to point (P2P) connection, the system comprising |
| [1.1] | a network server having a list of networked devices that are pre-registered in the network server, wherein the network server associates a corresponding identification of each networked device with a corresponding IP address of the networked device for enabling terminal devices to establish P2P connections with the plurality of networked devices; |
| [1.2] | a first networked monitoring device, having a first identification embedded in the first networked monitoring device, wherein the first networked monitoring device registers the embedded first identification into the list of networked devices to associate a corresponding IP address of the first networked monitoring device with the first identification by connecting to the network server through the Internet; |
| [1.3] | an image pattern, being attached on the first networked monitoring device and comprising the first identification for establishing a P2P connection with the first networked monitoring device; and |
| [1.4] | a terminal device, wherein the terminal device generates a connection request signal when the image pattern is captured to the terminal device; and the terminal device transmits the connection request signal to the network server through the Internet, |
| [1.5] | wherein the network server obtains the first identification according to the connection request signal and obtains the corresponding IP address of the first networked monitoring device according to the obtained first identification for establishing a P2P connection between the terminal device and the first networked monitoring device, wherein the network |

| | |
|---|---|
| | server respectively transmits hole-punching messages to the terminal device and the first networked monitoring device via the Internet to establish the P2P connection, and |
| [1.6] | wherein the first networked monitoring device does not capture any image pattern associated with the terminal device for establishing the P2P connection between the terminal device and the first networked monitoring device. |
| [2] | The system according to claim 1, wherein the image pattern is a barcode, wherein a barcode image is generated in the terminal device. |
| [3] | The system according to claim 2, wherein the terminal device converts the barcode image into the first identification, wherein the connection request signal comprises the first identification. |
| [4] | The system according to claim 2, wherein the connection request signal comprises the barcode image and the network server converts the barcode image into the first identification. |
| [5] | [Canceled in Reissue] |
| [6] | The system according to claim 2, wherein the first networked monitoring device includes a default security password and the terminal device enters the default security password to log on the first networked monitoring device. |
| [7] | The system according to claim 6, wherein an image capture unit of the terminal device captures the barcode to generate the barcode image, wherein the barcode image comprises the default security password. |
| [8] | The system according to claim 7, wherein the terminal device converts the barcode image into the first identification and the default security password, wherein the connection request signal comprises the first identification and the default security password. |

| | |
|---|---|
| [9] | The system according to claim 7, wherein the connection request signal comprises the barcode image, wherein the network server converts the barcode image into the first identification and the default security password. |
| [10] | The system according to claim 2, wherein the barcode is a quick response code (QR code). |
| [11] | The system according to claim 2, wherein the barcode is a one dimensional barcode. |
| [12.P] | A method to identify networked device for establishing a point-to point (P2P) connection, the method comprising the steps of: |
| [12.1] | (a) connecting a first networked monitoring device to a network server through the Internet, wherein the network server has a list of networked devices that are pre-registered in the network server, wherein the network server associates a corresponding identification of each networked device with a corresponding IP address of the networked device for enabling terminal devices to establish P2P connections with the plurality of networked devices; |
| [12.2] | (b) registering a first identification of the first networked monitoring device into the list of networked devices of the server; |
| [12.3] | (c) providing an image pattern comprising the first identification, wherein the image pattern is attached on the first networked monitoring device for establishing a P2P connection with the first networked monitoring device; |
| [12.4] | (d) generating a connection request signal by a terminal device when the image pattern is captured to the terminal device and transmitting the connection request signal to the network server by the terminal device through the Internet; and |
| [12.5] | (e) identifying the first networked monitoring device in the list of the networked devices of the network server to obtain the first identification according to the connection request signal |

| | |
|---|---|
| | and obtain the corresponding IP address of the first networked monitoring device according to the obtained first identification for establishing a P2P connection between the terminal device and the first networked monitoring device, wherein the network server respectively transmits hole-punching messages to the terminal device and the first networked monitoring device via the Internet to establish the P2P connection, and |
| [12.6] | wherein the first networked monitoring device does not capture any image pattern associated with the terminal device for establishing the P2P connection between the terminal device and the first networked monitoring device. |
| [13] | The method according to claim 12, wherein the image pattern is a barcode, wherein an image capture unit of the terminal device captures the barcode to generate a barcode image. |
| [14] | The method according to claim 13, wherein the step (d) further comprises the sub-steps of: (d1) interpret the barcode image to the first identification by an image interpreting unit of the terminal device; (d2) embed the first identification in the connection request signal. |
| [15] | The method according to claim 13, wherein the step (d) further comprises (d1) embedding the barcode image in the connection request signal; (d2) transmitting the connection request signal to the network server through the Internet. |
| [16] | The method according to claim 15, wherein the step (e) further comprises the sub-steps: (e1) receiving the connection request signal; (e2) interpreting the barcode image to the first identification by an image interpreting unit of the server. |
| [17] | The method according to claim 13, wherein the step (e) comprises the steps of: (f) inputting a security password through the terminal device; (g) determining whether the security password is the same as a default security password in the first networked monitoring device, if not, then back to step (f), and if so, allow the terminal device to log on the first networked monitoring device. |

| | |
|---|---|
| [18] | The method according to claim 13, wherein the barcode is a quick response code (QR code). |
| [19] | The method according to claim 13, wherein the barcode is a one dimensional barcode. |

Reolink Innovation Inc. and Shenzhen Reolink Technology Co., Ltd. (collectively, "Petitioners" or "Reolink") petition for *Inter Partes* Review ("IPR") of claims 1-4 and 6-19 of U.S. Patent RE47,842 ("the '842 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 '842 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 1-3 listed below. An expert declaration from Harry Bims, Ph.D. supports Grounds 1-3. *See* EX1001.

| Ground | Claims | Basis for Rejection |
|---|---|---|
| 1 | 1-3, 6, 10, 12-14, 17, and 18 | §103 – Obvious based on Lorex Guide (EX1006) in view of Kim (EX1007) |
| 2 | 1-3, 6, 10, 12-14, 17, and 18 | §103 – Kim in view of Lorex Video (EX1008) |
| 3 | 1-4, 6-19 | §103 – Obvious based on Throughtek-2012 (EX1017) in view of Lorex Video (EX1008) |

All Grounds 1-3 rely on publications that were published well before the April 16, 2013 filing date of the '842 patent's provisional application, and thus qualify as prior art under 35 U.S.C. § 102(a)(1):

| Reference | Prior Art Status |
|---|---|
| **Lorex Guide (EX1006)** | §102(a)(1) – published in 2012[1] |
| **Kim (EX1007)** | §102(a)(1) – published April 7, 2011 |
| **Lorex Video (EX1008)** | §102(a)(1) – published in October 2012[2] |
| **Throughtek-2012 (EX1016[3])** | §102(a)(1) – entry date April 17, 2012; publication date June 6, 2012 |

To the extent Patent Owner contends that Ground 3's Throughtek-2012 (or any of the other cited publications) is not prior art due to an exception in §102(b)(1), Petitioners note that the '842 patent is not entitled to the filing date of its provisional application because the provisional application is noticeably silent regarding the negative limitation (Elements [1.6] and [12.6]) amended into all claims of the '842 patent on September 20, 2016. *Infra,* Section II.C. Thus, new matter was injected into the '842 patent—a claim element never mentioned in the provisional application—and the effective filing date of the '842 patent is much later than April

[1] *See* EX1006, 177 (dated "2012"); EX1011, ¶¶5-9 (sworn testimony confirming the public dissemination of the Lorex Guide throughout 2012).

[2] *See* EX1008 (dated "October 19, 2012"); EX1011, ¶¶5-8 and 10 (confirming the public dissemination of the Lorex Video in October 2012).

[3] ThroughTek-2012 published in German. *See* EX1016. This Petition cites to a certified English translation of Througtek-2012 (EX1017).

16, 2013. *Infra,* Section II.C. For at least this reason, no exception in §102(b)(1) applies to Throughtek-2012 nor any other publication cited above. 35 U.S.C. § 102(b)(1); *see also* EX1011, ¶13 (confirming the Lorex disclosures were not obtained from any inventor listed on the '842 patent).

## II. SUMMARY OF THE '842 PATENT

### A. Brief Description

The '842 patent describes techniques for establishing P2P[4] connections between network endpoints such as a networked monitoring device (e.g., an IP camera) and a terminal device (e.g., a smartphone). EX1001, ¶¶24-39. The '842 patent briefly describes a hole-punching technique for forming P2P connections, and it admits such techniques were "well known." EX1002, 5:59-61, 5:40-41, 3:5-8; EX1018, 2. The evidence here confirms this admission—especially because hole-punching was commonly implemented to permit direct connections to be established between devices in different networks that would otherwise be unable

[4] The '842 patent uses the term "P2P" as shorthand for "point-to-point." *See* EX1002, 1:32-38, 9:8, 10:19. Another term that P2P commonly represents in the art is "peer-to-peer." EX1001, ¶24, FN1. The evidence here confirms that the '842 patent's "point-to-point" connections established over the Internet would plainly include conventional "peer-to-peer" connections. *Id.*

to communicate due to firewalls and/or network address translators (NATs). EX1001, ¶¶32-35 (citing corroborating exhibits EX1018, 1020, 1027-1028).

Conventional hole punching techniques often involved one device (e.g., a terminal device such as a smartphone) initiating a request for a P2P connection with another device (e.g., a networked monitoring device such as a webcam) by transmitting to a server a request that included an identifier of the other device. EX1001, ¶¶32-35. To relieve the burden of a user manually typing the identifier of the networked device in the terminal device, the "key focus" of the '842 patent was a "barcode" attached to the networked device so that a user could capture an image of the barcode with a smartphone to obtain the identifier of the networked device. EX1002, 4:50-55 ("key focus"), 3:30-38 ("[u]nlike prior art to manually enter the identification code word by word"); EX1001, ¶¶36-39. As Dr. Bims explains, however, even this "key focus" of the '842 patent was well known in the art. EX1001, ¶¶26-31 (citing corroborating exhibits EX1006, EX1008, EX1022, EX1024-1026).

FIGS. 3 and 4, reproduced below, illustrate the '842 patent's proposed use of barcode images "201" and "211" for identifying a networked device targeted for a P2P connection by a terminal device:

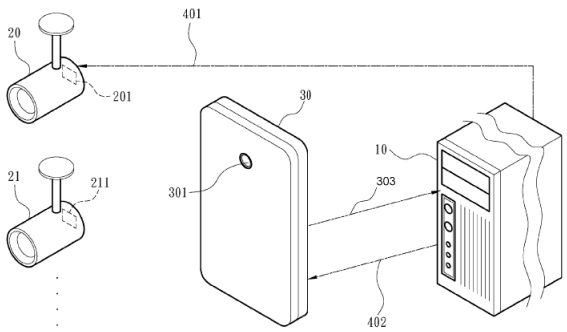



FIG. 3

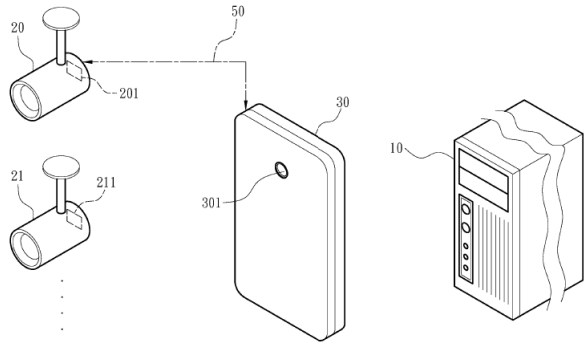



FIG. 4

EX1002, FIGS. 3-4; *see also id.*, 4:1-6:61, FIGS. 1-2, 5. As shown above, barcodes 201, 211 are respectively affixed to the first and second networked devices 20, 21, which encode the identifiers for the first and second networked devices 20, 21 that have been registered with the network server 10. *Id.*, 4:50-55. When the terminal device 30 attempts to connect to the first networked device 20, it sends an identifier of device 20 that the terminal device 30 read from the image of the barcode 201 to the network server 10 in a "connection request signal 303." *Id.*, 4:64-5:39, FIGS. 2-3. The network server 10 identifies the first networked device 20 using the identifier and employs "well-known" hole-punching techniques to establish a P2P connection between terminal device 30 and the first networked device 20. *Id.*, 5:40-67.

### B. Prosecution of the '842 Patent

The '842 Patent is a reissue of original U.S. Patent No. 9,787,498 ("the original '498 patent"), which claimed priority to Provisional Application No. 61/812,262 ("provisional application"). The three stages (provisional, utility, and reissue) are summarized here. EX1001, ¶¶40-48.

*The Provisional Application*

The provisional application was filed on April 16, 2013, and the specification was predominantly in Chinese. EX1003, 4-26. Shortly thereafter, the PTO notified the Applicant that an English translation "must be filed in the provisional application." EX1003, 37. The Applicant delayed for three years before doing so. EX1003, 42.

The English translation confirmed that the provisional never expressly described the negative limitation that was later amended into all claims of the '842 patent—namely, Elements [1.6]/[12.6] mandating that "the first networked monitoring device does <u>not</u> capture any image pattern associated with the terminal device for establishing the P2P connection between the terminal device and the first networked monitoring device." EX1003, 42-75; EX1001, ¶¶41. This silence in the provisional application is meaningful, as explained below.

*The Utility Application*

The utility application was filed on July 25, 2013. EX1004, 47; EX1003, 37. The utility application injected new matter—at least a new figure (FIG. 6) and text associated with FIG. 6. EX1002, FIG. 6, 3:58-59, 4:1-17, 8:35-49, 8:60-9:5; *compare* EX1004, 32-33, 39 (new FIG. 6 and new text), *with* EX1003, 43-53 (lacking FIG. 6 and such new text); EX1001, ¶¶42-47.

During examination, there were three office actions, which included prior art

rejections based upon patent literature not raised in this Petition. EX1004, 52-61, 84-106, 133-161. The Examiner asserted that the claims were obvious based on prior art including Jain (EX1023). *Id.*, 84-106. In September 2016, the Applicant attempted to distinguish Jain's "pairing" procedure that was said to involve two mobile phones "captur[ing] an image pattern of each other" by adding the negative limitation recited in Elements [1.6]/[2.6]. *Id.*, 133; *see also id.*, 125-135, 77-88, 92-114. Following this amendment, the Examiner withdrew his reliance on Jain as a primary reference but further identified §112 defects. EX1004, 141-169. For instance, the Examiner specifically noted that the negative limitation lacked written description support. EX1004, 148. In reply, the Applicant refused to delete or modify the negative limitation but rather argued that the limitation is "inherently implied" in the specification. EX1004, 188-189.

Following this response, the Examiner allowed the application but provided no reasons for allowance. EX1004, 197-202. As demonstrated by Grounds 1-3 of this Petition, however, the application never should have been allowed. *Infra,* Section II.C. The Examiner had not considered more pertinent prior art set forth in Grounds 1-3, each of which demonstrates compellingly that the Challenged Claims would have been obvious.

*The Reissue Application*

The reissue application was filed about 14 months after the original '498

patent issued, and it was filed for the purported reason of adding three coinventors. EX1005, 3. In the first and only office action, dependent claim 5 was rejected as being duplicative with an element already recited in claim 1. EX1005, 73-74. Patent Owner canceled claim 5, and all remaining original claims were reissued. There were no prior art rejections during prosecution of the reissue application. Again, the '842 patent is ripe for meaningful review. EX1001, ¶48.

### C. The '842 Patent Is Entitled to an Effective Filing Date No Earlier Than September 20, 2016

The evidence here demonstrates that all claims of the '842 patent recite new matter that was plainly never described in the provisional application. EX1001, ¶¶49-54. In particular, the negative limitation recited by Elements [1.6] and [12.6]—which requires that "the first networked monitoring device does <u>not</u> capture any image pattern associated with the terminal device for establishing the P2P connection"—is never expressed in the provisional application. *Id.*

To be sure, the law mandates that "silence will not generally suffice to support a negative claim limitation," but that is exactly what is present in the provisional application—silence. *Novartis Pharms. Corp. v. Accord Healthcare, Inc.*, 38 F.4th 1013, 1017-18 (Fed. Cir. 2022). The Federal Circuit explained that "[s]ilence is generally not disclosure. … If it were, then every later-added negative limitation would be supported so long as the patent makes no mention of it." *Id.*

In more detail, the provisional application only generically states that "[t]hrough hole-punching technique, which is well known in the field, the server 10 respectively transmits hole-punching messages 401, 402" resulting in "a direct communication passage 50" between the devices 20 and 30. *Id.* But the provisional application's sparse disclosure regarding its "hole-punching technique" or how the "direct communication passage 50" is established between devices 20, 30 falls well short of supporting the negative limitation in Elements [1.6]/[12.6]. EX1001, ¶¶51-52.

Indeed, the ambiguity in the '842 patent indicates the negative limitation was not necessarily present. The provisional application generically describes that the networked devices 20, 21 (webcams) "connect to the network server 10 through the internet" (col. 4:32-36), but nothing in the provisional application forbids those webcams from the conventional option of scanning a QR code on a wifi-connected smartphone to receive the wifi connection information used for establishing the P2P connection. EX1001, ¶52. And, apart from setting a "default security password," the provisional application provides little to no detail regarding the specific procedures for ensuring mutual authorization of the connection between the terminal device 30 and the first networked device 20—yet Jain amply demonstrated the traditional option of capturing a QR code on both camera-equipped devices to verify authorization for a connection. EX1001, ¶52; EX1004, 133 ("must both capture an

image pattern of each other"). Simply put, a POSITA would have recognized known options for implementing the first networked device 20 that in fact could have involved such image capture by the first networked device 20. EX1001, ¶52. As such, the Applicant's contention that the negative limitation was "inherently implied" (EX1004, 188-189) was noticeably inaccurate and lacked candor. EX1001, ¶¶52-53 (citing corroborating exhibits EX1021, EX1023, EX1024).

Based on these facts and the *Novartis* precedent, it is clear the Elements [1.6] and [12.6] were new matter injected into the '842 patent beyond the express teaching in the provisional application. The Challenged Claims of the '842 patent therefore are not entitled to the benefit of the provisional application's filing date.

Because the negative limitations of Elements [1.6]/[12.6] were never expressed until the September 20, 2016 amendment, the Challenged Claims are entitled to an effective filing date no earlier than September 20, 2016. EX1004, 125-129; EX1001, ¶¶49-54. All publications cited in Grounds 1-3 were published before April 2013, so they surely predate September 2016.

Notably, even if Patent Owner contended that the new matter added on the July 25, 2013 filing date of the utility application (EX1002, FIG. 6, 3:58-59, 4:1-17, 8:35-49, 8:60-9:5) somehow provided a disclosure for the negative limitations of Elements [1.6]/[12.6], such a contention does not affect Grounds 1-3. All publications cited in Ground 3 were published more than a year before July 25, 2013.

*Id.* And all publications cited in Grounds 1-2 were published in 2012 or earlier and their teachings were certainly not obtained, directly or indirectly, from the named inventors of the '842 patent; they are prior art regardless of whether the effective filing date is September 20, 2016, July 25, 2013, or April 16, 2013. *Supra*, Section II.B (citing to EX1011, ¶13). Dr. Bims considered each of these various dates in his analysis and concluded that the Challenged Claims would have been obvious regardless of which date applied. EX1001, ¶54.

## III. LEVEL OF ORDINARY SKILL

The evidence here confirms that a POSITA would have had a bachelor's degree in electrical engineering and two years of work experience with network and communication technologies. EX1001, ¶¶15-16.

## 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 '842 patent and the prior art/predictable combinations articulated in Grounds 1-3, Petitioners submit that no claim elements need a formal construction for purposes of resolving the controversy 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

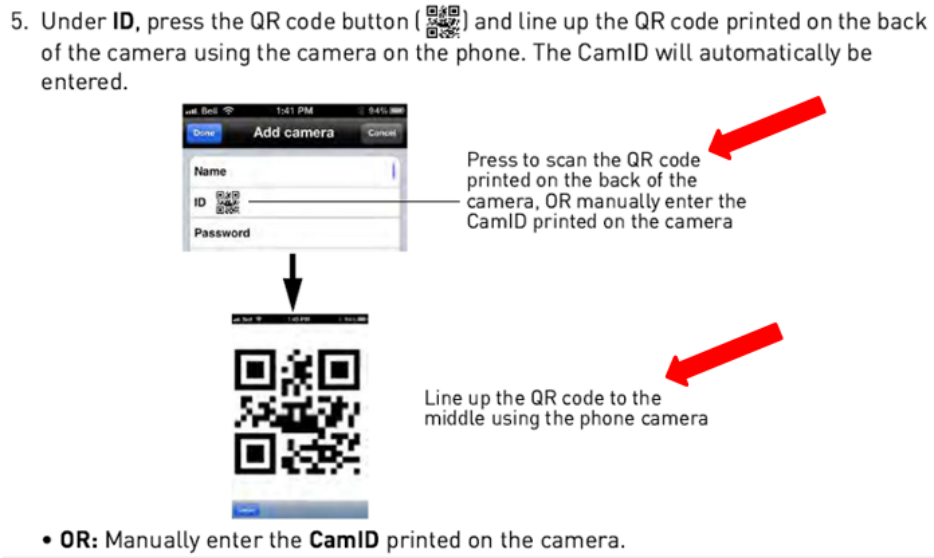
"resolv[ing] the parties' patentability arguments"); EX1001, ¶55.

## V. DETAILED EXPLANATION OF GROUNDS

### A. GROUND 1: Lorex Guide in View of Kim Would Have Rendered Obvious Claims 1-3, 6, 10, 12-14, 17, and 18

#### 1. Lorex Guide

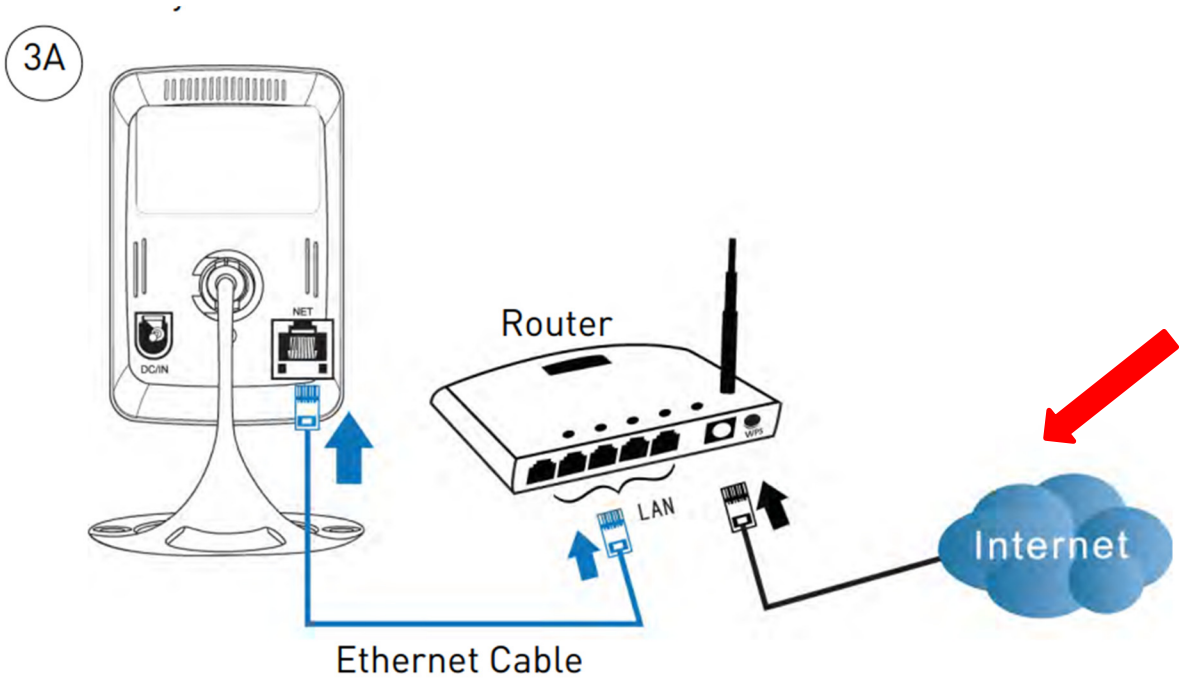
Similar to the '842 patent, Lorex Guide describes the use of a camera of a user/terminal device (e.g., an iPhone, iPad, or Android device) to capture a quick response (QR) code "printed on the back" of a "Lorex"-branded IP camera (e.g., a webcam). EX1006, 13, 12-20; EX1001 ¶¶57-60. The captured QR code provides a simple alternative to manually entering the 'CamID', and the QR code is used in a process for connecting the terminal device to the IP camera through the Internet. For example, Lorex Guide includes a step of "using the camera of the phone" to automatically enter the "CamID" of the IP camera as follows:




EX1006, 13 (annotated), 16, 19; EX1001 ¶58. According to Lorex Guide, the

user/terminal device uses the "CamID" and a password to connect to the IP camera. EX1006, 14; 17, 20. From there, the user can "Press Done" and the mobile app on the user/terminal device "connects to the camera"—all without the IP camera being used to capture any image pattern associated with the phone. EX1006, 13-14, 16-17, 19-20.

Lorex Guide teaches the camera connecting to the "Internet" to establish a direct connection with the phone:

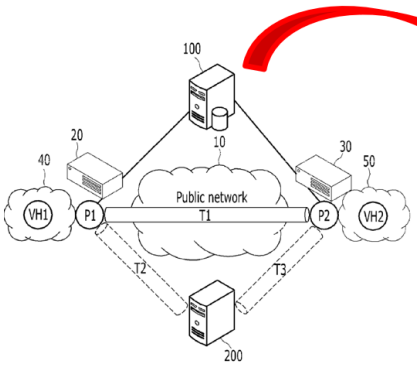



EX1006, 4, *see also id.*, iv, 1, 5-20; EX1001 ¶¶59-60. As such, Lorex Guide plainly indicates the use of an Internet-connected server, especially for interfacing with the Lorex Guide mobile applications at each user's/terminal device (e.g., each user's smartphone). EX1001 ¶59. Indeed, the '842 patent acknowledges that such

a network server was conventional for connecting IP cameras with smartphones. EX1002, 1:36-68, 5:59-62; EX1001 ¶60.

**2. Kim**

Kim is like Lorex Guide in that both references describe establishing a connection between networked devices such as a smartphone and a camera. EX1007, [0052], [0053]; EX1001, ¶¶61-62. Although Lorex Guide does not expressly describe a network server using a conventional hole-punching technique, Kim does. And Kim plainly suggests the known benefits of using this common practice to establish a peer-to-peer connection between IP cameras and smartphones. EX1007, FIG. 6, [0079]-[0085]; EX1001, ¶61. For example, Kim describes a server storing IDs and network addresses for peer devices such as peer nodes P1 and P2 (shown in FIG. 1), and the network address includes an IP address, which can be a private or public IP address:




| ID | Virtual address | | | Network address | | NAT address | | Network connection type |
|---|---|---|---|---|---|---|---|---|
| | Virtual IP | Network prefix | prefix length | IP | Port | IP | Port | |
| Abc@xyz.com | x.x.x.x | - | - | 192.168.1.2 | 1000 | 100.1.1.2 | 1024 | NAT-Full Cone |
| ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ |
| def@zyx.com | y.y.y.y | 1.1.2.0 | 24 | 192.168.2.2 | 2000 | 200.1.1.2 | 2024 | NAT-Restricted Cone |

EX1007, FIGS. 1 and 5 (annotated), [0040]-[0042], [0075]; EX1001, ¶61.

Peer nodes P1 and P2 pre-register their IDs and network addresses with server 100, and the peers then maintain connections to server 100 (or re-connect to server 100 at a later time). EX1007, [0078]-[0079], FIG. 6 ("S602", "S604"); *see also id.*, FIG. 2 ("S210"), [0055]-[0060]; EX1001, ¶62. To establish direct communications with the second peer P2, the first peer P1 transmits a "tunnel query request" message to the server (which includes an ID of P2). EX1007, [0081] FIG. 6; EX1001, ¶62. In response to the "tunnel query request" message, the server 100 replies to P1 with a "tunnel query response" message (which includes the registered network addresses of P2) and additionally sends a "tunnel query notification" message to P2 (which includes the stored network addresses of P1) through the server 100's existing connection with P2. EX1007, [0079]-[0084]. Peers P1 and P2 then use each other's network addresses as received from server 100 to "punch[] a TCP or UDP hole" through each other's respective firewalls or NATs (represented by elements 20 and 30 in FIG. 1), and to thereby establish a peer-to-peer connection for "[d]irect communication between P1 and P2." EX1007, [0083]-[0084], FIG. 6, *see also* [0084], [0013]; EX1001, ¶62.

Notably, Kim teaches that this conventional hole-punching server for establishing P2P connections was "very effective for constructing a service environment" (much like the Lorex service environment) and that, advantageously, "an existing application" (much like the Lorex Ping application) can be used for

constructing a direct communication environment for a camera." EX1007, [0123], [0122] (beneficial "flexibility can be provided").

### 3. The Lorex Guide-Kim Combination

For multiple reasons articulated below, a POSITA would have been motivated to implement Lorex Guide in a predictable manner that employs Kim's suggested use of a network server and conventional hole-punching techniques. EX1001, ¶¶63-71. Applying Kim's suggestions to Lorex Guide would have predictably allowed the Lorex Guide's user/terminal device (e.g., iPhone, iPad, or Android device) and IP camera to establish a P2P connection using a conventional hole-punching technique, which was particularly beneficial when the endpoints of the connection are positioned behind respective NATs or firewalls (much like Kim's peer nodes P1 and P2 are located behind NATs 20, 30). EX1001, ¶¶63-64. For example, in the combination, Lorex Guide's IP camera would predictably register its 'CamID' (which is encoded in the IP camera's QR code) and network addresses with a server on the Internet, as suggested in Kim. EX1001, ¶64. Consistent with Kim's teachings, the user/terminal device and IP camera would then connect to the outside server, and when a user desires to connect to the IP camera following the instructions in Lorex Guide, the user/terminal device would send a tunnel query request message to the server to initiate a process for punching holes in the NATs and establishing a P2P connection with the IP camera (e.g., as suggested by Kim's FIG. 6 process).

EX1001, ¶64. Multiple reasons would have prompted a POSITA to implement such a combination.

**First**, a POSITA would have understood that implementing Lorex Guide's system to include a conventional "network server" that facilitates hole-punching (as suggested by Kim) would have advantageously allowed "for direct communication between a monitoring device and a terminal device in an IP network with a firewall and/or Network Address Translation (NAT)"—even when the firewall and/or NAT would otherwise block inbound communications from the user/terminal device to the IP camera. EX1001, ¶66. Indeed, Kim expressly suggests using the hole-punching server for the "advantages of allowing to perform direct communication between Peer-to-Peer (P2P) … in an IP network in which a firewall or a NAT exists," which Kim describes as beneficially "simplifying a processing procedure." EX1007, [0018]-[0019], [0121]; EX1001, ¶66.

**Second**, a POSITA would have been motivated to implement Lorex Guide in a predictable manner that employs Kim's suggested use of a network server and hole punching for connecting the Lorex Guide's terminal device (e.g., iPhone, iPad, or Android device) to the IP camera is that Kim's network server can conveniently work with an "existing application" like Lorex Guide's "Ping" app to advantageously "construct[] a direct communication environment for … a video camera." EX1007, [0123] ("very effective for constructing a service environment

such as … P2P"); EX1001, ¶67.

**Third**, a POSITA would have understood that implementing Lorex Guide's system to include a "network server" that uses hole-punching (as suggested by Kim) would predictably form a "direct communication environment of an IP level" between Lorex Guide's IP camera and the user's/terminal 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." EX1007, [0122]; EX1001, ¶68.

**Fourth**, a POSITA would have understood that implementing Lorex Guide's system to include a "network server" that uses hole-punching while also using registered "connection type" information from peer nodes (as suggested by Kim) would beneficially allow the server to confirm whether a direct tunnel can be formed between the IP camera and user's/terminal device. EX1007, [0078]-[0083], [0094]-[0099], [0014]-[0018], FIGS. 6, 8; EX1001, ¶69.

Finally, both Lorex Guide and Kim are directed to connecting network endpoint devices (e.g., peer devices) including smart phones and cameras, and the evidence here confirms that a POSITA would have been sufficiently skilled to implement such a combination given the predictable electrical/network components and the relatively advanced state of the art at the time. EX1001, ¶70. This is consistent with the admission in the '842 patent that such network server technology

was previously known for connecting IP cameras with smartphones. EX1002, 1:36-68, 5:59-62. Accordingly, for these reasons articulated above, a POSITA would have had a reasonable expectation of success in achieving the Lorex Guide-Kim combination in the manner described herein. EX1001, ¶¶70-71.

#### 4. Application to Challenged Claims

***Element [1.P]***

Even if the preamble is treated as a limitation (which Petitioners do not concede), the Lorex Guide-Kim combination would have rendered such a system obvious. EX1001, ¶72. For example, Lorex Guide describes a system for establishing a connection between an IP camera and a user/terminal device (e.g., iPhone, iPad, or Android device). EX1006, 12-20; *supra*, Section V.A.1. Kim likewise describes in detail techniques for establishing a P2P connection between peer nodes, which would have been obvious to apply in combination with Lorex Guide for the reasons described above. EX1007, [0006], [0018], [0123]; *supra*, Sections V.A.2-3; EX1001, ¶72.

***Element [1.1]***

The Lorex Guide-Kim combination would have rendered obvious Element [1.1]. EX1001 ¶¶73-76. Lorex Guide teaches the IP camera being connected to the "Internet" to establish a connection with the smartphone or similar user/terminal device (equipped with the Lorex Guide "Ping" app). EX1006, 4; *see*

*also* iv, 1, 5, 7, 9, 11, 33, 34, 43, 55, 59, 85, 107, 129, 132, 137, 139, 149, and 150. A POSITA would have understood the teachings in Lorex Guide as plainly indicating the use of an Internet-connected server, especially for interfacing with the Lorex Guide mobile application at each user's smart phone. EX1001 ¶73.

Even if Lorex Guide did not suggest a network server having all of the "list of devices"/functionality recited in Element [1.1], the predictable Lorex Guide-Kim combination would have provided the claimed network server. For example, Kim describes "direct communication of a P2P Layer 4 (L4) level through help of a server." EX1007, [0006], *see also* [0010] ("the sender and the receiver can perform communication when acquiring a changed IP and port information of another terminal through help of a server."), [0011], [0012], [0013], [0020], [0021], [0039], [0040] [0043], [0047], [0054]-[0076], [0078]-[0084], [0094]-[0098]; FIGS. 1-3, 6; *supra*, Section V.A.3; EX1001, ¶74.

In combination with Lorex Guide, and consistent with Kim's teachings, the server would predictably manage network addresses of the peer nodes. EX1007, [0040]; EX1001, ¶¶75-76. According to Kim, the server includes a storage unit that includes an ID (e.g., Lorex Guide's "CamID" from the QR code) and IP addresses for pre-registered network devices. EX1007, FIG. 5 and [0075], *see also* [0071]; EX1001 ¶75. The devices are pre-registered in the server. EX1007, FIGs. 2, 3, [0055], [0056], [0067], [0068]; EX1001 ¶75.

FIG. 5

120

| ID | Virtual address | | | Network address | | NAT address | | Network connection type |
|---|---|---|---|---|---|---|---|---|
| | Virtual IP | Network prefix | prefix length | IP | Port | IP | Port | |
| Abc@xyz.com | x.x.x.x | - | - | 192.168.1.2 | 1000 | 100.1.1.2 | 1024 | NAT-Full Cone |
| ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ |
| def@zyx.com | y.y.y.y | 1.1.2.0 | 24 | 192.168.2.2 | 2000 | 200.1.1.2 | 2024 | NAT-Restricted Cone |

EX1007, FIG. 5 (annotated).

Kim describes the server as including "information in which a direct tunnel can be set between the two peer nodes P1 and P2" and the "tunnel information that is transmitted to the peer node P1 includes a virtual address, a network address, and a NAT address of the peer node P2 to communicate, and similarly, tunnel information that is transmitted to the peer node P2 includes a virtual address, a network address, and a NAT address of the peer node P1 to communicate." EX1007 [0083], *see also id.*, FIG. 6, [0013], [0084]; EX1001 ¶76.

***Element [1.2]***

The Lorex Guide-Kim combination would have rendered obvious Element [1.2]. EX1001, ¶¶77-79. As an initial matter, Lorex Guide describes a first networked monitoring device (e.g., the IP camera), having a first identification

embedded in the first networked monitoring device. For example, Lorex Guide describes the IP camera as having an embedded "CamID." EX1006, 13 ("QR code printed on the back of the camera"), *see also* 11, 16, 19; EX1001 ¶77.

Kim similarly describes peer nodes are each provided with an embedded ID. EX1007, [0056] ("the ID is an identifier that can distinguish the peer node P1 in the server 100 and is formed with a string"), [0059], [0063], [0064], [0075], [0081], FIG. 5. Kim's first networked monitoring device (e.g., P1 in FIG. 2 or P2 in FIG. 6) registers its embedded ID (a first identification) into the server's list of networked devices to associate a corresponding IP address of the first networked monitoring device with its embedded ID by connecting to the network server through the Internet. *Supra*, [1.1]. For example, Kim teaches that "in order to register information such as an ID and a password to the server 100, [a] peer node … transmits a registration request message including an ID and a password to the server 100." EX1007, [0055], *see also* [0056], [0067], [0068], [0075] and FIGS. 2-3, 5 (showing the list of networked devices); EX1001 ¶78. Kim explicitly teaches that server 100 associates a registered peer node's ID with multiple IP addresses, including IP addresses contained in the peer node's virtual address, network address, and NAT address. EX1007, FIG. 5, [0074] ("controller 110 processes a registration request of a network address, a NAT address, and a network connection type from the peer node P1, and stores the network address, and the network connection type

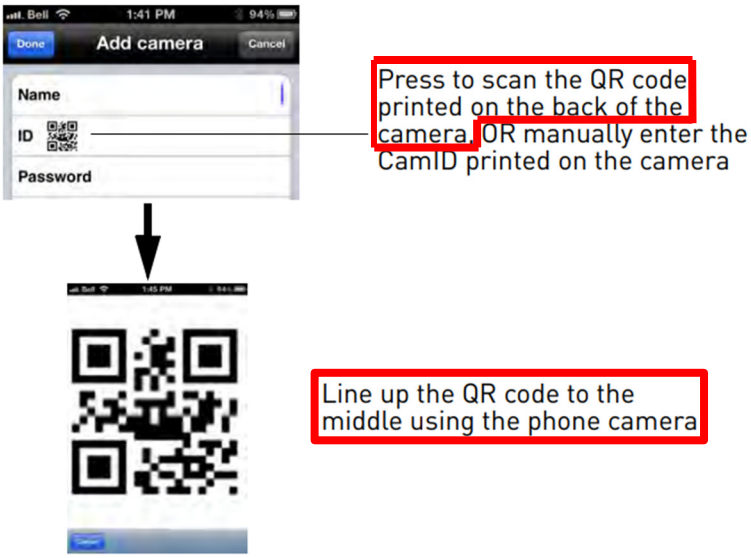
of the peer node P1 in the storage unit 120"), [0040]-[0042], [0054]-[0060], FIGS. 1-2. The server and peer nodes are connected through a public network (e.g., the Internet), and the registration of Kim's embedded ID is performed by the first networked monitoring device connecting to the network server through the Internet. EX1007 FIG. 1, [0038], [0045], [0046]; EX1001 ¶78.

As described above, in the predictable Lorex Guide-Kim combination, it would have been obvious for Lorex Guide's IP camera to register its embedded "CamID" and/or QR code identification with the network server consistent with Kim's teachings. *Supra*, Section V.A.3; EX1001 ¶79.

***Element [1.3]***

The Lorex Guide-Kim combination would have rendered obvious Element [1.3]. EX1001, ¶¶80-82. For example, Lorex Guide describes entering a "CamID" by scanning "the QR code printed on the back of the camera." EX1006, 13, *see also* 11, 16, 19; EX1001 ¶80. The "CamID" is used to establish a connection between the camera and the phone. EX1006, pp. 12-20; EX1001 ¶80.

5. Under **ID**, press the QR code button ( ) and line up the QR code printed on the back of the camera using the camera on the phone. The CamID will automatically be entered.




EX1006, 13 (cropped, annotated).

Lorex Guide explains that the QR code is "printed on the back of the camera," and is therefore "attached" to the first networked monitoring device. EX1006, 13; EX1001 ¶81.

To the extent Lorex Guide does not expressly state that the connection between the IP camera and the IP phone is a P2P connection, the predictable Lorex Guide-Kim combination provides such a P2P connection as taught in Kim. EX1007, [0005], [0018], [0078]-[0089], FIG. 6; *supra*, Section V.A.3; EX1001 ¶82.

***Element [1.4]***

The Lorex Guide-Kim combination would have rendered obvious Element

[1.4]. EX1001 ¶¶83-85. Lorex Guide, for example, discloses a terminal device such as an iPad, iPhone, or Android device having an embedded camera that captures an image of the QR code printed on the IP camera and that transmits information to connect the terminal device to the IP camera when the QR code is scanned. EX1006, 12-20; *supra*, Section V.A.1; EX1001 ¶83. Lorex Guide also discloses that the terminal device can communicate with the IP camera through the Internet. EX1006, 7 ("Connecting to a Camera Over the Internet"), 59 ("Select Internet connection speed"), 12-20.

Kim further discloses a terminal device (e.g., "P1" in FIG. 6) that transmits a "tunnel query request" message that includes an ID of the first networked monitoring device (e.g., "P2" in FIG. 6) to the network server 100. EX1007, FIG. 6, [0080]-[0081]; EX1001 ¶84. P1 transmits the "tunnel query request" message to the server to "set a tunnel for performing direct communication with the peer node P2." EX1007 [0081], *see also* FIG. 6; EX1001 ¶84. The network server and P1 are connected through a public network (e.g., the Internet), indicating that the "tunnel query request" message is transmitted by P1 to the server through the Internet. EX1007, FIG. 1, [0038], [0045], [0046]; EX1001 ¶84.

As described above, in the Lorex Guide-Kim combination, the terminal device (e.g., Lorex Guide's iPhone, iPad, or Android device) predictably transmits a connection request signal like Kim's "tunnel query request" containing the IP

camera's 'CamID' to the network server to set a tunnel and connect to the IP camera, consistent with the actions of peer P1 in Kim. *Supra*, Section V.A.3; EX1001 ¶85. Indeed, the Lorex Guide-Kim terminal device would predictably transmit such a connection request signal "when" the QR code is captured by following the connection procedure described in Lorex Guide—especially since Lorex Guide discloses that the terminal device captures an image of the QR code during a process of generating a request to connect to the IP camera and add the camera to the user's camera list. EX1002, 13-14; EX1001 ¶85.

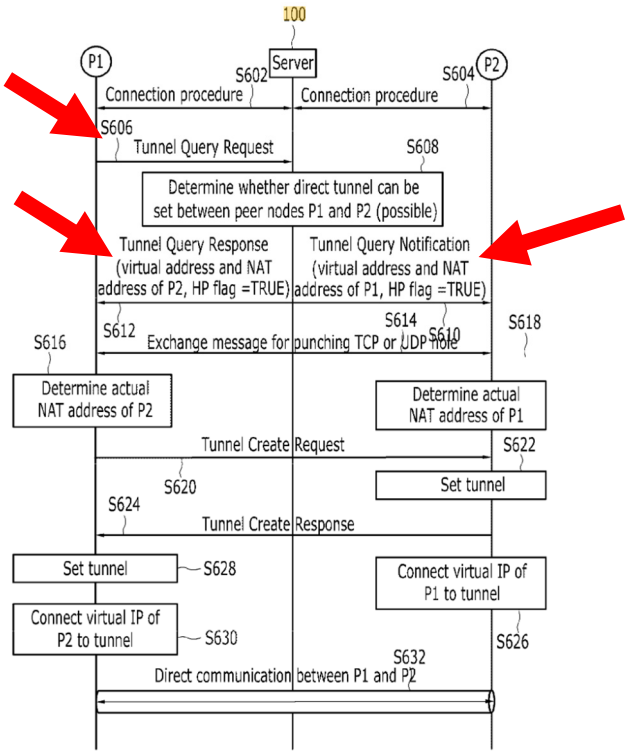
***Element [1.5]***

The Lorex Guide-Kim combination would have rendered obvious Element [1.5]. EX1001 ¶¶86-89. Kim, for example, teaches that server 100 receives the "tunnel query request" message from the terminal device (e.g., P1 in FIG. 6), and the "tunnel query request message includes an ID of the peer node P2." EX1007, [0081]-[0082], FIG. 6. The ID carried in the tunnel request message of the predictable Lorex Guide-Kim combination can be the Lorex Guide IP camera's "CamID" obtained by reading the captured image of the QR code printed on the IP camera with the terminal device (e.g., the iPhone, iPad, or Android device). EX1006, 12-20; *supra*, Section V.A.3; EX1001 ¶86.

Kim further teaches that, responsive to the terminal device's (P1's) tunnel query request message, the server determines whether a "direct tunnel can be set

between peer nodes P1 and P2," and if a direct tunnel can be set, the server (i) replies to the terminal device (P1) with a "tunnel query response" message and (ii) transmits a "tunnel query notification" message to the networked monitoring device (P2) identified in P1's tunnel query request. EX1007, [0082]-[0084].

FIG. 6




EX1007, FIG. 6 (annotated).

According to Kim, the server includes the virtual, network, and NAT addresses (each of which includes an IP address) of the first networked monitoring device (e.g., P2 in FIG. 6) in the "tunnel query response" message and transmits this message to the terminal device (e.g., P1 in FIG. 6). EX1006, [0083], FIG. 6. For example, the network address in the "tunnel query response" message includes

an IP address of the first networked monitoring device, which can be a private or public IP address. EX1007, [0078]-[0084], FIGS. 5-6. EX1007, [0078]-[0084], FIGS. 5, 6. Likewise, the server includes the virtual, network, and NAT addresses (each of which includes an IP address) of the terminal device (e.g., P1) in the "tunnel query notification" message and transmits this message to the first networked monitoring device (e.g., P2). EX1006, [0083], FIG. 6. For example, the network address in the "tunnel query notification" message includes an IP address of the terminal device, which can be a private or public IP address. EX1007, [0078]-[0084], FIGS. 5-6. EX1007, [0078]-[0084], FIGS. 5, 6. The server's mapping of peer IDs to the peers' respective virtual, network, and NAT addresses allows the server to look-up and obtain these addresses (including the respective IP addresses) for inclusion in the "tunnel query response" and "tunnel query notification" messages using the peers' respective registered IDs (including the ID of the first networked monitoring device P2 identified in the "tunnel query request" message). *Id.*, [0071]-[0076], [0080]-[0084], FIG. 5; EX1001, ¶88.

Kim's "tunnel query response" and "tunnel query notification" messages are "hole-punching messages" that allow the terminal device (P1) and the first networked monitoring device (P2) to establish a P2P connection. EX1001 ¶89. For example, Kim explains that "[t]he peer nodes P1 and P2, having received a tunnel query response message and a tunnel query request message, respectively,

exchange a message for punching a TCP or UDP hole (S614)." EX1007, [0084]; *see also* [0018]-[0019], [0066], [0083], FIG.6. The "tunnel query response" and "tunnel query notification" messages specifically include a "hole punching flag (HP flag)" that indicates whether "a direct tunnel can be set between [the] two peer nodes P1 and P2," and which is used by P1 and P2 to set a tunnel for "[d]irect communication" between the nodes. EX1007, [0083], FIG. 6. "The peer nodes P1 and P2, having received a tunnel query response message and a tunnel query request message, respectively, exchange a message for punching a TCP or UDP hole." EX1007, [0084]; EX1001, ¶89.

***Element [1.6]***

The Lorex Guide-Kim combination would have rendered obvious Element [1.6]. EX1001, ¶¶90-93. Lorex Guide is notably a "guide" that describes a step-by-step process instructing a user how to connect a terminal device (e.g., an iPhone, iPad, or Android device) to an IP camera over the Internet. EX1006, 12-20; *supra*, Section V.A.1. Lorex Guide's step-by-step instructions direct the user to acquire the "CamID" of the IP camera by capturing an image of a QR code printed on the IP camera. EX1006, 13-14. After capturing the QR code to obtain the "CamID" and entering a password (e.g., "lorex"), the Lorex Ping app on the user's phone simply "connects to the camera" without the need to scan any image pattern on the user's phone. *Id.*; *generally id.*, 12-20. To be clear, throughout the

entire step-by-step user-guide instructions, Lorex Guide never once instructs the user to use the IP camera to capture any image pattern associated with the terminal device (e.g., the iPhone, iPad, or Android device) for establishing a connection between the IP camera and the terminal device. EX1001, ¶¶91-92. The evidence here corroborates this fact. *See* EX1011, ¶7 ("without requiring…" and "[t]he simplicity was noticed"). Thus, Lorex Guide discloses, or certainly plainly suggests, the functionality of Element [1.6]. EX1001, ¶¶90-93 (citing corroborating exhibits EX1011, ¶¶3, 7; EX1008, 1:00-1:37, EX1010, 00:29-00:39).

***Element [2]***

Lorex Guide describes a barcode in the form of a "QR code printed on the back of the camera," where the terminal device (e.g., iPhone, iPad, or Android device) captures the QR code to generate a barcode image. EX1006, 13, *see also* 16, 19; EX1001, ¶94. The image of the QR code is both shown on the screen when the QR code is scanned and the image is at least temporarily stored in the terminal device to permit the image to be processed and the CamID to be read from the image. *Id.*

Line up the QR code to the middle using the camera on the phone or tablet

EX1006, 19 (cropped, annotated).

***Element [3]***

Lorex Guide discloses that the terminal device (e.g., iPhone, iPad, or Android device) converts the QR code into a "CamID" that constitutes a first identification for the IP camera. EX1006, 13 ("[L]ine up the QR code printed on the back of the camera using the camera on the phone. The CamID will automatically be entered."), 16, 19; EX1001, ¶95. As described above, in the Lorex Guide-Kim combination, it would have been obvious for the terminal device to transmit to the network server a connection request signal (e.g., a "tunnel query request message") containing the "CamID." *Supra*, Element [1.4]; Section, V.A.3; EX1007, [0079]-[0081], FIG. 6; EX1001, ¶95.

***Element [6]***

Lorex Guide discloses that the IP camera (e.g., a first networked monitoring device) includes a default security password and the terminal device (e.g., iPhone, iPad, or Android device) presents a user interface for entering the default password to log on the IP camera. EX1006, 14 ("Under Password, enter the camera password."; "If this is the first time connecting to the camera, you will be prompted to create your own password."); *see also id.*, 8, 11, 17, 20; EX1001, ¶96.

***Element [10]***

Lorex Guide describes a "QR code printed on the back of the camera."

EX1006, 13; *see also id.*, 16, 19; EX1001, ¶97.

***Element [12.P]***

Even if the preamble is treated as a limitation (which Petitioners do not concede), the Lorex Guide-Kim combination would have rendered it obvious. *Supra*, Element [1.P]; *see also* EX1006, 12-20 (describing connection methods); EX1007, [0078] ("method of setting direct communication"), [0054] ("method of allocating a virtual address"), FIGS. 2, 6; EX1001, ¶98.

***Element [12.1]***

The Lorex Guide-Kim combination would have rendered obvious Element [12.1], and would have provided the step of connecting the IP camera (e.g., a first networked monitoring device) to a network server through the Internet for at least the reasons described above with respect to Element [1.1]. EX1006, 12-20; EX1007, [0054]-[0060] & FIG. 2, [0061]-[0070] & FIG. 3, [0078]-[0079] & FIG. 6; *supra*, Element [1.1]; EX1001, ¶99.

***Element [12.2]***

The Lorex Guide-Kim combination would have rendered obvious Element [12.2], and would have provided the step of registering a first identification (e.g., the "CamID") of the first networked monitoring device (e.g., the IP camera) into the list of networked devices of the server for at least the reasons described above with respect to Element [1.2]. EX1006, 12-20; EX1007, [0055], *see also* [0056],

[0067], [0068], [0075] and FIGS. 2-3, 5; *supra*, Element [1.2]; EX1001, ¶100.

***Element [12.3]***

The Lorex Guide-Kim combination would have rendered obvious Element [12.3], and would have provided the step of providing an image pattern (e.g., a QR code) comprising the first identification (e.g., the "CamID"), wherein the image pattern is attached on the first networked monitoring device (e.g., the IP camera) for establishing a P2P connection with the first networked monitoring device, for at least the reasons described above with respect to Element [1.3]. EX1006, 12-20; *supra*, Element [1.3]; EX1001, ¶101.

***Element [12.4]***

The Lorex Guide-Kim combination would have rendered obvious Element [12.4], and would have provided the steps of (i) generating a connection request signal (e.g., a tunnel query request message) by a terminal device (e.g., an iPhone, iPad, or Android device) when the image pattern (e.g., the QR code printed on the IP camera) is captured to the terminal device and (ii) transmitting the connection request signal to the network server by the terminal device through the Internet, for at least the reasons described above with respect to Element [1.4]. EX1006, 12-20; EX1007, [0038], [0045], [0046], [0080]-[0081], FIG. 6; *supra*, Element [1.4]; EX1001, ¶102.

***Element [12.5]***

The Lorex Guide-Kim combination would have rendered obvious Element [12.5], and would have provided the "identifying" step (and, indeed, all of the additional features recited in Element [12.5]), for at least the reasons described above with respect to Element [1.5]. EX1006, 12-20; EX1007, [0018]-[0019], [0066], [0078]-[0084], FIGS. 5, 6; *supra*, Element [1.5]; EX1001, ¶103.

***Element [12.6]***

The Lorex Guide-Kim combination would have rendered obvious Element [12.6], including the negative limitation that precludes the first networked monitoring device (e.g., the IP camera) from capturing any image pattern (e.g., a QR code) associated with the terminal device (e.g., the iPhone, iPad, or Android device) for establishing the P2P connection between the terminal device and the first networked monitoring device, for at least the reasons described above with respect to Element [1.6]. EX1006, 12-20; EX1007, [0074]-[0089], FIG. 6; *supra*, Element [1.6]; EX1001, ¶104.

***Element [13]***

The Lorex Guide-Kim combination would have rendered obvious Element [13] for at least the reasons described above with respect to Element [2]. *Supra*, Element [2]; EX1001, ¶105.

***Element [14]***

The Lorex Guide-Kim combination would have rendered obvious Element

[14] for at least the reasons described above with respect to Element [3]. *Supra*, Element [3]; EX1001, ¶¶106-107.

For example, Lorex Guide discloses that the terminal device (e.g., iPhone, iPad, or Android device) interprets the captured image of the QR code to extract the "CamID" (e.g., a first identification) so that "[t]he CamID will automatically be entered" in the user interface of the terminal device. EX1006, 13; *see also id.*, 16, 19; EX1001, ¶107. The terminal device would predictably include an image interpreting unit to interpret the barcode image and extract the CamID as described in Lorex Guide. EX1001, ¶107. Further, as described above, in the Lorex Guide-Kim combination, it would have been obvious for the terminal device to transmit to the network server a connection request signal (e.g., a "tunnel query request message") in which the "CamID" is embedded. *Supra*, Element [1.4]; Section, V.A.3; EX1007, [0079]-[0081], FIG. 6; EX1001, ¶107.

***Element [17]***

The Lorex Guide-Kim combination would have rendered obvious Element [17] for at least the reasons described above with respect to Element [6]. *Supra*, Element [6]; EX1001, ¶¶108-109.

For example, Lorex Guide discloses that the IP camera (e.g., a first networked monitoring device) includes a default security password and the terminal device (e.g., iPhone, iPad, or Android device) presents a user interface for

inputting a security password to log on the IP camera. EX1006, 14 ("Under Password, enter the camera password."; "If this is the first time connecting to the camera, you will be prompted to create your own password."); *see also id.*, 8, 11, 17, 20; EX1001, ¶108.

Moreover, a POSITA would have understood that passwords are conventionally implemented for security and access control. EX1001, ¶109 (citing corroborating exhibit EX1029). Considering the ubiquitous and conventional use of passwords in software-based systems before the '842 patent, it would have been obvious to implement the Lorex Guide-Kim combination such that the terminal device would only log on the IP camera if a correct password is entered; otherwise, the user would predictably be presented with another opportunity to enter a security password that correctly matches the default security password of the IP camera. EX1001, ¶109. A POSITA would have been prompted to implement the system in this manner to realize predictable benefits, including blocking unauthorized users if the password cannot be verified while still providing authorized users with additional opportunities to correctly enter the password. EX1001, ¶109.

***Element [18]***

The Lorex Guide-Kim combination would have rendered obvious Element [18] for at least the reasons described above with respect to Element [10]. *Supra*,

Element [10]; EX1001, ¶110.

### B. GROUND 2: Kim in View of Lorex Video Would Have Rendered Obvious Claims 1-3, 6, 10, 12-14, 17, and 18

#### 1. Lorex Video

Lorex Video is akin to Kim in that both references describe establishing a connection between a terminal device (e.g., a smart phone) and a networked monitoring device (e.g., a camera). EX1008, 1:00-1:40; EX1001, ¶¶111-112. Although Kim (summarized above) does not describe an image pattern such as a QR code being attached to a networked monitoring device and comprising the ID for establishing a peer-to-peer connection, Lorex Video does. EX1008, 1:08-1:24; EX1001, ¶111. Lorex Video plainly suggests the known benefits of using a QR code to quickly enter an ID to establish a peer-to-peer connection between IP cameras and smartphones. EX1008, 1:00-1:40; EX1001, ¶111.

Notably, the Lorex Video expressly discloses that it was conventional to use a QR code to quickly establish a connection between a smart phone and an IP camera and describes the process as being "very simple" and quick. EX1008, 1:00-1:40; EX1001, ¶112.

EX1008, 1:17 (cropped, annotated).

### 2. The Kim-Lorex Video Combination

A POSITA would have been motivated to implement Kim in a predictable manner that employs Lorex's suggested benefits for using a conventional QR code to quickly obtain an ID of a device targeted for a direct connection (e.g., a P2P connection). EX1001, ¶¶113-114. Indeed, multiple reasons would have prompted a POSITA to implement such a combination.

**First**, a POSITA would have understood that implementing Kim's system, which includes a first peer node sending an ID of a second peer node to a server (EX1007, [0081]), to include a conventional QR code attached to the second peer node (as suggested by the QR code attached to the camera in the Lorex Video) would predictably provide a simple and quick mechanism for Kim's first peer node (P1) to obtain the ID of the second peer node (P2) when establishing a P2P connection.

EX1001, ¶115. Indeed, Lorex Video expressly emphasizes the speed and simplicity of using such a system to establish a peer-to-peer connection between a smart phone and a camera. EX1008, 1:08-1:40 ("activate the camera – very simple because we have a QR code on the back").

**Second**, Lorex Video expressly suggests a known technique to address a conventional problem—namely, inputting the ID of the IP camera/peer node that is desired for a connection—and Lorex Video does so in a rapid and error-free manner. EX1001, ¶116. Here, Kim describes that the request from one peer node to connect with a second peer node "includes an ID of the peer node P2" but does not detail a solution for inputting any such ID. EX1007, [0081], FIG. 6. Lorex Video details a known technique to input such an ID while beneficially avoid transcription errors that might otherwise occur from manually typing a (lengthy) ID code of an IP camera into a user interface. EX1008, 1:08-1:40. The law is clear in such circumstances. *Intel Corp. v. PACT XPP Schweiz AG*, 61 F.4th 1373, 1380 (Fed. Cir. 2023) ("[I]f there's a known technique to address a known problem using prior art elements according to their established functions, then there is a motivation to combine.").

Finally, both Kim and Lorex Video are directed to connecting peer devices including smart phones and cameras, and the evidence here confirms that a POSITA would have been sufficiently skilled to implement such a combination given the predictable electrical/network components and the relatively advanced state of the

art at the time. EX1001, ¶117. This is consistent with the admission in the '842 patent that such network server technology was previously known for connecting IP cameras with smartphones. EX1002, 1:36-68, 5:59-62. Accordingly, for these reasons articulated above, a POSITA would have had a reasonable expectation of success in achieving the Kim-Lorex Video combination in the manner described herein. EX1001, ¶¶117-118.

### 3. Application to Challenged Claims

***Element [1.P]***

Even if the preamble is treated as a limitation (which Petitioners do not concede), the predictable Kim-Lorex Video combination would have rendered such a system obvious. For example, Kim describes in detail techniques for establishing a P2P connection between peer nodes. EX1007, [0006], [0018], [0078]-[0089], [0123], FIGS. 1-2, 6; *supra*, Sections V.A.2; EX1001, ¶119. Lorex Video also describes a process for establishing a connection between peer devices including a smartphone and a camera. EX1008, 1:00-1:40; *supra*, Section V.B.1; EX1001, ¶119.

***Element [1.1]***

The Kim-Lorex Video combination would have rendered obvious Element [1.1]. EX1001, ¶¶120-122. For example, Kim describes "direct communication of a P2P Layer 4 (L4) level through help of a server." EX1007, [0006], *see also*

[0010] ("the sender and the receiver can perform communication when acquiring a changed IP and port information of another terminal through help of a server."), [0011], [0012], [0013], [0020], [0021], [0039], [0040] [0043], [0047], [0054]-[0076], [0078]-[0084], [0094]-[0098]; EX1001, ¶120.

The server manages network addresses of the peer nodes. EX1007, [0040]; EX1001, ¶121. The server includes a storage unit that includes and ID and IP addresses for pre-registered network devices. EX1007, FIG. 5 and [0075], *see also* [0071]; EX1001, ¶121. The devices are pre-registered in the server. EX1007, FIGs. 2, 3, [0055], [0056], [0067], [0068]; EX1001, ¶121.

FIG. 5

120

| ID | Virtual address | | | Network address | | NAT address | | Network connection type |
|---|---|---|---|---|---|---|---|---|
| | Virtual IP | Network prefix | prefix length | IP | Port | IP | Port | |
| Abc@xyz.com | x.x.x.x | - | - | 192.168.1.2 | 1000 | 100.1.1.2 | 1024 | NAT-Full Cone |
| ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ |
| def@zyx.com | y.y.y.y | 1.1.2.0 | 24 | 192.168.2.2 | 2000 | 200.1.1.2 | 2024 | NAT-Restricted Cone |

EX1007, FIG. 5 (annotated).

Kim describes the server as including "information in which a direct tunnel can be set between the two peer nodes P1 and P2" and the "tunnel information that

is transmitted to the peer node P1 includes a virtual address, a network address, and a NAT address of the peer node P2 to communicate, and similarly, tunnel information that is transmitted to the peer node P2 includes a virtual address, a network address, and a NAT address of the peer node P1 to communicate." EX1007 [0083], *see also id.*, FIG. 6, [0013], [0084]; EX1001, ¶122.

***Element [1.2]***

The Kim-Lorex Video combination would have rendered obvious Element [1.2]. EX1001, ¶¶123-124. For example, Kim teaches that peer nodes are each provided with an embedded ID. EX1007, [0056] ("the ID is an identifier that can distinguish the peer node P1 in the server 100 and is formed with a string"), [0059], [0063], [0064], [0075], [0081], FIGS. 2, 5. Kim's first networked monitoring device (e.g., P1 in FIG. 2 or P2 in FIG. 6) registers its embedded ID (a first identification) into the network server's list of networked devices to associate a corresponding IP address of the first networked monitoring device with the ID. *Supra*, [1.1]. For example, Kim teaches that "in order to register information such as an ID and a password to the server 100, [a] peer node … transmits a registration request message including an ID and a password to the server 100." EX1007 [0055], *see also* [0056], [0067], [0068], [0075] and FIGS. 2-3, 5-6 (showing the list of networked devices); EX1001 ¶123. Kim explicitly teaches that the server 100 associates a registered peer node's ID with multiple IP addresses, including IP

addresses contained in the peer node's virtual address, network address, and NAT address. EX1007, FIG. 5, [0074] ("controller 110 processes a registration request of a network address, a NAT address, and a network connection type from the peer node P1, and stores the network address, and the network connection type of the peer node P1 in the storage unit 120"), [0040]-[0042], [0054]-[0060], FIGS. 1-2. The server and peer nodes are connected through a public network (e.g., the Internet), and the registration of Kim's embedded ID is thus performed by the first networked monitoring device connected to the network server through the Internet. EX1007, FIG. 1, [0038], [0045], [0046]; EX1001 ¶123. Kim also teaches that the first networked device (a peer node) can be "a video camera that perform[s] IP-based communication." EX1007, [0052].

Lorex Video similarly describes an IP camera as a first networked monitoring device that has a first identification (e.g., the camera's "ID") encoded in the QR code attached to the camera. EX1008, 1:11-1:22. As described above, it would have been obvious to implement Kim using Lorex Video's camera ID that is encoded in the QR code as the unique identifier for Kim's first networked monitoring device (e.g., P1 in FIG. 2 or P2 in FIG. 6). *Supra*, Section V.B.2; EX1001 ¶124.

***Element [1.3]***

The Kim-Lorex Video combination would have rendered obvious Element

[1.3]. EX1001, ¶¶125-126. For example, Lorex Video shows an image pattern in the form of a QR code being attached on the IP camera (a first networked monitoring device). EX1008, 1:08-1:24; EX1001, ¶125. Lorex Video shows the ID for the camera being automatically entered in an "ID" field of the user interface on the user's iPhone (a terminal device), thus indicating that the QR code comprises the ID (a first identification). EX1008, 1:08-1:24. Lorex Video explains that the camera's ID (first identification) is used to establish a connection between the iPhone and the camera. EX1008, 1:08-1:40.

EX1008, 1:17 (left, cropped), 1:20 (right, cropped).

Further, as described above, it would have been obvious to implement Kim using Lorex Video's camera ID from the QR code as the unique identifier for Kim's first networked monitoring device (e.g., P1 in FIG. 2 or P2 in FIG. 6).

*Supra*, Section V.B.2; EX1001, ¶126. Kim confirms that the ID is used to establish a peer-to-peer connection between the terminal device (e.g., P1 in FIG. 6) and the first networked monitoring device (e.g., P2 in FIG. 6). EX1007, [0080] ("perform direct communications"), [0018] ("allowing to perform direct communication between Peer-to-Peer (P2P)"); *see also id.*, [0078]-[0089], FIG. 6.

***Element [1.4]***

The Kim-Lorex Video combination would have rendered obvious Element [1.4]. EX1001, ¶¶127-128. For example, Kim discloses a terminal device (e.g., P1 in FIG. 6) that transmits a "tunnel query request" message that includes an ID of the first networked monitoring device (e.g., "P2" in FIG. 6) to the network server 100. EX1007, FIG. 6, [0080]-[0081]; EX1001 ¶127. P1 transmits the "tunnel query request" message to the server to "set a tunnel for performing direct communication with the peer node P2." EX1007 [0081], *see also* FIG. 6; EX1001 ¶127. The network server and P1 are connected through a public network (e.g., the Internet), indicating that the "tunnel query request" message is transmitted by P1 to the server through the Internet. EX1007, FIG. 1, [0038], [0045], [0046]; EX1001 ¶127.

Further, as described above, it would have been obvious to implement Kim according to Lorex Video's suggestion for the terminal device (e.g., an iPhone as taught in Lorex Video / P1 in Kim's FIG. 6) to obtain the first networked

monitoring device's (e.g., the IP camera in Lorex Video / P2 in Kim's FIG. 6) unique identifier (first identification) by using a camera in the terminal device to capture a QR code on the first networked monitoring device, and implementing the terminal device to automatically read the identifier from the QR code. EX1008, 1:16-1:36; *supra*, Section V.B.2; EX1001, ¶128. Lorex Video shows how the iPhone captures the QR code on the IP camera during a process of generating a request to connect to the IP camera and add the camera to the user's camera list. EX1008, 1:16-1:36. Applying this process to Kim's system, the first terminal device (e.g., P1 in Kim's FIG. 6) would predictably generate the "tunnel query request" message (a connection request signal) when the QR code is captured to the first terminal device. EX1001, ¶128.

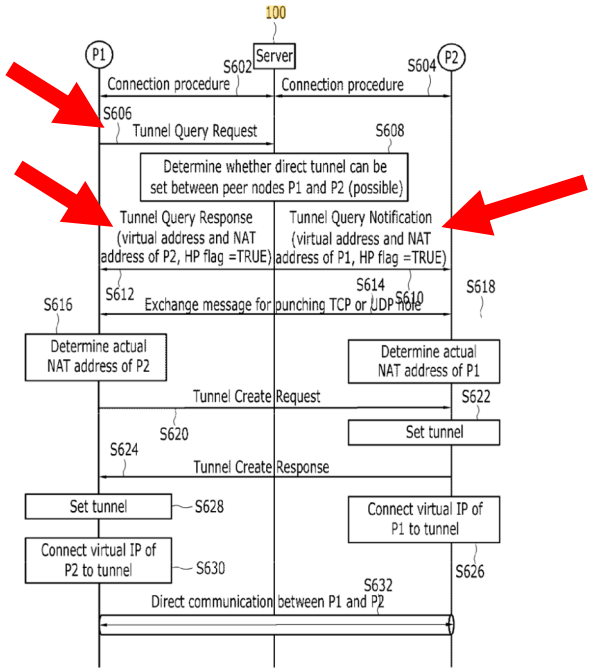
***Element [1.5]***

The Kim-Lorex Video combination would have rendered obvious Element [1.5]. EX1001, ¶¶129-132. Kim, for example, teaches that server 100 receives the "tunnel query request" message from the terminal device (e.g., P1 in FIG. 6), and the "tunnel query request message includes an ID of the peer node P2" such as the ID of the camera that was read from a QR code as taught in Lorex Video. EX1007, [0081]-[0082], FIG. 6; *supra*, Section V.B.2; EX1001 ¶129.

Kim further teaches that, responsive to the terminal device's (e.g., P1's) tunnel query request message, the server determines whether a "direct tunnel can

be set between peer nodes P1 and P2," and if a direct tunnel can be set, the server (i) replies to the terminal device (P1) with a "tunnel query response" message and (ii) transmits a "tunnel query notification" message to the networked monitoring device (P2) identified in P1's tunnel query request. EX1007, [0082]-[0084]; EX1001, ¶130.

FIG. 6




EX1007, FIG. 6 (annotated).

According to Kim, the server includes the virtual, network, and NAT addresses (each of which includes an IP address) of the first networked monitoring device (e.g., P2 in FIG. 6) in the "tunnel query response" message and transmits this message to the terminal device (e.g., P1 in FIG. 6). EX1006, [0083], FIG. 6. For example, the network address in the "tunnel query response" message includes

an IP address of the first networked monitoring device, which can be a private or public IP address. EX1007, [0078]-[0084], FIGS. 5-6. EX1007, [0078]-[0084], FIGS. 5, 6. The server's mapping of peer IDs to the peers' respective virtual, network, and NAT addresses allows the server to look-up and obtain these addresses (including the respective IP addresses) for inclusion in the "tunnel query response" and "tunnel query notification" messages using the peers' respective registered IDs (including the ID of the first networked monitoring device P2 identified in the "tunnel query request" message). *Id.*, [0071]-[0076], [0080]-[0084], FIG. 5; EX1001, ¶131.

Kim's "tunnel query response" and "tunnel query notification" messages are "hole-punching messages" that allow the terminal device (e.g., P1) and the first networked monitoring device (e.g., P2) to establish a P2P connection. EX1001, ¶132. For example, Kim explains that "[t]he peer nodes P1 and P2, having received a tunnel query response message and a tunnel query request message, respectively, exchange a message for punching a TCP or UDP hole (S614)." EX1007, [0084]; *see also* [0018]-[0019], [0066], [0083], FIG.6. The "tunnel query response" and "tunnel query notification" messages specifically include a "hole punching flag (HP flag)" that indicates whether "a direct tunnel can be set between [the] two peer nodes P1 and P2," and which is used by P1 and P2 to set a tunnel for "[d]irect communication" between the nodes. EX1007, [0083], FIG. 6. "The peer

nodes P1 and P2, having received a tunnel query response message and a tunnel query request message, respectively, exchange a message for punching a TCP or UDP hole." EX1007, [0084]; EX1001, ¶132.

***Element [1.6]***

The Kim-Lorex Video combination would have rendered obvious Element [1.6]. EX1001, ¶¶133-135. Lorex Video discloses a complete process for establishing a direct connection between a terminal device (e.g., an iPhone) and a first networked monitoring device (e.g., an IP camera). EX1008, 1:00-1:40; EX1001, ¶133. During this process, the IP camera is never used to capture any image pattern associated with the iPhone for establishing the connection between the iPhone and the IP camera. EX1008, 1:00-1:40; EX1001, ¶133. Lorex Video's instructor specifically notes that "All I have to do is add this camera to my camera list," which is "very simple because we have a QR code on the back" of the IP camera. EX1008, 1:06-1:12. As plainly taught in the Lorex Video, the P2P connection between the iPhone and IP camera is established when the user captures an image of the QR code on the back of the IP camera ("here it is")—all without using the IP camera to capture any image pattern associated with the iPhone. EX1008, 1:31-35 ("Once that happens … here it is."); EX1001, ¶¶133-134 (citing corroborating exhibits EX1011, ¶¶3, 7; EX1006, 29-30; EX1010, 00:29-00:39).

Implementing Kim in accordance with Lorex Video's suggestion to capture a QR code of the first networked monitoring device (but without capturing any image pattern associated with the terminal device) to establish a P2P connection would have been obvious for each of the reasons described in detail above. *Supra*, Section V.B.2; EX1001, ¶135.

***Element [2]***

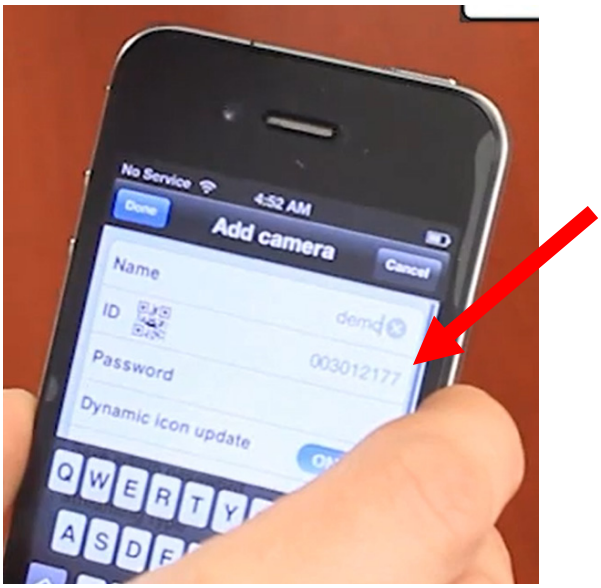
Lorex Video shows the barcode in the form of a QR code on the IP camera and an image of the QR code is generated in the iPhone when the QR code is scanned.

EX1008, 1:17; EX1001, ¶¶136-137. Lorex Video shows that the image of the QR code is both displayed on the screen of the iPhone when the QR code is scanned, and Lorex Video indicates that the image is at least temporarily stored in the iPhone to permit the iPhone to process the image and read the IP camera's

identifier from the QR code. EX1008: 1:08-1:40; EX1001, ¶137.

***Element [3]***

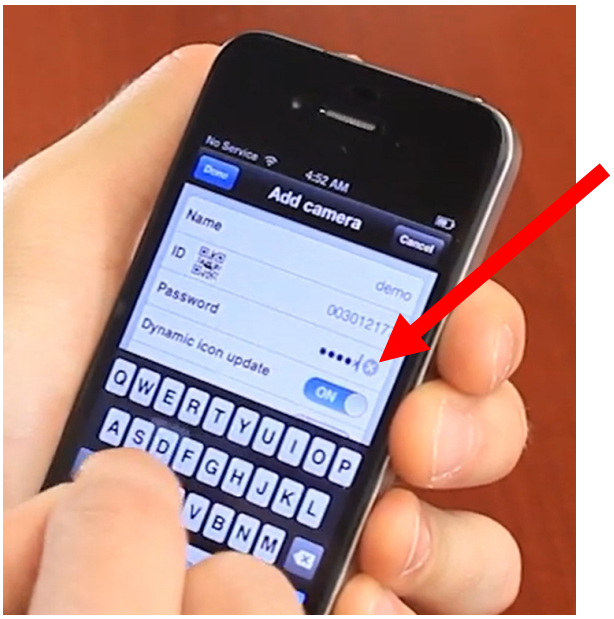
Lorex Video shows the iPhone converting the captured image of the QR code into the specific value of the IP camera's unique identifier (first identification) and using this identifier to connect the iPhone to the IP camera . EX1008, 1:00-1:40; EX1001, ¶138. As described above, the terminal device (e.g., the iPhone / P1 in Kim's FIG. 6) in the Kim-Lorex Video combination would predictably include the IP camera's unique identifier that was extracted from the image of the QR code in a connection request signal such as a "tunnel query request" message as taught in Kim. EX1007, [0081] ("a tunnel query request message includes an ID of the peer node P2 to communicate"), [0056], FIG. 6; *supra*, [1.4], Section V.B.2; EX1001, ¶138.




EX1008, 1:20 (cropped, annotated).

***Element [6]***

Kim discloses that peer nodes—including a first networked monitoring device such as P1 in FIG. 1 or P2 in FIG. 6—can register a "password" with the network server 100. EX1007, [0055]-[0056], [0052], [0123]. Lorex Video further discloses a default password being entered at the iPhone to log on the IP camera. EX1008, 1:20-1:36; EX1001, ¶¶139-140.




EX1008, 1:25 (cropped, annotated); *see also id.*, 1:22-27 ("Just plug in the password. By default its 'lorex'."). A POSITA would have found it obvious to implement Kim according to Lorex Video's suggested use of a default security password to improve security of the system and to block unauthorized users from connecting to the first networked monitoring device. EX1001, ¶140. A POSITA would have reasonably expected success implementing such features in Kim,

especially since Kim also contemplates that a "password" can be registered for a peer node (although Kim discloses no additional details regarding the password) and because default security passwords were conventional and commonly used security features before the '842 patent. EX1001, ¶140.

***Element [10]***

Lorex Video shows the barcode in the form of a QR code. EX1008, 1:08-1:24; EX1001, ¶141.

EX1008, 1:17 (cropped, annotated).

***Element [12.P]***

Even if the preamble is treated as a limitation (which Petitioners do not concede), the Kim-Lorex Video combination would have rendered it obvious. *Supra*, Element [1.P]; *see also* EX1007, [0023] ("method of allocating a virtual address"), [0027] ("method of setting direct communication"), [0054]-[0060],

[0078]-[0089], FIGS. 2, 6; EX1001, ¶142.

***Element [12.1]***

The Kim-Lorex Video combination would have rendered obvious Element [12.1], and would have provided the step of connecting first networked monitoring device (e.g., P1 in Kim's FIG. 2 / P2 in Kim's FIG. 6) to a network server through the Internet for at least the reasons described above with respect to Element [1.1]. EX1007, [0054]-[0060] & FIG. 2, [0061]-[0070] & FIG. 3, [0078]-[0079] & FIG. 6; *supra*, Element [1.1]; EX1001, ¶143.

***Element [12.2]***

The Kim-Lorex Video combination would have rendered obvious Element [12.2], and would have provided the step of registering a first identification of the first networked monitoring device (e.g., the identifier encoded in a QR code attached to the IP camera) into the list of networked devices of the server for at least the reasons described above with respect to Element [1.2]. *Supra*, Element [1.2]; EX1001, ¶144.

***Element [12.3]***

The Kim-Lorex Video combination would have rendered obvious Element [12.3], and would have provided the step of providing an image pattern (e.g., a QR code) comprising the first identification, wherein the image pattern is attached on the first networked monitoring device (e.g., Kim's P2 in FIG . 6 / Lorex Video's IP

camera) for establishing a P2P connection with the first networked monitoring device, for at least the reasons described above with respect to Element [1.3]. *Supra*, Element [1.3]; EX1001, ¶145.

***Element [12.4]***

The Kim-Lorex Video combination would have rendered obvious Element [12.4], and would have provided the steps of (i) generating a connection request signal (e.g., a tunnel query request message) by a terminal device (e.g., Kim's P1 in FIG. 6 / Lorex Video's iPhone) when the image pattern (e.g., the QR code on the IP camera) is captured to the terminal device and (ii) transmitting the connection request signal to the network server by the terminal device through the Internet, for at least the reasons described above with respect to Element [1.4]. *Supra*, Element [1.4]; EX1001, ¶146.

***Element [12.5]***

The Kim-Lorex Video combination would have rendered obvious Element [12.5], and would have provided the "identifying" step (and, indeed, all of the additional features recited in Element [12.5]), for at least the reasons described above with respect to Element [1.5]. *Supra*, Element [1.5]; EX1001, ¶147.

***Element [12.6]***

The Kim-Lorex Video combination would have rendered obvious Element [12.6], including the negative limitation that precludes the first networked

monitoring device (e.g., Kim's P2 in FIG. 6 / Lorex Video's IP camera) from capturing any image pattern (e.g., a QR code) associated with the terminal device (e.g., Kim's P1 in FIG. 6 / Lorex Video's iPhone) for establishing the P2P connection between the terminal device and the first networked monitoring device, for at least the reasons described above with respect to Element [1.6]. *Supra*, Element [1.6]; EX1001, ¶148.

***Element [13]***

The Kim-Lorex Video combination would have rendered obvious Element [13] for at least the reasons described above with respect to Element [2]. *Supra*, Element [2]; EX1001, ¶149.

***Element [14]***

The Kim-Lorex Video combination would have rendered obvious Element [14] for at least the reasons described above with respect to Element [3]. *Supra*, Element [3]; EX1001, ¶150.

***Element [17]***

The Kim-Lorex Video combination would have rendered obvious Element [17] for at least the reasons described above with respect to Element [6]. *Supra*, Element [6]; EX1001, ¶151.

Moreover, a POSITA would have understood that passwords are conventionally implemented for security and access control. EX1001, ¶¶152, 109

(citing corroborating exhibit EX1029). Considering the ubiquitous and conventional use of passwords in software-based systems before the '842 patent, it would have been obvious to implement the Kim-Lorex Video combination such that the terminal device would only log on the first networked monitoring device if a correct password is entered; otherwise, the user would predictably be presented with another opportunity to enter a security password that correctly matches the default security password of the IP camera. EX1001, ¶¶109, 152. A POSITA would have been prompted to implement the system in this manner to realize predictable benefits, including blocking unauthorized users if the password cannot be verified while still providing authorized users with additional opportunities to correctly enter the password. EX1001, ¶152.

***Element [18]***

The Kim-Lorex Video combination would have rendered obvious Element [18] for at least the reasons described above with respect to Element [10]. *Supra*, Element [10]; EX1001, ¶153.

### C. GROUND 3: Throughtek-2012 in View of Lorex Video Would Have Rendered Obvious Claims 1-4, 6-19

#### 1. Throughtek-2012

Throughtek-2012 is a publication of a German utility model that was filed by Throughtek Co., Ltd.—i.e., the same entity that owns the '842 patent—and that published no later than June 6, 2012—i.e., barely a year before the '842 patent's

provisional application was filed in the United States (April 16, 2013). EX1017, 1. The disclosure of Throughtek-2012 is substantially the same as much of the disclosure of the specification of the '842 patent itself. EX1001, ¶¶154-155. Indeed, FIGS. 1-5 of Throughtek-2012 are nearly identical to FIGS. 1-5 of the '842 patent and the description of these figures is also substantially similar in each document. EX1017, FIGS. 1-5; EX1001, ¶154. Throughtek-2012 thus expressly discloses all limitations of the Challenged Claims at least to the same extent as the '842 patent itself (and its provisional application). In short, Throughtek-2012 effectively anticipates all elements of the '842 patent, except for the negative limitation recited in Elements [1.6] and [12.6], which is equally lacking from the similar specifications of Throughtek-2012 and the later April 13, 2016 provisional application. EX1001, ¶155.

**2. The Througtek-2012-Lorex Video Combination**

Although Throughtek-2012 does not expressly disclose the claimed negative limitation (Elements [1.6]/[12.6]), the feature recited by the negative limitation was nonetheless known in the prior art as expressly demonstrated by Lorex Video. EX1008, 1:00-1:40 ("once that happens ... here it is"); EX1001, ¶¶156-157; *supra*, Section V.B.3 (Element [1.6]). As articulated below, multiple reasons would have prompted a POSITA to implement Throughtek-2012 in accordance with Lorex Video's suggestion for a simplified connection procedure without the first

networked monitoring device (IP camera) capturing any image pattern associated with the terminal device (smartphone). EX1001, ¶¶156-157; EX1008, 1:05-1:12 ("very simple"), 3:07-3:15 ("how long did that take? Simple, under three minutes. What more do you need from a network camera?").

**First**, a POSITA would have been motivated to implement Throughtek-2012 according to Lorex Video's suggestion to advantageously achieve the "quick and easy" connection between a smartphone and an IP camera by simply scanning the QR code on the back of the camera without the need for additional image capture or prior networking skills. EX1008, 0:05-0:11 ("show you how quick and easy it is"), 1:05-1:12 ("all I have to do is add this camera to my camera list … very simple because we have a QR code on the back"), EX1008, 1:17-1:40 ("once that happens ... here it is"); EX1001, ¶158.

**Second**, a POSITA would have been motivated to implement Throughtek-2012 according to Lorex Video's suggestion because to do so would have provided a detailed example to further Throughtek-2012's general goal to "quickly establish a direct connection." EX1017, [0007], [0016] ("[a] direct connection … can be established quickly"); EX1001, ¶159. By following Lorex Video's express suggestion to not require the IP camera to capture an image pattern on the smartphone, the user would have more easily established a connection by scanning the IP camera's QR code alone. EX1001, ¶159; EX1008, 1:05-1:40 ("very simple

because we have a QR code on the back"), 3:07-3:15 ("Simple, under three minutes. What more do you need from a network camera?").

Finally, both Throughtek-2012 and Lorex Video are directed to connecting peer-to-peer devices including smartphones and cameras, and the evidence here confirms that a POSITA would have been sufficiently skilled to implement such a combination given the predictable electrical/network components and the relatively advanced state of the art at the time. EX1001, ¶160. Accordingly, for these reasons articulated above, a POSITA would have had a reasonable expectation of success in achieving the Throughtek-2012-Lorex combination in the manner described herein. EX1001, ¶¶160-161.

### 3. Application to Challenged Claims

***Element [1.P]***

Even if the preamble is treated as a limitation (which Petitioners do not concede), the Throughtek-2012-Lorex Video combination would have rendered such a system obvious. For example, Throughtek-2012 describes "[a] system for detecting network apparatuses for establishing a point-to-point connection." EX1017, [0001] *see also* [0008], [0009], [0023], [0034], [0039], [0040], claim 1; *supra*, Section V.C.1-2; EX1001, ¶162.

***Element [1.1]***

Throughtek-2012 describes "a network server which is provided with an

apparatus list." EX1017 [0009], EX1001, ¶163. Throughtek-2012 describes first and second network apparatuses 20, 21 that "enter their respective identification codes A, B and address information into an apparatus list of the network server 10 when logging in." EX1017 [0026]. The network server 10 uses their identification codes and network addresses to establish a P2P connection between a terminal apparatus 30 and one of the network apparatuses 20, 21. EX1017 [0030]; *see also* EX1017 [0005], [0024], [0034], [0035], [0038], [0040], claim 1, FIGS. 1-5; EX1001, ¶163; *supra*, Section V.C.1-2.

***Element [1.2]***

Throughtek-2012 describes "at least one network apparatus provided with a built-in identification code … wherein the network apparatus is connected to the network server via the Internet for entering the identification code into the apparatus list." EX1017 [0009]; EX1001, ¶164. Throughtek-2012 describes network apparatuses 20, 21 as entering "their respective identification codes A, B and address information into an apparatus list of the network server." EX1017 [0026]. Throughtek-2012 describes "[t]he first and second network apparatus 20, 21 may each be a network camera, a webcam or a network monitor." EX1017 [0024]; *see also* EX1017 [0005], [0024]-[0028], [0030], [0034], [0036], [0040], claim 1, FIGS. 1-5; *supra*, Section V.C.1-2; EX1001, ¶164.

***Element [1.3]***

Throughtek-2012 describes "the first network apparatus 20 is provided with a first bar code 201 … wherein the first bar code 201 contains information about the first identification code A." EX1017 [0026]. The first identification code A is used to establish a direct connection with the first network apparatus 20. EX1017 [0027]; *see also* EX1017 [0009], [0026]-[0028], [0034], [0039], [0040] claim 1, FIGS. 1-5; *supra* Section V.C.1-2; EX1001, ¶165.

***Element [1.4]***

Throughtek-2012 describes a video capture module 301 of a terminal apparatus 30 that " captures the first bar code 201 arranged on the first network apparatus" and "[s]ubsequently, a request signal 303 containing the first identification code A is generated in the terminal apparatus 30 and forwarded to the network server 10." EX1017 [0027]; *see also* [0009], [0016], [0024], [0028]-[0030], [0034], [0037], [0039], [0040], claim 1, FIGS. 1-5; *supra* Section V.C.1-2; EX1001, ¶166.

***Element [1.5]***

Throughtek-2012 describes "the network server 10 receives a request signal 303 used to establish a connection", "[u]sing the first identification code A, the network server 10 searches in its apparatus list for a network address of the network apparatus corresponding to the first identification code", and "[b]ased on the known hole-punching technique, the network server 10 forwards a hole-

punching connection message 401, 402 to the first network apparatus 20 and the terminal apparatus 30, respectively, so that a direct communication channel 50 is established between the network apparatus 20 and the terminal apparatus 30." EX1017 [0030], *see also* [0009], [0010], [0034], [0038], [0040], FIGS. 3-4, claims 1, 5; *supra*, Section V.C.1-2; EX1001, ¶167.

***Element [1.6]***

The Throughtek-2012-Lorex Video combination would have rendered obvious Element [1.6]. Like the '842 patent and its provisional application, Throughtek-2012 does not expressly disclose or reasonably convey possession of the negative limitation recited in [1.6]. *Supra*, Sections II.C, V.C.1; EX1001, ¶¶168-169. Nonetheless, techniques for establishing a P2P connection without the first networked monitoring device capturing an image pattern associated with the terminal device were well known in the prior art as demonstrated by Lorex Video. *Supra*, Section V.B.1. Lorex Video discloses the entire/complete process for establishing a direct connection between a terminal device (e.g., an iPhone) and a first networked monitoring device (e.g., an IP camera). EX1008, 1:00-1:40; EX1001, ¶168. During this process, the IP camera is never used to capture any image pattern associated with the iPhone for establishing the connection between the iPhone and the IP camera. EX1008, 1:00-1:40; EX1001, ¶¶168-169. For the reasons described above, it would have been obvious to implement Throughtek-

2012 according to Lorex Video's suggestion for the first networked monitoring device to not capture any image pattern associated with the terminal device. *Supra*, Section V.C.2.

***Element [2]***

Throughtek-2012 describes a terminal apparatus 30 with a video capture module 301 that "captures the first bar code 201 arranged on the first network apparatus 20 and generates a corresponding bar code image." EX1017, [0027], *see also* claim 2; *supra*, Sections V.C.1-2; EX1001, ¶170.

***Element [3]***

Throughtek-2012 describes "the terminal apparatus (30) is provided with a bar code reader module (302) which can convert the bar code image used to establish the connection into an identification code, wherein the request signal (303) comprises the identification code." EX1017, claim 3, *see also* [0027]; *supra*, Section V.C.1-2; EX1001, ¶171.

***Element [4]***

Throughtek-2012 describes "the request signal (303) contains a bar code image used to establish the connection, while the network server (10) has a bar code reader module (101) which converts the bar code image used to establish the connection into an identification code." EX1017, claim 4, [0029]; *supra*, Sections V.C.1-2; EX1001, ¶172.

***Element [6]***

Throughtek-2012 describes "the network apparatus (2) can be protected by a previously agreed password, wherein the terminal apparatus (30) can log into the network apparatus (2) by means of the previously agreed password." EX1017, claim 7, *see also* [0031]; *supra*, Sections V.C.1-2; EX1001, ¶173.

***Element [7]***

Throughtek-2012 describes "the bar code (200) used to establish the connection comprises the previously agreed password, so that the video capture module (301) can generate a bar code image used to establish the connection after capturing the bar code (200) arranged in the second network apparatus (2)." EX1017, claim 8, *see also* [0012], [0032]; *supra*, Sections, V.C.1-2; EX1001, ¶174.

***Element [8]***

Throughtek-2012 describes "the terminal apparatus (30) is provided with a bar code reader module (302) which can convert the bar code image used to establish the connection into an identification code and a previously agreed password, wherein the request signal (303) simultaneously contains the identification code and the previously agreed password." EX1017, claim 9; *see also* [0013], [0032]; *supra*, Sections V.C.1-2; EX1001, ¶175.

***Element [9]***

Throughtek-2012 describes "the request signal (303) contains a bar code image used to establish the connection, while the network server (10) has a bar code reader module (101) which converts the bar code image used to establish the connection into an identification code and a previously agreed password." EX1017, claim 10, *see also* [0014]; *supra*, Sections V.C.1-2; EX1001, ¶176.

***Element [10]***

Throughtek-2012 describes "the bar code used to establish the connection is a QR code." EX1017, [0015], *see also* claim 11; *supra*, Sections V.C.1-2; EX1001, ¶177.

***Element [11]***

Throughtek-2012 describes "the bar code used to establish the connection is … a one-dimensional bar code." EX1017, [0015], *see also*, claim 12; *supra*, Sections V.C.1-2; EX1001, ¶178.

***Element [12.P]***

Even if the preamble is treated as a limitation (which Petitioners do not concede) the Throughtek-2012-Lorex Video combination would have rendered it obvious for at least the reasons described above with respect to Element [1.P]. *Supra,* Element [1.P]; *see also* EX1017, [0008], [0009], [0023], [0034]-[00340], claim 1, FIGS. 1-5; EX1001, ¶179.

***Element [12.1]***

*Supra*, Element [1.1]; *see also id.*, EX1017 [0005], [0009], [0024]-[0028], [0030], [0034], [0036], [0040], claim 1, FIGS. 1-5; EX1001, ¶180.

***Element [12.2]***

*Supra,* Element [1.2]; *see also id.*, EX1017 [0005], [0009], [0026], [0036] [0040], FIG. 5, claim 1; EX1001, ¶181.

***Element [12.3]***

*Supra,* Element [1.3]; *see also id.*, EX1017 [0009], [0026]-[0028], [0034], [0039], [0040] claim 1, FIGS. 1-5; EX1001, ¶182.

***Element [12.4]***

*Supra*, Element [1.4]; *see also id.*, EX1017 [0009], [0016], [0024], [0027]-[0030], [0034], [0037], [0039], [0040], claim 1, FIGS. 1-5; EX1001, ¶183.

***Element [12.5]***

*Supra* Element [1.5]; *see also id.*, EX1017 [0009], [0010], [0030], [0034], [0038], [0040], FIGS. 3-4, claims 1 and 5; EX1001, ¶184.

***Element [12.6]***

The Throughtek-2012-Lorex Video combination would have rendered obvious Element [12.6] for at least the reasons described above with respect to Element [1.6]. *Supra,* Element [1.6]; *see also id.*, EX1008, 1:00-1:40; EX1001, ¶185.

***Element [13]***

*Supra*, Element [2]; EX1001, ¶186.

***Element [14]***

*Supra*, Element [3]; EX1001, ¶187.

***Element [15]***

*Supra*, Element [4]; EX1001, ¶188. .

***Element [16]***

*Supra*, Element [4]; EX1001, ¶189.

***Element [17]***

*Supra*, Element [6]; EX1001, ¶190.

***Element [18]***

*Supra*, Element [10]; EX1001, ¶191.

***Element [19]***

*Supra*, Element [11]; EX1001, ¶192.

## 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, all Grounds 1-3 are based upon prior art references that were absent during prosecution of the original '498 patent and prosecution of the reissue application. *See generally* EX1004 and EX1005.

Moreover, this Petition specifically identifies material errors in the less-than-candid "key focus" of the '842 patent (col. 4:50-55) and the examiner's apparent belief of such an inaccurate statement. *Supra*, Section II.B.

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

Virtually all of the *Fintiv* factors weigh against exercising discretionary denial. The related litigation is in its infancy.

*Factor 1: Whether a Stay Exists or Is Likely to Be Granted if a Proceeding Is Instituted*

No motion to stay has been filed at this time, and therefore, this factor is neutral.

*Factor 2: Proximity of the Court's Trial Date to the Board's Projected Statutory Deadline*

Even though the Complaint (EX1019) was served on March 1, 2023, Reolink's initial motion to dismiss is still pending and no Answer to the Complaint has been filed. In other words, the present Petition is being filed *before* any Answer in the litigation, so no scheduling order/trial date has been established. The Board's final decision will surely precede the not-yet-scheduled jury trial in the Reolink litigation at the District of Delaware. This should be dispositive—the timing undercuts the fundamental premise for a *Fintiv* denial. Indeed, this conclusion is corroborated by the fact that the current median-time-to trial in Delaware is 37.8 months—indicating a jury trial date long after any final decision

in this IPR. *See*

https://www.uscourts.gov/sites/default/files/fcms_na_distprofile0930.2023.pdf, 14.

Factor 2 weighs heavily against exercising discretion to deny.[5]

*Factor 3: Investment in the Parallel Proceeding by the Court and Parties*

Neither Patent Owner nor Reolink has invested in *Markman* briefing, substantive fact discovery, expert discovery, summary judgment motions, and pre-trial preparations. Again, 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*, at 27. Factor 3 weighs heavily against exercising discretion to deny.

*Factor 4: Overlap between Issues Raised in the Petition and in the Parallel Proceeding*

Again, 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

[5] Reolink notes that trial dates (if any) for other defendants in other district courts will be addressed in Factor 6, as confirmed in *Illumina, Inc. v. Ravgen, Inc.*, IPR2021-01271, Paper 12, 26-27 (January 26, 2022).

overlap of issues cannot be fully assessed, and Patent Owner cannot point to any evidence to the contrary. Factor 4 is neutral.

*Factor 5: Whether the Petitioner and the Defendant in the Parallel Proceeding Are the Same Party*

Petitioners are the defendants in the Reolink lawsuit. 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: Other Circumstances that Impact the Board's Exercise of Discretion, Including the Merits*

The PTAB's guidance plainly states that, "where the PTAB determines that the information presented at the institution stage presents a compelling, unpatentability challenge, that determination alone demonstrates that the PTAB should not discretionarily deny institution under *Fintiv*." *See* Interim Procedure for Discretionary Denials in AIA Post-Grant Proceedings with Parallel District Court Litigation, 4-5 (June 21, 2022) ("Guidance Memo"). That is the scenario here.

We know several critical truths. That the '842 patent alleges a relatively late priority date in 2013 with a "key focus" (col. 4:50-55) on capturing a barcode attached to an IP camera. *Supra*, Section II.A. That multiple publications from 2012 demonstrate this feature was already in the public domain. EX1006, 13, EX1008, EX1009, EX1010, EX1011, ¶5. That the examination suffered from significant errors along with Patent Owner's injection of new matter into the

claims. *Supra*, Section II.B-C. And that Grounds 1-3 are obviousness grounds "in which the evidence, if unrebutted in trial, would plainly lead to a conclusion that one or more claims are unpatentable by a preponderance of the evidence"—the very definition of "[c]ompelling, meritorious challenges" set forth by the Director. *See* Guidance Memo, 4. The '842 patent was erroneously allowed; now is the time for review. Under the AIA, PTAB trials were created for this very reason. Factor 6 weighs heavily in favor of institution.

Finally, as noted below, the '842 patent was also asserted in two other district courts (WDWA and EDTX) against different defendants (Anker and Amcrest). *Infra*, Section VIII. At least one of those third-party lawsuits is now terminated (WDWA), and the EDTX litigation is at an early stage before *Markman* briefing and without any docket items indicating investments toward expert discovery, summary judgment motions, and pre-trial preparations. Given the early stage of the EDTX litigation, there is little or no evidence of overlap with specific §103 grounds in this Petition. And even if one assumes some (speculative) overlap to be given weight, "that weight is diminished to a degree because [the third party] is unrelated to Reolink (*Fintiv* factor 5) and due to uncertainty about when and if trial in the [EDTX] lawsuit will occur." *Illumina*, at 32.

## VII. PAYMENT OF FEES—37 C.F.R. §42.103

Petitioners authorize the Patent and Trademark Office to charge any fees to Deposit Account No. 06-1050.

## VIII. MANDATORY NOTICES—37 C.F.R §42.8(a)(1)

### A. Real Party-In-Interest—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—37 C.F.R. §42.8(b)(2)

Petitioners are not aware of any disclaimers, reexamination certificates, or other petitions for IPR of the '842 patent. The '842 patent is the subject of civil action captioned *ThroughTEK Co., Ltd. v. Reolink Innovation Inc. et al.*, Case No. 1-23-cv-00218 (DDE), Document 1 (Complaint), February 28, 2023. *See* EX1019. This litigation complaint was initially asserted against Reolink and a variety of retailers, but all of those retailers were dismissed from the litigation.

Petitioners are aware that the '842 patent was also asserted in different districts against different defendants:

- *ThroughTEK Co., Ltd. v. Amcrest Technologies LLC et al.*, Case No. 2-23-cv-00035 (EDTX)
- *Throughtek Co Ltd v. Anker Innovations Co Ltd et al.*, Case No. 2-23-cv-00515 (WDWA)

At least the WDWA litigation was terminated, and the docket of the EDTX litigation reveals an early posture (e.g., no *Markman* briefing, no depositions or expert discovery). Again, none of these defendants in the WDWA litigation and the EDTX litigation had access or control over this Petition; this Petition was exclusively controlled and funded by Reolink.

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

Petitioners provide the following designation of counsel.

| Lead Counsel | Backup counsel |
|---|---|
| Michael T. Hawkins, Reg. No. 57,867<br>Fish & Richardson P.C.<br>60 South Sixth Street, Suite 3200<br>Minneapolis, MN 55402<br>Tel: 202-783-5070<br>Fax: 877-769-7945<br>Email: hawkins@fr.com | Nicholas W. Stephens, Reg. No. 74,320<br>Joseph Bauer, Reg. No. 81,218<br>Fish & Richardson P.C.<br>60 South Sixth Street, Suite 3200<br>Minneapolis, MN 55402<br>Tel: 202-783-5070<br>Fax: 877-769-7945<br>Email: IPR52472-0005IP1@fr.com |

### D. Service Information

Please address all correspondence and service to the address listed above. Petitioners consent to electronic service by email at IPR52472-0005IP1@fr.com.

Respectfully submitted,

Dated: January 30, 2024

/Nicholas W. Stephens/

Michael T. Hawkins, Reg. No. 57,867
Nicholas W. Stephens, Reg. No. 74,320
Joseph Bauer, Reg. No. 81,218
Fish & Richardson P.C.
60 South Sixth Street, Suite 3200
Minneapolis, MN 55402
Tel: 202-783-5070
Fax: 877-769-7945

(Case No. IPR2024-00509)

*Attorneys for Petitioners*

## 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 13,946 words, which is less than the 14,000 allowed under 37 CFR § 42.24.

Dated: January 30, 2024

/Nicholas W. Stephens/

Michael T. Hawkins, Reg. No. 57,867
Nicholas W. Stephens, Reg. No. 74,320
Joseph Bauer, Reg. No. 81,218
Fish & Richardson P.C.
60 South Sixth Street, Suite 3200
Minneapolis, MN 55402
Tel: 202-783-5070
Fax: 877-769-7945

*Attorneys for Petitioners*

**CERTIFICATE OF SERVICE**

Pursuant to 37 CFR §§ 42.6(e)(4)(i) *et seq.* and 42.105(b), the undersigned certifies that on January 30, 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:

WPAT, PC
INTELLECTUAL PROPERTY ATTORNEYS
8230 BOONE BLVD. SUITE 405
VIENNA VA 22182
UNITED STATES

/Crena Pacheco/

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