

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

DECLARATION OF HARRY BIMS, Ph.D.

TABLE OF CONTENTS

I.	Introduction	4
II.	Background and Qualifications	4
III.	Level of Ordinary Skill in the Art	7
IV.	Materials Considered and Relied Upon	9
V.	Legal Principles.....	12
A.	Anticipation	12
B.	Obviousness.....	12
VI.	Overview of the '842 Patent.....	14
A.	The Advanced State of the Art	14
B.	The '842 Patent Describes a Predictable Application of Conventional Barcode-based Device Identifiers to a Conventional Hole-Punching System.....	26
C.	File History of the '842 Patent and its Related Applications	30
D.	The Effective Filing Date of the '842 Patent.....	34
E.	Interpretation of the '842 Patent Claims at Issue.....	40
VII.	GROUND 1 – Obviousness of Claims 1-3, 6, 10, 12-14, 17, and 18 Based on Lorex Guide (EX1006) and Kim (EX1007).....	41
A.	Overview of Lorex Guide	41
B.	Overview of Kim	43
C.	The Predictable Combination of Lorex Guide and Kim.....	45
VIII.	GROUND 2 – Obviousness of Claims 1-3, 6, 10, 12-14, 17, and 18 Based on Kim (EX1007) and Lorex Video (EX1008).....	72

A.	Overview of Lorex Video	72
B.	The Predictable Combination of Kim and Lorex Video	74
IX.	GROUND 3 – Obviousness of Claims 1-4 and 6-19 Based on Throughtek-2012 (EX1017) and Lorex Video (EX1008).....	98
A.	Overview of Throughtek-2012	98
B.	The Predictable Combination of Throughtek-2012 and Lorex Video 100	100
X.	Conclusion.....	117

I, Harry Bims, Ph.D., declare that:

I. Introduction

1. I have been retained by counsel for Reolink Innovation Inc. and Shenzhen Reolink Technology Co., Ltd. (“Petitioners”) as an expert witness to provide assistance regarding Reissue Patent No. RE47,842 (“the ’842 Patent”). Specifically, I have been asked to consider the validity of claims 1-4 and 6-19 of the ’842 Patent (the “Challenged Claims”) in view of certain prior art publications.

2. I am being compensated for my time at my standard consulting rate. I am also being reimbursed for expenses that I incur during the course of this work. My compensation is not contingent upon the results of my study, the substance of my opinions, or the outcome of any proceeding involving the challenged claims. I have no financial interest in the outcome of this matter.

3. My independent analysis here is based on my years of education, research and experience, as well as my investigation and study of relevant materials, including those cited herein.

II. Background and Qualifications

4. I am over the age of 18 and am competent to provide this testimony. I have personal knowledge, or have developed knowledge of these technologies based upon education, training, or experience, of the matters set forth herein.

5. I believe that I am well qualified to serve as a technical expert in this matter based upon my qualifications, discussed in detail below. A copy of my curriculum vitae is attached as an appendix to this declaration.

6. Based on my education, research, and work experience, I am knowledgeable about the subject matter of the '842 patent and the related prior art.

7. For more than 30 years, since approximately 1981, I have studied, designed, and worked in the field of telecommunications, including wireless communications. During this period, I have designed and implemented various products involving cellular communication technology.

8. I received a B.S. in Computer and Systems Engineering from Rensselaer Polytechnic Institute in 1985. I received an M.S. in Electrical Engineering in 1988 and a Ph.D. in Electrical Engineering in 1993, both from Stanford University. As a graduate student, I studied the principles of Digital Communications theory, including data modulation and demodulation, signal constellations and lattices, channel estimation, equalization, filtering, precoding, synchronization, and trellis coding. My Ph.D. thesis addressed the application of trellis coding and precoding to a digital modulation system, and was titled "Trellis Coding for Multi-Level, Partial Response Continuous Phase Modulation with Precoding."

9. After receiving my Ph.D. in 1993, I worked for Glenayre Technologies – Wireless Access Group, where I worked on applications for wireless communication,

including inventing, designing, and building a patented two-way pager test system and co-developing a wireless application protocol.

10. In January of 1999, I launched a technology consulting company, Protocomm Systems Inc., which focuses on the development of advanced wireless communications protocols and related software implementations for wireless product companies.

11. From 1999 to 2001, I was also the Director of Software Architecture for Symmetry Communications System. In this position, I was responsible for the software architecture for core SGSN (Serving GPRS Support Node) and GGSN (Gateway GPRS Support Node) products for the GPRS (Generic Packet Radio Services) market. I also held management responsibility for the Firmware, Hardware, Performance, and Systems Engineering Groups.

12. In 2001, I developed a business plan for building network belowstructure for Institute of Electrical and Electronics Engineers (“IEEE”) 802.11 standard (“Wi-Fi”) enterprise networks, and then later that year founded AirFlowNetworks, Inc. where I invented and received eleven patents on a distributed antenna system design for wireless networks, based on the 802.11 wireless local area network specification. The AirFlow Networks product was an enterprise-classs Wi-Fi network that supported network layer routing and forwarding of data streams between the Internet and end-user devices.

13. I am currently the President of Protocomm Systems, LLC and Bims Laboratories, LLC, both of which I founded. As the President of Bims Laboratories, I perform technical research in wireless technology standards, such as UMTS, LTE/4G, 5G, Wi-Fi, Bluetooth, and other network communication protocols. I am named as an inventor of twenty-three telecommunications related patents.

14. In addition, I am a named Technical Expert and former Vice-Chair and Secretary of the IEEE 802.16 Working Group, which develops technical standards for the wireless protocol commonly known as WiMax. I am also a voting member of the IEEE 802.11 Working Group (which develops technical standards for WiFi), and the IEEE 802.15 Working Group (which develops standards for a variety of specialty wireless networks). Within the IEEE 802.15 Working Group, I am the technical editor for IEEE 802.16t, an amendment to the WiMAX standard that supports long-range wireless networks for the railroad industry. Within the IEEE 802.11 Working Group, I routinely participate and vote on discussions relating to the design of wireless communications, including packet prioritization, transmission, acknowledgment, and retransmission.

III. Level of Ordinary Skill in the Art

15. Based on my knowledge and experience in the field and my review of the '842 patent and its file history, a person of ordinary skill in the art before the effective filing date of the '842 Patent would have had a bachelor's degree in

electrical engineering and two years of work experience with network and communication technologies. Additional relevant education could compensate for less work experience and additional relevant work experience could compensate for less education. I refer to such a person as a “POSITA” in this declaration.

16. Regarding the timeframe in ¶15 above (“before the effective filing date”), I know that the ’842 patent claims priority to a provisional application filed on April 16, 2013 and to a utility application filed three months later on July 25, 2013. Further, as I describe in detail below (Section VI.D), all claims of the ’842 patent require a negative limitation directed to subject matter that was first disclosed in an amendment to the claims of the utility application on September 20, 2016. I have applied April 16, 2013 as the effective filing date of the claims of the ’842 patent for purposes of analyzing issues related to Grounds 1-2 in this declaration, and my analysis and the conclusions that I have provided herein with respect to Grounds 1-2 are based on the perspective of a POSITA as of April 16, 2013. However, I have also considered the issues addressed in this declaration from the perspective of a POSITA as of both July 25, 2013 and September 20, 2016, and my analysis and the conclusions that I have drawn herein would remain unchanged with respect to Grounds 1-2 of this declaration if the effective filing date of the claims of the ’842 patent was later than April 16, 2013 (as all of the prior art in Grounds 1-2 was published or filed before April 16, 2013). I have applied September 20, 2016 as the

effective filing date of the claims of the '842 patent for purposes of analyzing issues related to Ground 3 in this declaration, and my analysis and the conclusions that I have drawn herein with respect to Ground 3 are based on the perspective of a POSITA as of September 20, 2016. However, I have also considered the issues addressed in this declaration with respect to Ground 3 from the perspective of a POSITA as of both April 16, 2013 and July 25, 2013, and my analysis and the conclusions that I have drawn herein would remain unchanged with respect to Ground 3 if the effective filing date of the claims of the '842 patent was April 16, 2013, July 25, 2013, or later (as all of the prior art in Ground 3 was published before April 16, 2013). Regardless of which of these dates applies, my level of skill in the art was at least that of a POSITA as defined above in ¶15 before each of these dates. I am qualified to provide opinions concerning the knowledge and perspective of a POSITA.

IV. Materials Considered and Relied Upon

17. In forming my opinions and reaching the conclusions described in this declaration, I have relied on the documents and materials cited herein as well as those identified in this declaration, including the '842 Patent, the prosecution history of the '842 Patent, and prior art references cited herein. These materials comprise patents, related documents, and printed publications. Each of these materials is a type of document that experts in my field would have reasonably relied upon when

forming their opinions. I have also relied on my education, training, research, knowledge, and personal and professional experience in the relevant technologies and systems that were already in use prior to, and within the timeframe of the Critical Date of the '842 Patent.

18. Accordingly, as part of my independent analysis of the '842 patent, I have analyzed the following publications and materials:

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), <i>available at</i> 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), <i>available at</i> 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), <i>available at</i> 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), <i>available at</i> https://www.youtube.com/watch?v=HzJfkqg2VWY (“Lorex QR Codes”)
EX1011	Declaration of Vlad Kardashov
EX1015	Certified English Translation of Korean Patent No. KR100984288B1 (“Park”)

EX1017	Certified English Translation of German Utility Model No. DE202012101164U1 (“Throughtek-2012”)
EX1018	Throughtek Co. Ltd., <i>CSJ233 P2P IP Camera Plug and View Instant Surveillance</i> (2011) (“2011 Brochure”)
EX1019	<i>ThroughTEK Co., Ltd. v. Reolink Innovation Inc. et al.</i> , Case No. 1-23-cv-00218 (DDE), Document 1 (Complaint), February 28, 2023
EX1020	Ford et al., <i>Peer-to-Peer Communication Across Network Address Translators</i> , USENIX Annual Technical Conference, pp. 179-192 (2005)
EX1021	Reolink Technology Co., Ltd., <i>Reolink Support Initial Setup for Reolink Argus Series Cameras via Reolink App</i> (Aug. 22, 2019), available at https://www.youtube.com/watch?v=jn2BhMmKcyg (“Reolink Video”)
EX1022	U.S. Pub. 2014/0013100 (“Menzel”)
EX1023	U.S. Pub. 2012/0287290 (“Jain”)
EX1024	Saxena et al., <i>Secure Device Pairing based on a Visual Channel</i> , IEEE Symposium on Security and Privacy (2006) (“Saxena”)
EX1025	U.S. Pub. 2010/0259549 (“Brown”)
EX1026	Scott et al., <i>Using Visual Tags to Bypass Bluetooth Device Discovery</i> , <i>Mobile Computing & Communications Review</i> , Vol. 1, No. 2 (2005) (“Scott”)
EX1027	Eppinger, <i>TCP Connections for P2P Apps: A Software Approach to Solving the NAT Problem</i> , Carnegie Mellon University Institute for Software Research International (2005) (“Eppinger”)
EX1028	Maier et al., <i>NAT Hole Punching Revisited</i> , 36 th Annual IEEE Conference on Local Computer Networks (2011) (“Maier”)
EX1029	U.S. Pub. 2008/0313721 (“Corella”)

19. Although this declaration refers to selected portions of the cited references, it should be understood that these are examples, and I recognize that a POSITA would have viewed the references cited herein in their entirety and in combination with other references cited herein or cited within the references themselves.

V. Legal Principles

A. Anticipation

20. I have been informed that a patent claim is invalid as anticipated under 35 U.S.C. § 102 if each and every element of a claim, as properly construed, is found either explicitly or inherently in a single prior art reference. Under the principles of inherency, if the prior art necessarily functions in accordance with, or includes the claimed limitations, it anticipates.

B. Obviousness

21. I have been informed that a patent claim is invalid as “obvious” under 35 U.S.C. § 103 in light of one or more prior art references if it would have been obvious to a POSITA before the effective filing date of the claimed invention, taking into account (1) the scope and content of the prior art, (2) the differences between the prior art and the claims, (3) the level of ordinary skill in the art, and (4) any so called “secondary considerations” of non-obviousness, which include: (i) “long felt need” for the claimed invention, (ii) commercial success attributable to the claimed invention, (iii) unexpected results of the claimed invention, and (iv) “copying” of the claimed invention by others. I have been informed that the test for obviousness is not whether the features of a secondary reference may be “bodily incorporated” into the structure of the primary reference, but rather whether a POSITA would have

been motivated to combine the teachings of the prior art references to achieve the claimed invention.

22. For a claim to be obvious in light of multiple prior art references, there must be an articulated reason that would have prompted a POSITA to combine those prior art references in order to achieve the claimed invention. This reason may come from a teaching, suggestion, or motivation to combine, or may come from the reference or references themselves, the knowledge or “common sense” of a POSITA, or from the nature of the problem to be solved, and may be explicit or implicit from the prior art as a whole. I have been informed that, under the law, the combination of familiar elements according to known methods is likely to be obvious when it does no more than yield predictable results. Also I have been informed that, under the law, when a patent simply arranges old elements with each performing the same function it had been known to perform and yields no more than a POSITA would have expected from such an arrangement, the combination is obvious. Furthermore I have been informed that, under the law, if a technique has been used to improve one device, and a POSITA would have recognized that it would improve similar devices in the same way, using the technique is obvious unless its actual application is beyond his or her skill. I also understand it is improper to rely on hindsight in making the obviousness determination.

23. Regarding the timeframe in ¶21 above (“before the effective filing date”), I have applied April 16, 2013 as the effective filing date of the claims of the ’842 patent for Grounds 1-2, as I described above in ¶¶15-16. Again, all of the references in Grounds 1-2 published well before April 16, 2013. For Ground 3 below, I have applied September 20, 2016 as the earliest effective filing date, as I described above in ¶¶16-17 and below in ¶¶49-54. I note that, for Ground 3, my analysis and the conclusions that I have drawn herein would remain unchanged even if the effective filing date of the claims of the ’842 patent was as early as the utility filing date (July 25, 2013) because all of the prior art in Ground 3 was published well before July 25, 2013. For Ground 3, if the effective filing date was assumed to be April 16, 2013, I note that the references in Ground 3 were published before April 16, 2013, and I was informed that the Board would consider if those publications qualify as prior art. .

VI. Overview of the ’842 Patent

A. The Advanced State of the Art

24. The ’842 patent generally describes techniques for forming point-to-point¹ (P2P) connections between devices such as an IP camera and a smatphone by (1)

¹ The ’842 patent uses the term “P2P” as shorthand for “point-to point.” *See*

EX1002, 1:32-38, 9:8, 10:19. In the context of the ’842 patent, a POSITA would have understood that a “point-to-point” connection allows for direct

communication between two devices but does not require a direct physical link between the two devices. This is clear from the specification of the '842 patent, which explains that a “point-to-point” connection can be established between a pair of devices over the Internet in which there is plainly no direct physical link between the devices. *See, e.g.*, EX1002, 5:30-36 (“the Internet can be based on Ethernet, wireless networks, local area network (LAN), wide area network (WAN) or virtual private network (VPN)”); 7:47-49 (“the terminal device 30 then sends the security code to the first networked device 20 through the internet”). Such a “point-to-point” connection as described in the '842 patent would encompass certain TCP/IP connections that allowed for direct communication between the terminal device and the first networked monitoring device, for example—even where the information communicated between the devices is packetized and crosses multiple networks and multiple intervening nodes. Another term that is commonly used for such P2P connections in the art is “peer-to-peer” connections. *See, e.g.*, EX1007, [0018] (“Peer-to-Peer (P2P)”). Based on my review, the '842 patent’s “point-to-point” connections established over the Internet would plainly include conventional “peer-to-peer” connections, and the terms are largely interchangeable in the context of the '842 patent.

identifying a particular device (e.g., a particular camera) to which the user desires the smartphone to connect by capturing an image of a barcode associated with that device and by (2) “punching holes” through the boundaries of the local networks in which the camera and the smartphone reside.

25. None of the techniques described or claimed in the ’842 patent were new before the ’842 patent’s provisional application (April 16, 2013). Indeed, both the use of a barcode (e.g., a QR code) on one device that can be quickly and easily scanned by another device to establish a connection—which the ’842 patent identifies as its “key focus” (*see* EX1002, 4:50-55)—and the use of hole-punching techniques for forming P2P connections were conventional and well known in the art. The following sub-sections briefly overview the state of the art as it relates to these two concepts by the relevant timeframe of the ’842 patent. Further, the combination of these techniques as claimed was entirely predictable for the reasons detailed below in my analysis of Grounds 1-3.

1. Conventional Uses of Barcodes and Visual Markers for Identifying Devices as the Target of a Connection

26. As I alluded to above, the ’842 patent refers to the provision of a “barcode” on a networked device as a “key focus of the present invention.” EX1002, 4:50-55; *see also id.*, 3:30-39 (“[T]he present invention has the following advantages: It can quickly establish connections between mobile devices and networked devices. Unlike prior art to manually enter the identification code word by word, the image

capture unit of a mobile phone captures the barcode image of the networked device[] ... to establish a P2P connection between the networked device and the terminal device.”). But the use of barcodes or other visual markers as a mechanism to identify a device as the target of a requested connection, or for other analogous purposes, was well known in the prior art. Indeed, such techniques had been repeatedly discussed in the art years before even the earliest claimed priority date of the ’842 patent (April 2013).

27. By way of example, in 2006, a group of researchers from the University of California (Irvine) and the Nokia Research Center (Helsinki, Finland) published a paper in the proceedings of the IEEE Symposium on Security and Privacy titled “Secure Device Pairing based on a Visual Channel.” *See* EX1024. I will refer to this paper as the “Saxena” paper in recognition of the first-named author (Nitesh Saxena). Saxena explained that, by 2006, “[t]he popularity of short-range wireless technologies like Bluetooth and Wireless Local Area Networking [was] experiencing enormous growth.” *Id.*, 1. “This rise in popularity implies that an ever increasing proportion of the users of devices supporting short-range wireless communication are not technically savvy” and “[s]uch users need very simple and intuitive methods for setting up their devices.” *Id.* According to Saxena, “[a] common set up task is to initialize secure communication” (referred to as “pairing”). *Id.* “one approach to secure pairing is to use an additional physically authenticatable

‘out-of-band’ (OOB) channel in which “[t]he adversary is assumed to be incapable of modifying messages on the OOB channel.” *Id.* Notably, Saxena explained that one known OOB channel that could be used to establish a connection between devices was a “visual channel” (referred to as the “Seeing-is-Believing” (SiB) channel) based on a barcode (similar to that described in the ’842 patent):

sual channel. The SiB visual channel consists of a two-dimensional barcode displayed by (or affixed to) a device *A*, that represents security-relevant information unique to *A*. A user can point another camera-equipped device *B* at the barcode so that *B* can read the barcode visually, and use this information to set up an authenticated channel to *A*. If both devices are camera-equipped, they can mutually authenticate each other. “Authentication” in this case is based on demonstrative identification [1] rather than with respect to a claimed name.

EX1024, 1 (highlighting added); *see also id.*, 4 (“our visual tags are circular barcodes”).

28. In another example, in 2005, a group of researchers from the University of Cambridge and Intel Research Cambridge published in *Mobile Computing and Communications Review* (Vol. 1, No. 2) an article describing similar techniques titled “Using Visual Tags to Bypass Bluetooth Device Discovery.” *See* EX1026. I will refer to this paper as the “Scott” paper in recognition of the first-named author (David Scott). Scott explained that “[o]ne factor that has limited the use of Bluetooth as an underlying networking technology for publicly accessible mobile services is that its *device discovery* model is inappropriate for this kind of interaction.” *Id.*, 1.

Scott proposed to address this issue through the use of, among other things, “[v]isual tags [that] are used for out-of-band device selection, bypassing the standard Bluetooth discovery model.” *Id.* Scott explains the benefit of using visual tags in this context (in a manner that is strikingly similar to the ’842 patent’s own description of the benefit of such barcodes/visual tags (*see* EX1002, 3:30-38 (“quickly establish connections” without “manually enter[ing] the identification code word by word”))):

III.B. Tag-Based Device Discovery

In contrast, by using visual tags to identify devices and services, Alice can simply point their cameraphone at Bob's phone and click in order to establish a connection with it. In our framework Bob's cameraphone has a tag attached to it: either physically printed on the device itself, or displayed on the device's screen (perhaps as the default wallpaper). Then, to transfer the photo, Alice performs the following sequence of actions:

Select photo: As before, Alice uses the menu system on their phone to select the picture to transfer via Bluetooth.

Select Physical Device: After selecting a picture to transfer, Alice aims their cameraphone at the tag on Bob's cameraphone and presses the select button on their phone's keypad.

The tag is decoded yielding the Device Address of Bob's cameraphone. A Bluetooth connection is initiated immediately and the selected picture is transferred. By encoding Device Addresses in visual tags, we provide two significant benefits to the user:

1. The time taken to establish the connection and initiate the picture transfer is an order of magnitude faster than performing Device Discovery (see Section VI).
2. The Bluetooth Device Name is abstracted from the user.

EX1026, 3 (highlighting added); *see also id.*, (“Using our technology, a user can focus on performing the task in hand—connecting two physical devices to access a mobile service—rather than having to establish a connection via (arbitrarily chosen) device names.”), 11 (“visual tags can be used to initiate Bluetooth connections with mobile services, providing orders-of-magnitude time improvements over the standard ... model”).

29. U.S. Pub. 2014/0013100 (EX1022, “Menzel”) further illustrates the conventional use of barcodes for forming connections between devices in the prior art before the ’842 patent. Menzel describes a process for establishing P2P connections substantially similar to the processes described in the ’842 patent itself, e.g., as shown by the flowchart in FIG. 1:

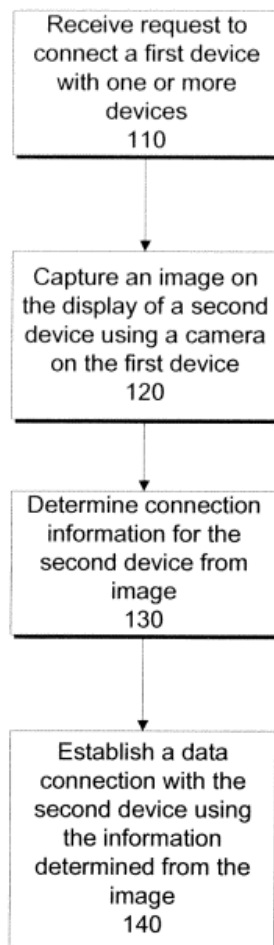


Fig. 1

EX1022, FIG. 1; *see also id.*, [0004] (“Embodiments related to techniques for forming secure bidirectional wireless communication between electronic devices using visual codes are described herein. Various configurations make use of one of many possible visual codes (such as an image, barcodes, qr codes, series of numbers, or other unique identification codes) to uniquely identify a nearby device by using a camera, and then automatically connect to it using wireless technology. In numerous embodiments of the invention, devices intended to communicate will each, on their own display devices, display an image containing information that can be used to connect to that particular device. Other devices can capture that image with their camera and establish a data connection using the information encoded within the image.”), [0005]-[0008], [0024]-[0040], FIGS. 5A-6C.

30. As yet another example, U.S. Pub. 2010/0259549 (EX1025, “Brown”)—published in October 2010—described techniques for “facilitat[ing] the display of a barcode at a computing device for capture by another computing device.” EX1025, Abstract. Before the alleged invention of the ’842 patent, Brown recognized that it would be more convenient for users who desired to join a social media group to scan a barcode displayed on an existing member’s smartphone or PDA rather manually inputting information identifying the group and authenticating the user:



FIG. 8

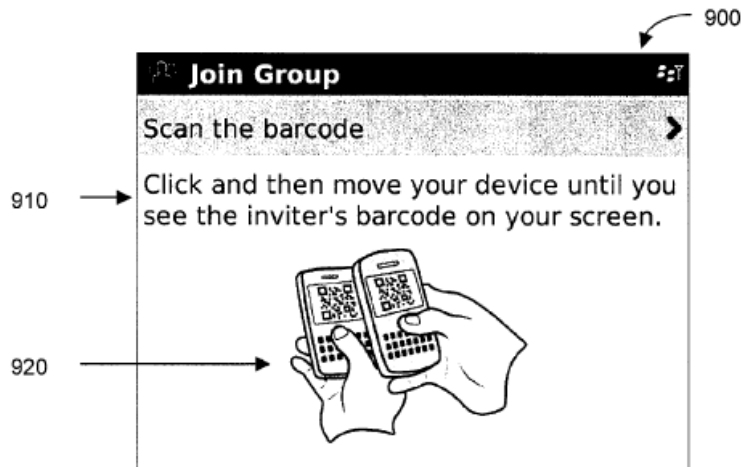


FIG. 9

EX1025, FIGS. 8-9; *see also id.*, [0011]-[0012], [0071]-[0072], [0063].

31. The use of barcodes and similar visual markers for device identification in connection procedures was not only a topic of academic research and thoroughly described in the patent literature, it was also described in non-patent literature and implemented in commercial products before the earliest effective filing date of the '842 patent, as evident from the Lorex Guide (EX1006) and Lorex Video

(EX1008). I have provided a more detailed overview of these references as they pertain to Grounds 1-3 further below. *See below*, Sections VII.A, VIII.A.

2. Conventional Hole-Punching Techniques for Establishing P2P Connections

32. A second aspect of the claimed technology in the '842 patent relates to the use of a network server to facilitate “hole punching” procedures that permit a P2P connection to be established between a terminal device and a first networked monitoring device. But establishing P2P connections using “hole-punching” was indisputably known before the '842 patent—i.e., a fact admitted by the '842 patent itself. EX1002, 5:59-61 (“well known in the field”), 5:40-41, 3:5-8; EX1018, 2.

33. By way of background, P2P connections known in the prior art conventionally allowed two network devices (sometimes referred to as “peer” devices) to directly communicate across one or more networks. Establishing P2P connections commonly involved “hole-punching,” a technique that was often employed to safely form connections between devices located in private networks having firewall(s) and/or network address translator(s) (NAT(s)) that would block unsolicited, inbound traffic from entering the private network. EX1015, 4-6 and FIGS. 2-6. Indeed, years before the '842 patent, Througtek confirmed this traditional practice in its own publications. *E.g.*, EX1018, 2.

34. Conventional hole-punching schemes circumvented firewalls/NATs by allowing network endpoints behind a firewall/NAT to register with a server on a

public network such as the Internet. The server stored a respective identifier for each registered endpoint along with a network address (e.g., an IP address) for the endpoint. A first endpoint can then maintain a connection to the server so that the server would be capable of notifying the endpoint of any requests by other endpoints to form a P2P connection over the pre-existing connection. The notification is not blocked by the firewall/NAT since the first endpoint's connection to the server is initiated by the first endpoint itself and hence there is no unsolicited, inbound connection request. *See, e.g.*, EX1020, 1-3, FIGS. 1-3; EX1027, Abstract (“Many P2P applications need to connect to each other via TCP, but are increasingly stymied by NA boxes. Some popular P2P applications do not address NAT traversal or do so poorly.”), FIG. 2 (proposed “NAT Traversal Protocol”), 5 (“Punching the Hole”); EX1028, 1 (“NAT hole punching is one technique to traverse NAT boxes. It has the advantage of not requiring any user configuration, and establishes direct connections between two peers.”).

35. A second endpoint (referred to as a “terminal device” in the ’842 patent) that targets a P2P connection with the first endpoint can also connect to the server and can send a request carrying the identifier of the first endpoint to the server to form a P2P connection with the first endpoint. Because the server is already connected to the first endpoint and stored the identifier for the first endpoint along with the network address of the first endpoint, the server can readily relay the second

endpoint's request to form a P2P connection to the first endpoint through the server's existing connection with the first endpoint. The server provides the respective network addresses for each endpoint to each other endpoint, and the endpoints use these addresses to initiate connections to each other—thereby “punching holes” through their respective firewall(s)/NAT(s) and establishing a P2P connection. An illustration of one example of a conventional hole-punching technique is depicted in the following figure:

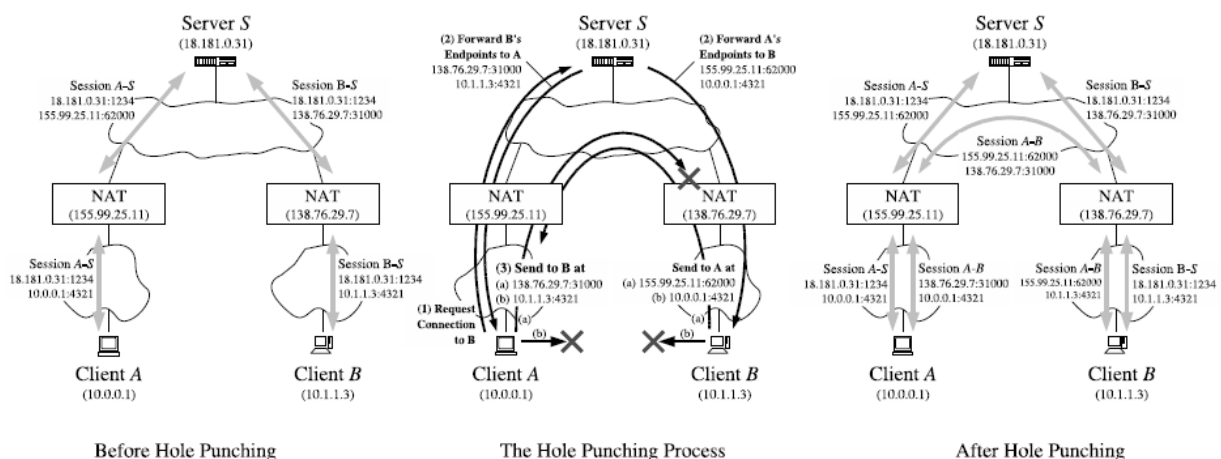


Figure 5: UDP Hole Punching, Peers Behind Different NATs

EX1020, FIG. 5; *see also* EX1002, 1:30-67, 5:59-60 (background description and statements of admitted prior art in the '842 patent).

B. The '842 Patent Describes a Predictable Application of Conventional Barcode-based Device Identifiers to a Conventional Hole-Punching System

36. The '842 patent describes nothing new or innovative given the relatively advanced state of the art (even in the timeframe of the provisional application's filing

in April 2013). To be sure, the '842 patent does not purport to disclose a new or improved hole-punching protocol. The specification instead admits that conventional hole-punching is entirely suitable to implement the '842 patent's technology. EX1002, 5:59-60, 5:40-41, 3:5-8. The "key focus" of the '842 patent was instead the use of a barcode to identify the target of a P2P connection. *Id.*, 4:50-55. But as I explained above, such techniques were widely described and implemented in the prior art before the '842 patent.

37. 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. EX1002, 5:40-6:34, FIGS. 3-4; *see also id.*, 4:1-5:39, 6:35-61, FIGS. 1-2, 5.

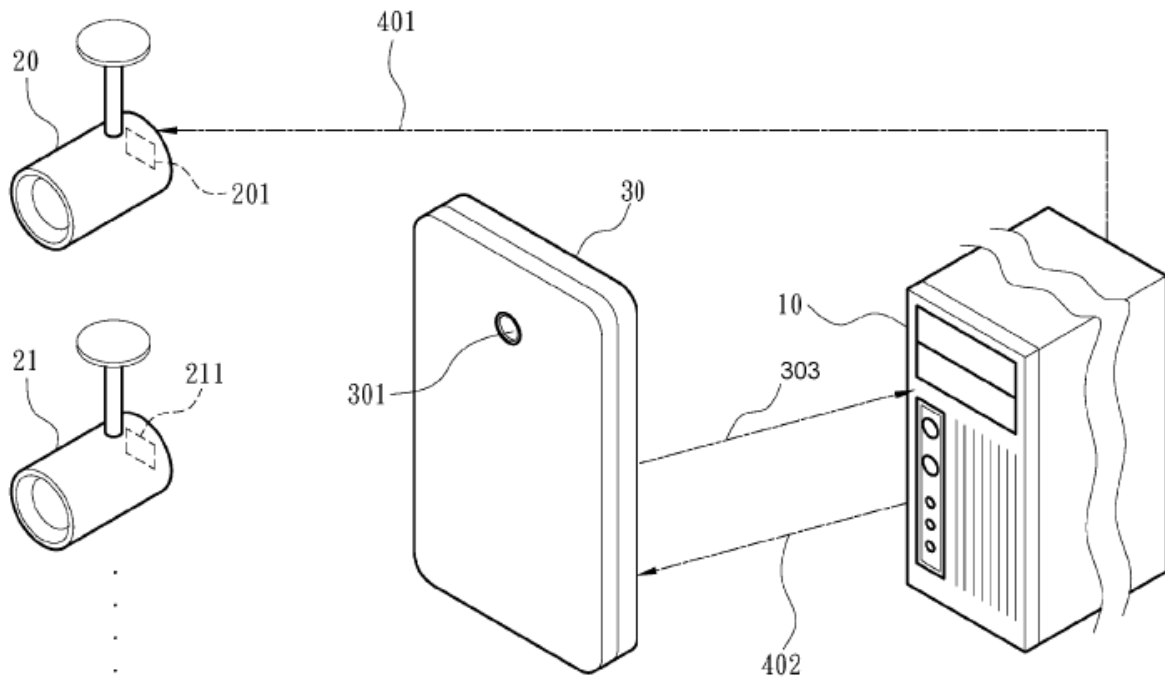


FIG. 3

EX1002, FIG. 3.

38. As shown in FIG. 3, “the system includes a network server 10, a first networked device 20, a second networked device 21 and a terminal device 30, wherein the terminal device 30 can be portable electronic devices such as mobile phones, tablet computers, notebook computers equipped with cameras, but not limit[ed] to; and the first and second networked device can be a web cam, a network surveillance camera or a network monitor, but not limit[ed] to.” EX1002, 4:20-27. 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.

39. 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.

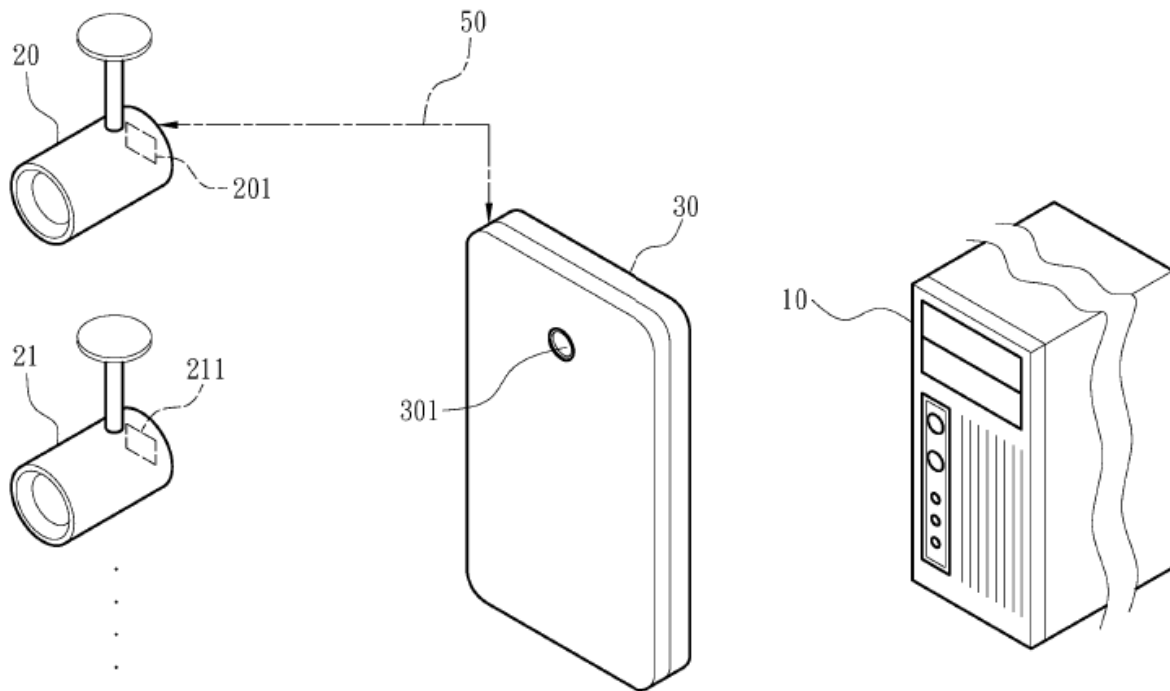


FIG. 4

EX1002, FIG. 4 (annotated).

C. File History of the '842 Patent and its Related Applications

40. The '842 Patent is a reissue of original U.S. Patent No. 9,787,498 (“the original '498 patent”). The reissue application was filed on December 13, 2018—about 14 months after the original '498 patent issued—and it was apparently filed for purposes of adding three additional co-inventors beyond the originally named inventor Kuo. EX1005, 3, 18. The original '498 patent was filed on July 25, 2013 as application serial no. 13/950,281 (“utility application”), which claimed priority to U.S. Provisional Application No. 61/812,262 (“provisional application”). EX1004, 9-10, 15. This provisional application was filed only three months before the utility application—on April 16, 2013—and it was filed entirely in a non-English language. EX1003, 4-26. I will briefly summarize the prosecution history of these three applications—the provisional application, the utility application, and the reissue application—in temporal order.

1. The Provisional Application

41. As previously noted, the provisional application was filed on April 16, 2013, and the text of the specification was mostly in Chinese. EX1003, 4-26. On May 31, 2013, the Patent Office notified the Applicant that an English translation “must be filed in the provisional application.” EX1003, 37. The Applicant did not do so until more than three years later. EX1003, 42. Even then, the English translation of the provisional application never expressly described the negative limitation that

ultimately appears in the Challenged Claims of the '842 patent—"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." EX1003-42-75. As noted below, this silence in the provisional application is pertinent.

2. The Utility Application

42. The utility application was filed about three months after the provisional application on July 25, 2013. The utility application noticeably included a new figure (FIG. 6) and corresponding text that was not disclosed in the provisional application. 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, 43-43 (lacking the flowchart of FIG. 6 from the utility application and such new text).

43. The Examiner issued three office actions during the course of prosecution of the utility application. EX1004, 52-61, 84-106, 133-161. The office actions rejected the claims as obvious based on various prior art references, although none of the references that the Examiner applied in rejecting the claims is relied upon in Grounds 1-3 of my analysis in this declaration. *Id.*

44. In response to the first office action, the Applicant amended the claims and argued that the applied prior art failed to disclose several limitations of independent claim 1. EX1004, 77-88. For example, addressing the Examiner's reliance on Jain

(EX1023, U.S. Pub. 2012/0287290), the Applicant argued that Jain’s “graphical indicator” failed to provide a “an image pattern comprising the first identification [that] is attached on the first networked device” since Jain’s indicator is “only displayed on a screen” rather than being “attached” to the device. EX1004, 87 (original emphases removed). The Applicant also argued that Jain’s mobile phones are not networked devices that are “pre-registered in the network server” since “each mobile phone must simultaneously capture an image pattern on the screen of the other mobile phone in order to identify and authenticate the other device.” EX1004, 87 (original emphases removed).

45. The Examiner maintained his reliance on Jain as the primary reference in an obviousness rejection in the second office action. EX1004, 92-114. The Applicant responded by adding the negative limitation (Elements [1.6]/[12.6]) to the independent claims and argued the following:

“In Jain, the first and second mobile phones (terminal device and first networked device respectively) must both capture an image pattern of each other in order to complete the pairing process, which is different from the above amended Claim 1, in which the first networked device does NOT capture any image pattern associated with the terminal device.”

EX1004, 133 (original emphases removed); *see also id.*, 125-135.

46. In the third office action, the Examiner withdrew his reliance on Jain as a primary reference but asserted new obviousness rejections based on Jiao (U.S. Patent 8,353,771) and further identified defects under 35 U.S.C. §112. EX1004, 141-169. Regarding the §112 defects, the Examiner specifically noted that the negative limitation that was amended into the claims in the Applicant's prior response lacked written description support in the specification. EX1004, 148. In reply to the written description rejection, the Applicant did not agree to delete or modify the negative limitation but rather argued that the limitation is "inherently implied" in the specification:

"Furthermore, the amended claim 1 has the limitation, '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 therefore, it does not make sense for the first networked device 20 to capture any image pattern associated with the terminal device for establishing the P2P connection"

EX1004, 188-189.

47. Following this response, the Examiner allowed the application but provided no reasons for allowance. EX1004, 197-202.

3. The Reissue Application

48. About 14 months after the original '498 patent issued, the Applicant filed the reissue application with a reissue declaration that alleged a need to correct the inventorship by adding three co-inventors. 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. *Id.*, 87-93. There were no prior art rejections during prosecution of the reissue application.

D. The Effective Filing Date of the '842 Patent

49. As I noted in the preceding section (§45), in responding to the second office action during prosecution of the '842 patent's original utility application, the Applicant amended each of independent claims 1 and 12 to recite the following language of Elements [1.6] and [12.6], respectively (which I refer to in this declaration as the "negative limitation"):

“the first networked monitoring device does not capture any image pattern associated with the terminal device for establishing the P2P connection”

EX1004, 126, 128 (from Applicant's response filed September 20, 2016).

50. I have thoroughly reviewed the disclosure of the '842 patent's provisional application (EX1003, pp. 43-73) and the entire specification of the '842 patent itself to assess whether the feature recited in the negative limitation was described

anywhere in these documents in a manner that would have reasonably conveyed to a POSITA that alleged inventors of the '842 patent possessed this feature as of the filing date of the provisional application (April 16, 2013) or as of the filing date of the original utility application (July 25, 2013). Based on my review and my knowledge and experience in this field, it is clear that the feature recited in the negative limitation was never so described in either the provisional application or the original utility application. Rather, the first time that this feature was expressly mentioned in the prosecution history of the '842 patent was in the Applicant's claim amendment in response to the second office action on September 20, 2016. EX1004, 126, 128. For this reason, it appears that the effective filing date of independent claims 1 and 12 of the '842 patent—and by extension, the effective filing date of each of their dependent claims—should be treated as no earlier than September 20, 2016.

51. I disagree with Patent Owner's earlier assertion that this negative limitation was somehow "inherently" disclosed—or necessarily present—in the specification of the provisional application. For example, I understand that the provisional application describes that "when the network server 10 receives the connection request signal 303, it will notify the first networked device 20 that the terminal device 30 is making a request to connect therewith[]" EX1003, 54. The provisional application also 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 to the first networked device 20 and the terminal device 30 respectively,” resulting in “a direct communication passage 50 ... between the first networked device 20 and the terminal device 30.” *Id.* However, nothing either here or elsewhere in the provisional application confirms the first networked monitoring device does not capture any image pattern associated with the terminal device for establishing the P2P connection. Indeed, the provisional disclosure regarding its “hole-punching technique” and how the “direct communication passage 50” is established between devices 20, 30 is especially sparse and simply does not preclude the possibility that the first networked monitoring device could capture an image pattern associated with the terminal device to establish the P2P connection. The negative limitation certainly was not inherent in the provisional application’s disclosure, especially since many conventional procedures for establishing P2P connections specifically require each device to identify each other—and in fact many such connections are established only when a barcode (or other visual marker) is scanned on each device. *See, e.g.*, EX1024, 1 (“If both devices are camera-equipped, they can mutually authenticate each other.”), Abstract (“Mutual authentication requires switching the roles of the devices and repeating the above process in the reverse direction”); EX1023, [0040] (“Upon detecting the event, the devices are positioned so that their respective ‘front faces’ (i.e., their respective

display screens and lens assemblies) face each other. Each device then captures an image of a graphical indicator displayed on the other device.”); EX1021, 00:34-00:50 (showing IP camera scanning QR code on smartphone after smartphone scans QR code on IP camera); *see also* EX1004, 133 (“In Jain, the first and second mobile phones (terminal device and first networked device respectively) must both capture an image pattern of each other in order to complete the pairing process.”).

52. To be clear, 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 precludes those webcams from scanning a conventional QR code on a wifi-connected smartphone to receive the wifi connection information used for establishing the P2P connection. Moreover, apart from setting a “default security password,” the provisional application provides little to no detail regarding the specific procedures for ensuring mutual authorization for the connection between the terminal device 30 and the first networked device 20—yet Jain and other references amply demonstrated the traditional option of capturing a QR code on both camera-equipped devices to verify authorization for a connection. EX1023, [0040]; EX1004, 133 (“must both capture an image pattern of each other”); *see also* EX1024, 1 (“Mutual authentication”), EX1021, 00:34-00:50. These examples show that 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. Accordingly, the Applicant's argument to the Examiner during prosecution of the '842 patent's original utility application that the negative limitation was "inherently implied" (EX1004, 188-189) is not accurate.

53. The utility application and the specification of the '842 patent likewise fail to expressly describe the negative limitation for similar reasons as the provisional application is deficient. As I noted above (§42), the Applicant included in the utility application a new figure (FIG. 6) and corresponding text that was not disclosed in the provisional application. 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, 43-43 (lacking the flowchart of FIG. 6 from the utility application and such new text). But nothing in the content added to the utility application describes that the first networked monitoring device does not capture any image pattern associated with the terminal device for establishing the P2P connection. Regarding, FIG. 6, for example, the specification discloses that "[i]n step 604," the "terminal device generate[s] a request signal ... when the image pattern is captured to the terminal device and transmits the connection request signal to the network server by the terminal device through the Internet." EX1002, 8:35-45. This again does nothing to forbid the webcam from scanning a conventional QR code on a wifi-connected smartphone to receive the wifi connection information used for establishing the P2P connection.

The utility application also provides little to no details apart from setting a “default security password” regarding the specific procedures for ensuring mutual authorization for the connection between the terminal device 30 and the first networked device 20. The utility application thus fails to support the negative limitation for substantially the same reasons as the provisional application fails to support the negative limitation.

54. As previously explained in ¶23, my analysis of Grounds 1-2 applies even if the earliest effective filing date was assumed to be April 16, 2013 (the filing date of the provisional application). All of the prior art relied upon in Grounds 1-2 predates April 16, 2013. For Ground 3, I have treated September 20, 2016 as the earliest effective filing date of the Challenged Claims for the reasons described above, yet my analysis and the conclusions for Ground 3 would remain unchanged even if the effective filing date of the claims of the '842 patent was as early as the provisional filing date (April 16, 2013) or the utility filing date (July 25, 2013) because all of the prior art in Ground 3 was published well before April 16, 2013 and July 25, 2013. Also, for Ground 3, if the effective filing date was assumed to be April 16, 2013, I was informed that the Board would consider if those publications qualify as prior art.

E. Interpretation of the '842 Patent Claims at Issue

55. I understand that, for purposes of my analysis in this IPR proceeding, the terms appearing in the patent claims should be interpreted according to their “ordinary and customary meaning,” which is often referred to as the *Phillips* standard. In determining the ordinary and customary meaning, I understand that the words of a claim are first given their plain meaning that those words would have had to a person of ordinary skill in the art at the time of the alleged invention. I also understand that the structure of the claims, the specification, and file history may be used to better construe a claim. Moreover, I understand that even treatises and dictionaries may be used, albeit under limited circumstances, to determine the meaning attributed by a person of ordinary skill in the art to a claim term.

56. Here, I have reviewed the claims of the '842 patent addressed in this proceeding. For purposes of addressing the anticipation and obviousness issues in this proceeding, the claim elements include straightforward language and are readily understandable according to their ordinary and customary meaning—without the need to inject specialized definitions or substitute terminology. As demonstrated below, there is a significant overlap between the preferred embodiment of the '842 patent and those prior art devices/predictable combinations set forth in Grounds 1-3 of this declaration. This overlap is evident when using the ordinary and customary meanings of terms in the claims. For purposes of comparing the claim elements with

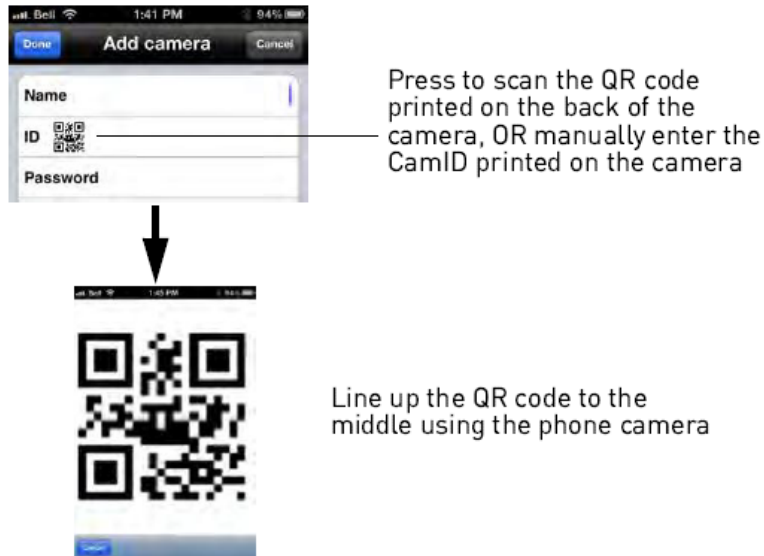
the prior art, it is not necessary to resort to formal definitions or substitute terminology when assessing the Grounds below.

VII. GROUND 1 – Obviousness of Claims 1-3, 6, 10, 12-14, 17, and 18 Based on Lorex Guide (EX1006) and Kim (EX1007)

A. Overview of Lorex Guide

57. I have reviewed Exhibit 1006, which is a publication of a User's Guide for the Lorex LNC100 Series Wireless Network Camera ("Lorex Guide"). Much like the '842 patent, Lorex Guide discloses 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. The captured QR code provides a simple alternative to the user manually entering the 'CamID', which is used in a process for connecting the terminal device to the IP camera through the Internet. For example, Lorex Guide's connection process includes a step of "using the camera of the phone" to automatically enter the "CamID" of the IP camera as follows:

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.

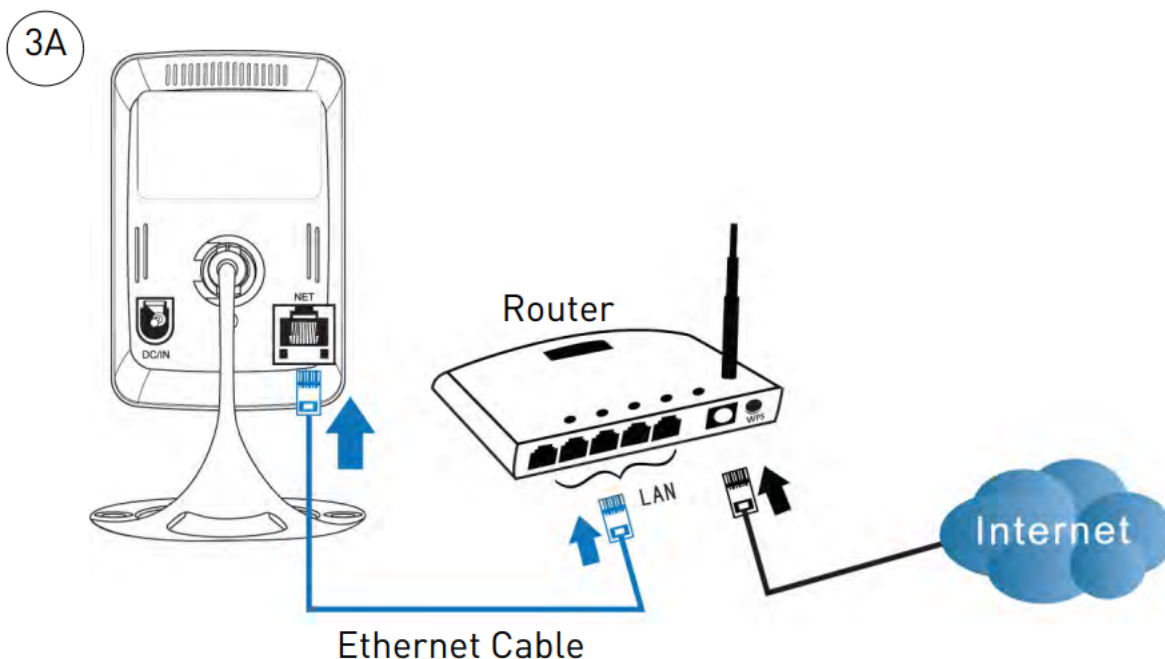


- **OR:** Manually enter the **CamID** printed on the camera.

EX1006, 13; *see also id.*, 16, 19.

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.

59. Lorex Guide teaches the camera connecting to the “Internet” to establish a direct connection with the phone:



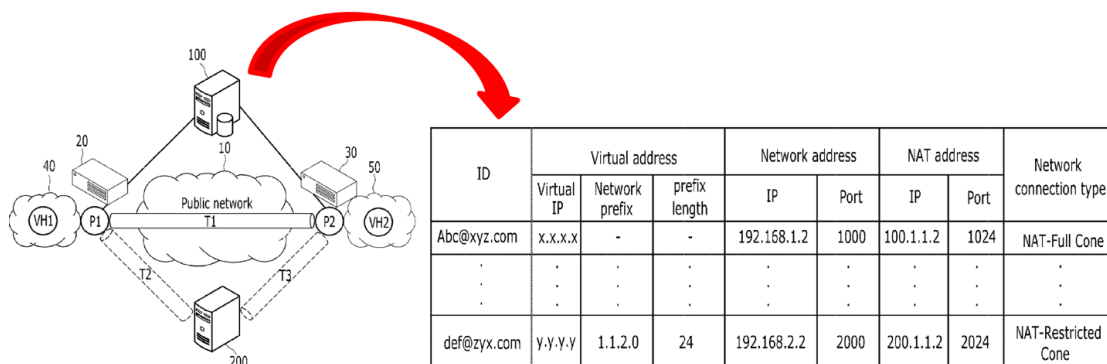
EX1006, 4, *see also id.*, iv, 1, 5-20.

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). 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.

B. Overview of Kim

61. I have reviewed U.S. Pub. 2011/0082941 (EX1007, "Kim"), which is a U.S. patent application titled "Method of Providing Direct Communication in Internet Protocol Network." EX1007. As with the Lorex Guide, Kim describes a process for establishing a connection for direct communication between networked devices such as a smartphone and a camera. EX1007, [0052], [0053]. Based on my review, Lorex

Guide does not expressly describe a network server using a conventional hole-punching technique. Nonetheless, 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]. 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:



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

62. Kim teaches that peer nodes P1 and P2 can pre-register their IDs and network addresses with server 100, and 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]. 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. 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].

C. The Predictable Combination of Lorex Guide and Kim

63. Based upon my knowledge and experience in this field and my review of Lorex Guide and Kim, it is clear that a POSITA would have been motivated to implement Lorex Guide to include Kim’s suggested use of a network server and conventional hole-punching techniques to achieve known benefits at the time. At a high level, Lorex Guide discloses the same solution that was the alleged “key focus” of the ’842 patent (EX1002, 4:50-55), and Kim suggests an improvement for accomplishing a conventional network server to provide hole-punching and a P2P connection for direct communications.

64. The application of Kim’s teachings in this regard 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. A POSITA would have understood that hole punching was especially useful when the endpoints of the connection are located behind respective NATs or firewalls like Kim's peer nodes P1 and P2 (which are located behind NATs 20, 30). 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. 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).

65. There are several rationales that would have prompted the POSITA to pursue this Lorex Guide-Kim combination. I provide an exemplary discussion of various reasons below, each of which independently supports the predictability and known advantages of the combination.

66. A **first** reason that a POSITA would have been prompted to implement Lorex Guide's system to include a conventional "network server" that facilitates hole-punching (as suggested by Kim) is that such techniques would have

beneficially 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.² Kim expressly

² Lorex Guide expressly teaches that the IP camera can connect to a router in a local area network (LAN), which in turn, connects to the Internet. EX1006, 4 (“Connect an Ethernet cable ... to an available LAN port ...”). As I explained in detail above (Section II.A) regarding the state of the art before even the earliest claimed priority date of the ’842 patent (April 16, 2013), firewalls and NATs were well known and widely implemented in this timeframe. In this context, a POSITA would have expected and found obvious for Lorex Guide’s IP camera and user’s/terminal device to reside in local/private networks protected by firewall(s) and/or NAT(s). Indeed, a POSITA would have recognized that firewalls were commonly employed to block unsolicited and/or otherwise undesired inbound traffic from penetrating a local/private network, thereby improving security. Likewise, a POSITA would have recognized that NATs were commonly employed to “allocate temporary public endpoints for outgoing connections” and to “translate the addresses and port numbers in packets comprising those sessions, while generally blocking all incoming traffic” EX1020, 1.

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].

67. A **second** reason that a POSITA would have been prompted to implement Lorex Guide’s system to include a conventional “network server” that facilitates hole-punching (as suggested by Kim) 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”).

68. A **third** reason that a POSITA would have been prompted to implement Lorex Guide’s system to include a conventional “network server” that facilitates hole-punching (as suggested by Kim) is to beneficially form a “direct communication environment” between Lorex Guide’s IP camera and the user’s/terminal device in a manner that renders it “unnecessary for each application service to form a special session.” EX1007, [0122]. This would have predictably improved the “flexibility” in “operating each service.” *Id.*

69. A **fourth** reason that a POSITA would have been prompted to implement Lorex Guide’s system to include a conventional “network server” that facilitates

hole-punching (as suggested by Kim) is that such techniques would provide the system with additional assurances that a direct tunnel can be established between the IP camera and the user's/terminal device based on the particular connection types associated with each of the peer nodes (e.g., Lorex Guide's terminal device and IP camera). EX1007, [0078]-[0083], [0094]-[0099], [0014]-[0018], FIGS. 6, 8.

70. Based upon my knowledge and experience in this field and my review of the relatively straightforward and predictable structures in Lorex Guide and Kim, it is clear that a POSITA would have possessed the level of skill to implement this combination given the overlapping technologies of Lorex Guide and Kim—with a reasonable expectation of success in achieving this combination in the manner described above. That is, both references are directed to technology for connecting networked devices (e.g., peer devices) including smart phones and cameras. As I have explained throughout this declaration, the state of the art for such networked devices and their interconnectivity was relatively advanced by the effective filing date of the '842 patent claims. Again, the specific technologies applied in Lorex Guide and Kim were common—e.g., an IP camera having a QR code for capture by a user's smartphone and a network server that facilitated hole-punching for the establishment of P2P connections. These were well within a POSITA's knowledge and skill level at the relevant time.

71. As detailed below, the predictable Lorex Guide-Kim combination renders obvious claims 1-3, 6, 10, 12-14, 17, and 18 of the '842 patent, with the resulting combination providing each of the claim elements, for the reasons explained below.

[1.P] A system to identify a networked device for establishing a point-to point (P2P) connection, the system comprising:

72. To the extent this preamble is treated as a claim limitation, the predictable Lorex Guide-Kim combination would have provided a system that identifies a networked device for establishing a point-to point (P2P) connection. 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; *above*, Section VII.A. 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]; *above*, Sections VII.B, VII.C (combination overview).

[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

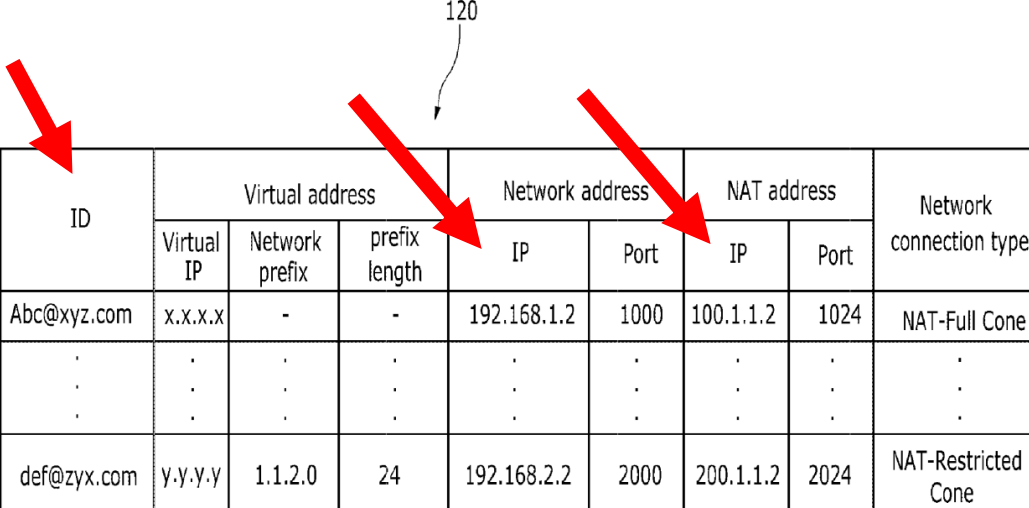
73. The predictable Lorex Guide-Kim combination would have provided the claimed network server having the recited features. Lorex Guide teaches the IP camera being connected to the “Internet” to establish a connection with the smartphone or similar user/terminal device (equipped with the Lorex Guide “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.

74. 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; *above*, Section VII.C (combination overview).

75. In the predictable Lorex Guide-Kim combination, the server would predictably manage network addresses of the peer nodes as taught in Kim. EX1007, [0040]. 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]. The devices are pre-registered in the server. EX1007, FIGs. 2, 3, [0055], [0056], [0067], [0068].

FIG. 5



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).

76. Kim further discloses that the server includes “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].

[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;

77. The predictable Lorex Guide-Kim combination would have provided the claimed first networked monitoring device having the recited features. 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.

78. Additionally, Kim discloses 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], 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. *Above*, [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). 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 performed by the first networked monitoring device connecting to the network server through the Internet. EX1007 FIG. 1, [0038], [0045], [0046].

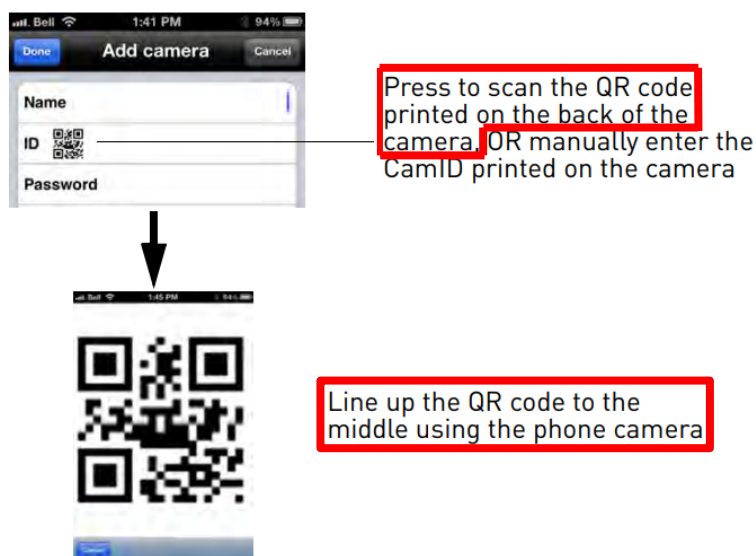
79. For the reasons that I described above, it would have been obvious for Lorex Guide's IP camera to register its embedded "CamID" and/or QR code identification with the network server consistent with Kim's teachings in the predictable Lorex Guide-Kim combination. *Above*, Section VII.C (combination overview).

[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

80. The predictable Lorex Guide-Kim combination would have provided the claimed image pattern having the recited features. 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. The “CamID” is used to establish a connection between the camera and the phone. EX1006, pp. 12-20.

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).

81. 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. Lorex Guide’s “printed” QR code is plainly different from the type of dynamic/temporary display of a QR code on an electronic screen that the Applicant sought to distinguish from the prior art asserted during prosecution of the original utility application. EX1004, 84 (“only displayed on a screen”).

82. 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 would have provided such a P2P connection as taught in

Kim. EX1007, [0005], [0018], [0078]-[0089], FIG. 6; *above*, Section VII.C (combination overview).

[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,

83. The predictable Lorex Guide-Kim combination would have provided the claimed terminal device having the recited features. For example, Lorex Guide 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; *above*, Section VII.A. 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.

84. 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]. 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. 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].

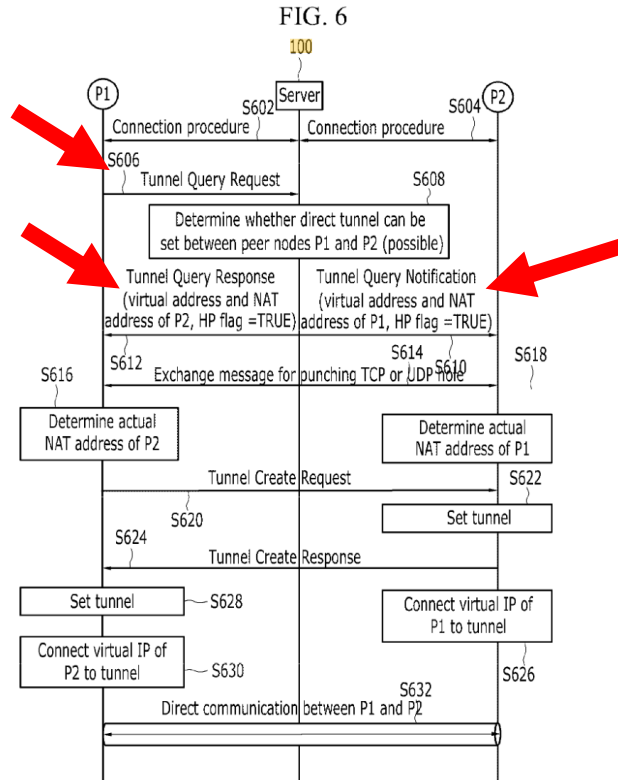
85. As described above, in the Lorex Guide-Kim combination, the terminal device (e.g., Lorex Guide's iPhone, iPad, or Android device) predictably transmits a connection request signal like Kim's "tunnel query request" containing the IP camera's 'CamID' to the network server to set a tunnel and connect to the IP camera, consistent with the actions of peer P1 in Kim. *Above*, Section VII.C (combination overview). 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.

[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

86. The predictable Lorex Guide-Kim combination would have provided the features recited in Element [1.5]. 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; *above*, Section VII.C (combination overview).

87. 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].



EX1007, FIG. 6 (annotated).

88. According to Kim, the “tunnel query response” message sent to the terminal device (e.g., P1 in FIG. 6) includes the virtual and NAT addresses (each of which includes an IP address) of the first networked monitoring device (e.g., P2 in FIG. 6). EX1007, [0078]-[0084], FIGS. 5-6. EX1007, [0078]-[0084], FIGS. 5, 6. Likewise, the “tunnel query notification” message sent to the first networked monitoring device (e.g., P2) includes the virtual and NAT addresses (each of which includes an IP address) of the terminal device (e.g., P1). *Id.* The server’s mapping of peer IDs to the peers’ respective network addresses in Kim indicates that the virtual and NAT addresses (including the IP addresses) provided in the “tunnel query response” and

“tunnel query notification” messages are identified or otherwise obtained by the server using the ID from the “tunnel query request” message as look-up key. *Id.*, [0071]-[0076], FIG. 5.

89. 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. 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].

[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.

90. The predictable Lorex Guide-Kim combination would have provided the features recited in Element [1.6]. Lorex Guide is notably a “user’s 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; *above*, Section VII.A. 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. 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.

91. Considering the Lorex Guide’s goal of offering a “user guide” that provides step-by-step instructions for establishing a connection between the IP camera and terminal device, Lorex Guide’s omission of any step for using the IP camera to acquire an image pattern associated with the terminal device would have plainly suggested to a POSITA that such a step is unnecessary and not performed in Lorex Guide’s connection procedure. Indeed, users who faithfully followed Lorex Guide’s instructions would otherwise fail to establish the desired connection, which would be contrary to Lorex Guide’s goal of allowing users to successfully establish the

connection. A POSITA would have expected such a step to be disclosed in Lorex Guide if it were required, and the absence of disclosure in this context clearly indicates that the step is not necessary or otherwise performed as part of Lorex Guide's connection procedure.

92. To be clear, the specific nature and context of Lorex Guide's disclosure plainly provides the functionality recited in Element [1.6] on its own accord. Nonetheless, this fact is further confirmed and corroborated by additional evidence of record regarding the functionality of the system described in Lorex Guide. For example, I have reviewed the declaration of Mr. Vlad Kardashov (EX1011), who was formerly a Project Lead and IP Products Line Manager at Lorex Technology, Inc. EX1011, ¶3. Mr. Kardashov "had personal knowledge of, and was highly familiar with, the Lorex LNC100 Series of IP cameras, the Lorex Ping app, the network server system, and all of the instructions/user guides/literature/how-to videos that were published by Lorex Technology during 2012 and later." *Id.* Mr. Kardashov testified that the LNC100 Series IP Camera and Lorex Ping app described in Lorex Guide allowed "the point-to-point connection [to be] established without requiring the user to point the IP camera at the smartphone to capture any image of the user's smartphone (or otherwise input information at the IP camera)." *Id.*, ¶7. Mr. Kardashov's testimony is consistent with the instructions provided in the Lorex Guide, as well as various videos demonstrating the functionality of the LNC100

Series IP Camera. See EX1008, 1:00-1:37 (“once that happens ... here it is”); EX1010, 00:29-00:39 (“All you have to do is activate your camera by simply scanning the QR code on the back of the camera with your smartphone or tablet.”); EX1006, 29-30. The evidence is thus clear that Lorex Guide teaches that the first networked monitoring device (the IP camera) does not capture any image pattern associated with the terminal device (the smartphone) for establishing the P2P connection between the terminal device and the first networked monitoring device, as recited in [1.6].

93. It is also notable that Kim’s network server and hole-punching procedures are compatible with Lorex Guide’s functionality in this regard. Kim does not mandate that either peer node acquires an image pattern associated with the other peer node, and in the combination, Kim would not alter the ability of Lorex Guide’s terminal device to establish a connection with the IP camera without the IP camera capturing an image pattern of the terminal device. See, e.g., EX1007 FIG. 6 & [0079]-[0089].

[2] The system according to claim 1, wherein the image pattern is a barcode, wherein a barcode image is generated in the terminal device.

94. The predictable Lorex Guide-Kim combination would have provided the additional features recited in Claim 2. For example, 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. 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).

[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.

95. The predictable Lorex Guide-Kim combination demonstrates it would have been obvious to provide the additional features recited in Claim 3. For example, 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. 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.” *Above,*

Element [1.4]; Section, VII.C (combination overview); EX1007, [0079]-[0081], FIG.

6.

[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.

96. The predictable Lorex Guide-Kim combination demonstrates it would have been obvious to provide the additional features recited in Claim 6. 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 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.

[10] The system according to claim 2, wherein the barcode is a quick response code (QR code).

97. The predictable Lorex Guide-Kim combination demonstrates it would have been obvious to provide the additional features recited in Claim 10. For example, Lorex Guide describes a “QR code printed on the back of the camera.” EX1006, 13; *see also id.*, 16, 19.

[12.P] A method to identify networked device for establishing a point-to point (P2P) connection, the method comprising the steps of:

98. To the extent the preamble is a limitation, the predictable Lorex Guide-Kim combination would have provided the recited method to identify networked device

for establishing a point-to-point (P2P) connection for each of the reasons that I described above with respect to Element [1.P]. *Above*, 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.

[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;

99. The predictable Lorex Guide-Kim combination would have provided the “connecting” step and the recited features of Element [12.1]. For example, the Lorex Guide-Kim combination 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; *above*, Element [1.1].

[12.2] (b) registering a first identification of the first networked monitoring device into the list of networked devices of the server;

100. The predictable Lorex Guide-Kim combination would have provided the “registering” step and the recited features of Element [12.2]. For example, the Lorex Guide-Kim combination 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; *above*, Element [1.2].

[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;

101. The predictable Lorex Guide-Kim combination would have provided the “providing” step and the recited features of Element [12.3]. For example, the Lorex Guide-Kim combination 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; *above*, Element [1.3].

[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

102. The predictable Lorex Guide-Kim combination would have provided the “generating” step and the recited features of Element [12.4]. For example, the Lorex Guide-Kim combination 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; *above*, Element [1.4].

[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

103. The predictable Lorex Guide-Kim combination would have provided the “identifying” step and the recited features of Element [12.5]. For example, the Lorex Guide-Kim combination 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; *above*, Element [1.5].

[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.

104. The predictable Lorex Guide-Kim combination would have provided the recited features of Element [12.6]. For example, the Lorex Guide-Kim combination

would have provided 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; *above*, Element [1.6].

[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.

105. The predictable Lorex Guide-Kim combination demonstrates it would have been obvious to provide the additional features recited in Claim 13 for each of the reasons that I addressed above with respect to Claim 2.

[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.

106. The predictable Lorex Guide-Kim combination demonstrates it would have been obvious to provide the additional features recited in Claim 14 for each of the reasons that I addressed above with respect to Claim 3.

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. The terminal device would predictably include an image interpreting unit to interpret the barcode image and extract the CamID as described in Lorex Guide. 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. *Above*, Element [1.4]; Section, VII.C (combination overview); EX1007, [0079]-[0081], FIG. 6.

[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.

108. The predictable Lorex Guide-Kim combination demonstrates it would have been obvious to provide the additional features recited in Claim 17 for each of the reasons that I described above with respect to Claim 6. 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.

109. Furthermore, a POSITA would have understood that passwords are conventionally implemented for security and access control. 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. 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. *See, e.g.,* EX1029, [0004] (corroborating that “one conventional countermeasure employed by Web applications is to lock out a user account, which is identified by the User ID, after a selected number of consecutive failed login attempts using the User ID but an incorrect password”), Abstract (“Access to the user account is denied when a consecutive number of times a login request for the user account is rejected reaches a selected limit”).

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

110. The predictable Lorex Guide-Kim combination demonstrates it would have been obvious to provide the additional features recited in Claim 18 for each of the reasons that I described above with respect to Claim 10.

VIII. GROUND 2 – Obviousness of Claims 1-3, 6, 10, 12-14, 17, and 18 Based on Kim (EX1007) and Lorex Video (EX1008)

A. Overview of Lorex Video

111. I have reviewed Exhibit 1008, which is a YouTube video titled “How-to Set Up and Connect the NEW Lorex LNC100 Series IP Network Camera.”³ Lorex

³ Based on my knowledge and experience in the field, YouTube was a popular video streaming platform that was commonly used by millions of users around the world by the earliest effective filing date of the '842 patent. A POSITA (as well as consumers and other interested persons more generally) would have known how to access and search YouTube for videos like Lorex Video in the relevant timeframe. Lorex Video’s descriptive title would have made it readily identifiable to interested persons exercising reasonable diligence, for example, especially since it specifically references an “IP Network Camera” and indicates that the video will instruct “How-to-Set Up and Connect” the IP camera. I also understand from Mr. Kardashov’s sworn testimony that he other leaders at Lorex Technology

Video is like Kim in that both references describe techniques for 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. 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. 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.

112. 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.

considered the publication of Lorex Video on YouTube to be “a success, with thousands of views on YouTube in 2012,” which they “believed led to many sales of the product in that year.” EX1011, ¶8.



EX1008, 1:17 (cropped, annotated).

B. The Predictable Combination of Kim and Lorex Video

113. Based upon my knowledge and experience in this field and my review of Kim and Lorex Video, it is clear that a POSITA would have been motivated to implement Kim to include Lorex Video's suggested use of a conventional QR code to quickly obtain an ID of a device targeted for a direct connection (e.g., a P2P connection). At a high level, Kim discloses a conventional approach to establishing P2P between peer devices such as a camera and a smartphone using a network server and hole punching, and Lorex Video suggests the same solution that was the alleged "key focus" of the '842 patent (EX1002, 4:50-55) for using a barcode (e.g., a QR code) to quickly and easily identify a device as the target of a connection request. For example, a Kim-Lorex Video combination would have predictably allowed Kim's first peer node (P1) in FIG. 6 to obtain a unique device identifier for the

second peer node (P2) by capturing an image of a QR code attached to the second peer node (P2), where the QR code encodes P2's device identifier.

114. There are several rationales that would have prompted the POSITA to pursue this Kim-Lorex Video combination. I provide an exemplary discussion of various reasons below, each of which independently supports the predictability and known advantages of the combination.

115. A **first** reason that a POSITA would have been prompted to implement Kim to include Lorex Video's suggested use of a conventional QR code to identify a targeted device for a connection would have been to 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 Kim's P2P connection. Lorex Video expressly emphasizes the speed and simplicity of using such a system to establish a P2P 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").

116. A **second** reason that a POSITA would have been prompted to implement Kim to include Lorex Video's suggested use of a conventional QR code is to identify a targeted device for a connection in a rapid and error-free manner. 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 expressly disclose a solution for inputting any such ID. EX1007, [0081], FIG. 6. Lorex Video details a known

technique to input such an ID while beneficially avoiding 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.

117. Based upon my knowledge and experience in this field and my review of the relatively straightforward and predictable structures in Kim and Lorex Video, it is clear that a POSITA would have possessed the level of skill to implement this combination given the overlapping technologies of Kim and Lorex Video—with a reasonable expectation of success in achieving this combination in the manner described above. That is, both references are directed to technology for connecting networked devices (e.g., peer devices) including smart phones and cameras. As I have explained throughout this declaration, the state of the art for such networked devices and their interconnectivity was relatively advanced by the earliest effective filing date of the '842 patent claims. Again, the specific technologies applied in Kim and Lorex Video were common—e.g., an IP camera having a QR code for capture by a user's smartphone and a network server that facilitated hole-punching for the establishment of P2P connections. These were well within a POSITA's knowledge and skill level at the relevant time.

118. As detailed below, the predictable Kim–Lorex Video combination renders obvious claims 1-3, 6, 10, 12-14, 17, and 18 of the '842 patent, with the resulting combination providing each of the claim elements, for the reasons explained below.

[1.P] A system to identify a networked device for establishing a point-to point (P2P) connection, the system comprising:

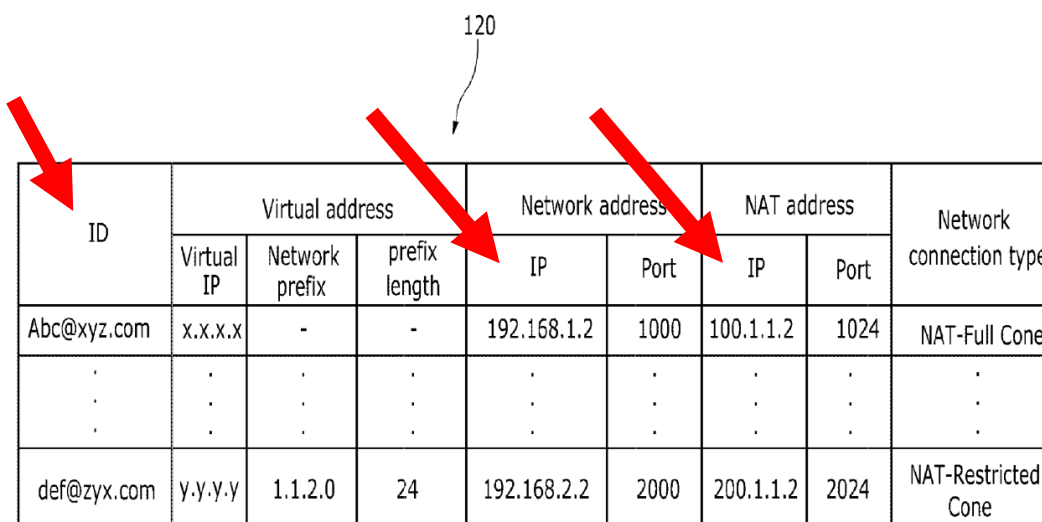
119. To the extent this preamble is treated as claim limitation, the predictable Kim-Lorex Video combination would have provided a system that identifies a networked device for establishing a point-to point (P2P) connection. For example, Kim describes in detail techniques for establishing a P2P connection between peer nodes. EX1007, [0006], [0018], [0078]-[0089], [0123], FIGS. 1-2, 6; *above*, Sections VII.B. Lorex Video also describes a process for establishing a connection between peer devices including a smartphone and a camera. EX1008, 1:00-1:40; *above*, Section VIII.A.

[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

120. The predictable Kim-Lorex Video combination would have provided the claimed network server having the recited features. 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].

121. The server manages network addresses of the peer nodes. EX1007, [0040]. 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]. The devices are pre-registered in the server. EX1007, FIGs. 2, 3, [0055], [0056], [0067], [0068].

FIG. 5



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).

122. 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].

[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;

123. The predictable Kim-Lorex Video combination demonstrates it would have been obvious to provide the claimed first networked monitoring device having the recited features. 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. *Above*, [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). 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]. Kim also teaches that the first networked device (a peer node) can be “a video camera that perform[s] IP-based communication.” EX1007, [0052].

124. 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). *Above*, Section VIII.B (combination overview).

[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

125. The predictable Kim-Lorex Video combination demonstrates it would have been obvious to provide the claimed image pattern having the recited features. 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. 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).

126. 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). Above, Section VIII.B (combination overview). 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.

[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,

127. The predictable Kim-Lorex Video combination demonstrates it would have been obvious to provide the claimed terminal device having the recited features. 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]. 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. 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].

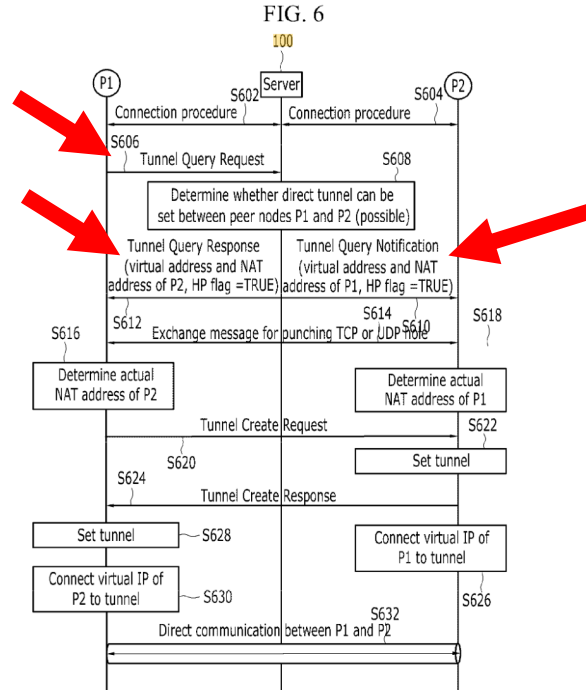
128. Further, as described above, it would have been obvious to implement Kim according to Lorex Video's suggestion for the terminal device (e.g., an iPhone as taught in Lorex Video / P1 in Kim's FIG. 6) to obtain the first networked monitoring device's (e.g., the IP camera in Lorex Video / P2 in Kim's 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; *above*, Section VIII.B (combination overview). 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.

[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

129. The predictable Kim-Lorex Video combination demonstrates it would have been obvious to provide the features recited in Element [1.5]. 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; *above*, Section VIII.B (combination overview).

130. 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].



EX1007, FIG. 6 (annotated).

131. According to Kim, the “tunnel query response” message sent to the terminal device (e.g., P1 in FIG. 6) includes the virtual and NAT addresses (each of which includes an IP address) of the first networked monitoring device (e.g., P2 in FIG. 6). EX1007, [0078]-[0084], FIGS. 5-6. EX1007, [0078]-[0084], FIGS. 5, 6. Likewise, the “tunnel query notification” message sent to the first networked monitoring device (e.g., P2) includes the virtual and NAT addresses (each of which includes an IP address) of the terminal device (e.g., P1). *Id.* The server’s mapping of peer IDs to the peers’ respective network addresses in Kim indicates that the virtual and NAT addresses (including the IP addresses) provided in the “tunnel query response” and “tunnel query notification” messages are identified or otherwise obtained by the server using the ID from the “tunnel query request” message as look-up key. *Id.*, [0071]-[0076], FIG. 5.

132. 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. 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].

[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.

133. The predictable Kim-Lorex Video combination demonstrates it would have been obvious to provide the features recited in Element [1.6]. Indeed, 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. 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. *Id.* 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.”). Implementing Kim in accordance with Lorex Video’s suggestion to capture a QR code of the first networked monitoring device (which does not involve 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. *Above*, Section VIII.B (combination overview).

134. To be clear, Lorex Video’s disclosure plainly provides the functionality recited in Element [1.6]. Nonetheless, this fact is further confirmed and corroborated by additional evidence of record regarding the functionality of the system described in Lorex Video. For example, I have reviewed the declaration of Mr. Vlad Kardashov (EX1011), who was formerly a Project Lead and IP Products Line Manager at Lorex Technology, Inc. EX1011, ¶3. Mr. Kardashov “had personal knowledge of, and was highly familiar with, the Lorex LNC100 Series of IP cameras, the Lorex Ping app, the network server system, and all of the instructions/user guides/literature/how-to videos that were published by Lorex Technology during 2012 and later.” *Id.* Mr. Kardashov testified that the LNC100 Series IP Camera and Lorex Ping app described in Lorex Video allowed “the point-to-point connection [to be] established without requiring the user to point the IP camera at the smartphone to capture any image of the user’s smartphone (or otherwise input information at the IP camera).” *Id.*, ¶7. Mr. Kardashov’s testimony is consistent with the

demonstration in the Lorex Video, as well as a user's guide and a second demonstration video for Lorex's LNC 100 Series IP Camera system. *See* EX1010, 00:29-00:39 ("All you have to do is activate your camera by simply scanning the QR code on the back of the camera with your smartphone or tablet."); EX1006, 29-30. The evidence is thus clear that Lorex Video teaches that the first networked monitoring device (e.g., the IP camera) does not capture any image pattern associated with the terminal device (e.g., the iPhone) for establishing the P2P connection between the terminal device and the first networked monitoring device, as recited in [1.6].

135. Lorex Video's disclosure of a connection procedure that does not involve use of the IP camera to capture any image pattern associated with the iPhone is also compatible with Kim's techniques for establishing a P2P connection using a network server and hole punching (even if Kim itself does not expressly disclose the functionality recited in Element [1.6]). For example, with respect to FIG. 6, Kim describes a process for "setting direct communication between peer nodes through a server." EX1007, [0027]; *see also id.*, [0078]-[0079], FIG. 6. As described above, Kim's process provides that the terminal device (e.g., P1 in FIG. 6) will identify a particular networked device (e.g., P2 in FIG. 6) as the target for the P2P connection with the terminal device by embedding an identifier of the targeted networked device in the "tunnel query request message." EX1007, [0081] ("a tunnel query request

message includes an ID of the peer node P2 to communicate”). By including P2’s identifier in the “tunnel query request” message, the network server 100 can generate “tunnel query response” and “tunnel query notification” messages for P1 and P2, respectively, to facilitate the establishment of a peer-to-peer connection. *Id.*, [0082]-[0087]. In the predictable Kim-Lorex Video combination, P2’s identifier can be captured for inclusion in the “tunnel query request” message by scanning the QR code on P2 (e.g., the IP camera). Kim’s connection process shown in FIG. 6 does not require that P2 obtain P1’s identifier from P1 or that P2 send P1’s identifier to the server 100, however. *See id.*, [0079]-[0086], FIG. 6. P2 instead receives P1’s network addresses from the server 100 itself in the “tunnel query notification” message. *Id.* Accordingly, there would be no need in the combination for P1’s identifier to be captured by scanning any QR code or other image pattern on P1 (e.g., the iPhone) to successfully establish a P2P connection between P1 and P2 as taught in Kim.

[2] The system according to claim 1, wherein the image pattern is a barcode, wherein a barcode image is generated in the terminal device.

136. The predictable Kim-Lorex Video combination demonstrates it would have been obvious to provide the additional features recited in Claim 2. For example, 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.



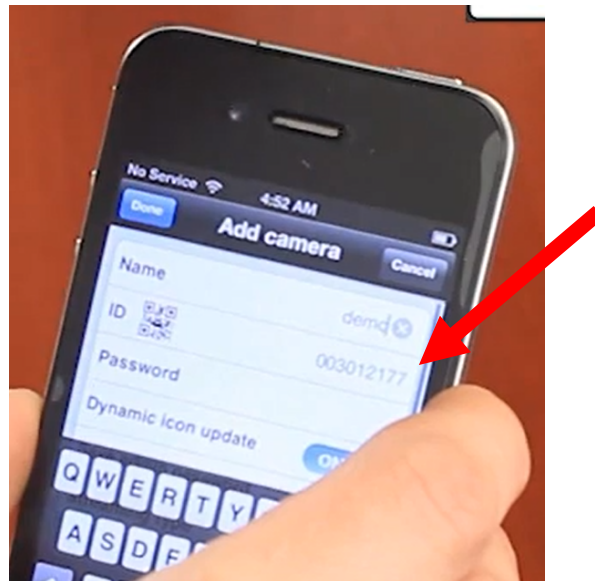
EX1008, 1:17.

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.

[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.

138. The predictable Kim-Lorex Video combination demonstrates it would have been obvious to provide the additional features recited in Claim 3. For example, 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. 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; *above*, [1.4], Section VIII.B (combination overview).

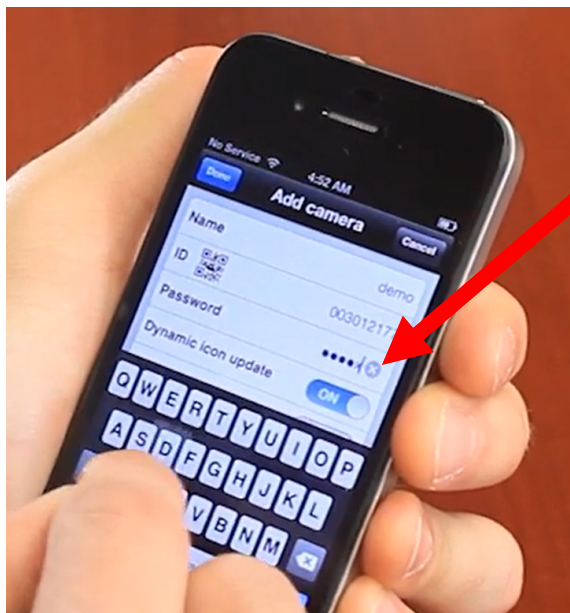


EX1008, 1:20 (cropped, annotated).

[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.

139. The predictable Kim-Lorex Video combination demonstrates it would have been obvious to provide the additional features recited in Claim 6. For example, 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.



EX1008, 1:25 (cropped, annotated); *see also id.*, 1:22-27 (“Just plug in the password. By default its ‘lorex’.”).

140. 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. 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.

[10] The system according to claim 2, wherein the barcode is a quick response code (QR code).

141. The predictable Kim-Lorex Video combination demonstrates it would have been obvious to provide the additional features recited in Claim 10. For example, Lorex Video shows the barcode in the form of a QR code. EX1008, 1:08-1:24.



EX1008, 1:17 (cropped, annotated).

[12.P] A method to identify networked device for establishing a point-to point (P2P) connection, the method comprising the steps of:

142. To the extent the preamble is a limitation, the predictable Kim-Lorex Video combination would have provided the recited method to identify networked device for establishing a point-to-point (P2P) connection for each of the reasons that I described above with respect to Element [1.P]. Above, 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.

[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;

143. The predictable Kim-Lorex Video combination would have provided the “connecting” step and the recited features of Element [12.1]. For example, the Kim-Lorex Video combination 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; *above*, Element [1.1].

[12.2] (b) registering a first identification of the first networked monitoring device into the list of networked devices of the server;

144. The predictable Kim-Lorex Video combination would have provided the “registering” step and the recited features of Element [12.2]. For example, the Kim-Lorex Video combination 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].

[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;

145. The predictable Kim-Lorex Video combination would have provided the “providing” step and the recited features of Element [12.3]. For example, the Kim-Lorex Video combination 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].

[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

146. The predictable Kim-Lorex Video combination would have provided the “generating” step and the recited features of Element [12.4]. For example, the Kim-Lorex Video combination 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].

[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

147. The predictable Kim-Lorex Video combination would have provided the “identifying” step and the recited features of Element [12.5]. For example, the Kim-Lorex Video combination 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].

[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.

148. The predictable Kim-Lorex Video combination would have provided the recited features of Element [12.6]. For example, the Kim-Lorex Video combination would have provided 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].

[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.

149. The predictable Kim-Lorex Video combination demonstrates it would have been obvious to provide the additional features recited in Claim 13 for each of the reasons that I described in detail above with respect to Claim 2.

[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.

150. The predictable Kim-Lorex Video combination demonstrates it would have been obvious to provide the additional features recited in Claim 14 for each of the reasons that I described in detail above with respect to Claim 3.

[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.

151. The predictable Kim-Lorex Video combination demonstrates it would have been obvious to provide the additional features recited in Claim 17 for each of the reasons that I described in detail above with respect to Claim 6.

152. Furthermore, a POSITA would have understood that passwords are conventionally implemented for security and access control. 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. 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.

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

153. The predictable Kim-Lorex Video combination demonstrates it would have been obvious to provide the additional features recited in Claim 18 for each of the reasons that I described in detail above with respect to Claim 10.

IX. GROUND 3 – Obviousness of Claims 1-4 and 6-19 Based on Throughtek-2012 (EX1017) and Lorex Video (EX1008)

A. Overview of Throughtek-2012

154. I have reviewed Exhibit 1017, which is a certified English translation of German utility model DE202012101164U1 (“Throughtek-2012”). In particular, Throughtek-2012 is a publication of a German utility model that was filed by Throughtek Co., Ltd. (which is the same entity that owns the ’842 patent). Throughtek-2012 published no later than June 6, 2012, which is barely a year before

the '842 patent's provisional application was filed in the United States (April 16, 2013). EX1017, 1. Since the provisional application fails to support the features recited in claim elements [1.6] and [12.6] (as I explained above in ¶¶49-54), Throughtek-2012 published more than one year before the July 25, 2013, filing date of the '842 patent's original non-provisional application—and several years before the new matter recited in claim elements [1.6] and [12.6] was added into the claims on September 20, 2016. I therefore understand that Throughtek-2012 qualifies as prior art to the Challenged Claims of the '842 patent.

155. The disclosure of Throughtek-2012 is substantially the same as much of the specification of the '842 patent itself. Notably, 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. Based on my review, Throughtek-2012 expressly discloses all limitations of the Challenged Claims at least to the same extent as the '842 patent itself (and its provisional application). Throughtek-2012 effectively anticipates all elements of the '842 patent, except for the negative limitation recited in claim 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.

B. The Predictable Combination of Throughtek-2012 and Lorex Video

156. Based upon my knowledge and experience in this field and my review of Throughtek-2012 and Lorex Video, it is clear that a POSITA would have been motivated to implement Throughtek-2012 to include 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). 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?"). At a high level, Throughtek-2012 provides substantially the same disclosure as the '842 patent's provisional application (and much of the specification of the '842 patent itself). Throughtek-2012 thus anticipates most elements of the Challenged Claims, although it does not expressly disclose the negative limitation recited by Elements [1.6] or [12.6]. Lorex Video nonetheless confirms that such a simplified connection procedure that does not involve capturing an image pattern associated with the terminal device (smartphone) was entirely conventional before the relatively late effective filing date of the '842 patent.

157. There are several rationales that would have prompted the POSITA to pursue this Throughtek-2012-Lorex Video combination. I provide an exemplary discussion of various reasons below, each of which independently supports the predictability and known advantages of the combination.

158. A **first** reason that a POSITA would have been prompted to implement Throughtek-2012 to include Lorex Video's suggestion (e.g. a simplified connection procedure that does not involve the first networked monitoring device capturing an image pattern associated with the terminal device) would have been 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").

159. A **second** reason that a POSITA would have been prompted to implement Throughtek-2012 to include Lorex Video's suggestion (e.g. a simplified connection procedure that does not involve the first networked monitoring device capturing an image pattern associated with the terminal device) would have been to further Throughtek-2012's general goal to "quickly establish a direct connection." EX1017, [0007], [0016] ("[a] direct connection ... can be established quickly"). 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. 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?”).

160. Based upon my knowledge and experience in this field and my review of the relatively straightforward and predictable structures in Throughtek-2012 and Lorex Video, it is clear that a POSITA would have possessed the level of skill to implement this combination given the overlapping technologies of Throughtek-2012 and Lorex Video—with a reasonable expectation of success in achieving this combination in the manner described above. Both references are directed to technology for establishing connections between networked devices including smart phones and cameras. As I have explained throughout this declaration, the state of the art for such networked devices and their interconnectivity was relatively advanced by the earliest effective filing date of the ’842 patent claims. Again, the specific technologies applied in Throughtek-2012 and Lorex Video were common—e.g., an IP camera having a QR code for capture by a user’s smartphone and a network server that facilitated hole-punching for the establishment of P2P connections. These were well within a POSITA’s knowledge and skill level at the relevant time.

161. As detailed below, the predictable Throughtek-2012–Lorex Video combination renders obvious claims 1-4 and 6-19 of the ’842 patent, with the resulting combination providing each of the claim elements, for the reasons explained below.

[1.P] A system to identify a networked device for establishing a point-to point (P2P) connection, the system comprising:

162. To the extent this preamble is treated as claim limitation, the predictable Throughtek-2012-Lorex Video combination would have provided a system that identifies a networked device for establishing a point-to point (P2P) connection. 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; *above*, Sections IX.A, IX.B (combination overview).

[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

163. The predictable Throughtek-2012-Lorex Video combination would have provided the claimed network server having the recited features. For example, Throughtek-2012 describes “a network server which is provided with an apparatus list.” EX1017 [0009]. 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; *above*, Section IX.A-2.

[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;

164. The predictable Throughtek-2012-Lorex Video combination would have provided the claimed first networked monitoring device having the recited features. For example, 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]. 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; *above* Section IX.A-2.

[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

165. The predictable Throughtek-2012-Lorex Video combination would have provided the claimed image pattern having the recited features. For example, 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; *above* Section IX.A-2.

[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,

166. The predictable Throughtek-2012-Lorex Video combination would have provided the claimed terminal device having the recited features. For example, 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; *above* Section IX.A-2.

[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

167. The predictable Throughtek-2012-Lorex Video combination would have provided the features recited in Element [1.5]. For example, 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; *above*, Section IX.A-2.

[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.

168. The predictable Throughtek-2012-Lorex Video combination would have provided the features recited in Element [1.6]. Like the '842 patent and its provisional application, the Throughtek-2012 does not expressly or inherently

disclose the negative limitation recited in [1.6]. *Above*, Sections II.C, IX.A. 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. *Above*, Section VIII.A. Lorex Video discloses the entire 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. 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. 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."). 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. *Above*, Section IX.B (combination overview).

169. To be clear, Lorex Video’s disclosure plainly provides the functionality recited in Element [1.6]. Nonetheless, this fact is further confirmed and corroborated by additional evidence of record regarding the functionality of the system described in Lorex Video. For example, I have reviewed the declaration of Mr. Vlad Kardashov (EX1011), who was formerly a Project Lead and IP Products Line Manager at Lorex Technology, Inc. EX1011, ¶3. Mr. Kardashov “had personal knowledge of, and was highly familiar with, the Lorex LNC100 Series of IP cameras, the Lorex Ping app, the network server system, and all of the instructions/user guides/literature/how-to videos that were published by Lorex Technology during 2012 and later.” *Id.* Mr. Kardashov testified that the LNC100 Series IP Camera and Lorex Ping app described in Lorex Video allowed “the point-to-point connection [to be] established without requiring the user to point the IP camera at the smartphone to capture any image of the user’s smartphone (or otherwise input information at the IP camera).” *Id.*, ¶7. Mr. Kardashov’s testimony is consistent with the demonstration in the Lorex Video, as well as a user’s guide and a second demonstration video for Lorex’s LNC 100 Series IP Camera system. *See* EX1010, 00:29-00:39 (“All you have to do is activate your camera by simply scanning the QR code on the back of the camera with your smartphone or tablet.”); EX1006, 29-30. The evidence is thus clear that Lorex Video teaches that the first networked monitoring device (e.g., the IP camera) does not capture any image pattern

associated with the terminal device (e.g., the iPhone) for establishing the P2P connection between the terminal device and the first networked monitoring device, as recited in [1.6].

[2] The system according to claim 1, wherein the image pattern is a barcode, wherein a barcode image is generated in the terminal device.

170. The predictable Throughtek-2012-Lorex Video combination would have provided the additional features recited in Claim 2. For example, 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; *above*, Sections IX.A-2.

[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.

171. The predictable Throughtek-2012-Lorex Video combination would have provided the additional features recited in Claim 3. For example, 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]; *above*, Section IX.A-2.

[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.

172. The predictable Throughtek-2012-Lorex Video combination would have provided the additional features recited in Claim 4. For example, 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]; *above*, Sections IX.A-2.

[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.

173. The predictable Throughtek-2012-Lorex Video combination would have provided the additional features recited in Claim 6. For example, 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]; *above*, Sections IX.A-2.

[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.

174. The predictable Throughtek-2012-Lorex Video combination would have provided the additional features recited in Claim 7. For example, 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]; *above*, Sections, IX.A-2.

[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.

175. The predictable Throughtek-2012-Lorex Video combination would have provided the additional features recited in Claim 8. For example, 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]; *above*, Sections IX.A-2.

[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.

176. The predictable Throughtek-2012-Lorex Video combination would have provided the additional features recited in Claim 9. For example, 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]; *above*, Sections IX.A-2.

[10] The system according to claim 2, wherein the barcode is a quick response code (QR code).

177. The predictable Throughtek-2012-Lorex Video combination would have provided the additional features recited in Claim 10. For example, Throughtek-2012 describes “the bar code used to establish the connection is a QR code.” EX1017, [0015], *see also id.*, Claim 11; *above*, Sections IX.A-2.

[11] The system according to claim 2, wherein the barcode is a one dimensional barcode.

178. The predictable Throughtek-2012-Lorex Video combination would have provided the additional features recited in Claim 11. For example, Throughtek-2012 describes “the bar code used to establish the connection is ... a one-dimensional bar code.” EX1017, [0015], *see also*, Claim 12; *above*, Sections IX.A-2.

[12.P] A method to identify networked device for establishing a point-to point (P2P) connection, the method comprising the steps of:

179. To the extent the preamble is a limitation, the predictable Throughtek-2012-Lorex Video combination would have provided the recited method to identify networked device for establishing a point-to-point (P2P) connection for the reasons that I described above with respect to Element [1.P]. *Above*, Element [1.P]; *see also above* Element [1.P]; EX1017, [0008], [0009], [0023], [0034]-[00340], Claim 1, FIGS. 1-5.

[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;

180. The predictable Throughtek-2012-Lorex Video combination would have provided the “connecting” step and the recited features of Element [12.1] for each of the reasons that I described above with respect to Element [1.1]. *Above*, Element [1.1]; EX1017 [0005], [0009], [0024]-[0028], [0030], [0034], [0036], [0040], Claim 1, FIGS. 1-5.

[12.2] (b) registering a first identification of the first networked monitoring device into the list of networked devices of the server;

181. The predictable Throughtek-2012-Lorex Video combination would have provided the “registering” step and the recited features of Element [12.2] for each of the reasons that I described above with respect to Element [1.2]. *Above*, Element [1.2]; EX1017 [0005], [0009], [0026], [0036] [0040], FIG. 5, Claim 1.

[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;

182. The predictable Throughtek-2012-Lorex Video combination would have provided the “providing” step and the recited features of Element [12.3] for each of the reasons that I described above with respect to Element [1.3]. *Above*, Element [1.3]; EX1017 [0009], [0026]-[0028], [0034], [0039], [0040], Claim 1, FIGS. 1-5.

[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

183. The predictable Througthtek-2012-Lorex Video combination would have provided the “generating” step and the recited features of Element [12.4] for each of the reasons that I described above with respect to Element [1.4]. Above, Element [1.4]; EX1017 [0009], [0016], [0024], [0027]-[0030], [0034], [0037], [0039], [0040], Claim 1, FIGS. 1-5.

[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

184. The predictable Througthtek-2012-Lorex Video combination would have provided the “identifying” step and the recited features of Element [12.5] for each of the reasons that I described above with respect to Element [1.5]. Above Element [1.5]; EX1017 [0009], [0010], [0030], [0034], [0038], [0040], FIGS. 3-4, Claims 1 and 5.

[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.

185. The predictable Througthtek-2012-Lorex Video combination would have provided the recited features of Element [12.6] for each of the reasons that I

described above with respect to Element [1.6]. Above, Element [1.6]; EX1008, 1:00-1:40.

[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.

186. The predictable Throughtek-2012-Lorex Video combination would have provided the additional features recited in Claim 13 for each of the reasons that I described above with respect to Claim 2.

[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.

187. The predictable Throughtek-2012-Lorex Video combination would have provided the additional features recited in Claim 14 for each of the reasons that I described above with respect to Claim 3.

[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.

188. The predictable Throughtek-2012-Lorex Video combination would have provided the additional features recited in Claim 15 for each of the reasons that I described above with respect to Claim 4.

[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.

189. The predictable Throughtek-2012-Lorex Video combination would have provided the additional features recited in Claim 16 for each of the reasons that I described above with respect to Claim 4.

[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.

190. The predictable Throughtek-2012-Lorex Video combination would have provided the additional features recited in Claim 17 for each of the reasons that I described above with respect to Claim 6. EX1017, Claim 7, *see also* [0031]

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

191. The predictable Throughtek-2012-Lorex Video combination would have provided the additional features recited in Claim 18 for each of the reasons that I described above with respect to Claim 10.

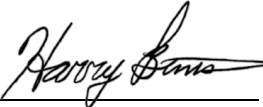
[19] The method according to claim 13, wherein the barcode is a one dimensional barcode.

192. The predictable Throughtek-2012-Lorex Video combination would have provided the additional features recited in Claim 19 for each of the reasons that I described above with respect to Claim 11.

X. Conclusion

193. I hereby declare that all statements made are of my own knowledge, are true and that all statements made on information and belief are believed to be true. I further declare that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of the Title 18 of the United States Code and that such willful false statements may jeopardize the validity of this proceeding.

Dated: January 29, 2024

By: 
Harry Bims, Ph.D.

APPENDIX

Dr. Harry V. Bims
Protocomm Systems, LLC
2665 Marine Parkway, Suite 1140
Mountain View, CA 94043
harrybims@me.com
650-283-4174

PROFESSIONAL SUMMARY

Harry Bims, PhD, EE, provides expert witness support services for telecommunications-related intellectual property litigation. These services include deposition and court testimony, expert reports, and infringement research, for patent, copyright, and trade secret litigation matters. He has 30+ years of telecommunications industry experience, and holds twenty-two US patents in network architecture and chip design for wireless communications.

EMPLOYMENT HISTORY

12/2001 - 05/2004 AirFlow Networks, Inc. LLC • Sunnyvale, California

Position: *CEO/CTO & Founder*

As the sole founder of the company, created the original business plan, raised venture capital, and hired the core engineering team. Grew the company to 32 people and shipped products for revenue in the US and overseas. Fifteen patents on the core technology have issued. These patents, which relate to wireless network infrastructure based on the 802.11 specification, have been sold to Broadcom.

03/2001 - 12/2001 Bay Partners LLC • Cupertino, California

Position: *Entrepreneur in Residence*

Reported to the partners of this VC firm as a technology expert on a range of wireless and networking subjects. Reviewed business plans and participated in due diligence activities related to several startups seeking funding. Developed a business plan for a startup that builds network infrastructure for 802.11 enterprise networks.

09/1999 - 03/2001 Symmetry Communications Systems LLC • San Jose, California

Position: *Director, Software Architecture*

Reporting to the CEO, responsible for the software architecture of their core SGSN and GGSN products for the GPRS market. Formulated a software technology roadmap, showing the evolution from 2.5G to 3G SGSN and GGSN products. Management responsibility for Firmware, Hardware, Performance, and Systems Engineering Groups. Provided management support of early field trials of the system on a global basis.

07/1999 - 09/1999 **T-SPAN Systems Corporation LLC • Palo Alto, California**

Position: *Member of Technical Staff*

Designed a wireless home LAN protocol for the company. Also designed and built a PC-based platform to demonstrate their technology. Company is now publicly traded as Atheros Communications.

07/1992 - 12/1998 **Glenayre Technologies-Wireless Access Group • San Jose, California**

Position: *Member of Technical Staff; Sr. Member of Technical Staff; Manager of NOC Systems*

Employee #6 at the company, which was acquired by Glenayre Technologies, Nov 1997. Designed and built a 4-channel ReFLEX50 pager demonstration in 1 week. Participated in early field trials and feasibility studies, culminating in a Pioneer's Preference license award from the FCC to SkyTel Corporation for Narrowband PCS development.

Invented, designed, and built from concept through full implementation, a patented two-way pager test system for the ReFLEX50 and ReFLEX25 protocols. This system was used throughout company operations for performance testing of the ReFLEX pager designs from Wireless Access, and Motorola. Over 16 systems were deployed around the country for manufacturing tests, engineering protocol tests, antenna tests, and pager repair tests.

The project required technical skills in PC hardware design, C++, object-oriented programming, signal processing techniques, NT device driver development, Win32 user interface development, real-time, multi-threaded control, and proficiency with wireless communications lab equipment. Three patents have been issued based on technical inventions in this capacity.

Co-developed a wireless application protocol for sending and receiving encrypted email messages over the paging channel. Led the project team that deployed a software encryption module based on this protocol for government agencies.

8/2018 – Present **CUPP Cybersecurity, LLC • Palo Alto, California**

Position: *CEO*

Developing a suite of network security products and technologies aimed at consumers to protect their online internet access.

10/2012 – Present **BoughtStuff, Inc • Palo Alto, California**

Position: *Founder*

The company has developed a mobile application for storage and delivery of product information to smartphones over wireless networks.

Bims Laboratories, Inc Work History

6/2009 – 7/2009 **Eastman Kodak Company • Rochester, NY**

Position: *Technology Consultant*

Providing technology assessment on certain wireless communication patents.

10/2009 – 1/2017 **IEEE 802.16 Working Group**

Position: *Task Group Secretary, Task Group Vice-Chair, Task Group Chair, Working Group Vice-Chair & Secretary, IEEE 802.16 Expert*

Served in several leadership capacities within this group that is working on improvements to the IEEE 802.16 standard, otherwise known as WiMAX. The 802.16 Working Group entered hibernation on March 2018. From that time until the present, I am on the roster of Experts designated by the Chair to answer questions and provide clarification about the 802.16 standards.

2/2014 – Present **Access Network Protocol Development**

Position: *Technical Lead Developer*

Developing a C++17-based DES of SDRs for wired and wireless network protocols, that includes IMT-2020 channel models. Implementations of the IEEE 802 and LTE protocol families, plus PTP, PPoE, IPv6, digital cable, Bluetooth, DSL, frame relay and many other managed node models for smart grid and vertical IoT applications. Used for technical analysis of emerging wireless standards amendments.

Protocomm Systems, LLC Consulting History

04/1999–07/1999 **Gigabit Wireless, Inc. • San Jose, California**

Position: *Technical Leader*

Technical leader for the Wireless MAC design group. Responsible for comparative analysis of competing wireless MAC protocol standards. Responsible for the creation of a proprietary MAC protocol specification document, simulation of the protocol, and implementation in a prototype. Participated in early 802.16 protocol standards. This company was acquired by Intel Corporation.

3/2007 – 10/2009 **Apple, Inc. • Cupertino, CA**

Position: *Technology Consultant*

Participating in IEEE 802.16 standards meetings as an affiliate of the client.

7/2003 – Present **Various expert witness engagements (see below)**

Position: *Technical Expert Witness*

Testified as a wireless technology expert in patent infringement cases. For a list of such cases, see below.

Technical Expert Witness Experience

5/2023 – Present **Client: Fish & Richardson LLP (representing Samsung Electronics, Co. Ltd.)**

Case: In the Matter of an Arbitration Pursuant to the Rules of the International Court of Arbitration of the International Chamber of Commerce (ICC Case No. 27699/PDP)

Location: INTERNATIONAL CHAMBER OF COMMERCE

Testifying expert in these matters involving international patent arbitration between Interdigital and Samsung.

Attorneys: For Plaintiff: Alston & Bird LLP

For Defendant: Fish & Richardson LLP

Status: Case ongoing

10/2022 – Present **Client: Finnegan, Henderson, Farabow, Garrett & Dunner LLP (representing Samsung Electronics, Co. Ltd.)**

Case: IPR Petition relating to Apex Beam Technologies, LLC v. Samsung Electronics, Co. Ltd., Civil Action No. 2:22-cv-00188)

Location: UNITED STATES PATENT AND TRADEMARK OFFICE BEFORE THE PATENT TRIAL AND APPEAL BOARD

Testifying expert in these matters involving smart antenna technology.

February 27, 2023: Expert Declaration ISO petition for Inter Partes review

February 28, 2023: “Xia” Expert Declaration ISO petition for Inter Partes review

February 28, 2023: “Liu” Expert Declaration ISO petition for Inter Partes review

Attorneys: For Plaintiff: Russ, August & Kabat LLP

For Defendant:

Status: Case ongoing

7/2022 – Present **Client: Russ, August & Kabat LLP (representing Vivato, Inc.)**

Case: XR Communications, LLC d/b/a Vivato Technologies, Civil Action No. 8:17-cv-00596-DOC(JDE)

Location: UNITED STATES DISTRICT COURT FOR THE CENTRAL DISTRICT OF CALIFORNIA – Hon. David O. Carter

Testifying expert in these matters involving smart antenna technology.

Expert Declaration:

August 23, 2022 Rebuttal Expert Report on Validity

Attorneys: For Plaintiff: Russ, August & Kabat LLP

For Defendant:

Status: Case ongoing

6/2022 – Present **Client: Fish & Richardson LLP (representing Samsung Electronics, Co. Ltd.)**

Case: G+ Communications, LLC v Samsung Electronics Co. Ltd. et. al, Civil Action No. 2:22-cv-78

Location: UNITED STATES DISTRICT COURT FOR THE EASTERN DISTRICT OF TEXAS – Hon. Rodney Gilstrap

Testifying expert in these matters involving smart antenna technology.

March 13, 2023: Expert Declaration ISO Samsung Defendants’ Claim Construction Proposals

Attorneys: For Plaintiff: Russ, August & Kabat LLP

For Defendant:

Status: Case ongoing

5/2022 – Present **Client: Kilpatrick Townsend LLP (representing Apple, Inc.)**

Case: IPR Petition relating to Apple, Inc. v. Mullen Industries LLC, Civil Action No. 6:22-cv-00145

Location: UNITED STATES PATENT AND TRADEMARK OFFICE BEFORE THE PATENT TRIAL AND APPEAL BOARD

Testifying expert in these matters involving remote notification devices.

August 8, 2022: Expert Declaration

May 23, 2023: Expert Deposition

Attorneys: For Petitioner: Kilpatrick Townsend LLP

For Plaintiff: Mintz, Levin, Cohn, Ferris, Glovsky, and Popeo, P.C.

Status: Case ongoing

3/2022 – Present **Client: Kirkland & Ellis LLP (representing Samsung Electronics Co. Ltd.)**

Case: California Institute of Technology v Samsung Electronics Co. Ltd., Civil Action No. 2:21-cv-00446

Location: UNITED STATES DISTRICT COURT FOR THE EASTERN DISTRICT OF TEXAS – Hon. Rodney Gilstrap

Testifying expert in these matters involving LDPC codes.

November 22, 2022: Declaration regarding claim construction

December 20, 2022: Rebuttal Declaration regarding claim construction

May 22, 2023: Rebuttal expert report on non-infringement

May 31, 2023: Deposition testimony
Attorneys: For Petitioner: Kirkland & Ellis LLP
For Plaintiff: Mintz, Levin, Cohn, Ferris, Glovsky, and Popeo, P.C.
Status: Case ongoing

2/2022 – 12/2022 Client: Fish & Richardson LLP (representing Apple, Inc.)

Case: Litigation between Ericsson and Apple in Belgium, Brazil, Germany, Netherlands, and Colombia, and US matters:

Ericsson Inc. et. al. v. Apple Inc., Civil Action No. 6:22-cv-00061-ADA

Ericsson Inc., et. al. v. Apple Inc., Civil Action No. 2:21-cv-00376

Apple Inc. v. Telefonaktiebolaget LM Ericsson, et. al., Civil Action No. 2:21-cv-00460

In the Matter of Certain Mobile Phones Tablet Computers, Smart Watches, Smart Speakers, and Digital Media Players, and Products Containing Same.

U.S. Int'l Trade Commission Inv. No. 337-TA-3596

Location: UNITED STATES DISTRICT COURT FOR THE WESTERN DISTRICT OF TEXAS WACO DIVISION – Hon. Alan D. Albright

UNITED STATES DISTRICT COURT FOR THE EASTERN DISTRICT OF TEXAS

UNITED STATES INTERNATIONAL TRADE COMMISSION

Testifying expert in these matters involving 5G networking technology.

Expert Declaration:

May 18, 2022 COLOMBIA: Invalidity and Non-Infringement Technical Opinion regarding certain Colombia patents

April 27, 2022 COLOMBIA: Invalidity and Non-Infringement Technical Opinion regarding certain Colombia patents #1

April 27, 2022 COLOMBIA: Invalidity and Non-Infringement Technical Opinion regarding certain Colombia patents #2

March 28, 2022 COLOMBIA: Invalidity and Non-Infringement Technical Opinion regarding certain Colombia patents

March 9, 2022 BRAZIL: Invalidity Technical Opinion regarding Brazil patents

May 26, 2022 BRAZIL: Response to Ericsson Statement regarding Brazil patents

August 25, 2022 BRAZIL: Live testimony before the Brazil Patent and

Trademark Office regarding invalidity

Attorneys: For Plaintiff:

For Defendant: Fish & Richardson, LLP

Status: Case settled

1/2022 – Present **Client: Finnegan LLP (representing Toyota Motor Corp., et. al.)**

Case: Intellectual Ventures I LLC, et. al. v. Toyota Motor Corp., et. al., Civil Action No. 2:21-cv-389

Toyota Motor Corp. (Petitioner) v. Intellectual Ventures II, LLC (Patent Owner)
Case No. IPR2022-01355

Location: UNITED STATES DISTRICT COURT FOR THE WESTERN DISTRICT OF TEXAS WACO DIVISION –

UNITED STATES PATENT AND TRADEMARK OFFICE BEFORE THE PATENT TRIAL AND APPEAL BOARD

Testifying expert in this District Court and PTAB matter involving IEEE 802.11 wireless networking.

Expert Declaration:

August 25, 2022 PTAB Declaration ISO Petition for IPR

Attorneys: For Plaintiff:

For Defendant/Petitioner: Finnegan, LLP

Status: Case ongoing

1/2022 – Present **Client: Stroock LLP (representing TrackThings LLC)**

Case: TrackThings LLC v. NETGEAR, Inc.; TrackThings LLC v. NETGEAR, Inc.; TrackThings LLC v. Amazon.com, Inc. and Amazon.com Services LLC, and eero LLC., Civil Action No. 6:21-cv-00720

Location: UNITED STATES DISTRICT COURT FOR THE WESTERN DISTRICT OF TEXAS WACO DIVISION – Hon. Alan D. Albright

Testifying expert in this District Court matter involving wireless network reconfiguration.

March 10, 2022: Expert declaration ISO claim construction responses

February 24, 2023: Expert report on Validity

Attorneys: For Plaintiff:

For Defendant: Stroock, LLP

Status: Case ongoing

12/2021 – Present **Client: BlankRome (representing Samsung Electronics Co., Ltd)**

Case: IPR Petition relating to TOT Power Control, S.L. v. Samsung Elecs. Co., Ltd and Samsung Elecs. Am. Inc., Civil Action No. 1:21-cv-01305.

Location: UNITED STATES PATENT AND TRADEMARK OFFICE BEFORE THE PATENT TRIAL AND APPEAL BOARD

Testifying expert in this IPR proceeding involving power control methods in wireless systems.

September 12, 2022: 865 Expert Declaration

Attorneys: For Plaintiff: Blank Rome

For Defendant: Hausfeld, LLP

Status: Case ongoing

10/2021 – Present **Client: Wilkie Farr & Gallagher LLP (representing Lenovo and Motorola)**

Case: IPR Petitions relating to Bell Northern Research, LLC. v. Lenovo Group, Ltd., Lenovo (United States) Inc., and Motorola Mobility LLC, Civil Action No. 6:21-cv-00847

Location: UNITED STATES PATENT AND TRADEMARK OFFICE BEFORE THE PATENT TRIAL AND APPEAL BOARD

Testifying expert in this IPR proceeding case involving training sequences in wireless networks.

Status: Case ongoing

10/2021 – 5/2022 **Client: Finnegan, Henderson, Farabow, Garrett & Dunner, LLP (representing MediaTek Inc.)**

Case: NXP USA, Inc. v. MediaTek Inc., et. al., Civil Action No. 2:21-cv-000318-JRG – Hon. Rodney Gilstrap

Location: UNITED STATES DISTRICT COURT FOR THE EASTERN DISTRICT OF TEXAS MARSHALL DIVISION

Testifying expert in this District Court matter involving 802.11n, 802.11ac, and 802.11ax chipsets.

Expert Report:

February 3, 2022 Declaration ISO Defendant's Claim Construction Brief

Attorneys: For Plaintiff: Duane Morris, LLP

For Defendant: Finnegan, LLP

Status: Case settled

09/2021 – Present **Client: Fish & Richardson, LLP (representing Samsung Electronics Co., Ltd., et. al.)**

Case: Smart Mobile Technologies, LLC v. Samsung Electronics Co., Ltd., et. al., Civil Action No. 6:21-cv-00701-ADA. Hon. Alan D. Albright

Location: UNITED STATES DISTRICT COURT FOR THE WESTERN DISTRICT OF TEXAS WACO DIVISION

Testifying expert in this District Court matter involving wireless voice and data transfer.

Expert Report:

June 8, 2022 Declaration ISO Defendant's Claim Construction Brief

Attorneys: For Plaintiff: Hagens Berman Sobol Shapiro, LLP

For Defendant: Fish & Richardson, LLP

Status: Case ongoing

05/2021 – Present **Client: Sidley Austin (representing HP Inc. and Microsoft Corporation)**

Case: SynKloud Technologies, LLC v. HP Inc., Civil Action No. 1:19-cv-01360-RGA and Microsoft Corporation v. SynKloud Technologies, LLC, Civil Action No. 1:20-cv-00007-RGA

Location: UNITED STATES DISTRICT COURT FOR THE DISTRICT OF DELAWARE

Testifying expert in this District Court matter involving wireless cloud storage.

Expert Report:

June 25, 2021 Declaration ISO Microsoft and HP's Claim Construction Brief

Expert Testimony:

Attorneys: For Plaintiff:
For Defendant: Sidley Austin
Status: Case ongoing

05/2021 – 5/2022 **Client: DLA Piper (representing Motorola Mobility LLC)**

Case: U.S. Int'l Trade Commission Inv. No. 337-TA-1253
Certain LTE-Compliant Cellular Communication Devices
Motorola v. Evolved Wireless LLC.

Location: UNITED STATES INTERNATIONAL TRADE COMMISSION –
Administrative Law Judge Cameron R. Elliot
Testifying expert in this ITC matter involving LTE cellular device handover.

Expert Report:

November 16, 2021 Expert Report on NonInfringement and Lack of Technical
Domestic Industry

Expert Testimony:

December 15, 2021 Deposition testimony

Attorneys: For Plaintiff: Nelson Bumgardner Albritton P.C.; Adduci, Mastriani &
Schaumberg, LLP

For Defendant: DLA Piper

Status: Case settled

04/2021 – 6/2022 **Client: Desmarais LLP (representing Google LLC and FitBit Inc.)**

Case: Cellspin Soft, Inc. v. Fitbit, Inc., No. 4-17-cv-05928-YGR

Location: UNITED STATES DISTRICT COURT FOR THE NORTHERN DISTRICT OF
CALIFORNIA

Hon. Yvonne Gonzalez Rogers

Testifying expert in this patent case involving the distribution of real-time health
data.

Expert Testimony:

October 29, 2021 Expert Report on NonInfringement

Attorneys: For Plaintiff: Garteiser Honea PLLC and Corcoran IP Law PLLC

For Defendant: Desmarais LLP

Status: Case settled. Summary Judgment for Non-Infringement.

2/2021 – 11/2021 **Client: Fish & Richardson (representing Quectel)**

Client: Axinn, Veltrop & Harkrider LLP (representing Thales DIS AIS USA, LLC)

Client: Pearl Cohen LLP (representing Telit)

Case: U.S. Int'l Trade Commission Inv. No. 337-TA-1240

Certain UMTS and LTE Cellular Communication Modules and Products
Containing the Same

Koninklijke Philips N.V. v Quectel Wireless Solutions Co. Ltd., Thales DIS AIS
Deutschland GmbH, Thales S.A., Telit Wireless Solutions, Inc., Telit
Communications PLC, CalAmp Corp, Xirgo Technologies, LLC, Laird
Connectivity, Inc., Thales DIS AIS USA LLC

Case No. 1:20-cv-1713 (D. Del)

Location: UNITED STATES INTERNATIONAL TRADE COMMISSION –
Administrative Law Judge Hon. David P. Shaw

Testifying expert on 3GPP mobile device operation.

Expert Testimony:

July 21, 2021 Expert Report on Invalidity

August 6, 2021 Deposition Testimony

October 12, 2021 Live Testimony before ALJ David P. Shaw

Attorneys: For Plaintiff: Mayer Brown LLP

For Defendants: Fish & Richardson; Axinn, Veltrop & Harkrider LLP

Status: Case closed

11/2020– Present **Client: Orrick, Herrington & Sutcliffe LLP (representing PayPal Holdings, Inc.)**

Case: IOENGINE LLC v PayPal Holdings, Inc.

Civil Action No. 1:18-cv-00452-WCB

Location: UNITED STATES DISTRICT COURT FOR THE DISTRICT OF DELAWARE

Hon. William C. Bryson

Testifying expert in this patent case involving peripheral device communication to remote servers.

Expert Testimony:

November 19, 2021 Expert Report on Invalidity

January 7, 2022 Expert Report on Non-Infringement

January 20-21, 2022 Deposition Testimony on Invalidity and Non-Infringement

Status: Case ongoing

11/2020 – Present **Client: DLA Piper (representing Apple, Inc.)**

Case: Maxell v. Apple Inc. In the Matter of Certain Mobile Electronic Devices and Laptop Computers

U.S. Int'l Trade Commission Inv. No. 337-TA-1215

Location: UNITED STATES INTERNATIONAL TRADE COMMISSION –
Administrative Law Judge Hon. Dee Lord

Testifying expert on 3GPP mobile device operation.

Expert Testimony:

February 25, 2021: Opening Expert Report Regarding Invalidity

Attorneys: For Plaintiff: Mayer Brown LLP

For Defendant: DLA Piper LLP

Status: Case ongoing

9/2020– 9/2021 **Client: DickinsonWright (representing Nippon Telegraph & Telephone Co. and Essential WiFi, LLC)**

Case: NTT Corp., et. al. v. MediaTek, Acer, and Texas Instruments

Civil Action No. 1:20-cv-00632-ADA. Hon. Alan D. Albright

Location: UNITED STATES DISTRICT COURT FOR THE WESTERN DISTRICT OF TEXAS AUSTIN DIVISION – Hon. Alan Albright

Testifying expert in this patent case involving MIMO technology.

Expert Testimony:

Status: Case closed

8/2020– Present **Client: Folio Law Group PLLC (representing Dali Wireless)**

Case: Dali Wireless, Inc. v. Corning Optical Communications, LLC,
Civil Action No. 3:20-cv-06469-EMC

Location: UNITED STATES DISTRICT COURT FOR THE WESTERN DISTRICT OF
TEXAS – Hon. Edward M. Chen

Testifying expert in this patent case involving distributed antenna system
networks.

Expert Testimony:

November 6, 2020: Declaration Regarding Interpretation of Asserted Claims

February 12, 2021: Declaration Regarding Interpretation of Asserted Claims

August 22, 2022: Deposition Testimony

Status: Case ongoing

3/2020– Present **Client: Folio Law Group PLLC (representing Dali Wireless)**

Case: Dali Wireless, Inc. v. CommScope Technologies, LLC and CommScope Holding
Company, Inc..

Civil Action No. 1:19-cv-00952-MN

Location: UNITED STATES DISTRICT COURT FOR THE DISTRICT OF DELAWARE
– Hon. Maryellen Noreika

Testifying expert in this patent case involving distributed antenna system
networks.

Expert Testimony:

June 23, 2021: Expert report on infringement.

August 16, 2021: Reply Expert report on infringement of '338 Patent

Status: Case ongoing

03/2020 – Present **Client: Sidley Austin LLP (representing Lenovo and Motorola)**

Case: InterDigital Technology Corporation, IPR Licensing, Inc., InterDigital
Communications, Inc., InterDigital Holdings, Inc., and InterDigital, Inc. v.
Lenovo Holding Company, Inc., Lenovo (United States) Inc., and Motorola
Mobility LLC

Civil Action No. 19-1590-LPS

Location: UNITED STATES DISTRICT COURT FOR THE DISTRICT OF DELAWARE
Hon. Leonard P. Stark

Testifying expert in this patent case involving 3G and 4G cellular standards.

Expert Testimony:

June 16, 2022: Expert Report on Invalidity of 8,675,612 and 9,456,449 patents

June 16, 2022: Expert Report on Invalidity of 8,085,665 and 8,427,954 patents

August 8, 2022: Rebuttal Expert Report on Invalidity

August 31, 2022: Expert Deposition

Status: Case ongoing

3/2020– Present **Client: Finnegan, Henderson, Farabow, Garrett & Dunner LLC
(representing Google)**

Case: IPR Petition Google LLC, v. Sonos, Inc., Case No. IPR2021-01563

Location: UNITED STATES PATENT AND TRADEMARK OFFICE BEFORE THE
PATENT TRIAL AND APPEAL BOARD

Testifying expert in this IPR proceeding involving wireless home speaker
systems.

Expert Testimony:

September 27, 2021: Declaration ISO petition for Inter Partes Review

May 10, 2022: Supplemental declaration ISO petition for Inter Partes Review

Status: Case ongoing

08/2019 – Present **Client: Fish & Richardson (representing Finjan, Inc.)**

Case: Finjan, Inc. v. Cisco, Inc.

Civil Action No. 5:17-cv-00072-BLF-SVK

Location: UNITED STATES DISTRICT COURT FOR THE SOUTHERN DISTRICT OF
CALIFORNIA SAN DIEGO DIVISION – Hon. Susan Van Keulen

As a testifying expert, provided a technology tutorial in this patent case involving
internet security technology.

Expert Testimony:

August 14, 2019 Tutorial expert report on network security technology.

September 4, 2019 Deposition Testimony

Attorneys: For Plaintiff: Fish & Richardson

For Defendant:

Status: Case ongoing

8/2019 – 5/2020 **Client: Fish & Richardson (representing LG Electronics, Inc.)**

Case: Bell Northern Research, LLC v. LG Electronics, Inc., et. al.

USDC-SDCA Civil Action No. 18-cv-2864-CAB-BLM

Location: UNITED STATES DISTRICT COURT FOR THE SOUTHERN DISTRICT OF CALIFORNIA – Hon. Cathy Ann Bencivengo, Magistrate Judge: Hon. Barbara L. Major

Testifying expert on wired/wireless communication in gaming systems.

Expert Testimony:

November 20, 2019 Declaration ISO motion for summary judgment

Attorneys: For Plaintiff: Skiermont Derby LLP

For Defendant: Fish & Richardson

Status: Case closed

7/2019 – 05/2021 **Client: O'Melveny & Myers LLP (representing Apple Inc.)**

Case: Maxell, Ltd. v. Apple Inc.,

Case No. 5:19-cv-00036-RWS.

Location: UNITED STATES DISTRICT COURT FOR THE EASTERN DISTRICT OF TEXAS TEXARKANA DIVISION – Hon. Robert W. Schroeder III

Testifying expert on 3G cellular telephone technology.

Expert Testimony:

May 7, 2020: Opening Expert Report Regarding Invalidity

June 4, 2020: Rebuttal Expert Report on Non-Infringement

Deposition Testimony: June 24, 2020

Attorneys: For Plaintiff: Mayer Brown LLP

For Defendant: O'Melveny & Myers LLP

Status: Case settled.

4/2019 – Present **Client: Perkins Coie (representing Nintendo of America, Inc.)**

Case: Genuine Enabling Technology LLC v. Nintendo Company Ltd., and Nintendo of America, Inc., W.D. Wash.,

Civil Action No. 2:19-cv-00351-RSM

Location: UNITED STATES DISTRICT COURT FOR THE WESTERN DISTRICT OF WASHINGTON – Hon. Ricardo S. Martinez

Testifying expert on wired/wireless communication in gaming systems.

Expert Declarations:

October 23, 2019 Declaration ISO claim constructions

November 26, 2019 Sur-reply declaration ISO claim constructions

January 23, 2020 Declaration ISO motion for summary judgment

April 20, 2020 Opening Expert Report Regarding Invalidity

Expert Depositions:

December 19, 2019

Claim Construction Hearing Testimony:

February 24, 2020 Tutorial testimony on the technology of the Asserted Patents

Attorneys: For Plaintiff: Bayard, P.A.

For Defendant: Perkins Coie

Status: Case ongoing

12/2019 – 12/2019 **Client: Erise IP (representing Apple Inc.), Haynes and Boone, LLP (representing Ericsson Inc)**

Case: Ericsson Inc. (Petitioner) v. Uniloc 2017, LLC (Patent Owner)

Apple Inc. (Petitioner) v. Uniloc 2017, LLC (Patent Owner) Case No. IPR2020-00224

Location: UNITED STATES PATENT AND TRADEMARK OFFICE BEFORE THE PATENT TRIAL AND APPEAL BOARD

Testifying expert in this IPR proceeding involving ARQ data exchange on LTE networks.

Expert Declarations:

December 16, 2019 Declaration ISO Petition for Inter Partes Review of U. S. Patent No. 7,075,917

Attorneys: For Petitioner: Erise IP; Haynes and Boone, LLP
For Patent Owner:
Status: Case closed

6/2019 – 7/2020 **Client: Fish & Richardson (representing Microsoft Corporation)**

Case: Microsoft Corp. (Petitioner) v. Uniloc 2017, LLC (Patent Owner)

Uniloc 2017, LLC v. Microsoft Corp.

USDC Central District of California, Case Nos. 8:18-cv-2053, 8:18-cv-2054, 8:18-cv-2224; 8:19-cv-0428, 8:19-cv-0477, 8:19-cv-0196

Location: UNITED STATES PATENT AND TRADEMARK OFFICE BEFORE THE PATENT TRIAL AND APPEAL BOARD

Testifying expert in this IPR proceeding involving 3GPP transport formats and channels.

Expert Declarations:

August 6, 2019 Declaration in support of claim construction

Attorneys: For Plaintiff: Feinberg Day LLP

For Defendant: Fish & Richardson

Status: Case settled

2/2019 – 5/2020 **Client: Klarquist Sparkman, LLP (representing Microsoft Corporation)**

Case: Uniloc 2017, LLC v. Microsoft Corp.

Location: UNITED STATES PATENT AND TRADEMARK OFFICE BEFORE THE PATENT TRIAL AND APPEAL BOARD

Testifying expert in this IPR proceeding involving ARQ data exchange on LTE networks.

Expert Declarations:

April 14, 2019 Declaration ISO Petition for Inter Partes Review of U. S. Patent No. 7,075,917

Attorneys: For Plaintiff:

For Defendant: Klarquist LLP

Status: Case settled

10/2018 – Present **Client: Kramer Levin Naftalis & Frankel, LLP (representing Finjan, Inc.)**
Case: Finjan, Inc. v. Eset, Inc.
Civil Action No. 3:17-cv-00183-CAB-BGS
Location: UNITED STATES DISTRICT COURT FOR THE SOUTHERN DISTRICT OF CALIFORNIA SAN DIEGO DIVISION – Hon. Cathy Ann Bencivengo
As a testifying expert, provided a technology tutorial in this patent case involving internet security technology.
Expert Declaration:
October 5, 2018 Tutorial expert report on network security technology.
March 11, 2020 Jury trial testimony.
Attorneys: For Plaintiff: Kramer Levin, Naftalis, & Frankel LLP
For Defendant:
Status: Jury Trial Mistrial due to COVID-19.
Case ongoing

9/2018 – 5/2020 **Client: Kramer Levin Naftalis & Frankel, LLP (representing Finjan, Inc.)**
Case: Finjan, Inc. v. Juniper, Inc.
Civil Action No. 15-cv-03295-BLF-SVK
Location: UNITED STATES DISTRICT COURT FOR THE NORTHERN DISTRICT OF CALIFORNIA SAN JOSE DIVISION – Hon. Beth L. Freeman
As a testifying expert, provided a technology tutorial in this patent case involving internet security technology.
Expert Declaration:
September, 11, 2018 Tutorial expert report on network security technology.
Videotaped Deposition:
November 7, 2018
Attorneys: For Plaintiff: Kramer Levin, Naftalis, & Frankel LLP
For Defendant:
Status: Case closed

9/2017 – 9/2018 **Client: (Covington & Burling representing Huawei Device USA, Inc.)**

Case: Optis Wireless Technology, LLC, et. al. v. Huawei Technologies Co. Ltd, et. al.
Civil Action No. 2:17-cv-123-JRG-RSP

Location: UNITED STATES DISTRICT COURT FOR THE EASTERN DISTRICT OF TEXAS MARSHALL DIVISION – Hon. Roy S. Payne

Testifying expert regarding 3G and LTE technology.

Expert Declarations and Reports:

November 3, 2017: Declaration regarding Claim Construction.

March 26, 2018: Initial Expert Report Regarding Invalidity

April 23, 2018: Rebuttal Expert Report on Non-Infringement

April 27, 2018: Rebuttal Expert Report on Secondary Considerations

Videotaped Deposition: May 10, 2018

May 14, 2018: Declaration in support of Motion for Partial Summary Judgment

Jury Trial Testimony: August 22, 2018 and August 23, 2018

Attorneys: For Plaintiff: McKool Smith
For Defendant: Covington & Burling

Status: Jury award

6/2017 – 4/2018 **Client: Kramer Levin Naftalis & Frankel, LLP (representing Finjan, Inc.)**

Case: Finjan, Inc. v. Symantec, Inc.

Civil Action No. 4:14-cv-02998-HSG

Location: UNITED STATES DISTRICT COURT FOR THE NORTHERN DISTRICT OF CALIFORNIA OAKLAND DIVISION

As a testifying expert, provided a technology tutorial in this patent case involving internet security technology.

Expert Declaration:

July 27, 2017 Tutorial expert report on security technology.

Videotaped Deposition:

August 29, 2017

Attorneys: For Plaintiff: Kramer Levin, Naftalis, & Frankel LLP
For Defendant: Quinn Emmanuel

Status: Case settled

5/2017 – 3/2018 **Client: Barnes & Thornburg, LLP (representing Ooma, Inc.)**

Case: Ooma, Inc. (Petitioner) v. Deep Green Wireless, LLC (Patent Owner)

Location: UNITED STATES PATENT AND TRADEMARK OFFICE BEFORE THE
PATENT TRIAL AND APPEAL BOARD

As a testifying expert, provided a technology tutorial in this patent case involving
voice and data communications over wireless networks.

Expert Declaration:

June 8, 2017 Expert report on prior art wireless network technology.

Videotaped Deposition:

February 15, 2018

Attorneys: For Petitioner: Barnes & Thornburg LLP

For Defendant: Mischcon De Reya New York, LLP

Status: Case closed

3/2017 – 6/2019 **Client: Fish & Richardson (representing Apple, Inc.) / Gibson, Dunn &
Crutcher LLP (representing Compal Electronics, et. al.)**

Case: Apple Inc. v. Qualcomm Inc.

Qualcomm Inc. v. Compal Electronics, Inc., et. al.

Civil Action No. 3:17-cv-00108 / Civil Action No. 3:17-cv-01010

Location: UNITED STATES DISTRICT COURT FOR THE SOUTHERN DISTRICT OF
CALIFORNIA – Hon. Gonzalo P. Curiel, Magistrate Judge: Hon. Mitchell D.
Dembin

Testifying expert regarding LTE technology.

Expert Declaration:

December 11, 2017: Declaration regarding Claim Construction.

Expert Report:

June 29, 2018: Opening Expert Report regarding invalidity

August 3, 2018: Expert Report on infringement

October 2, 2018: Rebuttal Expert Report on Invalidity

Videotaped Deposition:

October 25, 2018

None

Attorneys: For Apple: Fish & Richardson

For Qualcomm: Quinn Emanuel Urquhart & Sullivan LLP / Cravath, Swaine & Moore LLP

For Compal Electronics, Inc., et. al: Gibson, Dunn & Crutcher LLP

Status: Case settled.

3/2017 – 1/2018 **Client: Kramer Levin Naftalis & Frankel, LLP (representing Finjan, Inc.)**

Case: Finjan, Inc. v. Blue Coat Systems, LLC

Civil Action No. 15-cv-03295-BLF-SVK

Location: UNITED STATES DISTRICT COURT FOR THE NORTHERN DISTRICT OF CALIFORNIA SAN JOSE DIVISION – Hon. Beth L. Freeman

As a testifying expert, provided an opening technology tutorial at trial in this patent case involving internet security technology.

Expert Declaration:

March 29, 2017 Tutorial expert report on security technology.

Videotaped Deposition:

May 2, 2017

October 31 – November 2, 2017: Jury Trial Testimony

January 8-10, 2018: Jury Trial Testimony (retrial after mistrial):

Live Testimony on Network Security Technology Tutorial

Attorneys: For Plaintiff: Kramer Levin, Naftalis, & Frankel LLP

For Defendant: Morrison & Forrester & Quinn Emmanuel

Status: Jury award

1/2017 – 7/2017 **Client: Foster Pepper LLP (representing Dali Wireless)**

Case: Dali Wireless, Inc. (Petitioner) v. CommScope Technologies, LLC (Patent Owner)

Location: UNITED STATES PATENT AND TRADEMARK OFFICE BEFORE THE PATENT TRIAL AND APPEAL BOARD

Testifying expert in this patent case involving RF transport networks.

Expert Reports:

4-26-17 Declaration ISO petition for IPR

6-30-17 Declaration ISO Opening claim construction brief

Videotaped Deposition:

July 24, 2017

Status: Case closed

1/2017 – 6/2019 **Client: Dorsey & Whitney LLP (representing Dali Wireless)**

Case: CommScope Technologies, LLC (Plaintiff/Counterclaim Defendant) v. Dali Wireless, Inc. (Defendant/Counterclaim Plaintiff)

Civil Action No.: 3:16-cv-477

Location: UNITED STATES DISTRICT COURT FOR THE NORTHERN DISTRICT OF TEXAS DALLAS DIVISION – Hon. Barbara M. G. Lynn

Testifying expert in this patent case involving RF transport networks.

Expert Reports:

8-24-18 Expert Report regarding Invalidity of CommScope patents

8-24-18 Expert Report regarding Infringement of Dali Wireless patents

11-5-18 Expert Report regarding Validity of Dali Wireless patents

11-5-18 Expert Report regarding Non-Infringement of CommScope patents

1-9-19 Declaration ISO opposition to MSJ

1-18-19 Declaration ISO partial MSJ on Non-infringement and Invalidity

5-2-19 Declaration ISO Motion for Sanctions

Videotaped Deposition:

November 20, 2018

Live Testimony at Jury Trial:

June 10-13, 2019

Attorneys: For Plaintiff: Dorsey & Whitney, LLC

For Defendant: Carlson Caspers, P.A.

Status: Jury award.

11/2016 – 4/2019 **Client: Boies, Schiller & Flexner LLP (representing Apple Inc.)**

Case: Evolved Wireless, LLC v. Apple, Inc.
Civil Action No.: 1:15-cv-00542-SLR
Location: UNITED STATES DISTRICT COURT FOR THE DISTRICT OF DELAWARE
– Hon. Sue L. Robinson
Testifying expert in this patent case involving LTE wireless networks.
Expert Reports:
11-06-17 Declaration ISO Summary Judgment of Validity
10-05-17 Declaration ISO Summary Judgment of Non-Infringement
10-03-17 Supplemental Expert Report on Non-Infringement
07-24-17 Supplemental Expert Report on Secondary Considerations of Non-Obviousness
6-26-17 Expert Report on Non-Infringement
5-22-17 Expert Report on Invalidity
Videotaped Deposition:
August 11, 2017
Live Testimony at Jury Trial:
March 29 - April 1, 2019

Attorneys: For Plaintiff: Boies, Schiller & Flexner LLP
For Defendant: Robins Kaplan LLP
Status: Jury verdict of non-infringement.

7/2016 – 4/2018 **Client: Jackson Walker LLP (representing D&M Holdings, Inc., *et. al.*)**

Case: Sonos, Inc., v. D&M Holdings, d/b/a The D+M Group, D&M Holdings U.S. Inc., and Denon Electronics (USA), LLC

Civil Action No.: 16-0141-RGA

D&M Holdings Inc., d/b/a The D+M Group, D&M Holdings U.S. Inc. v. Sonos, Inc.

Location: UNITED STATES DISTRICT COURT FOR THE DISTRICT OF DELAWARE
– Hon. Richard G. Andrews

Testifying expert in this patent case involving wireless speaker networks.

Expert Testimony:

9-11-17 Expert Report on Infringement

6-29-22 Remote Videotaped Deposition

Attorneys: For Plaintiff: Jackson Walker LLP

For Defendant: Potter Anderson & Corroon LLP

Status: Case settled

7/2016 – 1/2018 **Client: Kramer Levin Naftalis & Frankel, LLP (representing Finjan, Inc.)**

Case: Palo Alto Networks, Inc. (Petitioner) v. Finjan, Inc. (Patent Owner)

Case IPR2015-02001, Case IPR2016-00157. US Patent No. 8,225,408 B2

Case IPR2015-01974

Location: UNITED STATES PATENT AND TRADEMARK OFFICE BEFORE THE
PATENT TRIAL AND APPEAL BOARD

Testifying expert in this patent case involving wireless speaker networks.

Expert Declaration:

8-9-16 Expert Declaration, Patent 7,647,633

8-9-16 Expert Declaration, Patent 8,225,408

8-30-16 Supplemental Expert Declaration, 7,647,633

Status: Case settled

5/2016 – 7/2018 **Client: (Winston & Strawn LLP representing Atlantic Broadband Group, LLC, et. al.)**

Case: ChanBond LLC v. Atlantic Broadband Group, LLC, et. al.

Civil Action No: 15-842-RGA, 15-843-RGA, 15-844-RGA, , 15-845-RGA, , 15-846-RGA, , 15-847-RGA, , 15-848-RGA, , 15-849-RGA, , 15-850-RGA, , 15-851-RGA, , 15-852-RGA, , 15-853-RGA, , 15-854-RGA

Location: UNITED STATES DISTRICT COURT FOR THE DISTRICT OF DELAWARE
– Hon. Richard G. Andrews

Testifying expert regarding digital cable technology.

Expert Report:

10-24-17 Expert Report on Invalidity

Videotaped Deposition:

None

Attorneys: For Plaintiff: Bayard, P.A.
For Defendant: Winston & Strawn LLP
Status: Case settled

5/2016 – 11/2019 **Client: (Torys LLP representing Telus, Bell, and Rogers)**

Case: Wi-LAN Inc. v Telus Communications Company, Rogers Communications Canada Inc., and Bell Mobility Inc.

Court File No. T-301-16; Court File No. T-303-16; Court File No. T-304-16

Location: CANADIAN FEDERAL COURT – Hon. Mandy Ayles
Testifying expert regarding LTE technology.

Expert Report:

June 14, 2019 Expert Report regarding invalidity

Videotaped Deposition:

None

Attorneys: For Plaintiff: Torys LLP
For Defendant:
Status: Case settled

12/2015 – 4/2016 **Client: Kramer Levin Naftalis & Frankel, LLP (representing Acceleration Bay, LLC.)**

Case: Activision Blizzard, Inc., Electronic Arts Inc., Take-Two Interactive Software, Inc., 2K Sports, Inc., Rockstar Games, Inc., and Bungie, Inc., Petitioner v. Acceleration Bay, LLC, Patent Owner.

Case IPR2015-01951, Case IPR2015-01953, Case IPR2015-01964, Case IPR2015-01970, Case IPR2015-01996, Case IPR2016-00724, Case IPR2016-00747

Location: UNITED STATES PATENT AND TRADEMARK OFFICE BEFORE THE PATENT TRIAL AND APPEAL BOARD

Testifying expert in this IPR patent case involving internet data broadcasting.

Expert Declaration:

January 4, 2017 Supplemental Declaration ISO Patent Owner's Response -- Case IPR2016-00724

January 4, 2017 Supplemental Declaration ISO Patent Owner's Response -- Case

IPR2016-00747

December 7, 2016 Declaration ISO Patent Owner's Response – Case IPR2016-00724; Secondary Considerations of Non-Obviousness

December 7, 2016 Declaration ISO Patent Owner's Response – Case IPR2016-00747; Secondary Considerations of Non-Obviousness

July 17, 2016 Declaration ISO Patent Owner's Response – Patent 6,714,966; Secondary Considerations of Non-Obviousness

July 17, 2016 Declaration ISO Patent Owner's Response – Patent 6,829,634; Secondary Considerations of Non-Obviousness

July 17, 2016 Declaration ISO Patent Owner's Response – Patent 6,701,344; Secondary Considerations of Non-Obviousness

Videotaped Deposition:

February 7, 2017 and February 8, 2017

Attorneys: For Plaintiff: Kramer Levin, Naftalis, & Frankel LLP

For Defendant: DLA Piper

Status: Case closed

4/2016 – Present **Client: Kramer Levin Naftalis & Frankel, LLP (representing Acceleration Bay, LLC.)**

Case: Acceleration Bay, LLC v Activision Blizzard, Inc., Electronic Arts Inc., Take-Two Interactive Software, Inc.

Civil Action No.: 14-453 (RGA), 16-454 (RGA), 16-455 (RGA)

Location: UNITED STATES DISTRICT COURT FOR THE DISTRICT OF DELAWARE – Hon. Richard G. Andrews

Testifying expert in this IPR patent case involving internet data broadcasting.

Expert Declaration:

September 24, 2017: Expert Report Regarding Technology Benefits of the Asserted Patents

Videotaped Deposition: January 4, 2018

July 17, 2018: Reply Report Regarding Technology Benefits of the Asserted Patents

Attorneys: For Plaintiff: Kramer Levin, Naftalis, & Frankel LLP

For Defendant: DLA Piper

Status: Case ongoing

12/2015 – 9/2016 **Client: Kramer Levin Naftalis & Frankel, LLP (representing Finjan, Inc.)**

Case: Finjan, Inc. v. Sophos, Inc.
Civil Action No. 3:14-cv-01197-WHO

Location: UNITED STATES DISTRICT COURT FOR THE NORTHERN DISTRICT OF CALIFORNIA SAN FRANCISCO DIVISION – Hon. William H. Orrick

As a testifying expert, provided a technology tutorial in this patent case involving internet security technology.

Expert Declaration:
December 21, 2015 Tutorial expert report on network security technology.

Videotaped Deposition:
February 22, 2016

September 5 – 9, 2016 Jury Trial:
Live Testimony at Jury Trial regarding tutorial on network security

Attorneys: For Plaintiff: Kramer Levin, Naftalis, & Frankel LLP
For Defendant: DLA Piper

Status: Jury Trial

9/2015 – 2/2016 **Client: Brinks Gilson & Lione (representing LifeWatch Services, Inc., and Card Guard Scientific Survival, Ltd.)**

Case: Card Guard Scientific Survival Ltd.
Reexam Control No. 12/706,541

Location: UNITED STATES PATENT AND TRADEMARK OFFICE

Provided testimony in this Patent Office re-examination appeal.

Expert Declaration:
November 13, 2015 Declaration under 37 C.F.R §1.132.
February 13, 2016 Declaration ISO petition for IPR.

Attorneys: For Plaintiff: Brinks Gilson & Lione

Status: Re-examination appeal decision invalidated the patent.

9/2015 – 1/2017 **Client: Kramer Levin Naftalis & Frankel, LLP (representing Finjan, Inc.)**

Case: Finjan, Inc. v. Proofpoint, Inc. and Armorize Technologies, Inc.

Civil Action No. 13:cv-03999-BLF

Location: UNITED STATES DISTRICT COURT FOR THE NORTHERN DISTRICT OF CALIFORNIA SAN JOSE DIVISION – Hon. Howard R. Lloyd, Hon. Haywood S. Gilliam, Jr.

As a testifying expert, provided an opening technology tutorial report in this patent case involving internet security technology.

Expert Declaration:

October 7, 2015 Tutorial expert report on network security technology.

Videotaped Deposition:

November 6, 2015

Attorneys: For Plaintiff: Kramer Levin, Naftalis, & Frankel LLP

For Defendant: Quinn Emanuel

Status: Case settled

8/2015 – 12/2015 **Client: Brinks Gilson LLP (representing ZTE Corporation and ZTE (USA), Inc.)**

Case: Inter-System Handover of a Mobile Terminal Operable with a First and a Second Radio Access Network

ZTE v. Vringo Infrastructure, Inc.

Location: UNITED STATES PATENT AND TRADEMARK OFFICE BEFORE THE PATENT TRIAL AND APPEAL BOARD

Testifying expert in this IPR proceeding involving 3GPP cellular technology.

Expert Declarations:

08-28-15 Declaration ISO Petition for Inter Partes Review of U. S. Patent No. 7,126,940

09-04-15 Declaration ISO Petition for Inter Partes Review of U. S. Patent No. 7,242,943

09-04-15 Declaration ISO Petition for Inter Partes Review of U. S. Patent No. 7,558,283

09-04-15 Declaration ISO Petition for Inter Partes Review of U. S. Patent No. 8,812,000

09-04-15 Declaration ISO Petition for Inter Partes Review of U. S. Patent No. 7,724,720

10-12-15 Declaration ISO Petition for Inter Partes Review of U. S. Patent No. 7,242,933

Videotaped Deposition:

None

Attorneys: For Plaintiff:

For Defendant: Brinks Gilson, LLP

Status: Case settled.

11/2014 – Present **Client: Fish & Richardson (representing Regents of the University of Minnesota)**

Case: Regents of the University of Minnesota v. AT&T Mobility, LLC, Sprint Solutions, Inc., T-Mobile USA, Inc., Cellco Partnership d/b/a Verizon Wireless
Civil Action No. 14-cv-4666

Location: UNITED STATES DISTRICT COURT FOR THE DISTRICT OF MINNESOTA
– Hon. Tony N. Leung

Testifying expert on 3GPP error correction coding, precoding, and modulation.

May 12, 2023: Expert Deposition

April 14, 2023: Rebuttal Expert Report regarding Validity

Attorneys: For Plaintiff: Fish & Richardson

For Defendant:

Status: Case ongoing

10/2014 – 2/2015 **Client: Alston & Bird (representing Microsoft Corporation)**

Case: Microsoft Corporation. v. IPR Licensing, Inc.

Location: UNITED STATES PATENT AND TRADEMARK OFFICE BEFORE THE
PATENT TRIAL AND APPEAL BOARD

Testifying expert in this IPR proceeding involving cellular technology.

Expert Declarations:

10-16-14 Supplemental Declaration ISO Petition for Inter Partes Review of U. S. Patent No. 8,380,244

Attorneys: For Plaintiff: Alston & Bird LLP

For Defendant:

Status: Case settled

9/2014 – 4/2015 **Client: Reed & Scardino, LLP (representing Mobile Telecommunications Technologies, LLC)**

Case: Mobile Telecommunications Technologies LLC v. Amazon.com, Inc.

Civil Action No. 2:13-CV-883-JRG-RSP

Location: UNITED STATES DISTRICT COURT FOR THE EASTERN DISTRICT OF TEXAS MARSHALL DIVISION – Hon. Roy S. Payne

Testifying expert in this patent case involving package delivery notification systems.

Expert Reports:

4-06-15 Second Supplemental Expert Report on Infringement

2-10-15 Expert Report on Infringement

2-24-15 Supplemental Expert Report on Infringement

Videotaped Deposition:

2-25-15

Declaration:

3-20-15 Declaration ISO Response to Opposition Motion

Attorneys: For Plaintiff: Reed & Scardino LLP

For Defendant: Greenberg Traurig LLP

Status: Case settled

5/2014 – 7/2015 **Client: Kramer Levin Naftalis & Frankel, LLP (representing Finjan, Inc.)**

Case: Finjan, Inc. v. Blue Coat Systems, Inc.

Civil Action No. 3:13-cv-03999-BLF

Location: UNITED STATES DISTRICT COURT FOR THE NORTHERN DISTRICT OF CALIFORNIA SAN JOSE DIVISION – Hon. Beth L. Freeman

As a testifying expert, provided an opening technology tutorial at trial in this patent case involving internet security technology.

Expert Declaration:

January 12, 2015 Tutorial expert report on security technology.

Videotaped Deposition:

March 18, 2015

Live Jury Trial Testimony: July 20, 2015.

Live Bench Trial on Laches Testimony: September 8, 2015

Attorneys: For Plaintiff: Kramer Levin, Naftalis, & Frankel LLP

For Defendant: Wilson Sonsini

Status: Jury award.

4/2014 – 12/2014 **Client: Reed & Scardino, LLP (representing Mobile Telecommunications Technologies, LLC)**

Case: Mobile Telecommunications Technologies LLC v. United Parcel Service, Inc.
Civil Action No. 1:12-cv-03222-AT

Location: UNITED STATES DISTRICT COURT FOR THE NORTHERN DISTRICT OF
GEORGIA ATLANTA DIVISION – Hon. Amy Totenberg

Testifying expert in this patent case involving package delivery notification
systems.

Expert Reports:

7-3-14 Opening Expert Report regarding Infringement

8-11-14 Rebuttal Expert Report regarding Infringement

Videotaped Depositions:

10-7-14

Declaration:

11-24-14 Declaration ISO Response to MSJ

Attorneys: For Plaintiff: Reed & Scardino LLP

For Defendant: Alston & Bird LLP

Status: Case settled.

12/2013 – 9/2015 **Client: Brinks Gilson & Lione LLP (representing ZTE Corp, and ZTE (USA), Inc.)**

Case: ZTE Corporation and ZTE (USA) Inc. v. InterDigital Technology Corporation
Location: UNITED STATES PATENT AND TRADEMARK OFFICE BEFORE THE
PATENT TRIAL AND APPEAL BOARD

Testifying expert in this IPR proceeding involving cellular technology.

Expert Declarations:

3-21-14 Declaration in support of the Petition for Inter Partes Review of U. S.
Patent No. 8,380,244

Attorneys: For Plaintiff: Brinks Gilson & Lione
For Defendant: Latham & Watkins, LLP

Status: IPR Hearing before PTAB: All disputed claims are unpatentable.

12/2013 – 4/2014 **Client: Kramer Levin Naftalis & Frankel LLP (representing Sirius XM
Radio Inc.)**

Case: Catch a Wave Technologies, Inc. v. Sirius XM Radio Inc.
Case No. 3:12-cv-05791-WHA

Location: UNITED STATES DISTRICT COURT FOR THE NORTHERN DISTRICT OF
CALIFORNIA SAN FRANCISCO DIVISION – Hon. William Alsup

Testifying expert in this patent case involving satellite radio systems.

Expert Reports:

2-14-2014 Expert Report regarding non-infringement

Attorneys: For Plaintiff: Freitas Tseng & Kaufman LLP
For Defendant: Kramer Levin LLP

Status: Case settled

2/2013 – 7/2016 **Client: Reed & Scardino, LLP (representing Mobile Telecommunications
Technologies, LLC)**

Case: Mobile Telecommunications Technologies LLC v. BlackBerry Corporation.
Civil Action No. 3:12-cv-1652-M

Location: UNITED STATES DISTRICT COURT FOR THE NORTHERN DISTRICT OF
TEXAS DALLAS DIVISION – Hon. Barbara M. G. Lynn

Testifying expert in this patent case involving package delivery notification
systems.

Expert Reports:

9-3-15 Expert Report on Infringement

Videotaped Depositions:

November 18, 2015

Live Testimony at Jury Trial: July 13, 2016.

Attorneys: For Plaintiff: Baker Botts, LLP

For Defendant: Reed & Scardino LLP

Status: Jury verdict of non-infringement.

9/2013 – 1/2014 **Client: Reed & Scardino, LLP (representing Mobile Telecommunications Technologies, LLC)**

Case: Mobile Telecommunications Technologies, LLC v Clearwire Corporation

Civil Action No. 2:12-CV-308

Location: UNITED STATES DISTRICT COURT FOR THE EASTERN DISTRICT OF TEXAS MARSHALL DIVISION – Hon. Roy S. Payne

Testifying expert in this patent case involving wireless networking signals.

Expert Reports:

11-11-13 Rebuttal report regarding validity

Videotaped Depositions:

12-5-13

Declarations:

1-23-14 Declaration before the Patent Trial and Appeal Board in Case IPR2013-00306

Attorneys: For Plaintiff: Reed & Scardino LLP

For Defendant: Shook, Hardy & Bacon, LLP

Status: Case settled

10/2013 – 5/2015 **Client: Foley & Lardner, LLP (representing Motorola Mobility, LLC)**

Case: University of Florida Research Foundation Inc., and Rapid Mobile Technologies, Inc. v Motorola Mobility, LLC.

Case No. 13-cv-61120-KMM-EGT

Location: UNITED STATES DISTRICT COURT FOR THE SOUTHERN DISTRICT OF
FLORIDA FORT LAUDERDALE DIVISION – Hon. K. Michael Moore,
Magistrate Judge: Hon. Edwin G. Torres

Testifying expert in this patent case involving mobile device testing systems.

Expert Reports:

None.

Declarations:

11-21-13 Declaration ISO Motorola’s Responsive Claim Construction Brief

Attorneys: For Plaintiff: Meltzer & Meksraitis

For Defendant: Foley & Lardner LLP

Status: Case settled

7/2013 – 6/2015 **Client: WilmerHale (representing Broadcom)**

Case: Inter Partes Review of US Patent 6,424,625; 6,772,215; and 6,466,568 owned by
Ericsson

Docket No. 0111168-0240

Location: UNITED STATES PATENT AND TRADEMARK OFFICE BEFORE THE
PATENT TRIAL AND APPEAL BOARD

Testifying expert in this Inter Partes Review regarding ARQ mechanisms.

Expert Declarations:

9-19-13 Declaration regarding US Patent 6,772,215

9-19-13 Declaration regarding US Patent 6,466,568

9-29-13 Declaration regarding US Patent 6,424,625

Videotaped Deposition:

5-29-14, and 5-30-14

Attorneys: For Plaintiff: Meltzer & Mathis

For Defendant: Wilmer Cutler Pickering Hale and Dorr LLP

Status: IPR Petition granted. All claims invalidated

4/2013 – 4/2015 **Client: Kilpatrick Townsend & Stockton LLP (representing Google Inc. and Motorola Mobility LLC)**

Case: Fujifilm Corporation v. Motorola Mobility LLC

Case No. 3:12-cv-03587 WHO

Location: UNITED STATES DISTRICT COURT FOR THE NORTHERN DISTRICT OF CALIFORNIA SAN FRANCISCO DIVISION – Hon. Richard Seeborg

Testifying expert in this patent case involving smartphone technology.

Expert Declarations:

4-23-14 Declaration ISO Motion for Protective Order

12-9-14 Declaration ISO MSJ

Expert Reports:

10-3-14 Opening Expert Report Regarding Invalidity

10-31-14 Rebuttal Expert Report on non-infringement

10-31-14 Appendix A to Rebuttal Report of Dr. Alan Bovik

Videotaped Deposition:

11-19-14, and 11-20-14

Trial Testimony:

April 28, 2015 Non-infringement and invalidity of '970 Patent

Attorneys: For Plaintiff: Morgan, Lewis & Bockius LLP

For Defendant: Kilpatrick Townsend & Stockton LLP

Status: Jury verdict: '970 Patent claims not infringed and invalid.

2/2013 – 10/2013 **Client: Seyfarth Shaw LLP (representing Motorola Mobility LLC)**

Case: University of Florida Research Foundation, Inc. and Rapid Mobile Technologies, Inc. v. Motorola Mobility LLC

Civil Action No. 13-cv-61120-KMM-EGT

Location: UNITED STATES DISTRICT COURT FOR THE SOUTHERN DISTRICT OF FLORIDA – Hon. K. Michael Moore, Magistrate Judge: Hon. Edwin G. Torres

Testifying expert in this employment law case involving mobile device testing systems.

Expert Reports:

3-1-13 Expert Report regarding Non-Infringement

4-1-13 Declaration in Opposition to Plaintiff's MSJ

Attorneys: For Plaintiff: Meltzer & Mathis
For Defendant: Seyfarth Shaw LLP
Status: Case settled

5/2012 – 4/2013 **Client: Paul Hastings LLP (representing Apple, Inc.)**

Case: SmartPhone Technologies, LLC v Research in Motion Corporation, et. al.
Case No. 6:10-cv-00074

Location: UNITED STATES DISTRICT COURT FOR THE EASTERN DISTRICT OF
TEXAS TYLER DIVISION – Hon. John D. Love

Testifying expert in this patent case involving 3GPP technology.

Expert Reports:

12-31-12 Appendix A to Rebuttal Expert Report of Dr. David Wilson

3-13-13 Appendix A to Supplemental Expert Report of Dr. David Wilson

Attorneys: For Plaintiff: Mintz Levin Cohn Ferris Glovsky and Popeo PC
For Defendant: Paul Hastings LLP
Status: Case settled

8/2012 – 9/2013 **Client: Reed & Scardino, LLP (representing EON Corp. IP Holdings, LLC)**

Case: EON Corp. IP Holdings, LLC v. SKYGUARD, LLC et. al.
Case No. 6:11-cv-00015-LED

Location: UNITED STATES DISTRICT COURT FOR THE EASTERN DISTRICT OF
TEXAS TYLER DIVISION – Hon. John D. Love

Testifying expert in this patent case involving RF technology for WiFi
networking.

Expert Reports:

2-15-13 Expert Report regarding Infringement

Videotaped Deposition:

4-09-13

Attorneys: For Plaintiff: Reed & Scardino, LLP

For Defendant: K&L GATES LLP

Status: Case settled

5/2012 – 6/2014 **Client: Reed & Scardino LLP (representing Eon Corp. IP Holdings)**

Case: Eon Corp. IP Holdings, LLC v. Landis+Gyr, Inc., et. al.

Case No. 6:09-cv-00317-LED-JDL

Location: UNITED STATES DISTRICT COURT EASTERN DISTRICT OF TEXAS
TYLER DIVISION – Hon. John D. Love

Testifying expert in this patent case involving two-way wireless networks, before Judge Love.

Expert Report:

7-8-13 Expert Report regarding Infringement by Silver Spring Networks, Inc.

7-8-13 Expert Report regarding Infringement by Itron, Inc.

Videotaped Deposition: September 12, 2013

Live Testimony at Jury Trial: June 2, 2014 – June 6-2014

Attorneys: For Plaintiff: Reed & Scardino LLP

For Defendant: Dentons, LLP

Status: Jury award. All patents found valid and infringed.

3/2012 – 3/2014 **Client: Perkins Coie (representing Intel Corporation)**

Case: Stragent LLC, et. al. v. Intel Corp.,

Case No. 6:11-cv-421-LED (E.D. Tex.)

Location: UNITED STATES DISTRICT COURT FOR THE EASTERN DISTRICT OF
TEXAS TYLER DIVISION – Hon. Timothy Dyk, Hon. John D. Love

Testifying expert in this patent case involving the use of error detection technology in computer networking, before Judge Dyk.

Expert Reports:

08-23-13 Expert Report regarding Invalidity

09-23-13 Expert Report regarding Non-Infringement

Videotaped Deposition:

10-08-13, and 10-09-13

Jury trial testimony:

3-13-2014 Live trial testimony on non-infringement and invalidity before Judge Timothy Dyk

Attorneys: For Plaintiff: Nelson, Bumgardner & Casto

For Defendant: Perkins Coie

Status: Jury verdict for non-infringement and invalidity

2/2012 – 09/2015 **Client: Dewey & LeBoeuf LLP (representing Harris Corporation)**

Case: Harris Corporation v. Ruckus Wireless, Inc.

Case No. 6:11-cv-00618-CEM-CRS

Location: UNITED STATES DISTRICT COURT FOR THE MIDDLE DISTRICT OF FLORIDA ORLANDO DIVISION – Hon. Charlene Edwards Honeywell

Testifying expert in this patent case involving RF technology for WiFi networking.

Expert Reports:

3-5-12 Expert Report regarding Infringement

3-6-12 Supplemental Expert Report regarding Infringement

4-6-12 Expert Report regarding Validity

Declarations:

5-30-12 Declaration ISO Claim Construction

6-18-12 Declaration ISO Markman Motion

1-23-15 Declaration ISO Responsive Markman Brief

3-6-15 Supplemental Expert Report regarding Infringement

4-3-15 Rebuttal Expert Report regarding Validity

Videotaped Deposition:

4-30-12

Attorneys: For Plaintiff: Dewey & LeBeouf LLP

For Defendant: Lewis and Roca LLP

Status: Case settled

2/2012 – 2/2013 **Client: Common-Interest-Group (representing Nokia, Huawei, ZTE)**

Case: InterDigital Communications LLC, et. al. v. Huawei Tech Co., LTD., et. al.

Certain Wireless Devices With 3G Capabilities and Components Thereof

U.S. Int'l Trade Commission Inv. No. 337-TA-800

Location: UNITED STATES INTERNATIONAL TRADE COMMISSION –
Administrative Law Judge Hon. David P. Shaw and Administrative Law Judge
Hon. Theodore R. Essex

Testifying expert in this patent case involving 3G wireless, WiFi, and WCDMA
technology.

Expert Reports:

11-30-12 Expert Report regarding Non-infringement

7-31-12 Expert Report regarding Invalidity

11-19-10 Rebuttal Expert Report regarding Validity

12-6-10 Supplemental Expert Report regarding Infringement

Videotaped Deposition:

12-14-12, 12-15-12

ITC Trial testimony:

2-6 through 2-15/13 Non-infringement and Invalidity witness statements, live
testimony

Attorneys: For Plaintiff: Latham & Watkins, LLP

For Defendant: Alston & Bird, Covington & Burling, Brinks Hofer

Status: ITC hearing verdict: All patents not infringed and invalid

9/2010 – 4/2011 **Client: Reed & Scardino LLP (representing Eon Corp. IP Holdings)**

Case: Eon Corp. IP Holdings, LLC v. Sensus USA, Inc., et. al.

Case No. 6:09-cv-00116-LED-JDL

Location: UNITED STATES DISTRICT COURT EASTERN DISTRICT OF TEXAS
TYLER DIVISION – Hon. John D. Love

Testifying expert in this patent case involving two-way wireless networks

Expert Report:

10-22-10 Expert Report regarding Infringement (Sensus USA, Inc)

11-7-10 Expert Report regarding Infringement (Bell Industries)

11-19-10 Rebuttal Expert Report regarding Validity

12-6-10 Supplemental Expert Report regarding Infringement

Declaration:

12-28-10, 1-18-11

Videotaped Deposition:

12-8-10, 2-3-11

Attorneys: For Plaintiff: Reed & Scardino LLP

For Defendant: Jones Day

Status: Case settled

10/2009 – 2/2010 **Client: White & Case LLP (representing Marvell)**

Case: Marvell Semiconductor, Inc., et. al. v. Commonwealth Scientific Industrial Research Organisation

Case No. 6:07-CV-204 (LED)

Location: UNITED STATES DISTRICT COURT EASTERN DISTRICT OF TEXAS TYLER DIVISION – Hon. Leonard Davis

Testifying expert in this patent case involving wireless LAN protocols.

Expert Report:

11-24-09 Rebuttal Expert Report

Videotaped Deposition:

01-07-10

Attorneys: For Plaintiff: White & Case LLP

For Defendant: Townsend and Townsend and Crew LLP

Status: Case settled

9/2009 – 2/2010 **Client: Perkins Coie Brown & Bain PA (representing Intel)**

Case: Saxon Innovations, LLC v. Apple, Inc., et. al.

Case No. 6:08-cv-00265-LED

Location: UNITED STATES DISTRICT COURT FOR THE EASTERN DISTRICT OF TEXAS TYLER DIVISION – Hon. John D. Love

Testifying expert in this patent case involving wireless technology.

Declarations:

12-04-09 Declaration Regarding Claim Construction

Videotaped Deposition:

01-19-10

Attorneys: For Plaintiff: Susman Godfrey LLP

For Defendant: Perkins Coie Brown & Bain LLP

Status: Case settled

8/2008 – 10/2009 **Client: Reed & Scardino LLP (representing Eon Corp. IP Holdings)**

Case: Eon Corp. IP Holdings, LLC v. Verizon Clinton Center Drive Corp., et. al.

Case No. 6:08-cv-00385

Location: UNITED STATES DISTRICT COURT FOR THE EASTERN DISTRICT OF TEXAS TYLER DIVISION – Hon. John D. Love

Testifying expert in this patent case involving two-way wireless networks

Expert Report:

06-22-10 Expert Report

08-16-10 Supplemental Expert Report

Videotaped Depositions:

08-18-10, 08-26-10

Attorneys: For Plaintiff: Reed & Scardino LLP

For Defendant: Simpson Thacher & Bartlett LLP

Status: Case settled

4/2008 – 3/2009 **Client: McDermott, Will & Emery LLP (representing GE Licensing)**

Case: CIF Licensing, LLC d/b/a GE Licensing v. Agere Systems, Inc.

Case No. 07-170 (JJF)

Location: UNITED STATES DISTRICT COURT FOR THE DISTRICT OF DELAWARE – Hon. Joseph. J. Farnan, Jr.

Testifying expert in this patent case involving modem technology.

Expert Report:

09-05-08 Rebuttal Expert Report

Non-videotaped Depositions:

9-24-08, 9-26-08

Jury trial testimony:

2-04-09

Attorneys: For Plaintiff: McDermott, Will & Emery LLP

For Defendant: Townsend and Townsend and Crew LLP

Status: Jury award. 2 patents infringed and valid, remaining 2 patents non-infringed

2/2008 – 5/2010, **Client: Simpson Thacher & Bartlett LLP (representing Cisco Systems, Inc.)**
2/2011 – 4/2011

Case: Commil USA, LLC v. Cisco Systems, Inc., et. al.

Case No. 2:07-CV-341-DF-CE

Location: UNITED STATES DISTRICT COURT EASTERN DISTRICT OF TEXAS
MARSHALL DIVISION – Hon. Charles Everingham IV

Testifying expert on invalidity regarding short range communication protocols.

Opening Expert Report

12-23-09

Videotaped Depositions:

02-09-10

Attorneys: For Plaintiff: Sayles Werbner

For Defendant: Simpson Thacher & Bartlett LLP

Status: Jury award for original trial and retrial: patents found valid and infringed.

6/2007 – 4/2009 **Client: Common Interest Group of Co-Defendants**

11/2010 – 4/2012 **Client: Common Interest Group of Co-Defendants**

Case: Commonwealth Scientific and Industrial Research Organisation v. Toshiba
America Information Systems, Inc., et. al.

Case No. 6:06-cv-00550-LED

Case No. 6:09-CV-0399 (LED)

Location: UNITED STATES DISTRICT COURT EASTERN DISTRICT OF TEXAS
TYLER DIVISION – Hon. Leonard Davis

Testifying expert in this patent case involving wireless LAN technology.

Declarations:

06-05-08 Regarding claim construction

12-17-08 Supporting opposition to summary judgment

04-05-09 Supporting motion for reconsideration

02-24-12 Supporting opposition to summary judgment

Expert Reports:

10-08-08 Rebuttal Expert Reports- Re: TI Chips, Re: Marvell Chips, Re: Airgo Chips, Re: Broadcom Chips, Re: Conexant Chips, Re: Ralink Chips, Re: Atheros Chips

01-27-12 Rebuttal Expert Reports- Re: TI Chips, Re: Broadcom Chips, Re: Ralink Chips, Re: Atheros Chips

Videotaped Depositions:

11-1-08, 11-2-08, 02-14-12

Attorneys: For Plaintiff: Townsend & Townsend LLP

For Defendant: Keker & Van Nest, LLP

Status: Jury trial: patents found valid and infringed.

10/2006 – 8/2009 **Client: Keker & Van Nest (representing Comcast Corporation)**

Case: Rembrandt Technologies, Inc. v. Comcast Corporation

Case No. 2-05-CV-000443 (TJW)

Location: UNITED STATES DISTRICT COURT EASTERN DISTRICT OF TEXAS
MARSHALL DIVISION – Hon. T. John Ward

Testifying expert in this patent case involving physical layer and data link layer communication protocols for cable networks.

Declaration:

01-10-07 Support of Claim Construction Brief

Videotaped Deposition:

12-22-06 Regarding claim construction opinions

Attorneys: For Plaintiff: McKool Smith

For Defendant: Keker & Van Nest

Status: Case settled

3/2007 – 5/2007 **Client: Niro, Scavone, Haller and Niro (representing MLR, LLC)**

Case: MLR, LLC v. Kyocera Wireless Corporation and Novatel Wireless, Inc.
Case No. 05-CV-0935 B (AJB)

Location: UNITED STATES DISTRICT COURT SOUTHERN DISTRICT OF CALIFORNIA

Testifying expert in this patent case involving cellular phone technology.

Expert Report:

04-20-07 Expert Report regarding infringement

Attorneys: For Plaintiff: Niro, Scavone, Haller, and Niro

For Defendant: Hogan & Hartson, LLP

Status: Case settled

6/2006 – 10/2006 **Client: Thompson & Knight (representing Ericsson, Inc.)**

Case: Fenner Investments, Ltd., v. Juniper Networks, Inc. et. al.
Case No. 2:05–CV–05 JDL

Location: UNITED STATES DISTRICT COURT EASTERN DISTRICT OF TEXAS
MARSHALL DIVISION

Testifying expert in this patent case involving wireless communications services.

Expert report regarding infringement and invalidity

5-23-06 Rebuttal expert report regarding infringement and invalidity

Attorneys: For Plaintiff: Fulbright & Jaworski

For Defendant Ericsson: Thompson & Knight

Status: Case settled

12/2003 – 5/2006 **Client: Howrey LLP/ Winston & Strawn LLP (representing McKesson Information Solutions, Inc.)**

Case: McKesson Information Solutions, Inc. vs. Bridge Medical, Inc.
Case No. CIV S-02-2669 FCD KJM

Location: UNITED STATES DISTRICT COURT EASTERN DISTRICT OF CALIFORNIA – Hon. Peter A. Nowinski

Testifying expert in this patent case involving a patient on a patient identification and verification system that incorporates wireless technology.

Inequitable Conduct Trial live testimony:

5-04-06

Markman Hearing live testimony:
6-29/30-05

Videotaped Depositions:
2-14-04, 6-3-05

Declarations:

12-1-03 Dec. in support of MISI's Opening/Opposition re Claim Construction

12-24-04 Dec. in support of MISI's Motion for Preliminary Injunction

3-1-04 Dec. in support of Claim Construction

6-29-04 Dec. re meaning of "Communication"

7/15/05 Dec. in support of MISI's Opposition to Bridge's Motion for
Summary Judgment

Attorneys: For Defendant: Morrison & Foerster

For Plaintiff: Howrey Simon, Winston & Strawn, Morgan Lewis

Status: Bench trial on inequitable conduct: Verdict found inequitable conduct.

07/2003–02/2006 **Client: Heller Ehrman LLP (representing Texas Instruments, Inc.)**

Case: Texas Instruments, Inc. and Stanford University vs. GlobespanVirata, Inc.

Provided discovery of evidence used at trial, concerning the structure and operation of Globespan's ADSL products, and supported litigators in depositions of Globespan engineers.

Attorneys: For Plaintiff: Heller Ehrman

For Defendant: Covington & Burling, LLP

Status: Jury award.

Patents

<u>Patent Number</u>	<u>Date Issued</u>	<u>Title</u>
10,332,121	June 25, 2019	Light-based Data Entry for Personal Inventory and Product Support System
9,978,037	May 22, 2018	Personal inventory and product support system
8,995,996	March 31, 2015	Methods and apparatus for performance optimization of heterogeneous wireless system communities
8,935,580	January 13, 2015	Multimedia-aware quality-of-service and error correction provisioning

8,468,426	June 18, 2013	Multimedia-aware quality-of-service and error correction provisioning
8,189,538	May 29, 2012	Reconfiguration of a communication system
8,144,640	March 27, 2012	Location tracking in a wireless communication system using power levels of packets received by repeaters
8,064,380	November 22, 2011	Reconfiguration of a communication system
8,027,637	September 27, 2011	Single frequency wireless communication system
7,957,741	June 7, 2011	Token-based receiver diversity
7,876,704	January 25, 2011	Tunneling protocols for wireless communications
7,689,210	March 30, 2010	Plug-n-playable wireless communication system
7,672,274	March 2, 2010	Mobility support via routing
7,668,542	February 23, 2010	Token-based receiver diversity
7,515,557	Apr 7, 2009	Reconfiguration of a communication system
7,236,470	Jun 26, 2007	Tracking multiple interface connections by mobile stations
7,149,196	Dec 12, 2006	Location tracking in a wireless communication system using power levels of packets received by repeater
6,965,769	Nov 15, 2005	Testing Center
6,862,448	Mar 1, 2005	Token-based receiver diversity
6,788,658	Sep 7, 2004	Wireless communication system architecture having split MAC layer
6,760,318	Jul 6, 2004	Receiver diversity in a communication system
6,557,134	Apr 29, 2003	ARQ method for wireless communication
6,259,911	Jul 10, 2001	Network operations center hardware and software design

Education

<u>Year</u>	<u>College/University</u>	<u>Degree</u>
1993	Stanford University	PhD, Electrical Engineering Thesis: "Trellis Coding for Multi-Level, Partial-Response Continuous Phase Modulation with Precoding"
1988	Stanford University	MS, Electrical Engineering
1985	Rensselaer Polytechnic Institute	BS, Computer and Systems Engineering

Publications

- Goldhamer, M., Grandblaise, D., Bims, H., Feng, S., Piggin, P., Sydor, J., and Wu, X. “Coexistence between 802.16 Systems Operating in Shared Bands”, *Radio Resource Management in WiMAX*, John Wiley & Sons, 2009.
- Bims, Harry. “Surveying the Wireless LANdscape. Or Why Large Wi-Fi Networks Require Good Planning.” *Xchange*. [Online] Available <http://www.xchangemag.com/articles/391supsys1.html>, September 1, 2003.
- Bims, Harry. “Building Voice-Ready Wireless LANs” *Wireless Week*. [Online] Available <http://www.wirelessweek.com/article/CA319429.html?spacedesc=Departments>, September 1, 2003.
- Bims, Harry. “Enabling Voice over WLANs”. White Paper. [Online] Available. http://airflownetworks.com/solutions/pdf/vowlan_wp.pdf. September 2003.
- Bims, Harry. “Securing Enterprise WLANs”. White Paper. [Online] Available. http://web.archive.org/web/20040303212529/airflownetworks.com/solutions/pdf/securing_wlans_wp.pdf. August 2003.
- Bims, H. and Cioffi, J. “Trellis Coding for Full-Response CPM”, *Third Generation Wireless Information Networks*, Kluwer Academic Publishers, 1992.
- Bims, H. and Cioffi, J. “Trellis Coding for Full-Response CPM”, *WINLAB WORKSHOP*, East Brunswick, NJ. October 18-19, 1990.
- Bims, H. and Cioffi, J. “Trellis Coding for Partial-Response CPM”, *1991 International Symposium on Information Theory*, Budapest, Hungary. June 24-28, 1991.
- Bims, H. and Cioffi, J. “Trellis Coding with M-ary MSK Constraints”, *GLOBECOM '89*, Dallas TX. Nov. 1989.

Professional Associations and Achievements

- Jan 2009 – Present Vice-Chair and Board of Directors, Menlo Park Chamber of Commerce
- Nov 2007 – Sep 2010 Vice-Chair and Secretary, IEEE 802.16h License Exempt Group
- Feb 2002 – Jan 2011 Member, City of Menlo Park Planning Commission (2006 Chairperson, 2005 Vice-Chairperson)
- Feb 2012 – Present Senior Member, IEEE

- Jan 2000 – Dec 2000 Chair, IEEE Engineering Management Society – Silicon Valley Chapter
- Jun 1985 - Jun 1991 AT&T Bell Laboratories Cooperative Research Fellow