UNITED STATES PATENT AND TRADEMARK OFFICE

_____

BEFORE THE PATENT TRIAL AND APPEAL BOARD

_____

EXACQ TECHNOLOGIES, INC.,

Petitioner,

v.

JDS TECHNOLOGIES, INC.,

Patent Owner.

_____

U.S. Patent No. 8,185,964

IPR Case No.: 2016-00567

_____

PATENT OWNER'S PRELIMINARY RESPONSE TO PETITION FOR *INTER PARTES* REVIEW UNDER 37 C.F.R. § 42.107

TABLE OF CONTENTS

Table of Authorities

Cases

Statutes

Other Authorities

Rules

I. INTRODUCTION

Pursuant to 35 U.S.C. § 313 and 37 C.F.R. § 42.107, Patent Owner, JDS Technologies, Inc. ("Patent Owner"), submits the following Preliminary Response to the Petition for *Inter Partes* Review filed by Exacq Technologies, Inc. ("Petitioner") regarding claims 1-4 of U.S. Patent No. 8,185,964 ("the '964 patent").[1] Patent Owner respectfully requests that the Patent Trial and Appeal Board deny institution on every ground because, as explained in detail below, Petitioner has failed to show a reasonable likelihood of prevailing on any of the asserted grounds.

Petitioner's Ground 1 based on 35 U.S.C. § 102 fails to establish anticipation under the applicable legal standards. As set forth below, Ground 1 of the Petition should be rejected because the single prior art reference used by Petitioner does not expressly or inherently disclose each and every limitation as recited in claims 1 and 3. Rather, Petitioner relies on assertions "that a certain

[1] Claims of the '964 patent are the subject of two currently-pending IPR petitions: (1) IPR2016-00511 (claims 1-4); and (2) IPR2016-00567 (claims 1-4). Furthermore, certain claims of U.S. Patent No. 6,891,566—the parent patent of the '964 patent—are the subject of four additional IPR petitions: (1) IPR2016-00520 (claims 1, 6-10, 16-24, and 28); (2) IPR2016-00532 (claims 29-46); (3) IPR2016-00522 (claims 47-54); and (4) IPR2016-00568 (claims 1-10, 23-28 and 49-54).

thing may result" to argue that claims 1 and 3 are anticipated. Petitioner has not met its required proofs.

Institution should also be denied on both obviousness grounds because Petitioner's assertions of obviousness comprise a collection of conclusory statements, which ignore fundamental differences among the references themselves and between the proposed prior art combinations and the limitations of the challenged claims. As explained in detail below, Petitioner's reasoning is unduly vague and premised in nothing more than impermissible hindsight. Because they fail to provide persuasive analysis supporting Petitioner's conclusions of obviousness and lacks a cogent explanation of the motivation underpinning the combination of prior art teachings, the Board should deny the Petition in its entirety. Moreover, the proposed combinations of prior art references fail to meet a number of explicit limitations of the challenged claims as set forth herein.

As explained in the Office Patent Trial Practice Guide, the Board "may not authorize a trial where the information presented in the petition, taking into account any patent owner preliminary response, fails to meet the requisite standard for instituting the trial." 77 Fed. Reg. at 48,756 (Aug. 14, 2012); *see, e.g.*, 35 U.S.C. §§ 314, 324. Although it is not possible to fully address each and every deficiency of the Petition, Patent Owner respectfully submits that the deficiencies highlighted in this response preclude trial on any asserted grounds. *See,*

Travelocity.com L.P. et al. v. Cronos Technologies, LLC, CBM2014-00082, Paper 12 at 10 (Oct. 16, 2014) ("nothing may be gleaned from the Patent Owner's challenge or failure to challenge the grounds of unpatentability for any particular reason").

II. STANDARD FOR GRANTING *INTER PARTES* REVIEW

The Board has discretion to "deny some or all grounds for unpatentability for some or all of the challenged claims." 37 C.F.R. § 42.108(b); *see* 35 U.S.C. § 314(a). Petitioner bears the burden of demonstrating a reasonable likelihood that it would prevail in showing unpatentability on the grounds asserted in its petition. 37 C.F.R. § 42.108(c). The Board may only grant a petition for *inter partes* review where "the information presented in the petition . . . shows that there is a reasonable likelihood that the petitioner would prevail with respect to at least 1 of the claims challenged in the petition." 35 U.S.C. § 314(a); 37 C.F.R. § 42.108(c). Petitioner bears the burden of showing that this statutory threshold has been met. *See,* Office Patent Trial Practice Guide, 77 Fed. Reg. 48,756 (Aug. 14, 2012) [hereinafter "Practice Guide"] ("The Board. . . may institute a trial where the petitioner establishes that the standards for instituting the requested trial are met. . . ."). If *inter partes* review is granted, Petitioner then has the burden of proving unpatentability by a preponderance of the evidence. 35 U.S.C. § 316(e). As explained below, neither burden is met here.

Ground 1 is based on anticipation under 35 U.S.C. § 102. Petitioner must show where each claim limitation is found in a single reference, and the reference must enable one of skill in the field of the invention to make and use the claimed invention. *Merck & Co., Inc. v. Teva Pharmaceuticals USA, Inc.,* 347 F.3d 1367, 1372 (Fed. Cir. 2003); *Crown Packaging Tech., Inc. v. Ball Metal Beverage Container Corp.,* 635 F.3d 1373, 1383 (Fed. Cir. 2011) ("But disclosure of each element is not quite enough – [the Federal Circuit] has long held that '[a]nticipation requires the presence in a single prior art disclosure of a claimed invention *arranged as in the claim.*'" (citation omitted) (emphasis in original)).

Grounds 2 and 3 advanced by Petitioner in this Petition are based on claims of obviousness under 35 U.S.C. § 103. In connection with such grounds, Petitioner must show where each claim limitation is found in the prior art. *See, e.g.*, *Kinetic Concepts, Inc. v. Smith & Nephew, Inc.*, 688 F.3d 1342, 1360 (Fed. Cir. 2012). Failure to do so defeats a claim of obviousness. *Id.* The Office Patent Trial Practice Guide specifies that among the many responses a patent owner can submit to a petition include: "The prior art lacks a material limitation in all of the independent claims. . . . The prior art teaches or suggests away from a combination that the petitioner is advocating." Practice Guide, 77 Fed. Reg. at 48,764. The Petition fails for both of these reasons. Additionally, Petitioner's minimal discussion of the rationale to combine the cited references lacks the requisite

specificity to explain why one of ordinary skill would have been prompted to combine the prior art references and how such a combination would have worked.

III. U.S. PATENT NO. 8,185,964

A. Overview of Patent Owner and its Patented Technology

For nearly 20 years, Patent Owner, JDS, has developed, marketed and sold a suite of software applications and hardware systems for effectively and efficiently managing video received from networked surveillance cameras. The innovations described in the '964 patent—which depends from and shares a specification with U.S. Patent No. 6,891,566 ("the '566 patent")—are directly related to this work. In general, the claims of the '964 patent are directed to methods for controlling access by computers and computer programs to video servers and hardware devices, respectively, in relation to the licensing of video surveillance software.

JDS'S PATENTED TECHNOLOGY

Figure 1 of the '964 patent, reproduced below, illustrates the general network architecture associated with certain embodiments of the invention.

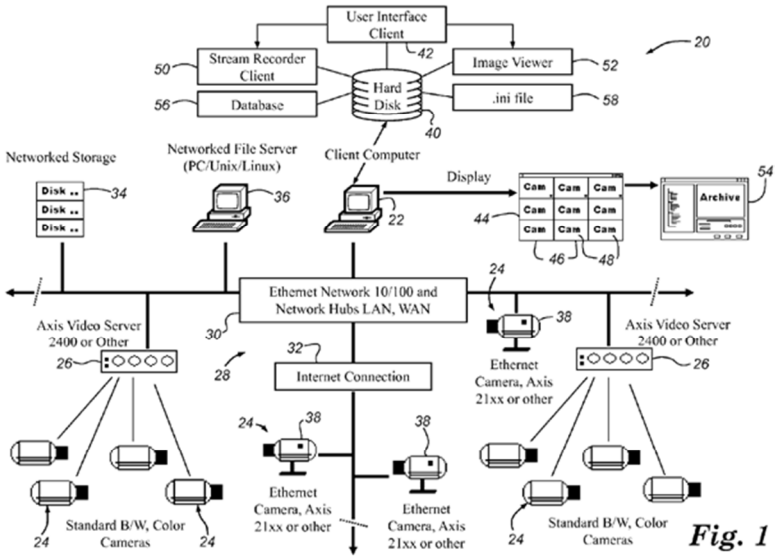

Fig. 1

'964 PATENT, FIGURE 1

B. Patent Owner's Licensing Innovation and the Challenged Claims of the '964 Patent

The claims at issue in this Petition—*i.e.*, 1-4—relate to methods for controlling access by computers and computer programs to video servers and hardware devices, respectively. The challenged claims describe novel computerized processes and software licensing techniques that are not found in the prior art.

In 1999, Patent Owner was confronted with a problem that many technology companies have faced over the years—the problem of unauthorized software usage. The ease with which software can be copied and used unlawfully creates both an enormous challenge and cost for software developers. A number of

approaches for combating unauthorized software use and software piracy have been developed over the years. In 1999, the inventor of the'964 patent developed a new technological solution to this problem.

The challenged claims of the '964 patent are directed to Patent Owner's innovative technology for protecting against unauthorized software use. Previous approaches employed localized methods that ensured a given software program was only installed on, and used with, approved computers. The '964 patent took a completely different and revolutionary approach to piracy protection. The '964 patent's solution allows for video surveillance software to be installed on any number of computers, at any location, without concern for theft. Rather than placing controls on the particular computer running the software, Patent Owner's patented approach restricts the software's use based on unique identifiers—*e.g.*, hardware addresses—stored in protected areas of peripheral hardware devices. The challenged claims require "determining if the computer program is authorized" and permitting functions "in response to the determination," which are directed to this technological innovation.

As explained in the specification of the '964 patent, certain embodiments of this advancement include a computer program that can be freely copied, installed, and executed while still preventing unlicensed use through peripheral validation and restriction. In accordance with this general approach, embodiments of the

'964 patent explain that "each camera and server . . . can be queried via FTP requests [by the software] to protected areas of the camera or server's memory" to obtain a unique MAC address that is embedded in the camera device. (Ex. 1001, '964 patent at 6:49-50.) The information received by the software is then "test[ed] for a valid MAC address" based on approved camera devices that have been established for use with the software. (*Id*. at 6:44-45.)

Patent Owner's patented approach to licensing—based on unique identifier authorization and validation—need not depend on user inputs at the computer on which the software is installed. Broadly, the patented procedures allow software itself to be installed on any number of computers without fear of piracy because operation of the program ensures that it is only used with approved cameras or servers. This innovation provides a novel mechanism for licensing that effectively inhibits software piracy without restricting installation of the software itself.

The claims at issue in this Petition are not set forth in their entirety within Petitioner's submission. The text of the independent claims at issue is reproduced in its entirety below with clarifying letter notations and paragraph breaks.

> **1.** A method of controlling access by a computer to a video server, comprising the steps of:
>
> **[a]** sending a request from the computer to a video server over a network;
>
> **[b]** receiving at the computer from the video server a unique

identifier stored in and identifying the video server, wherein the unique identifier is received by the computer over the network; and

[c] determining that access to the video server is authorized by comparing the unique identifier received by the computer to one or more authorized unique identifiers and

[d] in response to the determination, obtaining at the computer one or more images from the video server for displaying.

4. A method of controlling access by a computer to a hardware device, comprising the following steps performed at the computer:

[a] executing a computer program stored in computer readable form at the computer, the computer being connected to a hardware device via a network;

[b] accessing the hardware device from the computer over the network using an IP address associated with the hardware device;

[c] transmitting a request from the computer over the network for a MAC address of the hardware device;

[d] receiving at the computer the MAC address of the hardware device over the network; and

[e] determining if the computer program is authorized to access the hardware device by validating the MAC address using data accessible to the computer.

As shown above, the independent claims recite particular authorization and validation processes by which hardware addresses stored in accessible video servers (or other hardware devices) are requested, obtained, and determined if they are authorized. These limitations of the challenged claims "enable[] the software

to be licensed on a per-camera or per-server basis and can be used to prevent access to any cameras or servers for which the user is not licensed." (Ex. 1001, '964 patent at 6:53-56.)

C. The Prosecution History of the '964 Patent

The '964 patent is titled "Digital Video System Using Networked Cameras." The '964 patent is directed to methods of controlling access by a computer to a video server (claims 1-3) and by a computer program to a hardware device (claim 4).

During prosecution, as-filed claims 1-3 were rejected. (Ex. 1002 at 658-665.) Claims 1 and 2 were rejected as being obvious in light of the proposed combination of U.S. Pat. Nos. 5,790,548 to Sistanizadeh and U.S. Pat. No. 6,895,511 to Borsato. *Id.* Claim 3 was rejected as being anticipated by U.S. Pat. No. 5,790,664 to Coley. *Id.*

In response, applicant made amendments to claims 1 and 2, cancelled claim 3, and added claims 4 and 5. (*Id.* at 686-687.) The Examiner allowed the amended and new claims. (*Id.* at 742 and 743). The allowed claims 2, 4 and 5 were renumbered as issued claims 4, 2 and 3.

D. Level of Ordinary Skill in the Art

Petitioner's proposed description of the level of ordinary skill in the art (Pet. at 5) is too restrictive. Patent Owner contends that a person of ordinary skill in the

art would be an individual with an associate's or bachelor's degree in electrical engineering or computer science or an individual that has worked in the field of computer software for a year.

IV. CLAIM CONSTRUCTION

In an *inter partes* review, the Board construes claim terms in an unexpired patent according to their broadest reasonable construction in light of the specification of the patent in which they appear. 37 C.F.R. § 42.100(b); *In re Cuozzo Speed Techs., LLC*, 793 F.3d 1268, 1279 (Fed. Cir. 2015). The claim language should be read in light of the specification as it would be interpreted by one of ordinary skill in the art. *In re Am. Acad. of Sci. Tech. Ctr.*, 367 F.3d 1359, 1364 (Fed. Cir. 2004). The broadest reasonable meaning given to claim language must take into account any definitions presented in the specification. *Id.* (citing *In re Bass*, 314 F.3d 575, 577 (Fed. Cir. 2002)). Under this standard, claim terms are given their ordinary and customary meaning as would be understood by one of ordinary skill in the art in the context of the entire disclosure. *In re Translogic Tech., Inc.*, 504 F.3d 1249, 1257 (Fed. Cir. 2007) (citing *Phillips v. AWH Corp.*, 415 F.3d 1303, 1312-1315 (Fed. Cir. 2005) (*en banc*)).

A. Claim 1 Dictates that the Steps [a]-[d] Are Performed in Sequential Order

The claimed steps can be summarized as: step **[a]** Sending a request; step **[b]** Receiving based on the request sent; step **[c]** Determining based on what was

received; and step **[d]** Obtaining based on the determination. This is shown through the complete language of claim 1, which is reproduced below:

> A method of controlling access by a computer to a video server, comprising the steps of:
>
> **[a]** **sending a request** from the computer **to a video server** over a network;
>
> **[b]** **receiving** at the computer **from the video server a unique identifier** stored in and identifying the video server, wherein the unique identifier is received by the computer over the network; and
>
> **[c]** **determining that access** to the video server **is authorized by comparing the unique identifier** received by the computer to one or more authorized unique identifiers and
>
> **[d]** **in response to the determination, obtaining** at the computer one or more images from the video server for displaying.

"[A] claim 'requires an ordering of steps when the claim language, as a matter of logic or grammar, requires that the steps be performed in the order written, or the specification directly or implicitly requires' an order of steps." *mFormation Technologies v. Research in Motion Ltd.*, 764 F. 3d 1392, 1399-1400 (Fed. Cir. 2014). Here, both the claim language and specification require a sequential ordering of steps.

First, the order is required as a matter of logic based on a reading of the claim itself. If step **[a]** of sending a request from the computer to a video server did not occur before step **[b]** of receiving at the computer from the video server a

unique identifier, the sending step **[a]** would be rendered superfluous. *Id.*at 1399 (finding a sequence was required to avoid rendering a limitation superfluous). The receiving *from the video server* step **[b]** is a result of the sending *a request to a video server* step **[a]**. Without this sequencing requirement, sending step **[a]** would be an isolated, untethered limitation that has no relationship to any of the other steps of the claim, including receiving step **[b]**. Step **[b]** receives **a unique identifier** stored in the video server. Determining step **[c]** uses **the unique identifier** received in step **[b]**. Obtaining step **[d]** obtains in response to the determination of step **[c]**.

Second, the specification supports the order of the steps. The specification explains the sending of a request: "each camera and server . . . can be queried via FTP requests [by the software] to protected areas of the camera or server's memory" to receive a unique identifier that is embedded in the camera device. (Ex. 1001 at 6:49-51.) This procedure is further described in step 7 of the disclosed "initialization" process: "retrieving embedded MAC addresses for purposes of validating access to the cameras 24 identified in the database 56." (*Id.* at 6:36-38.) This is how the specification describes requesting and later receiving the unique identifier at the computer. Furthermore, there are no embodiments in the '964 specification where a unique identifier is received prior to a request (or

other positive action) from the computer to the video server. The specification directly requires an order of steps.

As shown above, the claim itself requires an order of steps. However, even if no such order is explicit in a claim, an order of steps may be found based on the specification. *Smart Modular Technologies Inc. v. Netlist, Inc.*, IPR2014-01371, Paper 12 at 9-10 and 16-17 (March 13, 2015) (Denying institution based on construction requiring a first transfer before a second transfer based on the specification).

Petitioner contends that the broadest reasonable interpretation of this claim is that the steps **[a]**-**[d]** are performed in order, which is consistent with the express language of the claim and the specification.

B. Petitioner's Implied Construction of "*unique identifier*" is Improper (claim 1)

Petitioner does not propose a construction for this term. Instead, Petitioner just assumes that a "unique identifier" only needs to be "unique within the system described by Acosta." (Pet. at 21.) That is not the limitation claimed. In a related Petition, IPR2016-00511, Petitioner Avigilon proposed a construction similar to the construction that is assumed in the present Petition.

In IPR2016-00511, Petitioner Avigilon proposed the following construction for this limitation: "data that uniquely identifies hardware ***on a network***, such as a MAC address." ('511 Pet. at 11, emphasis added.) Likewise, the Petitioner here

claims only "unique ***within the system described by Acosta***." The insertion of "on a network" or "within the system . . ." is not supported by the claims or specification. Claim 1 uses the term "over a/the network" in two places. Patent Owner chose not to use "on a network" or "within the system" to modify "unique identifier." The limitation "within the system" should not now be added through Petitioner's undisclosed constructions.

The specification describes unique identification of hardware **without** limiting the addition of "on a network" or "within a system." One example of a unique identifier in the specification is a MAC address. *See also*, claim 2 of the '964 patent. The specification explains that "MAC addresses are unique to each camera and server." (Ex. 1001 at 6:49.) The specification further states that a camera stores data that "uniquely identifies the cameras 24[.]" (*Id.* at 5:52-53.) In these instances, the specification does not limit the identification of the hardware in terms of its presence on a network. This proposed construction (whether express or by assumption) for "unique identifier" does not align with the claims or the specification, and therefore does not reflect the broadest reasonable construction in light of the specification.

C. Patent Owner Reserves All Remaining Claim Construction Issues

Petitioner's position that *all* claim terms should be given their broadest reasonable meaning (Pet. at 5) is inappropriate in view of the claim language at

issue, the '964 patent's specification, and the improper constructions implicit in many of Petitioner's arguments and conclusions.

Patent Owner reserves the right to present claim construction issues should the appropriate standard applicable to this Petition be modified or based on additional issues that arise in filings relating to this Petition.

V. THE PETITION DOES NOT MEET PETITIONER'S BURDEN TO SHOW A REASONABLE LIKELIHOOD OF SUCCESS ON ANY OF ITS ASSERTED GROUNDS OF INVALIDITY

Petitioner's Ground 1 based on 35 U.S.C. § 102 fails to establish anticipation under the applicable legal standards. "A claim is anticipated only if each and every element as set forth in the claim is found, whether expressly or inherently described, in a single prior art reference." *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631 (Fed. Cir. 1987). "[A] prior art reference without express reference to a claim limitation may nonetheless anticipate by inherency." *In re Cruciferous Sprout Litig.*, 301 F.3d 1343, 1349 (Fed. Cir. 2002). "If the prior art reference does not expressly set forth a particular element of the claim, that reference still may anticipate if that element is 'inherent' in its disclosure. To establish inherency, the extrinsic evidence 'must make clear that the missing descriptive matter is necessarily present in the thing described in the reference, and that it would be so recognized by persons of ordinary skill." *In re Robertson*, 169 F.3d 743, 745 (Fed. Cir. 1999). "Inherency, however, may not be

established by probabilities or possibilities. The mere fact that a certain thing may result from a given set of circumstances is not sufficient." *Id.* at 745.

As set forth below, Ground 1 of the Petition should be rejected because the single prior art Acosta reference used by Petitioner does not expressly or inherently disclose each and every limitation as recited in claims 1 and 3. Rather, Petitioner relies on assertions "that a certain thing may result" to argue that claims 1 and 3 are anticipated. *Id*. at 745. Petitioner has not met its required proofs.

Petitioner's asserted Grounds 2 and 3 rooted in 35 U.S.C. § 103 fail to establish *prima facie* obviousness. Petitioner's assertions of obviousness are riddled with hindsight reasoning and lack sufficient explanation of the motivation underpinning the combinations of prior art references relied upon for each ground of invalidity. Apart from issues surrounding the propriety of the proposed combinations themselves, the references simply fail to meet certain limitations of the challenged claims.

Following a general overview of the cited prior art references, Patent Owner will address these reasons supporting denial of the Petition.

A. Overview of Petitioner's Cited Prior Art

Petitioner asserts three grounds of invalidity. First, Petitioner asserts that claims 1 and 3 are anticipated under 35 U.S.C. § 102 in view of U.S. Patent No. 6,166,729 to Acosta et al. ("Acosta") (Ex. 1004). Second, Petitioner asserts that

claims 2 and 3 are obvious under 35 U.S.C. § 103 in view of Acosta and Axis 200 (Ex. 1009). Third, Petitioner asserts that claim 4 is obvious under 35 U.S.C. § 103 in view of Acosta, Axis 200 and U.S. Patent No. 6,292,838 to Nelson ("Nelson") (Ex. 1006).

1. Acosta

Acosta discloses a "remote viewing system . . . for viewing digital images of remote locations." (Ex. 1004 at Abstract.) The "remote viewing system 10 includes camera devices 12, a wireless network 14, a central office video management system (COVMS) 16, a World Wide Web server 18, a network 20, and a computer 22." (*Id.* at 4:26-29.) Figure 1 depicts this system architecture:

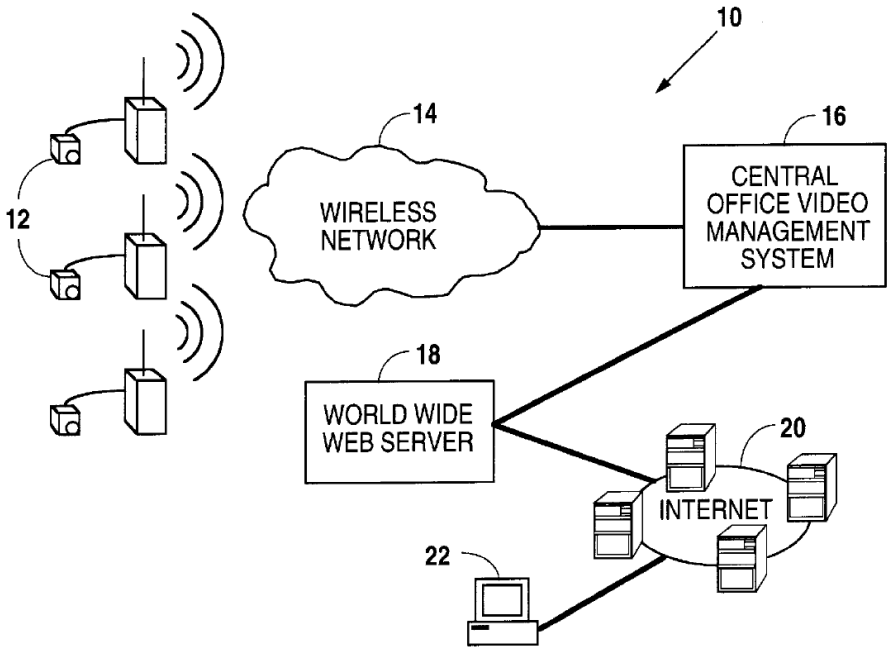

Fig. 1

While the "camera 12 communicates with the COVMS 16 over the wireless network 14," this communication does not use the "ARP protocol in the Ethernet environment." (*Id.* at 7:43-44 and 7:56-57.) Rather, the "ARP protocol in the Ethernet environment . . . is replaced with a static mapping mechanism specific to the radio frequency environment, e.g., the ARP protocol is replaced with a static routing table and routing according to the table." (*Id.* at 7:56-60.)

"There are four distinct operations that take place in the COVMS 16." (*Id.* at 12:64-65.) "The operations are the Business Manager, the CommLink Manager, the Image Processing Manager, and the Web Server Communication Manager." (*Id.* at 12:65-67.)

The "Business Manager opens a master database (the 'Master Camera Element Database') for the camera elements 12 for random access thereto and creates a table (the 'Active Camera Element Table') of the camera elements 12 that are active in the system 10 in the COVMS 16 memory." (*Id.* at 13:43-49.)

The CommLink Manager handles all communications between the camera elements 12 and the COVMS 16. (*Id.* at 17:28-29.) COVMS 16 assigns an identification (ID) to "each **communication** between any one of the camera elements 12 and the COVMS 16." (Ex. 1004 at 17:30-32) (emphasis added). "The ID is used by all other processes within the system 10." (*Id*. at 17:32-33.) "In processing **communication requests**, the CommLink Manager receives incoming

communication requests from the camera elements 12[.]" (*Id.* at 17:35-37) (emphasis added).

In the paragraph immediately after the description of an ID for each communication, Acosta refers to "the serial ID assigned to the camera element 12" (*Id.* at 17:48-49), which is referring to the previously assigned ID for each communication.

COVMS 16 passively listens for an incoming broadcast from a camera element 12. (*Id.* at 17:40-46.) The COVMS 16 does not access any camera elements 12 during the process of assigning an IP address to a camera element based on "incoming communication requests from the camera elements 12." (*Id*. at 17:37-38.) Acosta loosely refers to this assigning step as an "authentication." (*Id.* at 17:61-62: "the camera element 12 is authenticated according to the ID and is assigned an IP address.")

If an incoming broadcast is detected, COVMS 16 "looks up the serial ID assigned to the camera element 12 making the broadcast in a database of the COVMS 16 containing the serial ID's for all of the camera elements 12 **then operating** and obtains an IP address for the particular camera element 12." (*Id.* at 17:48-52, step 506) (emphasis added.) If the camera element is not operating, it is not assigned an ID.

COVMS 16 then determines "whether the particular ID and IP address match, and whether the related database record is found." (*Id.* at 17:53-55, step 508.) The IP address assignment process is shown in steps 506 to 514 (red box) of Figure 20:

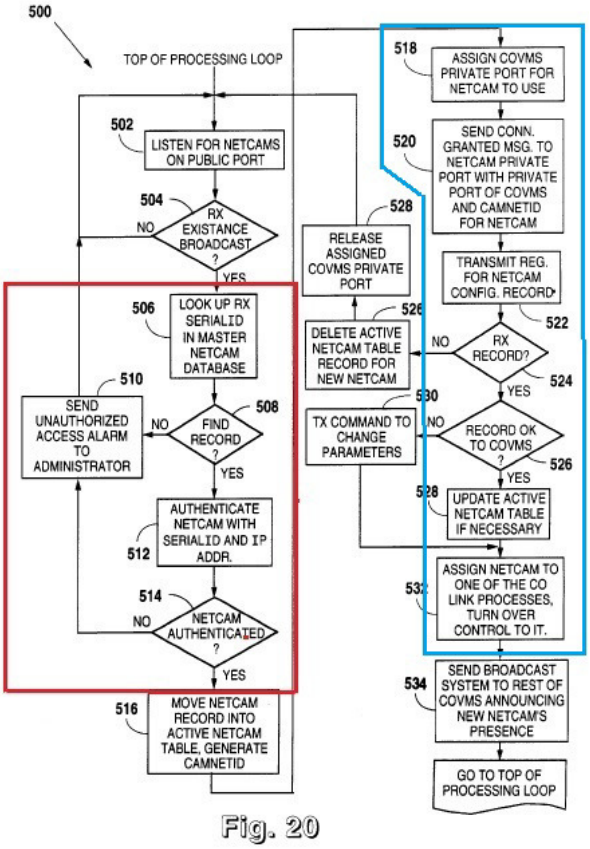

Fig. 20

If the process is successful, Acosta assigns an IP address to a camera element 12. (*Id.* at 17:60-65.) Accordingly, COVMS 16 does not access or attempt to access the camera elements 12 at any point during that process. It cannot do so because no IP address is assigned to camera element 12 until that process is successfully completed. (*See infra* at Section V.A.2; Ex. 1007 at 19.)

Only after an IP address has been assigned to camera element 12, COVMS 16 **generates** "a specific identifier" for the camera element 12. (*Id.* at 17:66-18:2, emphasis added) ("[T]he database record for the camera element 12 is moved, in a step 516, into an active table from which **is generated a specific identifier for the camera element 12**.") Accordingly, the serial communication ID earlier assigned to "each communication" is not "a specific identifier" for any camera element 12. Also, since "the specific identifier" is "generated" after the IP address assignment process is completed, it does not exist and cannot be stored in the camera element 12 before it is "generated."

The blue box around a portion of Fig. 20, reproduced above, shows the steps for the COVMS 16 accessing camera element 12. "In step 520, the COVMS 16 . . . sends a connection granted message to the camera element 12 via [a] . . . particular port and the specific identifier." (*Id.* at 18:5-7.) In step 522, "the COVMS 16 . . . sends a transmit request to the camera element 12 for a particular configuration record applicable to the camera element 12." (*Id.* at 18:7-9.) If the configuration record is received by the COVMS 16 (step 524) and is suitable (step 526), then "the camera element 12 is linked to the COVMS 16 in a step 532." (*Id.* at 18:27-23.) "When the Image Processing Manager receives the link message, it looks for the link and sets up a queue for input." (*Id.* at 18:26-28.)

2. Axis 200

This reference is the User's Manual for AXIS 200 Camera Servers. (Ex. 1007.) The Manual states: the "AXIS 200 Network Camera is a digital snapshot camera with a built-in Web server. Connecting directly to Ethernet networks, it provides a source for live color pictures over the Internet." (*Id.* at 7.)

In "Section 3:Assigning an Internet Address," the User Manual refers to an "Ethernet Address: Depending on the method you are using, you will need to know the Ethernet address of your AXIS 200. The Ethernet address is based upon the serial number found on the underside label of the unit." (*Id.* at 20.)

3. Nelson

U.S. Patent No. 6,292,838 to Nelson et al. ("Nelson") is titled "Technique for automatic remote media access control (MAC) layer address resolution." (Ex. 1006.) Nelson is directed to a "system and method for determining a MAC layer address of a network interface on a remote device, based on an IP address associated with the same network interface on the remote device." (Nelson, Ex. 1006 at Abstract.) This system and method is carried out using an Address Resolution Protocol ("ARP") cache and ARP software residing on a router:

> ARP is a known protocol for mapping IP addresses to MAC addresses. ***A table, usually called the ARP cache, is associated with the network interfaces within a router*** and is used to maintain a correlation between MAC addresses and corresponding IP addresses

> for network interfaces of other network devices in the subnet to which the router is connected.

(*Id.* at 9:59-65) (emphasis added).

> The present system takes advantage of the fact that ARP software maintains IP address to MAC address mappings in its address cache during normal packet forwarding operations of a router. Specifically, ***when an incoming packet***, destined for a network device on a specific subnet, *arrives at a router*, the router searches the ARP cache to find a MAC address that matches the IP address. ***If the router finds a corresponding MAC address***, then the packet can be converted to include the new MAC address. ***If no corresponding MAC address is found for that IP address, ARP software broadcasts a request packet*** in a special format to all network devices on the attached subnet to see if a network device has the IP address associated with one of its interfaces.

(*Id.* at 10:4-16.)

B. GROUND 1: Acosta Fails to Disclose "*receiving at the computer from the video server a unique identifier stored in and identifying the video server, wherein the unique identifier is received by the computer over the network*" (Claim 1[b])

Petitioner argues that this limitation is disclosed by Acosta. Acosta does not disclose, either expressly or inherently, this limitation. Petitioner relies on the operation of Acosta's CommLink Manager for a disclosure of step **[b]**. Contrary

to Petitioner's reading of Acosta, Acosta does not disclose "a unique identifier stored in and identifying the video server," as recited in the claims.

1. No Express Teaching

Acosta does not expressly disclose step **[b]**. Referring to the operation of the CommLink Manager, Acosta discloses an identification (ID) of "each **communication** between any one of the camera elements 12 and the COVMS 16." (Ex. 1004 at 17:30-32) (emphasis added). "The CommLink Manager maps each ID into an IP address before processing communication requests related to that **particular communication**." (*Id.* at 17:33-35) (emphasis added). "In processing **communication requests**, the CommLink Manager receives incoming **communication requests** from the camera elements 12[.]" (*Id.* at 17:35-37) (emphasis added). "The ID is used by all other processes within the system 10." (*Id.* at 17:32-33.)

The paragraph that follows Acosta's description of IDs for communications identified above refers to "the serial ID assigned to the camera element 12." (*Id.* at 17:49-50.) Reading Acosta in context, the "serial ID" is referring to the earlier described ID for each communication, which "is used by all other processes within the system 10." Accordingly, when Acosta listens for "camera elements 12 sending existent broadcasts in a step 502" (*Id.* at 17:41-44) and then "[i]f an incoming broadcast is detected, that broadcast includes the serial ID for the camera

12" (*Id.* at 17:46-48), Acosta is disclosing the serial ID for the camera element 12 "related to the particular communication." (*Id.* at 17:35.) Moreover, the IDs are not disclosed as stored in a camera element.

Acosta later "generate[s] a specific identifier for the camera element 12." Acosta states: "[a] determination is made in a step 514 whether the camera element 12 is authenticated." (*Id.* at 17:62-64.) The next step in Acosta's process is "[i]f the camera element 12 is authenticated, . . . the database record [in the Master Camera Element Database] for the camera element 12 is moved, in a step 516, into an active table for which is generated **a specific identifier** for the camera element 12." (*Id.* at 17:66-18:2). The specific identifier for a camera element 12 is generated **after** the serial ID is assigned to the camera element 12, and does not refer back to any other identifier. This demonstrates that the serial ID is not a "unique identifier."

The disclosed "serial ID" of Acosta is not "a unique identifier stored in and identifying the video server," as recited in the claims.

2. No Inherent Disclosure

Realizing the express shortcomings of Acosta, Petitioner resorts to the extrinsic record to implicitly argue that this limitation is inherently disclosed by Acosta. (Pet. at 20-21.) In citing to the Thompson Declaration, ¶¶ 50, 51 and 52, respectively, Petitioner states that one skilled in the art would understand that (1)

"**the serial ID** identifies camera element 12 to the COVMS 16"; (2) "because **the serial ID** is used to identify and authenticate the camera element 12, it **must be unique within the system described by Acosta** for the authentication function to be effective"; and (3) "**the serial ID** is necessarily stored by the camera element 12." (*Id.*) (emphasis added). Petitioner must prove all three assertions to support its inherency argument. Petitioner has failed in its proofs.

Regarding (1), Acosta expressly discloses that the serial ID is particular to the communication between a camera element 12 and the COVMS 16. Moreover, only after "authentication" does the COVMS 16 "generate a specific identifier for the camera element 12." (*Id*. at 17:66-18:2.) This conclusively establishes that a "unique identifier stored in and identifying the video server" is not "necessarily present" in the ID of Acosta.

Regarding (2), the serial ID is not even "unique within the system described by Acosta." First, Petitioner's argument assumes an incorrect claim construction. *See supra* Section IV.B. "Within the system" does not modify unique within the claim. Moreover, Acosta expressly teaches that "generating a specific identifier for the camera element 12" after assigning the communication serial ID. (*Id.* at 17:66-18:2). A specific identifier would not be generated if one already existed in the form of a communication serial ID as proposed by Petitioner. Instead, the ID disclosed in Acosta is assigned for each communication of a camera. Accordingly,

each communication between the camera and COVMS is identified with a different ID.

Regarding (3), Acosta is silent as to whether the serial ID is stored by the camera element 12. Petitioner has not established that the limitation "a unique identifier stored in . . . the video server" is "necessarily present" in Acosta. In Acosta, the ID could be assigned to each communication as it is received by the COVMS. This is what is disclosed in Acosta: "each communication between any of the camera elements 12 and the COVMS 16 is assigned an identification (ID). The ID is used by all the other processes within the system 10." (Ex. 1004 at 17:30-35.) Moreover, the ID need not necessarily be stored, as it could be generated in serial fashion. Further, the ID need not be necessarily "stored in and identifying the video server," as required by Claim 1.

In fact, when each of the cameras 12 is configured, the configuration does not include a unique ID—it does not even include the serial ID. (Ex. 1004 at 7:33-39) ("Each of the cameras 12 is configured, prior to being deployed at a location, with an ID record that includes geographic information about the location of the camera 12, the camera hardware and system settings of the camera 12, an IP address, and a primary and secondary COVMS 16 for connection upon startup.")

For at least these reasons, Acosta does not expressly or inherently disclose step **[b]** of claim 1. Consequently, institution of challenged claims 1 and 3 should be denied.

C. GROUND 1: Acosta Does Not Disclose the Required Sequence of Steps [a]-[d] of Claim 1

As discussed *supra* in Section IV.A., claim 1 requires that steps **[a]** through **[d]** are done in order. Accordingly, step **[a]** of "sending a request from the computer to a video server over a network" occurs before step **[c]** of "determining that access to the video server is authorized by comparing the unique identifier received by the computer to one or more authorized unique identifiers."

In contrast, Acosta's COVMS 16 does not send any request **to** a camera element 12 until after its "authentication" steps are successfully completed and an IP address is assigned to the camera. If the "authentication" steps are successful, Acosta assigns an IP address to a camera element 12. (*Id.* at 17:60-65.) Accordingly, COVMS 16 does not access or attempt to access the camera elements 12 at any point during that process. It cannot do so because no IP address is assigned to camera element 12 until that process is successfully completed.

After the IP address is assigned, the COVMS 16 sends requests to the camera element 12. "In step 520, the COVMS 16 . . . sends a connection granted message to the camera element 12 via [a] . . . particular port and the specific identifier." (*Id.* at 18:5-7.) In step 522, "the COVMS 16 . . . sends a transmit

request to the camera element 12 for a particular configuration record applicable to the camera element 12." (*Id.* at 18:7-9.) If the configuration record is received by the COVMS 16 (step 524) and is suitable (step 526), then "the camera element 12 is linked to the COVMS 16 in a step 532." (*Id.* at 18:27-23.)

Acosta's COVMS 16 "send[ing of] a connection granted message" is the first instance of a message sent from the COVMS 16 to the camera element 12. This occurs after the alleged "authentication" process is completed. This is the opposite of the required order of claim 1. Consequently, institution of challenged claims 1 and 3 should be denied.

D. GROUND 2: Petitioner's Proposed Camera Substitution or Addition Fails to Disclose or Suggest "*wherein the unique identifier is a MAC address*" (claim 2)

Petitioner seeks to modify Acosta's COVMS 16 with the substitution or addition of Axis 200 cameras to render claim 2 obvious.

Petitioner states:

> It would have been obvious to **modify Acosta's COVMS 16** to be interoperable **with the Axis 200 camera <u>instead of or addition to</u> camera elements 12**. (*See* Thompson Decl. ¶ 66 (Ex. 1003).)
>
> * * *
>
> It would have been within the skill of one in the art to **modify Acosta's COVMS 16 to be interoperable with the Axis 200 camera** without substantially modifying the architecture of the COVMS 16. (*See* Thompson Decl. ¶ 67 (Ex. 1003).)

* * *

> **[M]odifying Acosta's COVMS 16 to communicate with the Axis 200 camera <u>instead of, or in addition to</u>, camera elements 12** would be the simple substitution of one known, equivalent element for another to obtain the predictable result of interoperability the COVMS 16 and the Axis 200 camera. (*See* Thompson Decl. ¶ 67 (Ex. 1003).)

(Pet. at 30-31, emphasis added.)

Petitioner's proposed modifications can be summarized as: (1) adding Axis 200 cameras to the Acosta system including the COVMS 16; or (2) substituting Axis 200 cameras for Acosta's camera elements 12. These proposed modifications do not disclose or suggest claim 2 of the '964 patent.

Claim 2 depends on claim 1 and recites that "the unique identifier is a MAC address." Inserting "MAC address" for "unique identifier" in steps **[b]** and **[c]** of claim 1 follows: step **[b]** recites "receiving at the computer from the video server [a MAC address] … stored in and identifying the video server"; and step **[c]** recites "determining that access to the video server is authorized by comparing [the MAC address] … received by the computer to one or more authorized [MAC addresses]."

Regarding proposed modification (1), Axis 200 does not receive a MAC address at a computer, and Petitioner does not argue otherwise. Axis 200 refers to a serial number and Ethernet address, not a serial ID. Axis 200 mentions the serial

number in connection with "Assigning an Internet Address:" "Depending on the method you are using, you will need to know the Ethernet address of your AXIS 200. The Ethernet address is based upon the serial number found on the underside label of the unit." (Ex. 1007 at 20.) Accordingly, if the COVMS 16 is the claimed computer, as alleged by Petitioner, it would not receive a MAC address from an Axis 200 camera. This proposed modification does not disclose either steps **[b]** or **[c]** of claim 1 from which claim 2 depends.

Regarding proposed modification (2), the substitution of Axis 200 cameras for Acosta's camera elements 12 does not disclose or suggest claimed steps **[b]** or **[c]**. If the proposed modified system includes any camera elements 12, the COVMS 16 does not receive MAC addresses from the camera elements 12. Petitioner does not argue otherwise. (Pet. at 29) ("To the extent that Acosta does not disclose that the serial ID can be a MAC address, Axis 200 discloses this element.") However, simply substituting an Axis 200 camera for a camera element 12 does not provide claimed steps **[b]** or **[c]**. As explained above, the Axis 200 does not send a MAC address to a computer, and therefore, the COVMS 16 would not receive a MAC address from an Axis 200 camera. This proposed modification does not disclose either claimed steps **[b]** or **[c]**.

The modification proposed and argued by Petitioner does not arrive at claim 2 of the '964 patent. Petitioner makes this flawed modification to arrive at the following argument:

> In making the COVMS 16 interoperable with the Axis 200 camera, it would have been obvious to modify the COVMS 16 of Acosta to use the MAC address of the Axis 200 camera for authorization. (*See* Thompson Decl. ¶ 68 (Ex. 1003).)

(Pet. at 30-31.) Yet, the Petition is completely devoid of any motivation to make the changes required above to allegedly meet the claim language.

Petitioner seeks to use a MAC address for a purpose not recognized or appreciated in the art prior to the '964 patent. *See infra* Section V.F. The only reason to make this combination is impermissible hindsight based on the claimed computer access controlling procedures of the '964 patent. *MasterImage 3D, Inc. v. RealD Inc.*, IPR2015-00877, Paper 8 at 21–22 (September 9, 2015) ("Petitioner's approach and reasoning reflect reliance on hindsight in view of Patent Owner's claimed invention, which is inappropriate for an obviousness analysis."); *Endo Pharmaceuticals Inc. v. Depomed, Inc.*, IPR2014-00656, Paper 66 at 27 (September 21, 2015) ("Petitioner's obviousness challenge amounts to picking and choosing certain preferred attributes of the various references and combining them to yield the claimed invention…[and] such a piecemeal combination reflects impermissible hindsight").

For at least these reasons, the Board should reject Ground 2.

E. GROUND 3: Petitioner's Proposed Combination Fails to Disclose or Suggest "*transmitting a request from the computer over the network for a MAC address of the hardware device*" (Claim 4[c])

Petitioner applies Nelson to this limitation. (Pet. at 39.) However, Nelson discloses a router based broadcast ARP command. (Ex. 1006 at 9:59-65 and 10:4-16.) Step **[c]** requires "transmitting a request ***from the computer***." Nelson broadcasts an ARP command from a router.

Because of this, Petitioner sets forth an unsupported argument involving a reference modification. The Petitioner argues:

> One skilled in the art would have appreciated that in order to obtain the MAC address of the Axis 200 camera, the COVMS 16 could wait to passively receive it, as in Acosta, or actively request it, as in Nelson. (*See* Thompson Decl. ¶ 83 (Ex. 1003).)

(Pet. at 40.)

This argument is based on an addition of a router-based ARP command (Nelson) to a non-ARP protocol system (Acosta), but the Petitioner does not provide any rational underpinning for this wholesale change to and substitution of the wireless architecture of Acosta. It is well established that "rejections on obviousness cannot be sustained with mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the

legal conclusion of obviousness." *In re Kahn,* 441 F.3d 977, 988 (Fed. Cir. 2006); *see also KSR,* 550 U.S. at 418, (quoting Federal Circuit statement with approval). Moreover, in a clear teaching away from Nelson's router-based ARP command, AXIS 200 expressly states that the ARP "is not appropriate to use . . . over routers" to "enable access to your AXIS 200." (Ex. 1007, p. 19.) For this reason alone, Petitioner's Ground 3 fails.

F. GROUND 3: There is No Reason or Motivation To Combine Acosta, the Axis 200 Camera, and Nelson

Petitioner attempts to combine three references, *i.e.*, Acosta, Axis 200 and Nelson, to render claim 4 obvious. Petitioner argues:

> As discussed above with respect to claim 3, Acosta and Axis 200 disclose the COVMS 16 using a MAC address received from the Axis 200 camera to determine whether it is authorized to access the Axis camera 200 by comparing the received MAC address to as stored list of authorized MAC addresses. (See Thompson Decl. ¶ 81 (Ex. 1003).)

(Pet. at 39.)[2] Petitioner does not set forth an express motivation, but instead refers to Section VII of the Petition for a motivation to use a MAC address for authorization. (Pet. at 31.) In Section VII, Petitioner makes the proclamation that "MAC Addresses, and using them to identify devices in a network, were well-

[2] The Petition appears to mistakenly refer to claim 3, instead of claim 2, which includes the MAC address limitation in the '964 claims.

known in computer networking long before the '964 patent's earliest priority date." (Pet. at 12.) Petitioner continues to claim that "Using a MAC address to determine whether communications between systems on a network are authorized was also a known technique." (Pet. at 13.) Because of this, Petitioner improperly asserts that one of skill in the art can use a MAC address as opposed to the ID used in Acosta.

Petitioner does not use either references relied on for its motivation to combine (Holloway and Schell) in any of its obviousness combinations. This is fatal to the Petition. Each of these references has fundamental differences to the challenged claim. First, Petitioner cites to Holloway, which discloses a network design that only permits known computers (by MAC address) to use the network. Petitioner also cites to Schell, which discloses a design to create an environment of trusted workstations, so only communications from known devices are allowed.[3] Neither Holloway nor Schell concern the use of a particular computer program,

[3] Schell is explicit that if "a source address" is used from the data link layer which could include a MAC address, then the MAC address cannot even be received between disparate devices on a network using Schell. Schell explains in detail: "with data link layer source address enforcement, at least one of the retransmission devices needs to be involved in the source address enforcement since the data link layer source address ***is modified*** as it traverses many of these devices, including routers." (Schell at 3:15-19, emphasis added.)

and neither uses a MAC address related in any way to a computer program. Claim 4 of the '964 Patent is computer program-specific and uses a MAC address to determine whether the computer program is authorized to access the hardware device by validating the MAC address. No prior art reference uses a MAC address of a hardware device to restrict particular operation of a computer program on another device.

As explained in the '964 Patent, the claimed solution "enables the software to be licensed on a per-camera or per-server basis." (Ex. 1001 at 6:53-56.) The '964 claims and specification make clear that this solution allows software to be licensed by restricting the computer program. Unlike Schell and Holloway, in claim 4 a computer program is not prevented from communication over the network. Rather, claim 4 controls access to particular operations of a particular computer program. Schell and Holloway do not involve a software restriction. Petitioner cites no reference for this novel solution. Schell and Holloway involve security against intrusion into a network, whereas claim 4 involves computer program access controls. Petitioner's proposed combination and reasoning is based entirely on hindsight using the teachings of the '964 patent. *MasterImage 3D, Inc. v. RealD Inc.*, IPR2015-00877, Paper 8 at 21–22 (September 9, 2015) ("Petitioner's approach and reasoning reflect reliance on hindsight in view of

Patent Owner's claimed invention, which is inappropriate for an obviousness analysis.")

Tellingly, Petitioner does not identify any prior art that uses a MAC Address from a remote hardware device for restricting software program operation at the computer. Petitioner does not identify any prior art or provide any basis for arriving at the licensing benefit of the challenged claim. Petitioner does not explain why anyone would want to (let alone be motivated to) license particular software programs based on the MAC address of a remote hardware device. Petitioner provides no rational basis for this modification, no recognition of the solution provided by claim 4, and no reason why one skilled in the art would have been motivated to do what has never been done before. *Endo Pharmaceuticals Inc. v. Depomed, Inc.*, IPR2014-00656, Paper 66 at 27 (September 21, 2015) ("Petitioner's obviousness challenge amounts to picking and choosing certain preferred attributes of the various references and combining them to yield the claimed invention…[and] such a piecemeal combination reflects impermissible hindsight").

Petitioner further argues:

> One skilled in the art would have appreciated that in order to obtain the MAC address of the Axis 200 camera, the COVMS 16 could wait to passively receive it, as in Acosta, or actively request it, as in Nelson. (*See* Thompson Decl. ¶ 83 (Ex. 1003).) Whether Acosta's

> COVMS 16 waited to receive the MAC address or requested it would have been a matter of routine design choice yielding predictable results.

(Pet. at 39-40.) Nelson discloses ARP router broadcast software. (Ex. 1006 at 9:59-61) ("ARP is a known protocol for mapping IP addresses to MAC addresses."); (*Id.* at 10:4-7) ("The present system takes advantage of the fact that ARP software maintains IP address to MAC address mappings in its address cache during normal packet forwarding operations of the router.") Acosta replaces "the ARP protocol in the Ethernet environment" with "a static mapping mechanism specific to the radio frequency environment." (Ex. 1004 at 7:56-60.) Accordingly, Petitioner's attempt to modify Acosta using a non-ARP "static mapping mechanism" with the "ARP router broadcast software" of Nelson is unfounded.

Furthermore, similar to Holloway and Schell, Nelson does not teach or suggest using a MAC address of a hardware device to control access by a computer program. Nelson does not involve a software restriction, as claimed. Accordingly, regardless of which references are relied on by the Petitioner, it has not provided an adequate reason or motivation to combine.

For these additional reasons, Petitioner's Ground 3 fails.

VI. CONCLUSION

In light of the remarks herein, Patent Owner respectfully requests that the Board deny institution of the Petition for *inter partes* review of the '964 Patent.

Respectfully submitted,

Dated: May 17, 2016

/Marc Lorelli/

Marc Lorelli (Reg. No. 43,759)
Matthew M. Jakubowski (Reg. No. 44,801)
Adam R. Southworth (Reg. No. 65,407)
BROOKS KUSHMAN P.C.
1000 Town Center, 22nd Floor
Southfield, MI 48075
(248) 358-4400

Attorneys for Patent Owner,
JDS Technologies, Inc.

Certificate of Service

The undersigned hereby certifies that on May 17, 2016, a complete and entire copy of **Patent Owner's Preliminary Response to Petition for *Inter Partes* Review Under 37 C.F.R. § 42.107**, was served via electronic mail by serving the correspondence email address of record as follows:

LEAD COUNSEL	BACK-UP COUNSEL
Steven M. Bauer Reg. No. 31,481 Proskauer Rose LLP One International Place Boston, MA 02110 Tel: (617) 526-9600 Fax: (617) 526-9899 PTABMattersBoston@proskauer.com	Joseph A. Capraro Jr. Reg. No. 36,471 Proskauer Rose LLP One International Place Boston, MA 02110 Tel: (617) 526-9600 Fax: (617) 526-9899 jcapraro@proskauer.com

Respectfully submitted,

/Marc Lorelli/

Marc Lorelli (Reg. No. 43,759)
Matthew M. Jakubowski (Reg. No. 44,801)
Adam R. Southworth (Reg. No. 65,407)
BROOKS KUSHMAN P.C.
1000 Town Center, 22nd Floor
Southfield, MI 48075
(248) 358-4400

Attorneys for Patent Owner,
JDS Technologies, Inc.

Certificate of Compliance Pursuant to 37 C.F.R. § 42.24

This paper complies with the type-volume limitation of 37 C.F.R. § 42.24. The paper contains 8,675 words, excluding the parts of the paper exempted by §42.24(a).

This paper also complies with the typeface requirements of 37 C.F.R. § 42.6(a)(ii) and the type style requirements of § 42.6(a)(iii)&(iv).

Respectfully submitted,

Dated: May 17, 2016

/Marc Lorelli/

Marc Lorelli (Reg. No. 43,759)
Matthew M. Jakubowski (Reg. No. 44,801)
Adam R. Southworth (Reg. No. 65,407)
BROOKS KUSHMAN P.C.
1000 Town Center, 22nd Floor
Southfield, MI 48075
(248) 358-4400

Attorneys for Patent Owner,
JDS Technologies, Inc.