UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

SecureNet Technologies, LLC,
Petitioner

v.

iControl Networks, Inc.,
Patent Owner

U.S. Patent No. 8,473,619
Filing Date: Aug. 11, 2008
Issue Date: June 25, 2013

Title: Forming a Security Network Including Integrated Security System Components and Network Devices

---

Inter Partes Review No. _____

Petition for *Inter Partes* Review of U.S. Patent No. 8,473,619

Table of Contents

Page

Table of Contents
(continued)

Page

Table of Contents
(continued)

Page

EXHIBITS

Exhibit No.	Description of Document
1001	U.S. Patent No. 8,473,619 ("the '619 patent")
1002	Declaration of James Parker
1003	File History for U.S. Patent No. 8,473,619
1004	U.S. Patent Publication No. 2004/0260427 to Wimsatt ("Wimsatt")
1005	U.S. Patent No. 6,580,950 to Johnson et al. ("Johnson")
1006	U.S. Patent No. 4,951,029 to Severson ("Severson")
1007	U.S. Publication No. 2003/0062997 to Naidoo et al. ("Naidoo")
1008	U.S. Patent No. 6,748,343 to Alexander et al. ("Alexander")
1009	U.S. Publication No. 2003/0137426 to Anthony et al. ("Anthony")
1010	Installation Instructions for PC5401 Data Interface Module (2004)
1011	"Understanding Universal Plug and Play," White Paper, Microsoft (2000)
1012	Waiver of Service, *iControl Networks, Inc. v. SecureNet Techns., LLC*, No. 15-807-GMS, (D. Del. Sept. 30, 2015), ECF No. 5
1013	*Curriculum Vitae* of James Parker

I. INTRODUCTION

SecureNet Technologies, LLC ("Petitioner" or "SecureNet") petitions for *inter partes* review ("IPR") under 35 U.S.C. §§ 311-319 and 37 C.F.R. § 42 of claims 17, 18, 20-22, 29-31, 33, 35-41, 48-53 and 58 ("the Petitioned Claims") of U.S. Patent No. 8,473,619 ("the '619 patent") (Ex. 1001).

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

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

SecureNet Technologies, LLC is the real party-in-interest.

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

The '619 patent is asserted in *iControl Networks, Inc. v. SecureNet Technologies, LLC*, No. 15-807-GMS (D. Del.), which was filed on September 11, 2015.[1]

Petitioner is also concurrently filing an IPR petition covering claims 1-6, 14-46, 49-58 and 60-61 of U.S. Patent No. 8,073,931, which is assigned to the Patent Owner and claims priority to same applications as the '619 patent. Petitioner is also concurrently filing two IPR petitions covering claims 1-4, 6-50 of U.S. Patent

[1] iControl Networks, Inc. ("Patent Owner" or "iControl") filed a Waiver of Service in that case on September 30, 2015 (Ex. 1012). Based on the PTAB-designated informative decision docketed as Case No. IPR2013-00010 (Paper 20) (January 30, 2013), this Petition is being timely filed.

No. 8,478,844 ("the '844 patent"), which is assigned to the Patent Owner and is the child patent to the '619 patent. Petitioner is also concurrently filing an IPR petition for claims 25-40 and 42-50 of the '844 patent.

Petitioner is not aware of any other judicial or administrative matters that would affect, or be affected by, a decision in this proceeding.

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

Lead Counsel: Erik B. Milch (Reg. No. 42,887) / emilch@cooley.com
Back-up Counsel:
Jennifer Volk (Reg. No. 62,305) / jvolkfortier@cooley.com
Frank Pietrantonio (Reg. No. 32,289) / fpietrantonio@cooley.com
zSecureNetIPR@cooley.com
zpatdcdocketing@cooley.com
Cooley LLP ATTN: Patent Group
1299 Pennsylvania Ave., NW, Suite 700 Washington, DC 20004
Tel: (703) 456-8573 Fax: (703) 456-8100

D. Service Information

The Petition is being served by FEDERAL EXPRESS to the '619 Patent Owner's attorneys of record, IPR Law Group, PC and the known outside counsel to Patent Owner, Wilson Sonsini Goodrich & Rosati. Petitioner consents to service by e-mail at the addresses provided above.

E. Power of Attorney

Filed concurrently with this petition per 37 C.F.R. § 42.10(b).

III. PAYMENT OF FEES - 37 C.F.R. § 42.103

This Petition requests review of claims 17, 18, 20-22, 29-31, 33, 35-41, 48-53 and 58 (a total of 23 claims) of the '619 patent and is accompanied by a

payment of $26,800. 37 C.F.R. § 42.15. This Petition meets the fee requirements of 35 U.S.C. § 312(a)(1).

IV. REQUIREMENTS FOR *INTER PARTES* REVIEW UNDER 37 C.F.R. §§ 42.104 AND 42.108

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

Petitioner certifies that the '619 patent is eligible for IPR and further certifies that Petitioner is not barred or estopped from requesting IPR.

B. Identification of Challenge Under 37 C.F.R. § 42.104(b) and Statement of Precise Relief Requested

Petitioner requests that the Board institute *inter partes* review of claims 17, 18, 20-22, 29-31, 33, 35-41, 48-53 and 58 of the '619 patent and requests that each claim be found unpatentable as obvious under 35 U.S.C. § 103(a) on the following grounds:

Ground	'619 Claim(s)	Basis for Challenge
1.	17, 18, 21-22, 29-31, 33, 36, 58	Obvious over Wimsatt in view of Johnson, Severson and Naidoo under 35 U.S.C. § 103(a)
2.	20, 35	Obvious over Wimsatt in view of Johnson, Severson, Naidoo and Anthony under 35 U.S.C. § 103(a)
3.	37-41, 48-53	Obvious over Wimsatt in view of Johnson, Severson and Alexander under 35 U.S.C. § 103(a)

This petition is accompanied by the Declaration of James Parker (Ex. 1002, "Mr. Parker"), an expert in the field.

C. Threshold Requirement for *Inter Partes* Review 37 C.F.R. § 42.108(c)

Inter partes review of claims 17, 18, 20-22, 29-31, 33, 35-41, 48-53 and 58 should be instituted because this Petition establishes a reasonable likelihood that Petitioner will prevail with respect to each of the claims challenged. 35 U.S.C. § 314(a).

V. BACKGROUND OF TECHNOLOGY RELATED TO THE '619 PATENT

Mr. Parker provides a technology tutorial in his declaration. (Ex. 1002, ¶¶ 30-57.)

VI. SUMMARY OF THE '619 PATENT

The '619 patent was filed on August 11, 2008 and claims priority to a divisional application and a long list of continuation-in-part applications and provisional applications, the earliest of which has a filing date of March 16, 2005. (Ex. 1001.) For purposes of this proceeding, we assume that the earliest possible priority date of the '619 patent is March 16, 2005. We reserve the right to dispute this priority date at a later time or in another proceeding.

VII. CLAIM CONSTRUCTION UNDER 37 C.F.R. § 42.104(b)(3)

A. Legal Overview

A claim subject to IPR is given its "broadest reasonable construction in light

of the specification of the patent in which it appears."[2] 37 C.F.R. § 42.100(b).

B. Proposed Claim Constructions

Petitioner does not propose any claim constructions for this proceeding. All claim terms and clauses should be given their plain and ordinary meaning as understood by a person of ordinary skill in the art ("POSITA"). (*See* Ex. 1002, ¶ 59.)

VIII. PERSON HAVING ORDINARY SKILL IN THE ART & STATE OF THE ART

The '619 patent is directed to integrated security systems that are capable of being remotely accessed and controlled. (Ex. 1002, ¶¶ 17-24.) At the time of the alleged invention, a POSITA as of 2005 would hold a bachelor's degree or the equivalent in electrical engineering (or related academic fields) and at least three years of additional work experience in the area of digital and/or telecommunication system design, as applicable to safety and security systems, or equivalent work experience. (*Id*., ¶ 19.)

IX. CLAIMS 17, 18, 20-22, 29-31, 33, 35-41, 48-53 AND 58 OF THE '619 PATENT ARE UNPATENTABLE

As detailed in the sections below, claims 17, 18, 20-22, 29-31, 33, 35-41, 48-53 and 58 of the '619 patent are obvious in light of Wimsatt in view of Johnson

[2] Petitioners reserve the right to pursue different constructions in litigation. *In re Zletz*, 893 F.2d 319, 321 (Fed. Cir. 1989).

and/or one or more other prior art references cited below.

A. Overview Of The Prior Art

1. Overview of Wimsatt

Wimsatt published on December 23, 2004 and therefore qualifies as prior art under 35 U.S.C. § 102(a). The patent issuing from Wimsatt was cited by Patent Owner in an Information Disclosure Statement (IDS) during prosecution of the '619 patent but it was never applied against the claims.

Wimsatt describes a home automation system having a control panel 101 that is connected to a number of co-located devices, called "controlled devices", which manage already-existing systems, such as lighting systems or security systems. (Ex. 1004, ¶ 0023.) The control panel 101 displays an interactive graphical user interface (GUI) that allows the user (e.g., homeowner) to control the controlled devices. (*Id.*, ¶ 0022; Ex. 1002, ¶¶ 61-64.)

2. Overview of Johnson

Johnson issued on June 17, 2003 and therefore qualifies as prior art under 35 U.S.C. § 102(b). Johnson was cited by Patent Owner in an IDS during prosecution of the '619 patent but it was never applied against the claims.

Johnson discloses an "Internet based home communications system for allowing a homeowner to monitor and control various features of their home from a distant location via a global computer network." (Ex. 1005, Abstract.) For

example, Johnson provides a website where homeowners can log in to access, monitor and control a home's security system, lighting system, exterior cameras and the like. (*Id.*, 2:8-28, 6:35-59.) The web site is provided through one or more data center 20 servers that are located remotely from the home. (*Id.*, 4:15-53.)

3. Overview of Severson

Severson issued on August 21, 1990 and therefore qualifies as prior art under 35 U.S.C. § 102(b). Severson discloses a home security system controller that automatically discovers newly-added sensors its security network. (Ex. 1006, 23:60-26:7; Ex. 1002, ¶¶ 70-72.)

4. Overview of Naidoo

Naidoo published on April 3, 2003 and therefore qualifies as prior art under 35 U.S.C. § 102(b). Naidoo was used as a primary reference against the claims during prosecution. It is used here as a secondary reference for a few of the dependent claims. Naidoo discloses transmitting alarm and video data from a premise security gateway 115 to a security server 131, a central monitoring station 136, and/or a remote client device 155. (Ex. 1007, FIG. 7, ¶¶ 0069-0070, Ex. 1002, ¶ 73.)

5. Overview of Alexander

Alexander issued on June 8, 2004 and is prior art under 35 U.S.C. § 102(a). Alexander discloses an integrated security system connected to a remote server

capable of creating and modifying user accounts, and creating and modifying system devices. (Ex. 1008, Abstract, Ex. 1002, ¶74.)

6. Overview of Anthony

Anthony published on July 24, 2003 and therefore qualifies as prior art under 35 U.S.C. § 102(b). Anthony discloses security cameras for use in various security operations, including home security. (Ex. 1009, ¶¶ 31-33.) Anthony discloses a security system that allows continuous remote monitoring and analysis. (Ex. 1009, ¶ 38.) Audiovisual signals and other signals from the system can be transmitted via general packet radio service ("GPRS"). (Ex. 1009, ¶¶ 8, 29, 39, 40, 44, 57, 92, Ex. 1002, ¶ 75.)

B. The Cited References Are Analogous Art

As indicated in the section above and as explained in Mr. Parker's declaration, each of the prior art references combined in this Petition is analogous art to the '619 patent and to each other, as each reference is in the same field of endeavor as the '619 patent. (Ex. 1002, ¶ 76.)

C. Grounds 1-3 – Claims 17, 18, 20-22, 29-31, 33, 35-41, 48-53 and 58 Are Obvious over Wimsatt in view of Johnson and/or Other Prior Art References Under 35 U.S.C. § 103(a)

Claims 17, 18, 20-22, 29-31, 33, 35-41, 48-53 and 58 are rendered obvious under 35 U.S.C. § 103(a) for the reasons that follow. The elements of claims 1, 16, 24 and 32 are addressed herein despite the fact that claims 1, 16, 24 and 32 are not

the subject of this petition. The elements of claim 1 and 16 are addressed because claims 17, 18, 20-22, 29-31, 33, 35, 37-41 and 48-53 depend from claim 1 and/or 16. The basis of rejection for each of claims 1 and 16 is incorporated into each of the claims that depend therefrom.

1. Independent claim 1

a. Preamble: "A system comprising"

For the reasons discussed in the following sections, Wimsatt in view of Johnson and Severson discloses all the elements of the claimed system.

b. Claim element 1[a]: "a gateway located at a first location"

Wimsatt discloses a control panel 101 that is mounted within a user's home at a central location. (Ex. 1004, ¶ 0034.) The control panel 101 is the claimed "gateway" and the user's home is the claimed "first location."

c. Claim element 1[b]: "a connection management component coupled to the gateway and automatically establishing a wireless coupling with a security system installed at the first location"

Wimsatt discloses this limitation in its entirety. For clarity, this limitation is divided into two parts and discussed separately.

i. "a connection management component coupled to the gateway …"

A POSITA would understand that the "connection management component" (referred to also throughout as "CMC") would be a module implemented by a

processor to carry out the claimed operations. (Ex. 1002, ¶ 80.) A POSITA would also have understood that the control panel 101 in Wimsatt must also include a module to perform the discovery and connection processes that it describes and, thus, the control panel 101 in Wimsatt must indeed include the "connection management component" that would be responsible for the claimed couplings of the system. (*Id.*) Because the CMC is implemented by the control panel 101 (via its processor 201), Wimsatt discloses that the CMC is coupled to the control panel 101.

ii. "a connection management component … automatically establishing a wireless coupling with a security system installed at the first location"

Wimsatt discloses that the user's home (i.e., the claimed "first location") includes a security system. (*See, e.g.*, Ex. 1004, ¶ 0005 ("Home automation systems may be integrated with a home security system"), ¶ 0012 (describing a home automation system that controls "security systems"), ¶ 0023 (explaining that the "invention is particularly useful in home automation environments because it builds on top of the vast array of controlled devices and subsystems that already exist for managing … security systems"), ¶¶ 0029-0031 ("tripping a zone on a burglar alarm … may indicate a household member [is] entering the house"), ¶¶ 0043, 0057-0058, 0062, 0065, 0073-0074.)

Wimsatt discloses that its control panel 101 can implement a "system discovery process." A POSITA would have understood that the CMC module performs this process. (Ex. 1002, ¶¶ 82-83.) According to Wimsatt, "[w]hen a control panel 101 is coupled to a controlled device or subsystem, it interrogates that device or subsystem to learn details of the control interface of that particular system." (Ex. 1004, ¶ 0045.) "This interrogation may simply be a matter of determining the controller type in which case the control panel 101 can look up a command set and signaling protocol information for that controller type." (*Id.*) Wimsatt also explains that when the interrogation process does not work correctly, "the control panel can be **manually or semi-automatically** programmed to support that controlled device or subsystem." (*Id.* (emphasis added)) This last passage indicates that the interrogation process is automatic (i.e., the control panel 101 automatically discovers the controlled devices) because manual or semi-automatic programming is only performed when the automatic interrogation fails. (*See also,* Ex. 1004, ¶ 0006 (describing the difficulties of manually adding devices to a network).) Per this disclosure, the control panel 101 can automatically discover the home security system when the home security system is coupled to the control panel 101.

Wimsatt further discloses that its control panel 101 can be wireless (referred to as "control panel 107") and can wirelessly communicate with any of the

controlled devices of the security system as a result of the above discovery process (e.g., because it now has the signaling protocol information needed for communication). (Ex. 1004, ¶¶ 0037, 0043.)

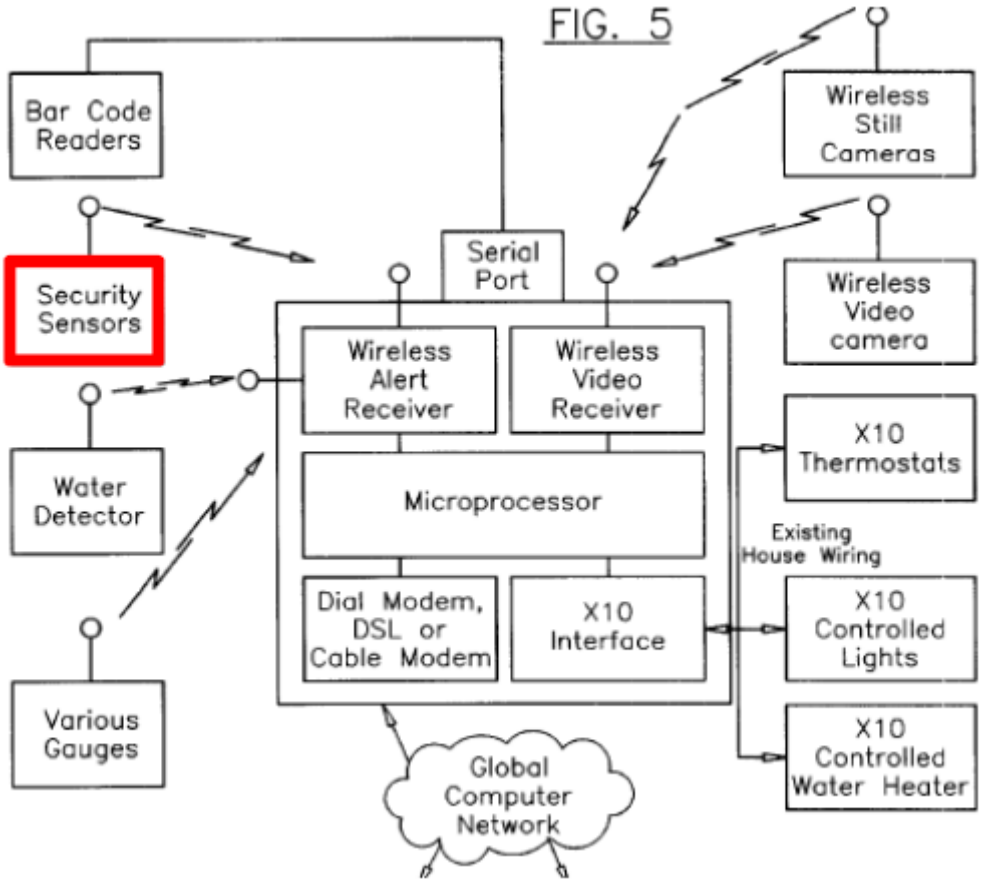
d. Claim element 1[c]: "the security system including security system components"

The '619 patent discloses that "security system components" can be sensors or any other components "belonging to the security system." (Ex. 1001, 4:40-45.) While Wimsatt does not illustrate sensors in its security system, a POSITA would have understood that the security system indeed includes sensors. (Ex. 1002, ¶ 85.) Wimsatt discloses at paragraph [0031] that "tripping a zone on a burglar alarm … causes the control units to display a security screen having controls that allow the alarm to be de-activated." (Ex. 1004, ¶ 0031.) A POSITA would have understood that a "burglar alarm" is a security system and that at least one sensor is located within each zone of the house. (Ex. 1002, ¶ 85.) It is this sensor (or sensors) that is "tripped" and sets off an alarm. Thus, sensors are inherent in Wimsatt.

To the extent Patent Owner disagrees, it would be obvious from Wimsatt that its security system includes sensors. It was well known at the time of the '619 patent that home security systems came equipped with multiple sensors (e.g., motion sensors, door sensors, window sensors, etc.) that could be mounted at various locations throughout a home. (Ex. 1002, ¶ 86.) As Mr. Parker explains in

his declaration, sensors are the "eyes" of a home security system. (*Id*.) Without sensors, a home security system is blind and cannot function. (*Id*.)

To the extent the Patent Owner further argues that a more specific disclosure of sensors is required, Johnson has that disclosure. As illustrated in the below excerpted and annotated Figure 5 of Johnson, the security system 60 includes "security sensors." (*See also*, Ex. 1005, FIG. 3 (illustrating icons for well-known components of a home security system, e.g., a door sensor, a window sensor and a smoke alarm).)



While a POSITA would have understood that Wimsatt already indicates the

presence of sensors, it would be obvious to modify Wimsatt to include the plurality of security sensors disclosed in Johnson to make this disclosure more explicit. (Ex. 1002, ¶ 88.)

e. Claim element 1[d]: "wherein the connection management component forms a security network by automatically discovering the security system components and integrating communications and functions of the security system components into the security network"

For clarity, this limitation is divided into three parts and discussed separately. Petitioner discusses "form[ing] a security network" last because it is the end result of "automatically discovering" and "integrating" the devices.

i. "the connection management component … automatically discovering the security system components"

Wimsatt discloses that its control panel 101, including the connection management component, can implement a "system discovery process." According to Wimsatt, "[w]hen a control panel 101 is coupled to a controlled device or subsystem, it interrogates that device or subsystem to learn details of the control interface of that particular system." (Ex. 1004, ¶ 0045.) Wimsatt also explains that when the interrogation process does not work correctly, "the control panel can be **manually or semi-automatically** programmed to support that controlled device or subsystem." (*Id.* (emphasis added)) This last passage indicates that the interrogation process is automatic (i.e., the control panel 101 automatically

discovers the controlled devices) because manual or semi-automatic programming is only performed when the automatic interrogation fails. (*See also,* Ex. 1004, ¶ 0006 (describing the difficulties of manually adding devices to a network).) Per this disclosure, the control panel 101 can automatically discover the home security system when the home security system is coupled to the control panel 101.

Wimsatt also discloses that its control panel 101 implements "Universal Plug-and-Play (UPnP™) processes." (Ex. 1004, ¶ 0054.) It was well known at the time of the '844 patent that UPnP™ was used to auto-discover 2-way devices connected to a shared network. (Ex. 1002, ¶ 91 (citing to Ex. 1011, 7).)

Wimsatt does not explicitly disclose that its security system's sensors are automatically discovered using this process – it only explicitly discloses that the "security system" is discovered. A POSITA would have understood that discovering the security system would also include discovering its sensors. (Ex. 1002, ¶ 92.) To the extent Patent Owner disputes this, Severson discloses a security system that includes a controller and a plurality of sensors. (Ex. 1006, FIG. 1, 4:3-29.) Severson explains that "without human intervention" "each system controller may be operated to 'self-learn' each of its sensors." (Ex. 1006, 25:3-13.) In describing a system installation process, Severson explains that the sensors and controller are mounted at the home and then "the controller is enabled and self-learns each of its sensors/transducers as they report their status." (Ex. 1006, 25:51-

26:7; *see also, id.*, 23:60-25:50.) As a result, "[i]nstallation time is thereby reduced with minimal potential installer error, due to the CPU self-learning its reporting sensors." (*Id.*, 25:51-26:7.) This is similar to the auto-discovery process described in the '619 patent. (*See, e.g.*, Ex. 1001, FIG. 14, 24:66-26:5.)

Motivation to Combine Severson with Wimsatt and Johnson: It would be obvious to a POSITA to combine the auto-discovery disclosure with Wimsatt and Johnson so that the control panel 101 in Wimsatt can auto-discover the security sensors in addition to the discovering the security system controller. (Ex. 1002, ¶ 93.) This would predictably result in an easier sensor installation process and reduce the likelihood of installer error. (Ex. 1002, ¶ 93; *see also*, Ex. 1006, 26:5-7.)

As previously discussed, Wimsatt already discloses an automatic discovery process for learning the security system so it would be obvious to a POSITA to further discover the sensors that form part of that system. (Ex. 1004, ¶ 0045; Ex. 1002, ¶ 94.) A POSITA would understand that the control panel 101 would want to "discover" all of the devices that it and the data center 20 server in Johnson controls. Severson illustrates the ability and desire for similar controllers to automatically discover devices at the security component level. A POSITA would understand that adding an extra step in the automatic discovery process to include discovery of the sensors would be easy to implement. (Ex. 1002, ¶ 94.)

ii. "the connection management component … integrating communications and functions of the security system components into the security network"

As background, Wimsatt discloses a home automation system. The purpose of a home automation system, in general, is to communicate with and control the functionality of multiple home-based devices such as lighting, heating and air conditioning, media equipment, and security systems. (Ex. 1004, ¶¶ 0005-0006.) In its background section, Wimsatt provides an example of how such systems were known to operate with home security systems: "Home automation systems may be integrated with a home security system so that when a fire alarm is raised, for example, internal and external lights will be turned on." (Ex. 1004, ¶ 0005.) In other words, it was well known at the time of the '619 patent that home automation systems communicated with home-based devices (such as the lights in the above example) and controlled their functionality (i.e., the system commanded the lights to "turn on"). Thus, the general concept of integrating communications and functions of home-based devices into a home automation system was well known long before the earliest priority date of the '619 patent. (Ex. 1002, ¶ 95.)

Looking at Wimsatt's system specifically, the control panel 101, including the connection management component, "integrat[es]" communications and functions of its home-based control devices through the system discovery process discussed above. (*See, e.g.,* Ex. 1004, ¶ 0045.) Through this discovery process, the

control panel 101 is able to "learn" various details about the controlled device, such as its command set, signaling protocol information, and the functionality available for that device. (Ex. 1004, ¶ 0046.) The control panel 101 is then able to communicate with and control the functions of that device. (Ex. 1002, ¶ 96.)

Wimsatt identifies the home's security system as one type of controlled device. (*See, e.g.*, Ex. 1004, ¶¶ 0012, 0029, 0058.) The specification also states that "control application software executes on the control unit to communicate control information such as commands, ***sensor messages***, status messages, and the like with … controlled systems (e.g., ***security systems*** …)." (*Id.* ¶ 0012 (emphasis added).) It further explains that this software "may enable features of the security system to be enabled/disabled." (Ex. 1004, ¶ 0058.) A POSITA would have understood that controlling features of a security system would include controlling features (i.e., functions) of the security system's sensors via the home's security system. (Ex. 1002, ¶ 97.) The control panel 101 would not otherwise have the ability to control or communicate with the devices if it had not discovered the devices and integrated their functionality into itself and the overall system. Thus, this portion of the limitation is satisfied by Wimsatt, Johnson and Severson.

iii. "the connection management component forms a security network …"

A POSITA would have understood that the claimed "security network" is formed in Wimsatt (as modified by Johnson and Severson) as a result of the

control panel's CMC integrating the functions of the security system sensors. (Ex. 1002, ¶¶ 98-100.) Wimsatt actually refers to its overall network more generically as a "home automation system" because its control panel 101 integrates the functions of many other types of home-based control devices, in addition to security-related devices. (*See, e.g.,* Ex. 1004, ¶¶ 0005, 0012.) But, a POSITA would have understood that this home automation system includes a security network, which is specific to the security-related devices. (Ex. 1002, ¶¶ 98-100.)

f. Claim element 1[e]: "a security server at a second location different from the first location, wherein the security server is coupled to the gateway"

This limitation is disclosed by Wimsatt and Johnson. Petitioner relies on Johnson for disclosing a remotely located server coupled to a control panel. (*See also*, Ex. 1002, ¶ 101.) Johnson discloses a control unit 30 that is similar to panel 101 in Wimsatt and that is located within a user's home. (Ex. 1005, 4:15-39.) Control unit 30 in Johnson is coupled to a remotely located data center 20 via a global computer network 12. (*Id*.) Johnson explains that its data center 20 comprises "**one** or more server computers" that are "capable of receiving, storing and transmitting various types of data related to the homeowner's home," including security data. (Ex. 1005, 4:40-53 (emphasis added); *see also, id.*, 4:16-39.) This data center 20 server is the claimed "security server." The data center 20

server in Johnson is located remotely from the user's home and is thus "in a second location different from the first location." (*See*, Ex. 1005, FIG. 5.)

Motivation to Combine Johnson with Wimsatt and Severson: It would be obvious to a POSITA to combine Johnson with Wimsatt and Severson so that panel 101 in Wimsatt is coupled to data center 20 server in Johnson. (Ex. 1002, ¶ 102.) As a result of this coupling, the control panel 101 can be remotely accessed and controlled through data center 20 server as described in Johnson. (*Id.*) Johnson specifically improves upon panel 101 in Wimsatt and explains that "[o]ur society has become extremely mobile with the reduced expense and ease of travel leaving many homes unattended while the homeowner is traveling or at work" (Ex. 1005, 1:14-16) and that "there is a need for a home monitoring system that allows a homeowner to monitor their home from a distant location." (*Id.*, 1:14-25.) Coupling panel 101 in Wimsatt to remotely located data center 20 server would allow for such remote monitoring and control. (Ex. 1002, ¶¶ 102-103.)

A POSITA would be further motivated to combine Johnson with Wimsatt because control unit 30 in Johnson is similar to panel 101 in Wimsatt. (Ex. 1002, ¶ 103.) Control unit 30 and panel 101 are systems that integrate functionality from multiple subsystems (e.g., security systems, lighting systems, entertainment systems, surveillance systems, etc.) into a single controller for user control and convenience. (*See, e.g.,* Ex. 1004, ¶¶ 0022-0023; Ex. 1005, 4:16-39.) Furthermore,

panel 101 in Wimsatt is already connected to the Internet so it would be an easy task for the panels to connect with data center 20 server in Johnson. (Ex. 1002, ¶ 103.) The end result would be a system that allows a homeowner to directly control aspects of the panels (and their subsystems) from remote locations similar to Johnson. Severson illustrates the ability and desire for similar controllers to automatically discover devices at the security component level. A POSITA would understand that adding an extra step in the automatic discovery process to include discovery of the sensors would be easy to implement. (Ex. 1002, ¶ 103.)

g. Claim element 1[f]: "wherein the gateway receives security data from the security system components, device data of a plurality of network devices coupled to a local network of the first location that is independent of the security network, and remote data from the security server,"

Wimsatt and Johnson disclose this limitation. In general, Wimsatt discloses that its control panel 101 receives "status signals" from the controlled devices. (Ex. 1004, ¶ 0044.) The controlled devices include, for example, IP cameras and the home's security system.

With respect to the security system's sensors specifically, Wimsatt discloses several scenarios where a burglar alarm (i.e., one or more sensors) is triggered, causing the control panel 101 to sound an alarm. (Ex. 1004, ¶¶ 0030-0031, 0059.) A POSITA would have understood that, in these particular scenarios, the status of the security system's sensors is sent to the control panel 101 in some form. (Ex.

1002, ¶ 105; *see also*, Ex. 1004, ¶¶ 0044, 0056, 0059; *compare to* Ex. 1001, 27:5-10.) Thus, it would be obvious to a POSITA that the control panel 101 in Wimsatt receives "security data" from the security system sensors. (Ex. 1002, ¶ 105.)

With respect to the "network devices", the '619 patent discloses that these can be IP cameras. (*See, e.g.*, Ex. 1001, 14:20-27, FIG. 5.) Wimsatt discloses IP cameras 109. (Ex. 1004, ¶¶ 0038, 0072 ("one or more monitor cameras such as IP camera 109").) As just discussed, the control panel 101 in Wimsatt receives "status signals" from the IP cameras. (Ex. 1004, ¶ 0044; *see also*, *id.*, ¶ 0038 (explaining that IP cameras "communicate control messages with a network-coupled control panel 101"), ¶ 0056 (describing "control messages" as "including command and status messages").) Wimsatt also discloses that the control panel 101 receives a streaming input from the IP cameras. (Ex. 1004, ¶¶ 0072, 0075, FIG. 6.) It further discloses that the control panel 101 receives details about the IP cameras (e.g., signaling protocol information) as part of the discovery process. (Ex. 1004, ¶ 0045.) Thus, Wimsatt clearly discloses that its control panel 101 receives "device data of the network devices" as recited in this limitation.

Wimsatt further discloses that the IP cameras are coupled to a local area network (LAN) via a hub 103, which is described as implementing an Ethernet connection among the system devices. (Ex. 1004, ¶ 0036, FIG. 1.) It is well known that Ethernet connections form LANs. (Ex. 1002, ¶ 107.). The hub 103 in Wimsatt

is located within the home and therefore the LAN is also located at the "first location." (*See, e.g.*, Ex. 1004, ¶¶ 0036, 0038, 0040 (each passage describing physical couplings between the hub 103 and system devices located within the home indicating the hub's physical presence within the home).) Because the IP cameras 109 are coupled to the hub 103 and not the control panel 101 in Wimsatt, the IP cameras can be considered part of a "local network" that is independent from the "security network" which consists of the security system and the sensors with which it directly communicates. (Ex. 1002, ¶ 107.) Thus, Wimsatt discloses that its IP cameras are coupled to a local network that is independent from the security network.

With respect to the security server and "remote data", as previously discussed, it would have been obvious to a POSITA to modify Wimsatt so that the control panel 101 is coupled to the data center 20 server in Johnson (i.e., the claimed "security server"). *See* **Part IX.C.1.f** above. Johnson discloses that its control unit 30 "may [] download any data from the data center 20 such as commands from the homeowner." (Ex. 1005, 5:13-18; *see also, id.*, 6:65-7:2, 7:67-8:4.) This data is the claimed "remote data." It would have been obvious to modify the control panel 101 in Wimsatt so that it receives data from the remotely-located data center 20 server in the same manner described for the control unit 30 in Johnson. (Ex. 1002, ¶ 108.) As such, a homeowner in Wimsatt would be able to

remotely control the control panel 101 and the networked controlled devices through the data center 20 server as described in Johnson. (*Id.*) The motivations to combine Wimsatt, Johnson and Severson discussed above in **Part IX.C.1.f** apply here. Thus, Wimsatt (as modified by Johnson and Severson) discloses that its control panel 101 receives "remote data from the security server" as recited in this limitation.

h. Claim element 1[g]: "wherein the gateway generates processed data by processing at the gateway the security data, the device data, and the remote data,"

Wimsatt and Johnson disclose this limitation. The control panel 101 in Wimsatt includes a processor 201 that "implements data processing functionality for accessing and manipulating data from various subsystems and memory." (Ex. 1004, ¶ 0047.) Thus, it would be obvious for this processor 201 to generate "processed data" by processing the "security data" from the security system sensors, the "device data" from the IP cameras, and the "remote data" from the data center 20 server in Johnson. (Ex. 1002, ¶ 109.)

With respect to the "security data", as previously discussed, when one or more security system sensors are activated (e.g., a burglar alarm is triggered), the sensors transmit a "status signal" that is received at the control unit 101. (*See, e.g.*, Ex. 1004, ¶¶ 0030-0031, 0059.) According to Wimsatt, the control panel's processor 201 includes a message broker process that receives this status signal,

interprets it, and then passes it to the security plug-in for further processing. (Ex. 1004, ¶¶ 0044, 0056, 0058-0059.) If the security plug-in (executed by the processor 201) determines that the received "security data" indicates an intrusion, it activates the necessary audio plug-in to sound an alarm on the control panel 101. (Ex. 1004, ¶ 0059.) Thus, the "security data" is "processed" by the control panel's processor 201.

With respect to the "device data", a POSITA would understand that any status signal from the IP cameras 109 would be processed by the processor 201 in a manner similar to that described above for the "security data". (Ex. 1002, ¶ 111.) Any streamed input received at the control panel 101 from the IP cameras 109 would also necessarily require processing. (Ex. 1002, ¶ 111.) Furthermore, when the "device data" is, for example, the signaling protocol information received by the control panel 101 as part of the IP camera discovery process, a POSITA would have understood that this information is processed by the processor 201 because the processor 201 uses this information to generate messages that can be communicated to the IP camera via that protocol. (Ex. 1002, ¶ 111; *see also*, Ex. 1004, ¶¶ 0038, 0045, 0054.)

Finally, with respect to the "remote data", as previously discussed, when the control panel 101 in Wimsatt is modified by Johnson, the control panel 101 is capable of receiving data from a remotely-located data center 20 server. *See* **Part**

IX.C.1.g above. The data can be, for example, commands entered by a homeowner instructing the control panel 101 to change one or more settings on a controlled device (e.g., the home security system). (*See, e.g.*, Ex. 1005, 4:15-53.) A POSITA would understand that data received at the control unit 101 from data center 20 server would be processed by the control unit's processor 201 so that the data can be interpreted and the appropriate actions taken by the control unit 101 to modify the settings of the particular controlled device. (Ex. 1002, ¶ 112.) The same motivations to combine Wimsatt and Johnson discussed in **Part IX.C.1.f** apply here.

i. Claim element 1[h]: "wherein the gateway determines a state change of the security system using the processed data and maintains objects at the security server using the processed data, wherein the objects correspond to the security system components and the plurality of network devices"

Wimsatt and Johnson disclose this limitation in its entirety. For clarity, this limitation is divided into two parts and discussed separately.

i. "wherein the gateway determines a state change of the security system using the processed data …"

Wimsatt and Johnson also disclose this limitation. Wimsatt discloses that the control panel 101 can be used to arm and disarm the home's security system. (Ex. 1004, ¶¶ 0065-0066, 0070-0071, 0074.) When Wimsatt is modified by Johnson, a homeowner can control this functionality remotely through the data center 20

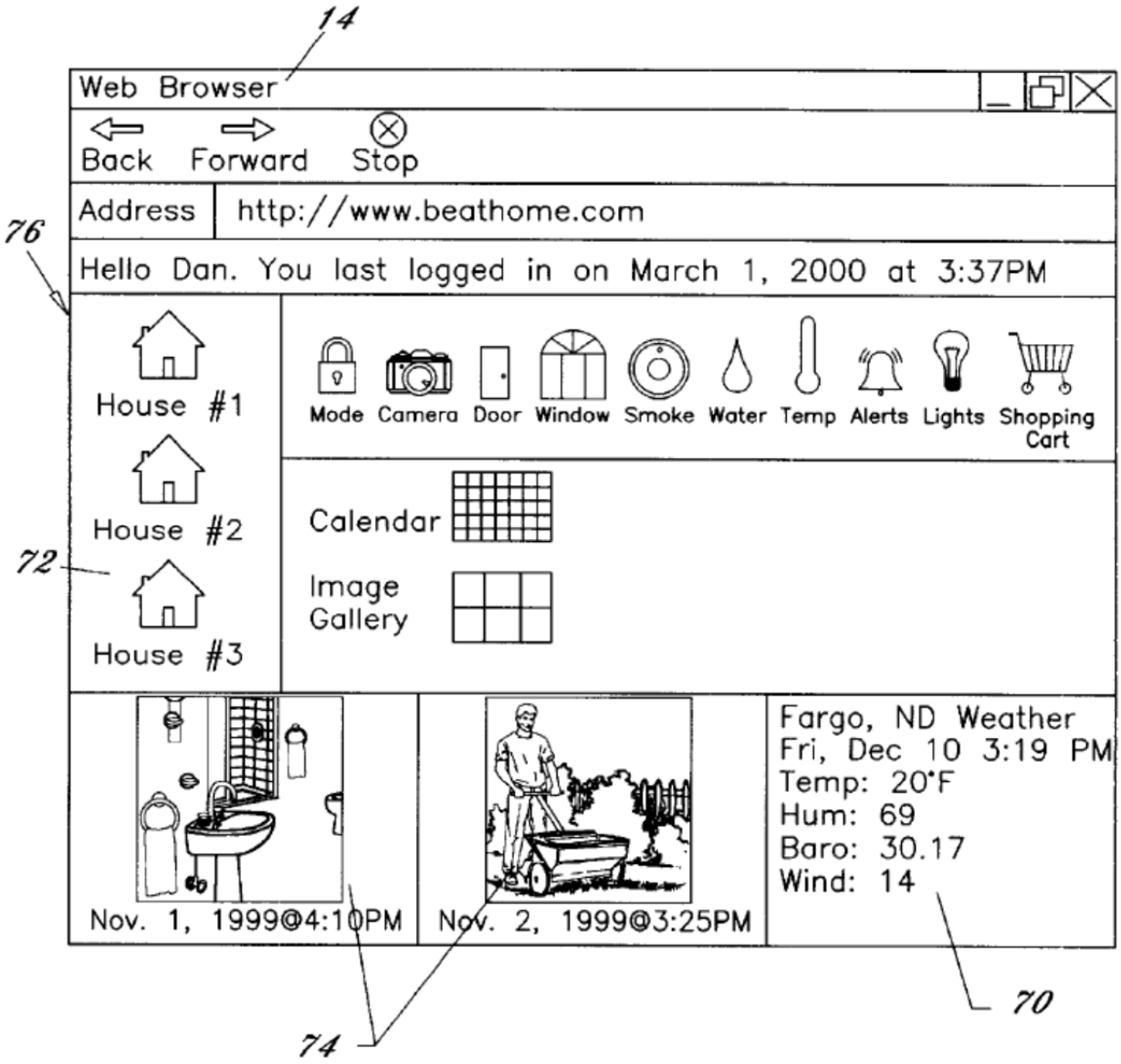
server. For example, if the status (or "state") of the security system (and its sensors) is "unarmed", then the homeowner can send a command signal though the data center 20 server to the control panel 101 instructing the control panel 101 to change the status (or "state") of the security system (and its sensors) to "armed". (Ex. 1002, ¶¶ 114-115.) A POSITA would have understood that the control panel 101 in Wimsatt must process this "remote data" from the data center 20 server to determine what command needs to be implemented. (*Id*.) Here, upon processing, the control panel 101 would have determined that the status (or "state") of the home security system needs to be changed from "unarmed" to "armed." (*Id*.)

ii. "wherein the gateway … maintains objects at the security server using the processed data, wherein the objects correspond to the security system components and the plurality of network devices"

The '619 patent explains that the remote security server "provide[s] access to, and management of, the objects associated with an integrated security system." (Ex. 1001, 8:29-41.) It further explains that "every **object** monitored by the gateway 102 is called a **device**." (*Id*. (emphasis added)) "Devices include the sensors, cameras, home security panels and automation devices." (*Id.*)

Wimsatt and Johnson disclose the above limitation consistent with this disclosure in the '619 patent. As shown below in Figure 3 of Johnson, the homeowner accesses a web page "displayed by the data center 20" and can

"monitor[] and control[]" aspects of the security system and cameras using that web page. (Ex. 1005, 4:30-36, 5:29-39, 6:35-59.)



Johnson explains that a homeowner can "modify any preprogrammed settings within the home" by "simply select[ing] the desired feature on the control page 76 of the desired home as shown in FIGS. 3 and 7." (Ex. 1005, 6:61-65.) "The homeowner may then enter the desired data into the computer 16 which is

transmitted to the data center 20 which forwards the information directly to the control unit 30 which transmits the data accordingly modifying any previous settings." (Ex. 1005, 6:65-7:4.) When Wimsatt is modified by Johnson, the homeowner is able to remotely control the control panel 101 and the controlled devices in the same manner. (Ex. 1002, ¶ 118.)

A POSITA would have understood that the icons illustrated on the above web page represent particular controlled devices located within the home in Wimsatt. (Ex. 1002, ¶ 119.) These icons are the claimed "objects" maintained and stored at the data center 20 servers. For example, the icon labeled "camera" is an object at the server corresponding to the IP cameras 109. Similarly, the icons labeled "door" and "window" are objects at the server corresponding to a door sensor and a window sensor, respectively.

A POSITA would have also understood that the data center 20 server maintains the status of each of these objects (corresponding to the camera, window and door sensors) using the processed data it receives from the control panel 101, as discussed in **Part IX.C.1.h** above. (Ex. 1002, ¶ 120.) As Mr. Parker explains in his declaration, it would be difficult to change a device's settings without knowing the current status of that device. (Ex. 1002, ¶ 120; *see also*, Ex. 1005, 7:6-8.) Thus, it would be obvious to a POSITA to conclude that the control panel 101 in Wimsatt transmits the processed security data and device data to the data center 20 server so

that the web page displayed for the homeowner has the most up-to-date information about the objects. (Ex. 1002, ¶ 120.) Thus, the control panel 101 in Wimsatt "maintains" the "objects at the security server using the processed data."

For at least these reasons, Wimsatt in view of Johnson and Severson disclose claim 1.

2. Dependent claim 16

16	The system of claim 1, wherein the security system is coupled to a central monitoring station via a primary communication link, wherein the gateway is coupled to the central monitoring station via a secondary communication link that is different than the primary communication link, wherein the central monitoring station is located at a third location different from the first location and the second location.

Claim 16 is rendered obvious by Wimsatt and Johnson. Johnson discloses that its control unit 30 can communicate over the Internet with an auxiliary service 80 to report a security breach. (Ex. 1005, 6:6-11, 6:27-29, 4:20-21, FIG. 5 ("security service").) A POSITA would understand from Johnson that the auxiliary service could be a security agency or service that can call the homeowner at, for example, their office to notify them of the breach. (*Id.*, 1:27-32.) This auxiliary service / agency is the claimed "central monitoring station" and is at a third location separate from the first location and second location. The Internet can be implemented by, for example, a "digital subscriber line (DSL)," which is the claimed "secondary communication link." Thus, Wimsatt in view of Johnson

discloses "*wherein the gateway is coupled to the central monitoring station via a secondary communication link.*"

In its background section, Johnson explains that conventional security system panels communicate directly with security agencies. (Ex. 1005, 1:27-32.) Nothing in Wimsatt suggests that its security system panel loses any functionality when it is connected to the control panel 101 as part of the home automation system. According to Wimsatt, the control panel 101 is intended to work with *existing devices* and merely provides a user-friendly interface through which those devices can be controlled. (Ex. 1004, ¶¶ 0023, 0065.) Wimsatt is silent with respect to the control panel 101 being capable of communicating with an outside service, such as a central monitoring station, so a POSITA would have understood that the security system in Wimsatt maintains the ability to contact the monitoring station even when it is part of the home automation system. (Ex 1002, ¶ 114.)

Wimsatt and Johnson do not disclose how the security system communicates with the monitoring center, but Severson does. Severson discloses that its security system controller communicates with a central monitoring station 4 via one or more telephone lines. (Ex. 1006, 3:57-4:2.) When Wimsatt is modified by Severson and Johnson, the security system in Wimsatt communicates with the security agency via a telephone line. This telephone line is the claimed "primary communication link." A telephone line is a different communication channel than a

DSL.

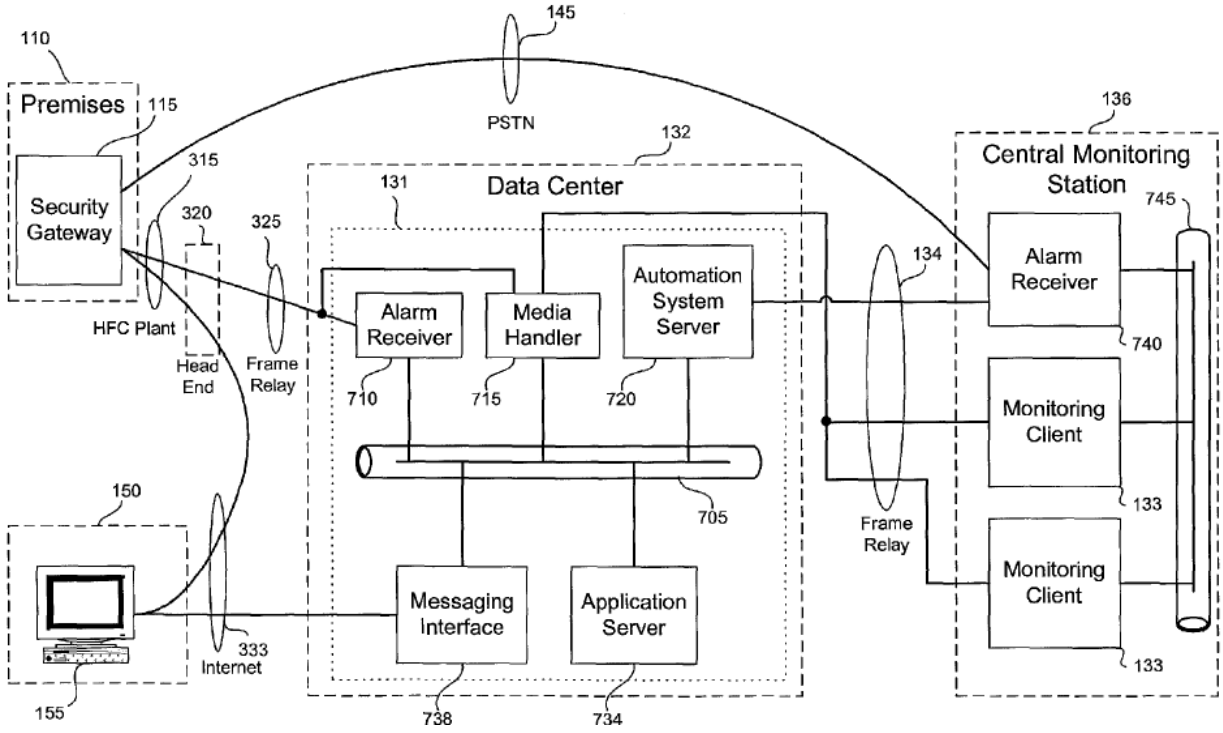
It would have been obvious to combine Wimsatt with Johnson and Severson so that both the security system and the control panel 101 in Wimsatt are capable of contacting a security agency (or central monitoring station). (Ex. 1002, ¶¶ 145-146.) A POSITA would have understood the benefit of having two devices capable of contacting a security agency on different communication channels. (*Id*.) For example, once device (e.g., the control panel 101) could act as a back-up in case the first device (e.g., the security system) failed to make contact with the central monitoring station.

3. Dependent claim 17 – Ground 1

17	The system of claim 16, wherein the gateway transmits event data of the security system components to the central monitoring station over the secondary communication link.

Claim 17 is disclosed by Wimsatt in view of Johnson, Severson and Naidoo. An overview of Naidoo's security system is illustrated below. (Ex. 1007, FIG. 7.) As shown, the security gateway 115 in Naidoo (which is located on a homeowner's premises) communicates directly with a data center 132 (similar to Johnson) as well as a central monitoring station 136 (also similar to Johnson). Naidoo discloses that, upon detection of an alarm event, the gateway 115 sends the central monitoring station 136 "notification of the alarm condition and information relating to the alarm condition, which may include alarm video." (Ex. 1007, ¶¶

0070-0071.)



When Wimsatt in view of Johnson is further modified by Naidoo, the control panel 101 in Wimsatt is capable of sending the security sensor alarm data to the central monitoring station 136, as described in Naidoo. Transmission between the control panel 101 and the central monitoring station 136 occurs over the DSL, as discussed in claim 16. (Ex. 1002, ¶ 148.)

It would have been obvious to a POSITA to combine Naidoo with Wimsatt, Johnson and Severson so that the control panel 101 in Wimsatt could communicate certain event data with the central monitoring station. (Ex. 1002, ¶ 149.) As discussed in Naidoo, by providing the sensor event data to the central monitoring

station, an operator, in short order, is able to "verif[y] whether the alarm signal corresponds to an actual alarm condition using the alarm signal information and the segment of real-time video," and then take appropriate action. (Ex. 1007, ¶¶ 0075, 0077, 0008, 0011, 0027.) "Timely response may increase the chance of apprehending an intruder, and in the case of life-threatening circumstances, reduce the likelihood of injury or death." (*Id.*, ¶ 0100.) A POSITA would have understood these benefits and been motivated to combine Naidoo with Wimsatt, Johnson and Severson to enhance their respective security capabilities and first-responder response times.

A POSITA would have also understood that sending sensor data and video data is a relatively easy task, especially since Johnson already provides for the connection between the control panel 101 in Wimsatt and a central monitoring station. (Ex. 1002, ¶ 150.)

4. Dependent claim 18 – Ground 1

18	The system of claim 17, wherein the event data comprises changes in device states of the security system components, data of the security system components, and data received by the security system components.

As discussed for claim 17, Naidoo discloses that, upon detection of an alarm event, the gateway 115 sends the central monitoring station 136 "notification of the alarm condition and **information relating to the alarm condition**." (Ex. 1007, ¶¶

0070-0071 (emphasis added).) Thus, for the same reasons discussed for claim 17, claim 18 is rendered obvious under Ground 1.

5. Dependent claim 20 – Ground 2

20	The system of claim 16, wherein the secondary communication link includes a General Packet Radio Service (GPRS) coupling.

It is well known that GPRS communications are a type of mobile communication. (Ex. 1002, ¶ 153.) Naidoo discloses that gateway 115 can transmit to a security server 131 (similar to the data center 20 server in Johnson) via a "mobile communications network." (Ex. 1007, ¶ 0043.) It would be obvious to a POSITA that the gateway 115 in Naidoo could also communicate with the central monitoring station 136 via this same mobile communications network as long as the station 136 is equipped to handle such communication. (Ex. 1002, ¶ 153.)

Anthony discloses a security system that allows continuous remote monitoring and analysis. (Ex. 1009, ¶ 38.) Audiovisual signals and other signals from the system can be transmitted via general packet radio service ("GPRS"), which is a mobile communication mode. (Ex. 1002, ¶ 154.)

It would be obvious to a POSITA to combine Naidoo with Wimsatt, Johnson and Severson so that the control panel 101 in Wimsatt can communicate with the central monitoring station via the mobile communications network disclosed in Naidoo. (Ex. 1002, ¶ 155.) It would further be obvious to a POSITA to combine Anthony with Naidoo, Wimsatt, Johnson and Severson to utilize available mobile

communication modes, such as GPRS. (*Id*.)

6. Dependent claim 21 – Ground 1

21	The system of claim 16, wherein the gateway transmits messages comprising event data of the security system components to remote client devices over the secondary communication link.

Naidoo discloses that its security server 131 can "create a data connection between remote station 155 and security gateway 115 such that communications between remote station 155 and security gateway 115 bypass security system server 131." (Ex. 1007, ¶ 0041.) Through this connection, the gateway 115 can "transmit the alarm signal and alarm video corresponding to the alarm condition automatically to [the] customer … at an email address [or] by any other electronic means." (*Id.*, ¶ 0069.) As discussed for claim 8, Johnson discloses various types of "remote client devices" that can be implemented in Wimsatt.

It would have been obvious to a POSITA to combine the above disclosures from Naidoo with Wimsatt, Johnson and Severson so that the control panel 101 in Wimsatt is capable of directly communicating event data with the remote client devices (such as those described in Johnson). (Ex. 1002, ¶ 157.) This communication would be over the DSL channel as described for claim 16 (the relevant arguments for which apply here) because that is the channel the control panel 101 uses when communicating with external devices / entities. (Ex. 1002, ¶ 157.)

Naidoo explains that bypassing a security server "avoids network bottlenecks" at the server – this is especially important during an alarm condition when server resources should be spent processing alarm data instead of sending messages to customers. (Ex. 1007, ¶ 0041.) In other words, the direct connection can provide a better allocation of resources. (Ex. 1002, ¶ 158.)

Also, a POSITA would have understood that creating this connection between devices would have been a relatively simple task since the control panel 101 and the remote client devices are already connected to the Internet (via DSL). (Ex. 1002, ¶ 159.) Furthermore, when a homeowner is remotely located from the home, receiving a message with this data would have brought "peace of mind" that the situation is being handled and it would quickly alert the homeowner of the alarm condition so they can appropriately. A POSITA would understand the aforementioned benefits and would have been motivated to combine these references. (Ex. 1002, ¶ 159.)

7. Dependent claim 22 – Ground 1

22	The system of claim 21, wherein the event data comprises changes in device states of the security system components, data of the security system components, and data received by the security system components.

As discussed for claim 21, the gateway 115 in Naidoo can "transmit the alarm signal and alarm video corresponding to the alarm condition automatically to [the] customer … at an email address [or] by any other electronic means." (1007, ¶

0069.) Thus, for the same reasons discussed for claim 21, claim 22 is rendered obvious.

8. Dependent claim 24

24	The system of claim 1, wherein the security network comprises network devices coupled to the gateway via a wireless coupling.

Wimsatt discloses "security cameras" that are understood to be part of the security network because they are a security-related device. (Ex. 1004, ¶ 0040, FIG. 1 (item 125).) Wimsatt also discloses that its control panels 101 can be wireless (referred to as control panels 107); thus, the control panel 101 can communicatively couple to the security camera, or any other such devices, via a "wireless coupling". (*Id.*, ¶¶ 0037, 0044, FIG. 1.)

9. Dependent claim 29 – Ground 1

29	The system of claim 24, wherein the gateway including the connection management component transmits event data of the network devices to remote client devices over at least one of a plurality of communication links.

Claim 29 is similar to claim 17 but recites that "event data of the network devices" is transmitted by the gateway to "remote client devices over at least one of a plurality of communication links". As discussed for claim 17, Naidoo discloses that, upon detection of an alarm event, the gateway 115 sends the central monitoring station 136 "notification of the alarm condition and information relating to the alarm condition, **which may include alarm video**." (Ex. 1007, ¶¶ 0070-0071 (emphasis added).)

As discussed for claim 21, Naidoo discloses that its security server 131 can "create a data connection between remote station 155 and security gateway 115 such that communications between remote station 155 and security gateway 115 bypass security system server 131." (Ex. 1007, ¶ 0041.) Through this connection, the gateway 115 can "transmit the alarm signal and **alarm video** corresponding to the alarm condition automatically to [the] customer … at an email address [or] by any other electronic means." (*Id.*, ¶ 0069 (emphasis added).) As discussed for claim 8, Johnson discloses various types of "remote client devices" that can be implemented in Wimsatt.

It would have been obvious to a POSITA to combine the above disclosures from Naidoo with Wimsatt, Johnson and Severson so that the control panel 101 in Wimsatt, including the CMC, is capable of directly communicating event data with the remote client devices (such as those described in Johnson). (Ex. 1002, ¶ 169.) This communication would be over the DSL channel as described for claim 16 (the relevant arguments for which apply here) because that is the channel the control panel 101 uses when communicating with external devices / entities. (Ex. 1002, ¶ 169.) As also discussed for claim 16, the combined system discloses a plurality of different communication links, such as DSL, telephone line, Internet, etc.

It would be obvious to combine Naidoo with Wimsatt, Johnson and Severson for the same reasons discussed for claim 21.

10. Dependent claim 30 – Ground 1

30	The system of claim 29, wherein the gateway receives control data for control of the network devices from remote client devices via at least one of the plurality of communication links.

Wimsatt in view of Johnson discloses that the user can control the security system (and its sensors) via the web page 76. (Ex. 1005, 6:35-7:4.) The user can select an item on the web page 76 and provide a "command" to change a specific setting. (Ex. 1005, 7:47-8:5.) The data center 20 server then transmits this "command" to the control panel 101 which transmits data to any of its controlled devices (including network devices, such as cameras) to modify the setting. (Ex. 1005, 7:47-8:5, 6:61-7:4.) This "command" is the claimed "control data." The control panel 101 communicates with the data center 20 server via the Internet, which is one of a plurality of communication links available in the combined system. Furthermore, as discussed for claim 6, the user accesses the web page 76 remotely via a remote device, such as a computer. (*See, e.g.*, Ex. 1005, FIG. 5, Abstract, FIG. 1, 4:30-36, 5:29-39, 6:35-59.)

11. Dependent claim 31 – Ground 1

31	The system of claim 29, wherein the event data comprises changes in device states of the network devices, data of the network devices, and data received by the network devices.

As discussed for claim 29, Naidoo discloses that, upon detection of an alarm event, the gateway 115 sends the central monitoring station 136 "notification of the alarm condition and **information relating to the alarm condition, which may**

include alarm video." (Ex. 1007, ¶¶ 0070-0071 (emphasis added).) Thus, for the same reasons discussed for claim 29, claim 31 is rendered obvious under Ground 1.

12. Dependent claim 32

32	The system of claim 24, wherein the security system is coupled to a central monitoring station via a primary communication link, wherein the gateway is coupled to the central monitoring station via a secondary communication link that is different than the primary communication link.

Claim 32 is substantively identical to claim 16 except for its dependency on claim 24, which has no bearing on the claim language. Thus, claim 32 is obvious for the same reasons discussed with respect to claim 16.

13. Dependent claim 33 – Ground 1

33	The system of claim 32, wherein the gateway transmits event data of the network devices to the central monitoring station over the secondary communication link.

Claim 33 recites "event data of the network devices" but is otherwise identical to claim 17. As discussed for claim 17, Naidoo discloses that, upon detection of an alarm event, the gateway 115 sends the central monitoring station 136 "notification of the alarm condition and information relating to the alarm condition, which may include **alarm video**." (Ex. 1007, ¶¶ 0070-0071 (emphasis added).) Thus, claim 33 is obvious for the same reasons discussed with respect to claim 17.

14. Dependent claim 35 – Ground 2

35	The system of claim 32, wherein the secondary communication link includes a General Packet Radio Service (GPRS) coupling.

Claim 35 is substantively identical to claim 20 except for its dependency on claim 32, which has no bearing on the claim language. Thus, for the same reasons discussed for claim 20, claim 35 is rendered obvious under Ground 2.

15. Dependent claim 36 – Ground 1

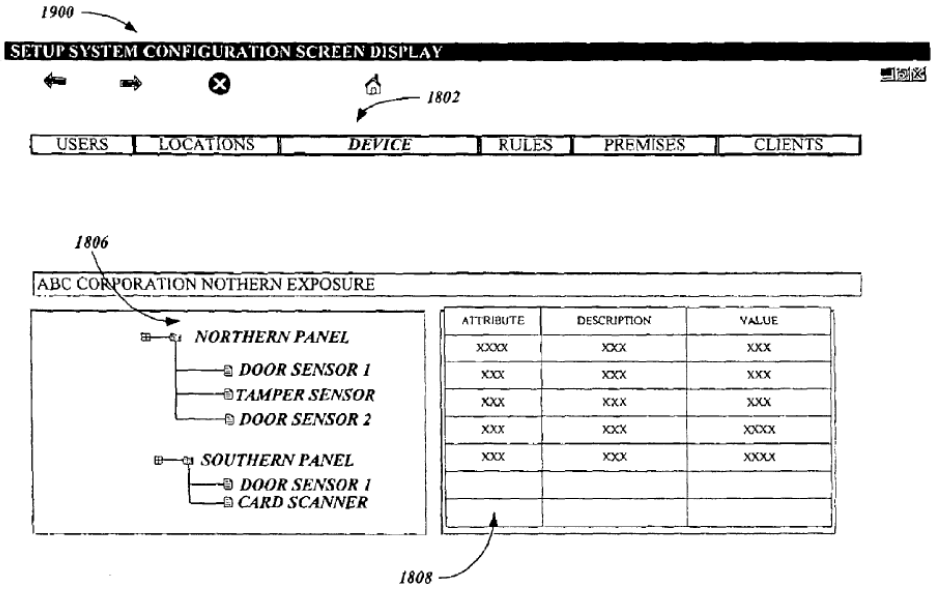
36	The system of claim 32, wherein the gateway transmits messages comprising event data of the network devices to remote client devices over the secondary communication link.

Claim 36 is substantively identical to claim 21 except that it recites "event data of the network devices" instead of event data of the security system components. As discussed for claim 17, however, Naidoo discloses that, upon detection of an alarm event, the gateway 115 sends the central monitoring station 136 "notification of the alarm condition and information relating to the alarm condition, **which may include alarm video**." (Ex. 1007, ¶¶ 0070-0071 (emphasis added).) This video comes from one of the network devices of Wimsatt. Thus, for the same reasons discussed in claim 21, claim 36 is rendered obvious under Ground 1.

16. Dependent claims 37 and 38 – Ground 3

37	The system of claim 24, wherein the security server creates, modifies and terminates couplings between the gateway and the network devices.
38	The system of claim 24, wherein the security server performs creation, modification, deletion and configuration of the network devices.

Alexander describes an integrated information system similar to Wimsatt and Johnson. It includes a premise server 202 (similar to the control panel 101 / unit 30) that controls monitoring devices 206 installed throughout a home. (Ex. 1008, FIG. 2, 7:1-14.) The monitoring devices can include video cameras. (*Id.*) The premise server 202 is connected to a remote central server 210 (similar to the data center 20 server in Johnson) that provides the user interface shown below in Figure 18, which allows users to input data to create (or install) a new monitoring device (*id.*, FIG. 13B, 18:65-19:22) and modify an existing monitoring device (*id.*, 17:54-18:12) to the integrated home system. (*See also, id.*, FIG. 5B (item 518 ("create or modify devices and rules")), FIGs. 13A-B, 14-18, 16:25-17:9, 11:13-17.) Although it does not describe deleting a monitoring device from the system, it would be obvious to a POSITA that "modifying" a device could include deleting it. (Ex. 1002, ¶ 178.)



Alexander further discloses that the central server 210 "configures each monitoring device" 206 using the information input by the user. (Ex. 1008, 19:49-20:2 (cl. 1), 19:23-37.)

It would be obvious to combine Alexander with Wimsatt, Johnson and Severson so that the data center 20 server in Johnson is capable of performing the same functions described in Alexander through its control page 76, thereby predictably resulting in enhanced functionality of the data center 20 server and a simplification of device installation. (Ex. 1002, ¶ 180.) Allowing a user to add and modify other device connections via the control page 76 and data center 20 server in the same manner disclosed in Alexander would enhance the functionality of the data center 20 server as well as allow the user to further customize his home security system. (Ex. 1002, ¶ 180.) A POSITA would understand that these device

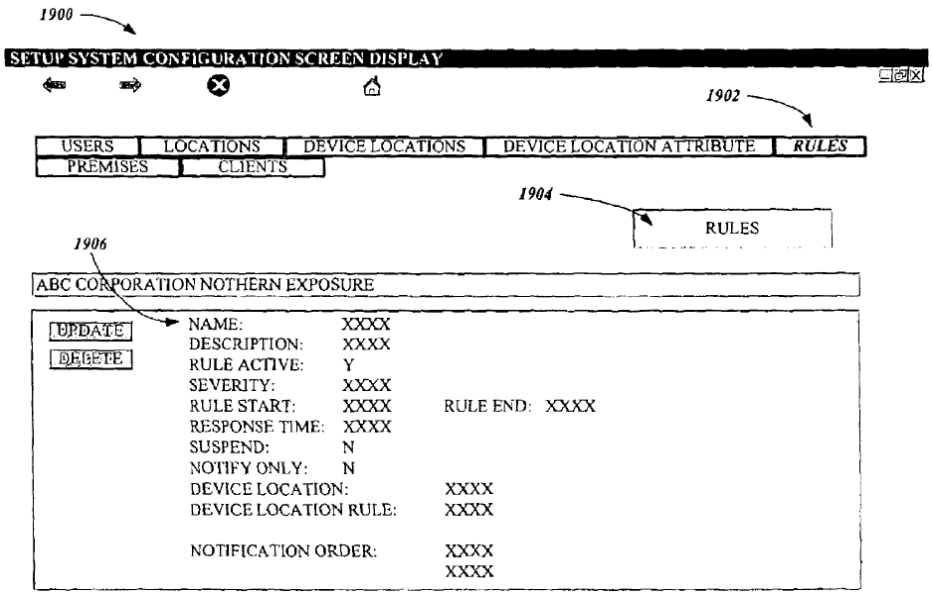
connections are "couplings" between the control panel 101 and the network devices because adding a device to the system necessarily requires that the device is coupled to the control panel 101 for operation as part of the system.

Alexander, Wimsatt, Johnson and Severson disclose similar integrated home monitoring systems and control panels. Thus, a POSITA would be motivated to combine the references to enhance their respective functionalities. (Ex. 1002, ¶ 181.)

17. Dependent claim 39 – Ground 3

39	The system of claim 24, wherein the security server creates automations, schedules and notification rules associated with the network devices.

Alexander describes a similar process for allowing a user to create rules for its monitoring devices, which include cameras. (Ex. 1008, 7:1-14, FIG. 13A, FIG. 16, FIG. 19, 18:13-64.) Figure 19 (shown below) illustrates an exemplary user interface provided by the central server 210 in Alexander that allows the user to specifically create notification rules for monitoring devices. (*Id.*, 18:55-61.)



Alexander does not describe creating automation and scheduling rules specifically (except in the context of sending notifications) but it generally refers to the rule as a "device rule" (*id.*, 18:25) and a "monitoring device processing rule" (*id.*, 18:37). (*See also, id.*, 18:51-55.) As automation and scheduling rules are associated with the device and device processing, it would have been obvious to a POSITA that a user would have been able to create automations and scheduling rules using the same process described in Alexander. (Ex. 1002, ¶ 183.)

Moreover, Wimsatt discloses scheduling the HVAC system, lighting, sound and other controlled devices using the control panel 101. (Ex. 1004, FIG. 4F, ¶¶ 0067-0068.)

It would be obvious to combine Alexander with Wimsatt, Johnson and Severson so that the data center 20 server in Johnson is capable of performing the same functions described in Alexander through its control page 76, thereby

predictably resulting in enhanced functionality of the data center 20 server and a simplification of device installation. (Ex. 1002, ¶ 185.) The rationale and motivations to combine these prior art references discussed for claims 37 and 38 also apply here.

18. Dependent claim 40 – Ground 3

40	The system of claim 24, wherein the security server manages access to current and logged state data for the network devices.

As previously discussed, Wimsatt in view of Johnson provides a control page 76 that allows users to access the current state of their home (and the devices therein). (Ex. 1005, FIG. 3, 6:35-59, 4:15-39, 7:47-50.) This control panel 76 is managed by the data center 20 server. (*Id.*) Johnson does not describe keeping a "log" of previous state data for its controlled devices but this is disclosed in Alexander. (*See*, Ex. 1005, 4:47-53 (listing data that the server stores).) The central server 210 in Alexander, which is similar to the server in Johnson, includes an "event logs database 214". (Ex. 1008, 7:59-65.) "Event data" is described in Alexander as data "obtained from a monitoring device corresponding to an on/off state." (*Id.*, 11:33-36, 7:1-14.)

It would be obvious to combine Alexander with Wimsatt, Johnson and Severson so that the data center 20 server logs the state data for the controlled devices in Wimsatt. (Ex. 1002, ¶ 187.) This is a simple process of storing data at the server in Johnson once it has been received and keeping it for a period of time.

(*Id.*) This would allow a user to access older data using the control page 76, if needed. (*Id.*) Other rationales and motivations to combine these references are discussed in connection with claims 37 and 38 apply here.

19. Dependent claim 41 – Ground 3

41	The system of claim 24, wherein the security server manages access to current and logged state data for couplings between the gateway and the network devices.

As previously discussed, Wimsatt in view of Johnson provides a control page 76 that allows users to access the current state of their home (and the devices therein). (Ex. 1005, FIG. 3, 6:35-59, 4:15-39, 7:47-50.) This control panel 76 is managed by the data center 20 server. (*Id.*) Johnson does not describe keeping a "log" of previous state data for its controlled devices but this is disclosed in Alexander. (*See*, Ex. 1005, 4:47-53 (listing data that the server stores).) The central server 210 in Alexander, which is similar to the server in Johnson, includes an "event logs database 214". (Ex. 1008, 7:59-65.) "Event data" is described in Alexander as data "obtained from a monitoring device corresponding to an on/off state." (*Id.*, 11:33-36, 7:1-14.)

It would be obvious to combine Alexander with Wimsatt, Johnson and Severson so that the data center 20 server logs the state data for the controlled devices in Wimsatt, including couplings between the devices and the control panel 101. (Ex. 1002, ¶ 189.) This is a simple process of storing data at the server in

Johnson once it has been received and keeping it for a period of time. (*Id.*) This would allow a user to access older data using the control page 76, if needed. (*Id.*) Other rationales and motivations to combine these references are discussed in connection with claims 37 and 38 apply here.

20. Dependent claim 48 – Ground 3

48	The system of claim 1, wherein the security server creates, modifies and terminates users corresponding to the security system.

Claim 48 is rendered obvious under Ground 3. Alexander describes an integrated information system similar to Wimsatt and Johnson. It includes a premise server 202 (similar to the control panel 101 / unit 30) that controls monitoring devices 206 installed throughout a home. (Ex. 1008, FIG. 2, 7:1-14.) The monitoring devices can include security sensors. (*Id.*) The premise server 202 is connected to a remote central server 210 (similar to the data center 20 server in Johnson), which provides a user interface allowing users to access data related to the monitoring devices. (*Id.*, 3:24-28, 10:57-11:17.) Alexander discloses that, through this interface, a user can "create or modify a number of users to the integrated information system." (Ex. 1008, 12:13-13:10, FIGs. 5A-7.) It would be obvious to a POSITA that "modifying" a user could include terminating a user. (Ex. 1002, ¶ 195.)

It would be obvious to combine Alexander with Wimsatt, Johnson and Severson so that the data center 20 server in Johnson is able to create, modify and

terminate users corresponding to the security system. (Ex. 1002, ¶ 196.) Johnson already discloses that its server provides users with control pages 76 where they can view and control their home security system. (Ex. 1005, 6:35-59.) Allowing a user to add and modify other users via the control page 76 and data center 20 server in the same manner disclosed in Alexander would enhance the functionality of the data center 20 server as well as allow the user to further customize his home security system. (Ex. 1002, ¶ 196.)

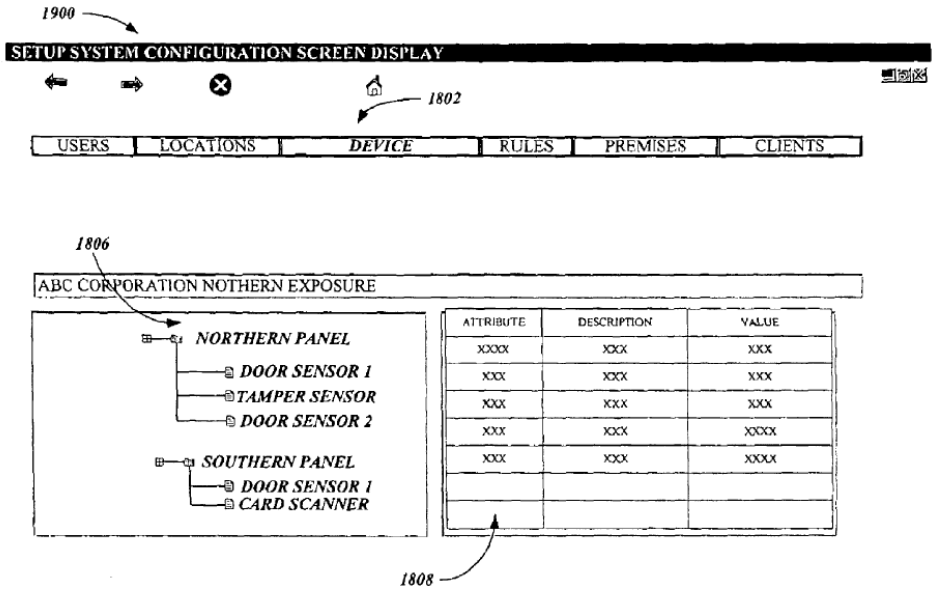
Alexander, Wimsatt, Johnson and Severson disclose similar integrated home monitoring systems and control panels. Thus, a POSITA would be motivated to combine the references to enhance their respective functionalities by providing this element in combination with those of claim 1. (Ex. 1002, ¶ 197.)

21. Dependent claims 49 and 50 – Ground 3

49	The system of claim 1, wherein the security server creates, modifies and terminates couplings between the gateway and the security system components.
50	The system of claim 1, wherein the security server performs creation, modification, deletion and configuration of the security system components.

Claims 49 and 50 are rendered obvious under Ground 3. Alexander describes an integrated home system having monitoring devices (e.g., sensors and cameras) similar to Wimsatt and Johnson and which also has a remote central server 210 similar to the data center 20 server in Johnson. (Ex. 1008, FIG. 2, 7:1-14, 3:24-28, 10:57-11:17.) The remote central server 210 in Alexander provides

the user interface shown below in FIG. 18, which allows users to input data to create (or install) a new monitoring device (*id.*, FIG. 13B, 18:65-19:22) and modify an existing monitoring device (*id.*, 17:54-18:12) to the integrated home system. (*See also, id.*, FIG. 5B (item 518 ("create or modify devices and rules")), FIGs. 13A-B, 14-18, 16:25-17:9, 11:13-17.) Although it does not describe deleting a monitoring device from the system, it would be obvious to a POSITA that "modifying" a device could include deleting it. (Ex. 1002, ¶ 198.)



Alexander further discloses that the central server 210 "configures each monitoring device" 206 using the information input by the user. (Ex. 1008, 19:49-20:2 (cl. 1), 19:23-37.)

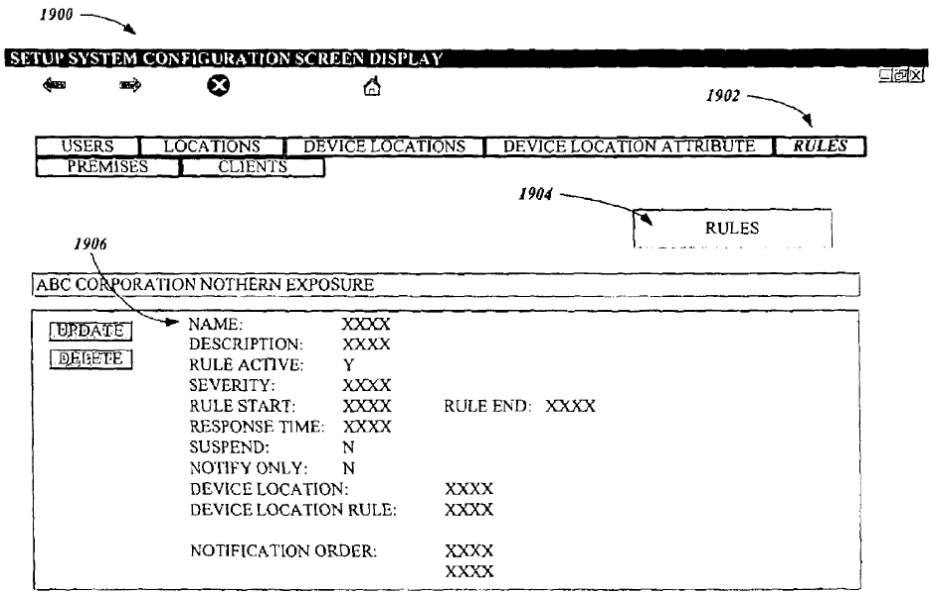
It would be obvious to combine Alexander with Wimsatt, Johnson and Severson so that the data center 20 server in Johnson is capable of performing the same functions described in Alexander through its control page 76, thereby

predictably resulting in enhanced functionality of the data center 20 server and a simplification of device installation. (Ex. 1002, ¶ 198.) A POSITA would understand that these device connections are "couplings" between the control panel 101 and the security system (and its sensors) because adding a device to the system necessarily requires that the device is coupled to the control panel 101 for operation as part of the system. The rationale and motivations to combine these prior art references discussed for claim 48, 37 and 38 also apply here.

22. Dependent claim 51 – Ground 3

51	The system of claim 1, wherein the security server creates automations, schedules and notification rules associated with the security system components.

Alexander describes a similar process for allowing a user to create rules for its monitoring devices, which include sensors and camera. (Ex. 1008, 7:1-14, FIG. 13A, FIG. 16, FIG. 19, 18:13-64.) Figure 19 (shown below) illustrates an exemplary user interface provided by the central server 210 in Alexander that allows the user to specifically create notification rules for monitoring devices. (*Id.*, 18:55-61.)



Alexander does not describe creating automation and scheduling rules specifically (except in the context of sending notifications) but it generally refers to the rule as a "device rule" (*id.*, 18:25) and a "monitoring device processing rule" (*id.*, 18:37). (*See also, id.*, 18:51-55.) As automation and scheduling rules are associated with the device and device processing, it would have been obvious to a POSITA that a user would have been able to create automations and scheduling rules using the same process described in Alexander. (Ex. 1002, ¶ 200.)

It would be obvious to combine Alexander with Wimsatt, Johnson and Severson so that the data center 20 server in Johnson is capable of performing the same functions described in Alexander through its control page 76, thereby predictably resulting in enhanced functionality of the data center 20 server and a simplification of device installation. (Ex. 1002, ¶ 200.) The rationale and

motivations to combine these prior art references discussed for claim 48, 37 and 38 also apply here.

23. Dependent claim 52 – Ground 3

52	The system of claim 1, wherein the security server manages access to current and logged state data for the security system components.

As previously discussed, Wimsatt in view of Johnson provides a control page 76 that allows users to access the current state of their home (and the devices therein). (Ex. 1005, FIG. 3, 6:35-59, 4:15-39, 7:47-50.) This control panel 76 is managed by the data center 20 server. (*Id.*) Johnson does not describe keeping a "log" of previous state data for its controlled devices but this is disclosed in Alexander. (*See*, Ex. 1005, 4:47-53 (listing data that the server stores).) The central server 210 in Alexander, which is similar to the server in Johnson, includes an "event logs database 214". (Ex. 1008, 7:59-65.) "Event data" is described in Alexander as data "obtained from a monitoring device corresponding to an on/off state." (*Id.*, 11:33-36, 7:1-14.)

It would be obvious to combine Alexander with Wimsatt, Johnson and Severson so that the data center 20 server logs the state data for the controlled devices in Wimsatt. (Ex. 1002, ¶ 202.) This is a simple process of storing data at the server in Johnson once it has been received and keeping it for a period of time. (*Id.*) This would allow a user to access older data using the control page 76, if

needed. (*Id.*) Other rationales and motivations to combine these references are discussed in connection with claim 48, 37 and 38 and apply here.

24. Dependent claim 53 – Ground 3

53	The system of claim 1, wherein the security server manages access to current and logged state data for couplings between the gateway and the security system components.

As discussed above with respect to claim 41, Wimsatt in view of Johnson provides a control page 76 that allows users to access the current state of their home (and the devices therein). (Ex. 1005, FIG. 3, 6:35-59, 4:15-39, 7:47-50.) This control panel 76 is managed by the data center 20 server. (*Id.*) Johnson does not describe keeping a "log" of previous state data for its controlled devices but this is disclosed in Alexander. (*See,* Ex. 1005, 4:47-53 (listing data that the server stores).) The central server 210 in Alexander, which is similar to the server in Johnson, includes an "event logs database 214". (Ex. 1008, 7:59-65.) "Event data" is described in Alexander as data "obtained from a monitoring device corresponding to an on/off state." (*Id.*, 11:33-36, 7:1-14.)

It would have been obvious to a POSITA that couplings between the gateway and security system components are also logged. By logging such couplings a user would be able to better track the various components of the security system. (Ex. 1002, ¶ 204.)

It would be obvious to combine Alexander with Wimsatt, Johnson and Severson for the same reasons as for claim 41. Other rationales and motivations to combine these references are discussed in connection with claim 48, 37 and 38 and apply here.

25. Dependent claim 58 – Ground 1

58	The system of claim 1, wherein the security server transmits event data of the security system components to a central monitoring station of the security system over the secondary communication link.

As an initial matter, this claim recites "over **the** secondary communication link" but no such communication link is disclosed in claim 1, to which claim 58 depends. Dependent claim 16 is the first claim to recite this secondary communication link but claim 58 does not depend from claim 16. Thus, the "secondary communication link" is interpreted here to mean any communication link as there is also no first / primary communication link recited in claim 1.

Claim 58 is rendered obvious under Ground 1. Johnson discloses that the data center 20 server communicates security alarm alerts (or event data) to an auxiliary service 80 via the Internet (i.e., the claimed "fourth communication channel") but is silent regarding sending video event data. (Ex. 1005, 6:6-11, 7:30-42.) This is disclosed in Naidoo. Naidoo discloses that, upon detection of an alarm event, the gateway 115 sends the security server 131 "a notification of the alarm condition and information relating to the alarm condition, which may include

alarm video." (Ex. 1007, ¶ 0070.) The security server 131 then relays the notification to the central monitoring station 133. (*Id.*, 0072.)

It would have been obvious to a POSITA to combine Naidoo with Wimsatt, Johnson and Severson so that the control panel 101 in Wimsatt transmits this "event data" to the data center 20 server in Johnson, which then relays that information to the central monitoring station in Naidoo. (Ex. 1002, ¶ 213.) These devices can be coupled together in this manner without any change in their respective functionalities, as they are all capable of communicating via the Internet. (Ex. 1002, ¶ 213.) Also, as discussed in Naidoo, by providing both the sensor event data to the central monitoring station, an operator, in short order, is able to "verif[y] whether the alarm signal corresponds to an actual alarm condition using the alarm signal information and the segment of real-time video," and then take appropriate action. (Ex. 1007, ¶¶ 0075, 0077, 0008, 0011, 0027.) "Timely response may increase the chance of apprehending an intruder, and in the case of life-threatening circumstances, reduce the likelihood of injury or death." (*Id.*, ¶ 0100.) A POSITA would have understood these benefits and been motivated to combine Naidoo with Wimsatt, Johnson and Severson to enhance their respective security capabilities and first-responder response times.

X. NO SECONDARY CONSIDERATIONS OF NON-OBVIOUSNESS EXIST

Patent Owner has not identified any evidence of secondary indicia of non-

obviousness for the '619 patent. Accordingly, there is no objective evidence of non-obviousness that might warrant a finding that the Petitioned Claims are patentable. (Ex. 1002, ¶ 234.)

XI. CONCLUSION

Petitioner respectfully requests that the Board institute *inter partes* review of claims 17, 18, 20-22, 29-31, 33, 35-41, 48-53 and 58.

Dated: September 30, 2016

Respectfully submitted,
COOLEY LLP

By: /Erik B. Milch/
Erik B. Milch
Reg. No. 42,887

COOLEY LLP
ATTN: Patent Group
1299 Pennsylvania Ave., NW, Suite 700
Washington, DC 20004
Tel: (703) 456-8000
Fax: (202) 842-7899

CERTIFICATE OF COMPLIANCE WITH WORD COUNT

Pursuant to 37 C.F.R. § 42.24(d), I certify that this Petition complies with the type-volume limits of 37 C.F.R. § 42.24(a)(1)(i) because it contains 12,191 words, according to the word-processing system used to prepare this petition, excluding the parts of this Petition that are exempted by 37 C.F.R. § 42.24(a) (including the table of contents, mandatory notices, a certificate of service or this certificate word count, appendix of exhibits, and claim listings).

Dated: September 30, 2016

By: /Erik B. Milch/
Erik B. Milch
Reg. No. 42,887

CERTIFICATE OF SERVICE

Pursuant to 37 C.F.R. §§ 42.6(e) and 42.105(b), the undersigned certifies that on September 30, 2016, a complete and entire copy of this **Petition for *Inter Partes* Review of Patent No. 8,473,619**, including Exhibit Nos. 1001-1013 and a Power of Attorney, was served via FEDERAL EXPRESS, costs prepaid, to the Patent Owner by serving the correspondence address of record as follows:

Richard Gregory Jr.
Barbara Courtney
IPR Law Group, PC
5338 Cornish Street
Houston, TX 77007

A courtesy copy was also served via FEDERAL EXPRESS on the Patent Owner at the following address:

Ryan Smith
Wilson Sonsini Goodrich & Rosati
650 Page Mill Road
Palo Alto, CA 94304

By: /Erik B. Milch/
Erik B. Milch
Reg. No. 42,887