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: Security Network Integrated with Premise Security System

DECLARATION OF JAMES PARKER IN SUPPORT OF PETITIONS FOR *INTER PARTES* REVIEW OF U.S. PATENT NO. 8,473,619

Inter Partes Review No. _____

1. I, James Parker, declare as follows:

2. I have personal knowledge of the facts stated in this declaration, and could and would testify to these facts under oath if called upon to do so.

I. INTRODUCTION AND QUALIFICATIONS

A. Engagement Overview

3. I have been retained by counsel for SecureNet Technologies, LLC (Petitioner) in this case as an expert in the relevant art. I am being compensated for my work at the rate of $350 per hour. No part of my compensation is contingent upon the outcome of these petitions.

4. I was asked to study U.S. Patent No. 8,473,619 ("the '619 patent"), its prosecution history, and the prior art and to render opinions on the obviousness or non-obviousness of certain ones of the claims of the '619 patent in light of the teachings of the prior art, as understood by a person of ordinary skill in the art in the 2005 time frame. I understand that the claims being challenged in the Petitions are claims 1-9 and 12-62 ("the challenged claims").

B. Summary of Opinions

5. After studying the '619 patent, relevant excerpts of its file history, and the prior art, and considering the subject matter of the claims of the '619 patent in light of the state of technical advancement in the area of security alarm systems in the 2005 time frame, I reached the conclusions discussed herein.

6. In light of these general conclusions, and as explained in more detail throughout this declaration, it is therefore my opinion that each of the challenged claims of the '619 patent addressed in this declaration are invalid as they were obvious in the 2005 time frame in light of the knowledge of skill in the art at that time and the teachings, suggestions, and motivations present in the prior art. This declaration, and the conclusions and opinions herein, provide support for the Petitions for *Inter Partes* Review of the '619 patent filed by Petitioner. I have reviewed the Petitions in their entireties as well as their corresponding exhibits (which are identical).

C. Qualifications and Experience

7. I possess the knowledge, skills, experience, training and the education to form an expert opinion and testimony in this matter. I have over 33 years of experience in the fields of Electronic Security Systems and Sensors.

1. Education

8. I attended the RCC Institute of Technology from 1979-1982 and graduated with a Diploma in Electronic Engineering Technology, Electronic Engineering (Hardware & Software). RCC Institute of Technology is a division of Yorkville University, located in Toronto, Canada. I understand my Canadian Diploma is more or less equivalent to a Bachelor's Degree in the US.

2. Career

9. I will discuss my current position first, followed by a synopsis of my career and work from shortly after I received my diploma to the present.

10. I am currently the President of EE Systems Group, Inc. Canada ("EE-SGI") of Richmond Hill, Ontario Canada. EE-SGI is an innovator and technical solution provider with extensive R&D capabilities in the Security and Life Safety products industry. As part of my work at EE-SGI, I am responsible for all hardware design and system and/or software architectures, interacting and negotiating with key customers in all areas of business, spearheading new product development, and overseeing EE-SGI's China operations, including all component sourcing and design oversight.

11. Previously, I spent 18 years working with Digital Security Controls (“DSC”), eventually becoming Vice President of Engineering. I first joined DSC in 1985 as a contractor. DSC is a major supplier of electronic security and monitoring systems. While at DSC, I had cross functional responsibilities in Marketing, New Business Development, and Manufacturing, and I managed 200 employees. I was the principal architect of the “Power” and “Maxsys” families, including the PC1550, one of the most widely installed alarm control panels in the world, with an installed base in the millions. In addition, my work at DSC

included software and hardware design, organizing and driving corporate speed to market initiatives, developing protocols for interconnecting components, negotiating agreements with key suppliers, and developing mixed mode ASIC's, among other things

3. Publications

12. I am a named inventor on over 25 patents (both domestic and foreign), in the areas of electronic security systems and sensors. The patent numbers and titles and abstracts are listed on the attached curriculum vitae. (Ex. 1013.)

4. Curriculum Vitae

13. Additional details of my education and employment history, patents, and publications are set forth in my current curriculum vitae, which is provided as Ex. 1013.

D. Materials Considered

14. My analysis is based on my experience in the alarm system, communications, and digital communications industries since 1983, including the documents I have read and authored and systems I have developed and used since then.

15. Furthermore, I have reviewed the various relevant publications from the art at the time of the alleged invention and the claim analysis that is included in the Petitions for *Inter Partes* Review of the ‘619 patent, to which this Declaration

relates. I have also reviewed the Petitions in their entireties. Based on my experience as a person having ordinary skill in the art ("POSITA") at the time of the alleged invention, the references accurately characterize the state of the art at the relevant time. Specifically, I have reviewed the following:

Exhibit No.[1]	Description of Document
1001	U.S. Patent No. 8,473,619 ("the '619 patent")
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

[1] The same exhibit numbers and exhibits are used for both petitions for ease of reference. For example, a reference to "Exhibit 1003", which is the file history for the '619 patent, is the same for both petitions filed for the '619 patent.

II. LEGAL PRINCIPLES USED IN THE ANALYSIS

16. I am not a patent attorney, nor have I independently researched the law on patent validity. Attorneys for the Petitioner explained certain legal principles to me that I have relied upon in forming my opinions set forth in this report.

A. Person Having Ordinary Skill in the Art ("POSITA")

17. I understand that I must undertake my assessment of the claims of the '619 patent from the perspective of what would have been known or understood by a POSITA as of the earliest claimed priority date of the patent claim, which I understand is March 16, 2005. The opinions and statements that I provide herein regarding the '619 patent and the references that I discuss are made from the perspective of the person of ordinary skill in the art in the early 2005 time frame.

18. Counsel has advised me that to determine the appropriate level of one of ordinary skill in the art, I may consider the following factors: (a) the types of problems encountered by those working in the field and prior art solutions thereto; (b) the sophistication of the technology in question, and the rapidity with which innovations occur in the field; (c) the educational level of active workers in the field; and (d) the educational level of the inventor.

19. The relevant technology field for the '619 patent is digital systems design, especially as pertains to telecommunication system design and operation,

as applicable to safety and security systems. Based on this, and the four factors above, it is my opinion that POSITA would hold a bachelor's degree or the equivalent in electrical engineering (or related academic fields) and at least three years of additional experience in the area of digital and/or telecommunication system design, as applicable to safety and security systems, or equivalent work experience.

20. Unless otherwise specified, when I mention a POSITA or someone of ordinary skill, I am referring to someone with at least the above level of knowledge and understanding.

21. Based on my experiences, I have a good understanding of the capabilities of a person of ordinary skill in the relevant field. Indeed, in addition to being a person of at least ordinary skill in the art, I have worked closely with many such persons over the course of my career.

22. Although my qualifications and experience exceed those of the hypothetical person having ordinary skill in the art defined above, my analysis and opinions regarding the '619 patent have been based on the perspective of a person of ordinary skill in the art in the March 2005 time frame.

23. My opinions regarding the level of ordinary skill in the art are based on, among other things, the content of the '619 patent, my years of experience in

the field of security alarm systems, my understanding of the basic qualifications that would be relevant to an engineer tasked with investigating methods and systems in the relevant area, and my familiarity with the backgrounds of colleagues and co-workers, both past and present.

24. My opinions herein regarding the person of ordinary skill in the art and my other opinions set forth herein would remain the same if the person of ordinary skill in the art were determined to have somewhat more or less education and/or experience than I have identified above.

B. Prior Art

25. I understand that the law provides categories of information that constitute prior art that may be used to anticipate or render obvious patent claims. To be prior art to a particular patent under the relevant law, a reference must have been made, known, used, published, or patented, or be the subject of a patent application by another, before the priority date of the patent. I also understand that the POSITA is presumed to have knowledge of the relevant prior art.

26. I understand that the challenged claims of the ‘619 patent may be entitled to a March 16, 2005 priority date.

C. Broadest Reasonable Interpretations

27. I understand that, in *Inter Partes* Review, the claim terms are to be given their broadest reasonable interpretation (BRI) in light of the specification.

See 37 C.F.R. § 42.100(b). In performing my analysis and rendering my opinions, I have interpreted claim terms for which the Petitioner has not proposed a BRI construction by giving them the ordinary meaning they would have to a POSITA, reading the '619 Patent with its earliest priority filing date (March 16, 2005) in mind, and in light of its specification and file history.

D. Legal Standards for Obviousness

28. I have been provided the following instructions from the Federal Circuit Bar Association Model Instructions regarding obviousness, which is reproduced in part below. I apply this understanding in my analysis, with the caveat that I have been informed that the Patent Office will find a patent claim invalid in *inter partes* review if it concludes that it is more likely than not that the claim is invalid (*i.e.*, a preponderance of the evidence standard), which is a lower burden of proof than the "clear and convincing" standard that is applied in United States district court (and described in the jury instruction below):

> 4.3c OBVIOUSNESS
>
> Even though an invention may not have been identically disclosed or described before it was made by an inventor, in order to be patentable, the invention must also not have been obvious to a person of ordinary skill in the field of technology of the patent at the time the invention was made.

> [Alleged infringer] may establish that a patent claim is invalid by showing, by clear and convincing evidence, that the claimed invention would have been obvious to persons having ordinary skill in the art at the time the invention was made in the field of [insert the field of the invention].
>
> In determining whether a claimed invention is obvious, you must consider the level of ordinary skill in the field [of the invention] that someone would have had at the time the [invention was made] or [patent was filed], the scope and content of the prior art, and any differences between the prior art and the claimed invention.
>
> Keep in mind that the existence of each and every element of the claimed invention in the prior art does not necessarily prove obviousness. Most, if not all, inventions rely on building blocks of prior art. In considering whether a claimed invention is obvious, you may but are not required to find obviousness if you find that at the time of the claimed invention [or the patent's filing date] there was a reason that would have prompted a person having ordinary skill in the field of [the invention] to combine the known elements in a way the claimed invention does, taking into account such factors as (1) whether the claimed invention was merely the predictable result of using prior art elements according to

their known function(s); (2) whether the claimed invention provides an obvious solution to a known problem in the relevant field; (3) whether the prior art teaches or suggests the desirability of combining elements claimed in the invention; (4) whether the prior art teaches away from combining elements in the claimed invention; (5) whether it would have been obvious to try the combinations of elements, such as when there is a design need or market pressure to solve a problem and there are a finite number of identified, predictable solutions; and (6) whether the change resulted more from design incentives or other market forces. To find it rendered the invention obvious, you must find that the prior art provided a reasonable expectation of success. Obvious to try is not sufficient in unpredictable technologies.

In determining whether the claimed invention was obvious, consider each claim separately. Do not use hindsight, i.e., consider only what was known at the time of the invention [or the patent's filing date].

In making these assessments, you should take into account any objective evidence (sometimes called "secondary considerations") that may shed light on the obviousness or not of the claimed invention, such as:

(a) Whether the invention was commercially successful as a result of the merits of the claimed invention (rather than the result of design needs or market-pressure advertising or similar activities);

(b) Whether the invention satisfied a long-felt need;

(c) Whether others had tried and failed to make the invention;

(d) Whether others invented the invention at roughly the same time;

(e) Whether others copied the invention;

(f) Whether there were changes or related technologies or market needs contemporaneous with the invention;

(g) Whether the invention achieved unexpected results;

(h) Whether others in the field praised the invention;

(i) Whether persons having ordinary skill in the art of the invention expressed surprise or disbelief regarding the invention;

(j) Whether others sought or obtained rights to the patent from the patent holder; and

(k) Whether the inventor proceeded contrary to accepted wisdom in the field.

Federal Circuit Bar Association Model Jury Instructions §4.3c (2014).

29. I am also informed that the United States Patent Office supplies its

examining corps with a Manual of Patent Examining Procedure that provides exemplary rationales that may support a conclusion of obviousness, including:

> (a) Combining prior art elements according to known methods to yield predictable results;
>
> (b) Simple substitution of one known element for another to obtain predictable results;
>
> (c) Use of known technique to improve similar devices (methods, or products) in the same way;
>
> (d) Applying a known technique to a known device (method, or product) ready for improvement to yield predictable results;
>
> (e) "Obvious to try" – choosing from a finite number of identified, predictable solutions, with a reasonable expectation of success;
>
> (f) Known work in one field of endeavor may prompt variations of it for use in either the same field or a different one based on design incentives or other market forces if the variations are predictable to one of ordinary skill in the art; or
>
> (g) Some teaching, suggestion, or motivation in the prior art that would have led one of ordinary skill to modify the prior art reference or to combine prior art reference teachings to arrive at the claimed invention.

MPEP § 2143. I apply these principles in my analysis below.

III. TECHNOLOGY TUTORIAL

A. Introduction

30. The '619 patent generally relates to security systems, particularly to local security systems that are in communication with centralized systems run by, for example, security companies.

B. Local Devices and Systems

1. Sensors

31. What I refer to as a "local" security system is a security system found in a particular location, usually a home or business. This location is often referred to in the security industry as the "premises", "site" or "protected area." A local security system usually consists of various components, which I will refer to as "devices."

32. Local devices can be put into several subcategories according to their functions in the security system: sensors, outputs, alarm system controllers (control panels) and user interfaces (keypads, screens, fobs, panic buttons).

33. A "sensor" is a device that provides information, usually to the local control panel. Sensors may be thought of as the eyes and ears of the control panel. They report to the control panel whatever information the particular device is able to detect (for example, open or closed status, motion within a particular area, an

image, temperature, the presence of smoke, etc.)

34. A sensor may be active or passive. An active sensor device is a sensor that requires power to operate, such as a motion detector, or a smoke detector. This power can be supplied by the control panel via a hard-wired connection or by a battery in the sensor.

35. A passive sensor is basically a switch, typically magnetic in nature. Passive sensors are primarily used to determine the condition (or state) of doors or windows. For example, a small magnet is attached to the movable part of a door or window, while the magnetic switch part of the passive sensor is attached to the door frame or window frame. If the door or window is opened, the loss of magnetic contact between the magnet and the magnetic switch causes a signal to be generated and sent to the control panel. In this manner, the open or closed state of the window or door can be provided to the control panel.

36. A sensor is either wired or wireless. A wired sensor communicates with the control panel via a hard-wired connection, while a wireless sensor communicates with the control panel through a RF (radio frequency) connection.

37. An "output" is a device that receives signals or commands from the control panel. Outputs are typically described based on what they are physically, for example, a relay output, a transistor output, a RS-232 serial interface, an X-10

power line interface (for control of lights and other high voltage 120VAC line powered appliances), etc. Examples of outputs include security devices such as sirens, as well as home automation devices such as remotely controlled lights and thermostats.

38. Outputs are driven by the control panel in response to various circumstances, including sensor inputs. For example, sensor input indicating a door has been opened could cause the control panel to send a signal that causes a light to go on.

2. Controllers and User Interfaces

39. Controllers, commonly known as "control panels" or "security panels", typically receive input from sensors, determine whether alarm conditions exist, and issue commands to outputs. Controllers typically have a power supply with a battery backup. They also have or are connected to some sort of user interface. I will generally refer to controllers as "control panels" in this document.

40. The user interface permits the user to control the local system, for example, by arming or disarming the system. Depending on the outputs in the local system, the user interface may also permit the user to control individual devices, for example, to turn on a light, open a garage door, etc.

41. A controller and user interface can be physically united in one

component (a so-called "all-in-one" system) or can be separate components (for example, a user may have a user interface keypad on the wall near an entrance to the home, while the control panel is located in the basement).

3. Security Systems

42. A local security system usually consists of one or more sensors communicating with a control panel, which further communicates with a user interface. Based on inputs from the sensors, the control panel determines whether or not an alarm condition exists. If an alarm condition exists, the control panel triggers local warning devices such as sirens or strobes. As discussed in greater detail below, the control panel may also notify a remote system of the alarm condition.

43. A security system may have various states, which affect whether sensor input results in an alarm condition. Generally, a security system will have two states referred to as "armed" and "disarmed." When a system is in a "disarmed" state, an input from a sensor (for example, indicating that a door has been opened) does not result in the control panel moving to an "alarm" state. By contrast, when the system is in an "armed" state, the same input from the sensor will result in the control panel moving to an "in alarm" state. I note that "in alarm" and "entry/exit" delays are also considered to be states of the security system.

44. A security system may have several levels of the "armed" state, which affect which particular sensors cause the system to move to an "alarm" state. For example, many systems have an "armed stay" level, which is meant to be used when the user is at home. In the "armed stay" level, inputs from sensors inside the home, such as motion detectors, do not trigger an alarm. By contrast, in the "armed away" level, which is meant to be used when the user is away from home, inputs from any sensor, including interior sensors trigger an alarm.

4. Security Systems and Home Automations

45. The field of "home automation" (or "building automation"—I will use those terms interchangeably in this document) involves, among other things, centralizing or extending control of household devices and appliances. For example, rather than lights being controlled simply by a traditional wall switch, a home automation system might include light controllers that respond to wireless transmissions. In this way, a user can turn on a light using a portable remote control and/or a central user interface in the home. Another familiar example of home automation is a garage door that opens automatically when a wireless remote is pressed. Devices other than lights or garage doors—for example, heating or cooling systems, sprinkler systems, door locks, or audiovisual components—can be similarly controlled, and the remote control or user interface can allow the user

to operate an entire set of home devices or appliances.

46. Over time, various technologies and standards have been used in the home automation context: technologies such as X10 (which sent control signals through a home's existing power lines), wired technologies such as CEBus, and wireless technologies such as Z-Wave, LONWorks or ZigBee.

47. As noted above, a control panel can be connected to outputs. Some of those outputs, like lights and sirens, have a security function. However, there is no reason why a control panel cannot be connected to outputs comprising home automation devices and controllers. To the contrary, the central control point provided by a control panel naturally suggests itself as a means for other forms of building control.

48. It has therefore long been a common feature for security systems to provide some level of home automation, either through a serial interface to a third-party home automation package or through a module that contains the appropriate hardware. For example, the DSC Maxsys system, which I was responsible for designing in 1992, utilized an "Escort 4580 Module" which allowed a traditional control panel to provide a user the ability to control not only the alarm system but to also control X10 devices through a locally or remotely (worldwide) connected touch tone telephone.

C. Remote Systems and Devices

49. What I refer to as "remote" systems and devices are located away from the home or premises. Remote systems and devices fall into two basic categories: (1) centralized monitoring systems and (2) remote user devices.

1. Centralized Monitoring Systems

50. Centralized monitoring systems fall into two broad categories: central stations and systems operated by value-added security companies.

51. The notion of a "central station" (also known as a "central monitoring station", "central monitoring system" or "CMS") has existed for decades, as long as local alarm systems have been connected by phone or other wired connection to remote facilities. When a local alarm system detects an alarm condition, it notifies the central station (traditionally by telephone). The central station then takes the appropriate action, including calling police, fire or ambulance services. Different geographic regions typically have different central stations. Alarm sales, service and installation companies may have their own central stations or they may contract for the service at the wholesale level. This typically depended on the size of their installed account base.

52. Presently, a central station is a facility that complies with two related UL Standards. UL Standard 827 pertains to the basic structure of the building and covers requirements such as walls, security and fire protection, power supply,

building cabling, receiver units, and other related requirements. UL Standard 1981 governs computerized central-station automation systems and contains requirements for receiving equipment utilized to handle automated signal and process of change-of-status signals. Stations that meet the requirements set out in these Standards may be certified as "UL Listed."

53. The second class of centralized monitoring system is something I call a "value added system." Value added systems do not directly call the authorities (police, fire and ambulance) during alarm events. Instead, the value added system receives an alarm condition from a local system and sends a notification to the central station, which in turn contacts the appropriate authorities.

54. I refer to such systems as "value added" because they provide features and functionalities in addition to those provided by a central station. For example, a value added system might provide customized alarm notifications, provide notifications based on non-alarm events (for example, a liquor cabinet being opened) or permit remote monitoring and control of the security system by the user.

2. Remote User Devices

55. Remote user devices permit monitoring or interaction with the local security system by a user when the user is away from the home or business. For

example, a remote user device may allow the user to arm and disarm the system remotely or may allow the user to remotely view video taken by cameras inside the home.

56. Some of the earliest remote user devices that provided extensive interactivity with local security systems were remote computers, usually utilizing a web browser interface.

57. In the past few years, mobile devices such as smartphones have become increasingly popular with consumers, and thus have become available to be used as remote user devices in connection with security systems.

IV. THE '619 PATENT

A. Overview of the '619 Patent

58. The '619 patent is generally directed to integrated security systems capable of being remotely accessed and controlled. The '619 patent includes many of the elements I discuss above, all of which are part of conventional integrated security systems.

B. Interpretation of Claim Limitations in the '619 Patent

59. I understand that the Petitioner has determined that all of the claim terms in the '619 patent should be construed according to their plain and ordinary meaning and none of them require determinations about their broadest reasonable

interpretations (BRIs). In some instances, I point to disclosures in the '619 patent that clarify the meaning of a particular term but this should in no way be deemed as a BRI – it is simply to add context and to show that elements in the prior art references are described similarly to those in the '619 patent.

C. The Priority Claims of the '619 Patent

60. I understand that the '619 patent claims priority to a long list of continuation-in-part applications and provisional applications, the earliest of which was filed on March 16, 2005. For purposes of this proceeding, I assume that the '619 patent has a priority date of March 16, 2005.

V. OVERVIEW OF THE PRIOR ART

A. Overview of Wimsatt

61. Wimsatt discloses a "home automation contextual user interface." (Ex. 1004, Title.) I rely on this reference to show many of the front-end features of the claims, including those related to the "touchscreen" and its capabilities.

62. Wimsatt describes a control panel 101 that is located in a controlled environment such as a home or office building. (Ex. 1004, ¶ 0012.) The control panel 101 is connected to a number of co-located devices, called "controlled devices", which manage already-existing systems, such as lighting systems, security systems, heating and air conditioning, audio/visual equipment, and other appliances in a home or office building. (*Id.*, ¶ 0023.) Figure 1 of this publication is

reproduced below and illustrates the control panel's connection to these devices.

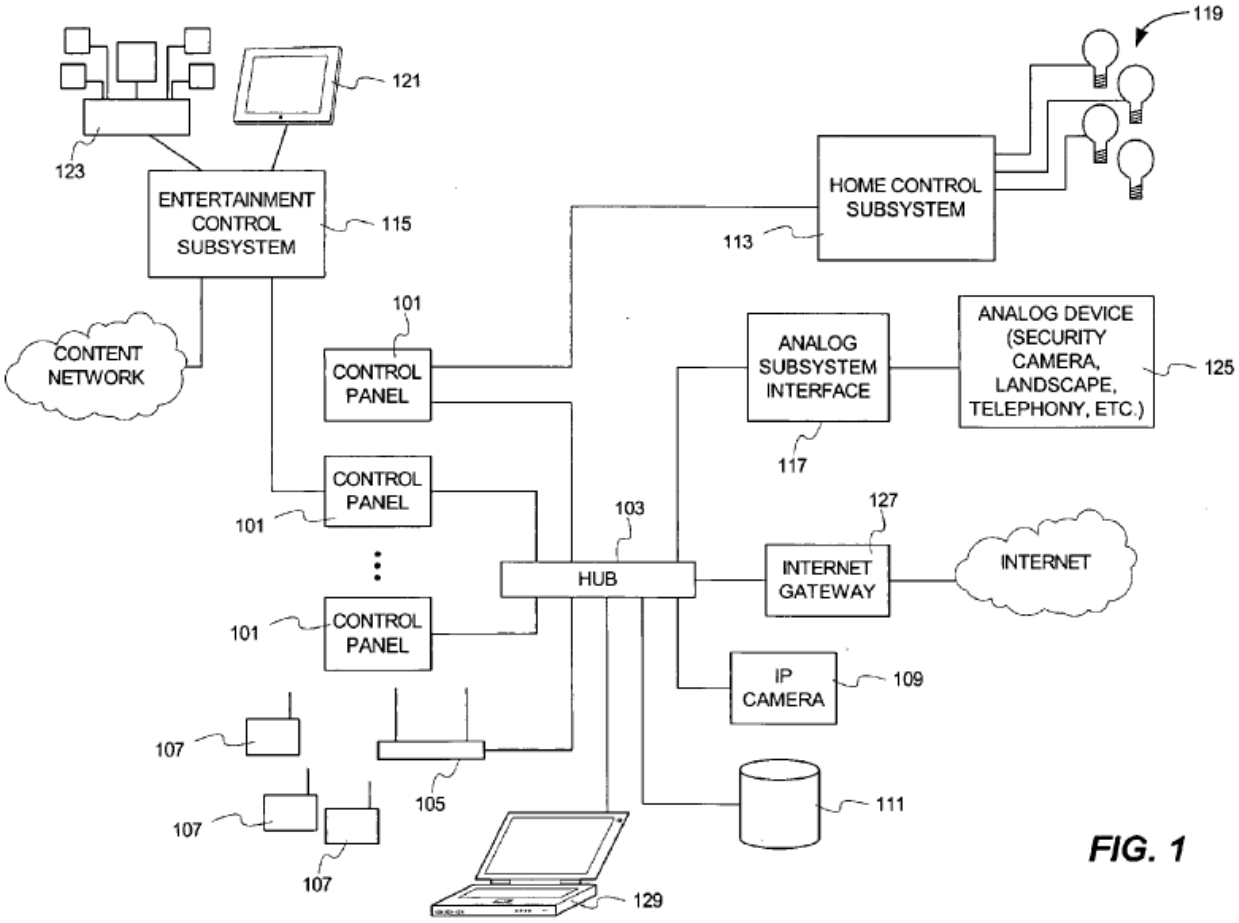


FIG. 1

63. According to Wimsatt, the control panel 101 can be implemented by the "Companion™ 6 and Companion™ touch-screen interface units produced by CorAccess Systems." (*Id.*, ¶ 0035.) The control unit 101 displays an interactive graphical user interface (GUI) that allows that user (e.g., homeowner) to control the controlled devices. For example, via the GUI, a user can "turn on/off a controlled device, adjust settings on a controlled device, query the status of a controlled device, and the like." (*Id.*, ¶¶ 0035, 0022.) Figure 4A, shown below, is

an example of a "home screen" displayed on the control unit 101.

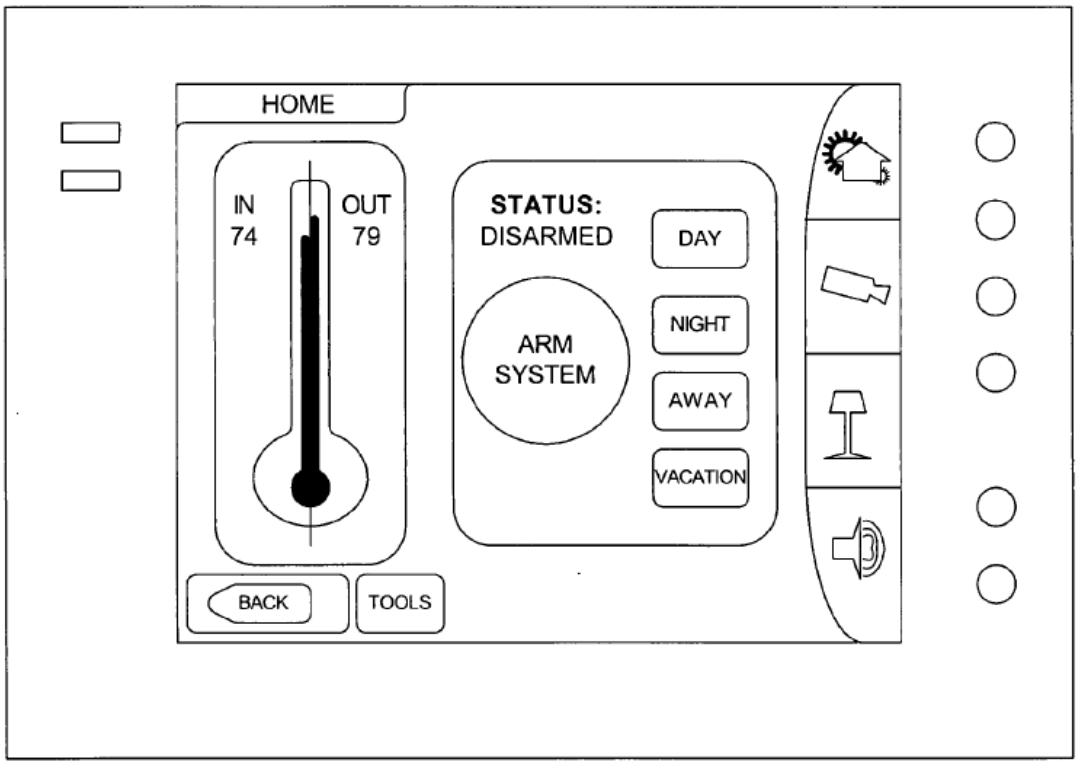


FIG. 4A

64. In addition to controlling the controlled devices, the GUI can implement web browser functionality so that the control panel 101 supports common web browsers such as Mozilla® or Internet Explorer®. (*Id.*, ¶ 0060.) I provide more details regarding the GUI and its functionality in the substantive sections that follow this overview.

B. Overview of Johnson

65. Johnson discloses an "Internet based home communications system." (Ex. 1005, Title.) The front-end of the system is set up much like that in Wimsatt.

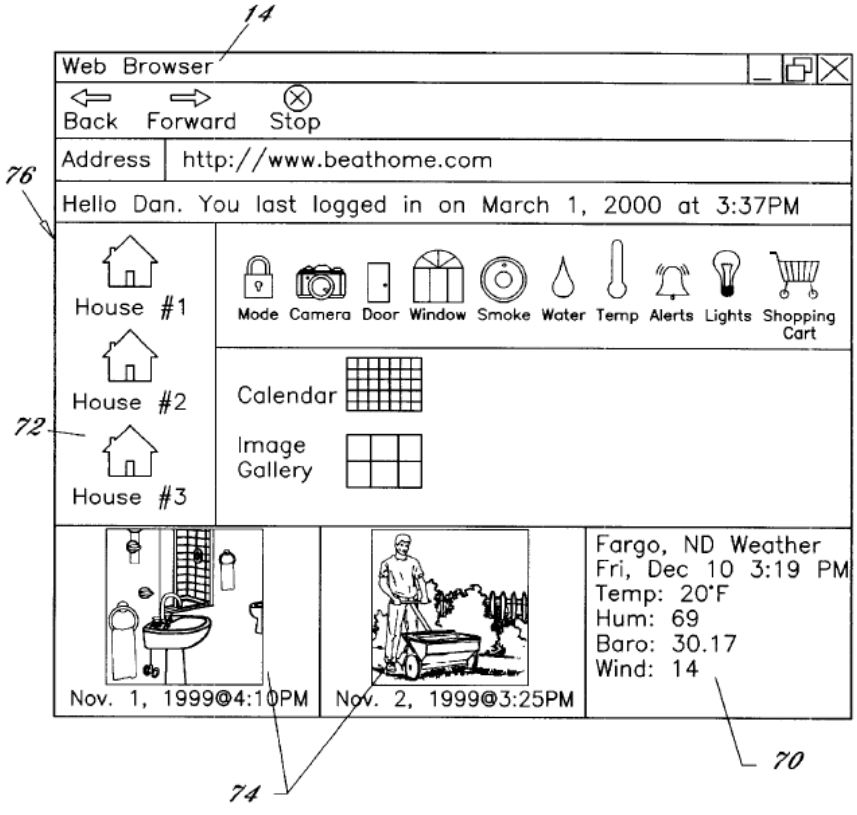
Namely, Johnson includes a control unit 30 that is capable of controlling various devices 40 in and around a home or building, such as lighting systems, cameras, security systems, and the like. (Ex. 1005, 2:8-19, FIG. 2.) Johnson differs from Wimsatt in that it also provides a back-end system that allows a homeowner to control the control unit 30, and thus the home-based devices, from a remote location. (Ex. 1005, 1:50-65.) Johnson is relied on primarily for this back-end disclosure.

66. Johnson explains that its control unit 30 is connected to a remotely located data center 20 via a global computer network 12 (i.e., the Internet). (*Id.*, 4:16-23, FIG. 1.) The data center 20 is comprised of "one or more server computers." Thus, Johnson contemplates that its entire data center 20 can be run on a single server, which I refer to in this declaration as the "data center 20 server."

67. According to Johnson, the data center 20 server is capable of "receiving, storing and transmitting various types of data related to the homeowner's home such as text, software, music, sound, temperature data, images 74, photographs, graphics, video, alerts, messages, advertisements, promotions or other information related to a home." (Ex. 1005, 4:47-53.) Johnson explicitly refers to this information collectively as "data". (Ex. 1005, 4:53.)

68. A homeowner is able to remotely access the above "data" stored on

the data center 20 server via a web page 76. (*Id.*, 6:36-38.) Johnson explains that the "web page is displayed by the data center 20 through a conventional web browser 14 on a computer." (*Id.*, 4:30-33.) This means that the web page 76 is populated with the data stored on the data center 20 server. Using this web page 76, the homeowner is able to monitor and control the devices 40 within the home while the homeowner is outside the home (e.g., on vacation or at work). (*Id.*, 4:30-39.) Shown below is Figure 3 from Johnson, which illustrates an exemplary control page 76 that would be displayed on the web browser 14.



69. From this page, the homeowner simply needs to select one of the

illustrated icons (labeled "mode", "camera", "door", "window", etc.) and then enter a desired setting change into the web page. (*Id.*, 6:61-65.) This information is transmitted to the data center 20 server, which then forward it to the home's control unit 30, which then facilitates modifying the setting changes. (*Id.*, 665-7:4.)

C. Overview of Severson

70. Severson describes a "micro-programmable security system." (Ex. 1006, Title.) Severson is specifically relied on for its disclosure regarding discovering security system sensors.

71. Severson discloses a front-end system similar to Wimsatt and Johnson, which includes a system controller SC1 and a plurality of sensors installed throughout a home. (*Id.*, FIG. 1) During installation of this system, Severson describes programming each of the sensors to include their assigned sensor number. (*Id.*, 23:60-25:2, 25:51-61.) This number is specifically associated with a "group" or "type" as shown in Tables 4-6 (not illustrated here). For example, sensor numbers "34-37" are described as "exterior delayed intrusion" sensors that are located at one or more "entrance doors." (*Id.*, 26:10-33:14 (Table 4), 34:37-36:62 (Table 6).) Once the sensors are programmed with this information, they can be installed within the home and begin transmitting their status to the system controller SC1. At this point, however, the system controller

SC1 does not realize that they exist.

72. Each system controller SC1 in Severson has an "install" mode and, while in that mode, it listens for signals. (*Id.*, 25:3-26:7.) When the sensors report their signals for the first time, the system controller SC1 hears the signals and "self-learns" each of the sensors. (*Id.*) The sensor number and the data the sensor provided is then stored within the system controller SC1's memory for future use. (*Id.*)

D. Overview of Naidoo

73. I understand that Naidoo was applied against the claims as a primary reference during prosecution. I rely on Naidoo here, however, for limited disclosures related to a few of the dependent claims. In particular, I rely on Naidoo's disclosure for 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.)

E. Overview of Alexander

74. Alexander is relied on for its remote server capabilities. Alexander discloses a system very similar to Johnson, which includes a remote server that communicates with a premises server (equivalent to the control panel 101 in Wimsatt or the control unit 30 in Johnson). (Ex. 1008, 3:24-28, 10:57-11:17.) The remote server provides a remote user with access to details about the premises

server and its controlled devices (e.g., sensors, cameras, appliances, etc.) through a user interface (similar to the control page 76 in Johnson). (*Id.*, FIG. 2, 7:1-14.) Alexander discloses additional remote server functionality that is not explicit in Johnson. For example, Alexander discloses that its remote server is capable of (1) adding and modifying user accounts (*id.*, 12:13-13:10, FIGs. 5A-7), (2) creating, modifying and configuring controlled devices at the premises (*id.*, FIG. 15B, 18:65-19:22, 17:54-18:12), (3) creating device rules, including notification rules, for the controlled devices (*id.*, 7:1-14, FIG. 13A, FIG. 16, FIG. 19, 18:13-64), and (4) managing access to logged state data associated with the controlled devices (*id.*, 7:59-65, 11:33-36, 7:1-14).

F. Overview of Anthony

75. 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.)

G. The Cited References Are Analogous Art

76. I understand that to combine prior art references when evaluating validity, those references must generally be "analogous." To be analogous, the art must be in the same field of endeavor as the '619 patent, and/or must be pertinent

to the problems at which the '619 patent is directed. This requirement is met by each of the references that are used in combination in this declaration. Each of the prior art references combined in these Petitions is analogous art to the '619 patent and to each other. Each reference is in the same field of endeavor as the '619 patent—the general field of integrated security systems. (Ex. 1004, Abstract, ¶ 0023; Ex. 1005, 2:8-28; Ex. 1006, Abstract; Ex. 1007, Abstract; Ex. 1008, 6:55-67; Ex. 1009, Abstract.) Because of these reasons and the reasons set forth below, it would have been obvious to an electronic engineer in 2005 to consult and combine the teachings of these cited prior art references.

VI. CLAIMS 1-9 AND 12-62 ARE OBVIOUS OVER WIMSATT IN VIEW OF JOHNSON, SEVERSON AND/OR OTHER REFERENCES UNDER 35 U.S.C. § 103(A)

A. Independent claim 1

1. Preamble: "A system comprising"

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

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

78. 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."

3. 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"

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

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

80. In my opinion, 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. 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. 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.

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

81. 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.)

82. Wimsatt discloses that its control panel 101 can implement a "system discovery process." In my opinion, a POSITA would have understood that the CMC module performs this 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.) "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.

83. A POSITA would understand that that claim element is in essence, describing the UPnP process. The Universal Plug-N-Play process was well understood at the time. Wimsatt states that the "Universal Plug-and-Play (UPnP™) processes support common protocols and procedures intended to enhance interoperability". As will be discussed a change in a sensors state (i.e. door / window being opened or closed) will ultimately be reflected in a change in the data object in the remote server (Johnson's Data Server 20). This demonstrates a complete coupling of data from initial event to data on the remote server.

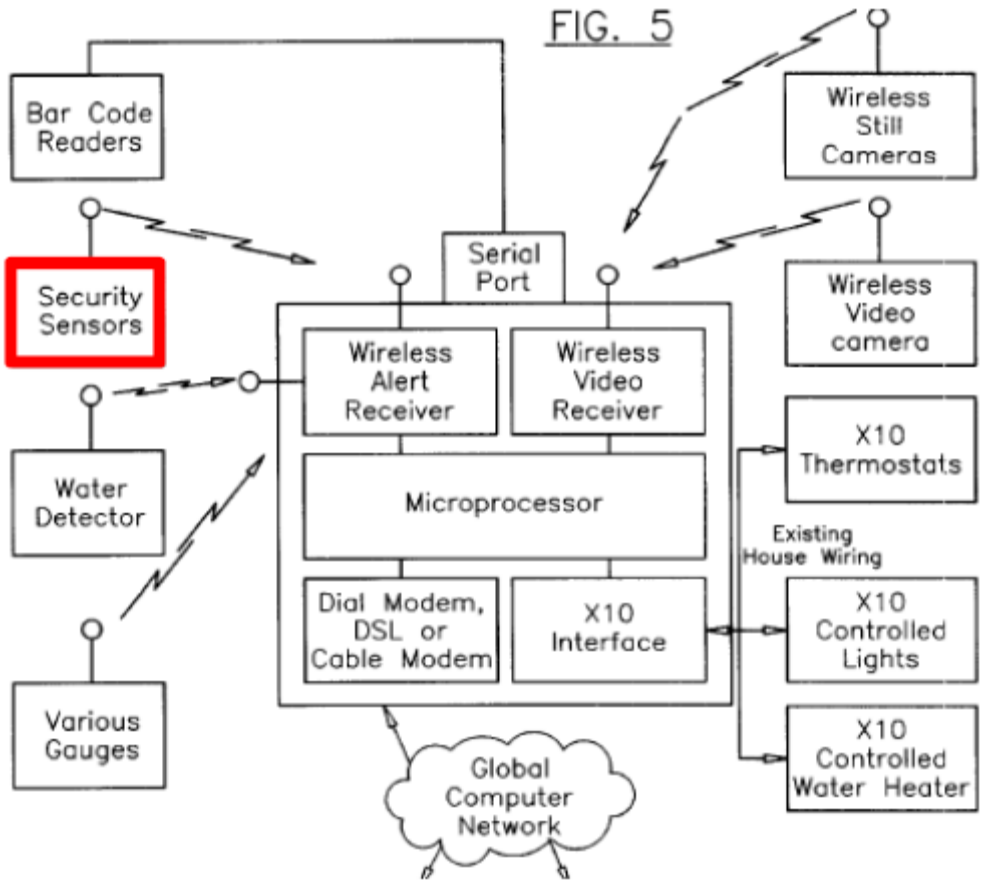
84. Wimsatt further discloses that its control panel 101 can be wireless (referred to as "control panel 107") and can wirelessly communicate with any of the controlled devices of the security system as a result of the above discovery process (e.g., because it now has the signaling protocol information needed for communication). (Ex. 1004, ¶¶ 0037, 0043.)

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

85. For context, 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. 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. It is this sensor (or sensors) that is "tripped" and sets off an alarm. Thus, sensors are inherent in Wimsatt

86. 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. Sensors are the "eyes" of a home security system. *See*, **Part III.B.1** above. Without sensors, a home security system is blind and cannot function. *Id.*

87. 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. 1004, 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).)



88. 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.

5. 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"

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

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

90. Wimsatt discloses that its control panel 101, including the connection management component, can implement a "system discovery process" as described above with respect to how Wimsatt also discloses element 1[b]. 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.

91. 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 '619 patent that UPnP™ was used to auto-discover 2-way devices connected to a shared network. (Ex. 1011, 7.)

92. 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. In my opinion, a POSITA would have understood that discovering the security system would also include discovering its sensors. 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.)

93. In my opinion, 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. This would predictably result in an easier, and quicker, sensor installation process and reduce the likelihood of installer error. (*See also,* Ex. 1006, 26:5-7.)

94. As I 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.) 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.

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

95. 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.

96. 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.

97. 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.* (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. 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.

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

98. In my opinion, 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. 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.

99. In fact, a POSITA would understand that several components of the home automation network, in particular everything to do with illumination (i.e. lights, lamps and their controllers) would typically be considered security components. For example, when an intrusion occurs, in addition to sounding the alarm, all of the lighting can be activated. This has the dual purpose of a) scaring away the intruder(s) and b) acting as a beacon to aid the police and other first responders to locate the premises in distress by, for example, flashing the exterior lights. This is a very useful method to attract attention to the home as it is often difficult to identify which home on a street full of homes the alarm bells or sirens

are actually coming from. The security system control of the lighting is also useful during entry to the premises (disarming) and exit from the premises (arming) to light the way for the homeowner or other users of the system.

100. A POSITA would understand that in order for all of the components involved in the above examples to work together they must of course be networked and since these same components are performing matters of security they must therefore, all be part of a security network.

6. 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"

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.)

102. In my opinion, 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. 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. 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.

103. In my opinion, a POSITA would be further motivated to combine Johnson with Wimsatt because control unit 30 in Johnson is similar to panel 101 in Wimsatt. 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. 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. A POSITA would be motivated to combine Wimsatt and Johnson with Severson for the reasons discussed above.

7. 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,"

104. 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.

105. 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.) In my opinion, 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. (*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.

106. 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.

107. 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. 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. Thus, Wimsatt discloses that its IP cameras are coupled to a local network that is independent from the security network.

108. 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* my opinions for claim element 1[e] 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 "remote data" as claimed. 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. 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 are discussed above for claim element

1[e] above. 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.

8. 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,"

109. 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.

110. With respect to the "security data", as previously discussed, when one or more security system sensors are activated (e.g., a door or window is opened), 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.

111. With respect to the "device data", a POSITA would understand that any signal (status or otherwise) from the IP cameras 109 would be processed by the processor 201 in a manner similar to that described above for the "security data". The "IP" in IP Camera stands for Internet Protocol. Any IP data received at the control panel 101 from the IP camera 109 would also necessarily require processing in order to convert the IP data back into imagery that can be used by the system. 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. (*See also*, Ex. 1004, ¶¶ 0038, 0045, 0054.)

112. 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*

my opinions for claim element 1[f] 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. The same motivations to combine Wimsatt and Johnson discussed for claim element 1[e] apply here.

9. 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"

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

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

114. One possible origin of a "state change of the security system" can be found in the status transmissions from the sensors. As mentioned above whenever a sensor changes state (from the opening or closing of the door or window it is

monitoring) it sends a status signal to the control panel 101. These status signals are processed by the control panel 101 to determine if for example, the system is (ready to arm), or (not ready to arm). Security systems typically do not let the user arm the system with open doors or windows. Each of these conditions, (ready to arm) and (not ready to arm) are valid states of the alarm system that resulted from processing the data present in the received status transmissions from the sensors. This (ready to arm / not ready to arm) state of the security system will be displayed to the user on the (touchscreen) system keypad. Similarly, this (ready to arm / not ready to arm) state will be communicated to the remote server at the Data Center 20 where it could be saved as a data object.

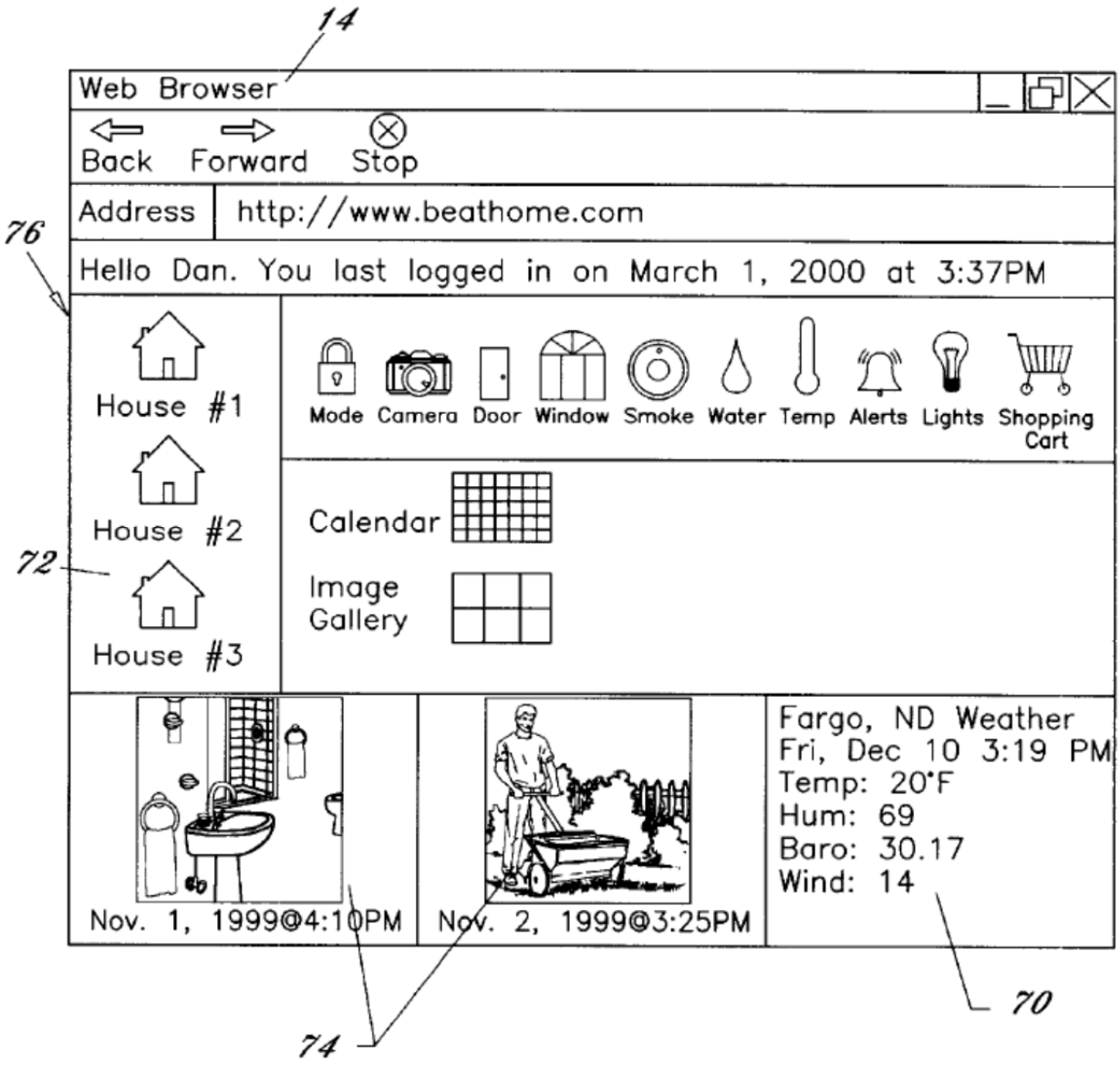
115. Wimsatt discloses that the control panel 101 can be used to arm and disarm the home's security system. (Ex. 1004, ¶¶ 0065-0066, 0070-0071, 0074.) When Wimsatt is modified by Johnson, a homeowner can control this functionality remotely through the data center 20 server. For example, when the homeowner sends 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", a POSITA would have understood that the control panel 101 in Wimsatt must process this "remote data" from the data center 20 server taking into account the (ready to arm / not ready to arm) state of the

system in order to determine if the homeowners request to arm the system can be honored or rejected. Here, upon processing, the control panel 101 would have determined that the status (or "state") of the home security system can be changed from "unarmed" to "armed."

c. "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"

116. For context, 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*.)

117. In my opinion, 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.)



118. 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.

119. A POSITA would have understood that the icons illustrated on the above web page represent particular controlled devices located within the home in Wimsatt. 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.

120. 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 for claim element 1[g] above. It would be difficult to change a device's settings without knowing the current status of that device. (*See,* Ex. 1005, 7:6-8.) Thus, in my opinion, 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

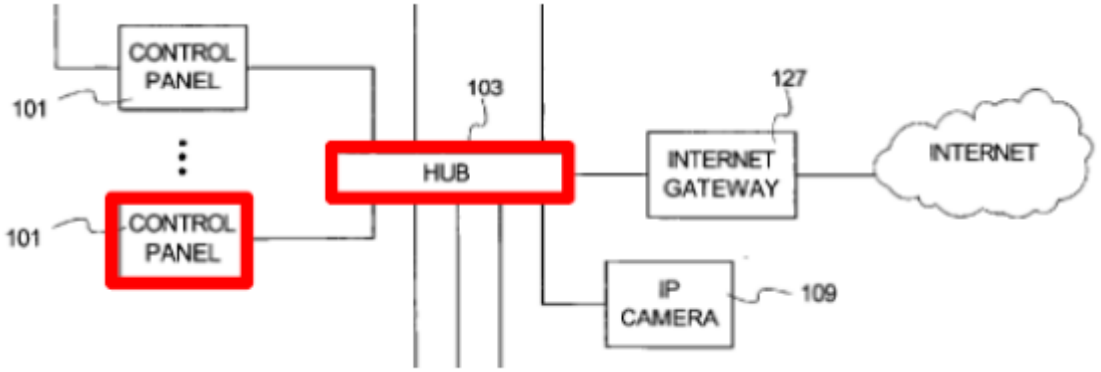
the most up-to-date information about the objects. Thus, the control panel 101 in Wimsatt "maintains" the "objects at the security server using the processed data."

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

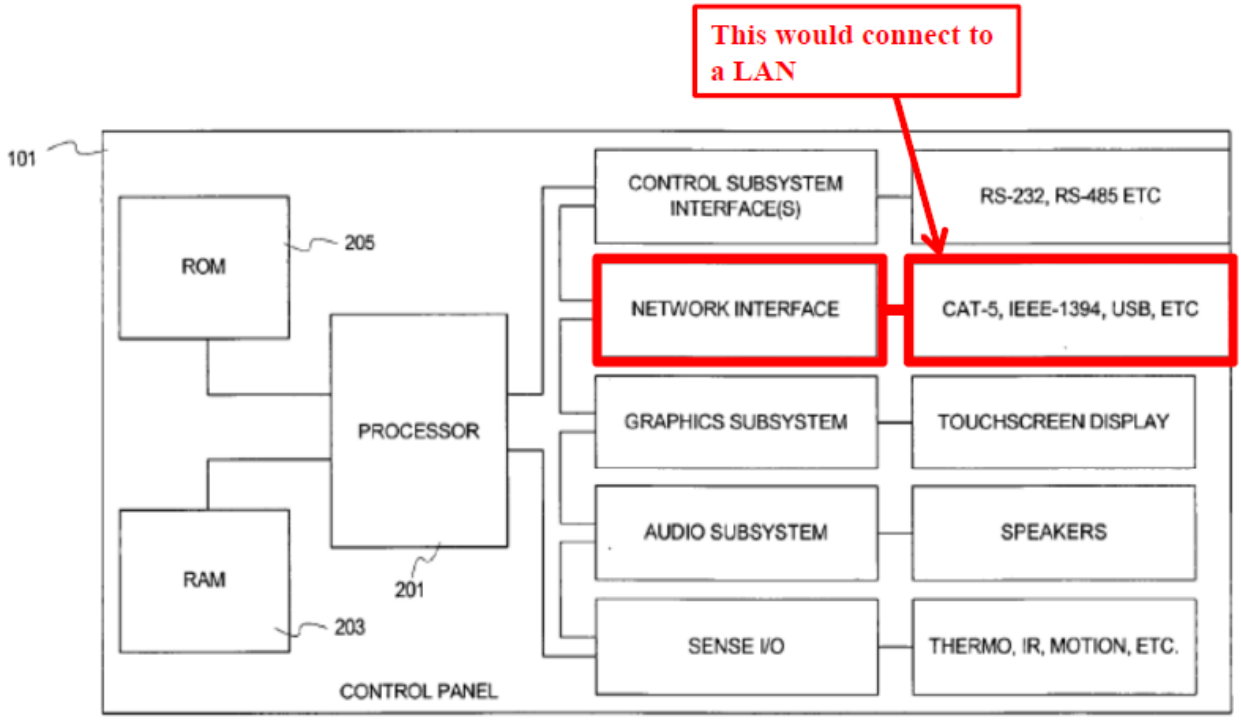
B. Dependent claim 2

2	The system of claim 1, wherein the gateway is connected to a local area network at the first location, and the local area network is coupled to a wide area network via a router at the first location.

122. With respect to the first part of the limitation, which recites "***wherein the gateway is connected to a local area network at the first location***," Wimsatt discloses that its control panel 101 is connected to a hub 103. This is shown below in annotated and excerpted Figure 1. The hub 103 is described as implementing an Ethernet connection among the system devices. (Ex. 1004, ¶ 0036.) It is well known that Ethernet connections form LANs. 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).)



123. Figure 2 of Wimsatt (annotated and shown below) provides a "hardware-oriented view" of the control panel 101 and shows that the panel 101 includes a "network interface" component. (Ex. 1004, ¶ 0016.) According to Wimsatt, the network interface's "functions are substantially similar to what might be found in a convention[al] personal computer network interface card (NIC)." (*Id.*, ¶ 0050.) A POSITA would have understood that a NIC is designed to couple or connect a computer to a LAN so that it can communicate over the LAN. (*See also,* Ex. 1004, ¶ 0024 (explaining that Wimsatt's system can be used in LAN environments).) Thus, for at least these reasons, a POSITA would have understood from the disclosures in Wimsatt that the control panel 101 is connected to a LAN located in the user's home.



124. With respect to the last part of the limitation, which recites "***the local area network is coupled to a wide area network via a router at the first location***," Wimsatt further discloses that the hub 103 can be a router. (Ex. 1004, ¶ 0036.) As also shown above in Figure 1, the hub 103 is connected to an Internet gateway 127 that provides access to the Internet, which is a "wide area network." (*Id.*, FIG. 1, ¶ 0041.)

C. Dependent claim 3

3	The system of claim 1, wherein the gateway is coupled to a wide area network and is coupled to a local area network at the first location via the connection management component and a router at the first location.

125. As discussed above for claim 2, the control panel 101 in Wimsatt, including the connection management component, is connected to a hub 103, which can be a router and which forms a LAN. (Ex. 1004, ¶ 0036.) Both the hub 103 and the LAN are in the "first location." As also discussed, the hub 103 is coupled to the Internet (i.e., a wide area network) via an Internet gateway 127. (*Id.*, FIG. 1, ¶ 0041.) Thus, the control panel 101 is coupled to the Internet via the hub 103 and intervening devices.

D. Dependent claim 4

4	The system of claim 1, wherein the gateway is coupled to the security server via the internet.

126. Claim 4 is disclosed by Wimsatt and Johnson. Johnson explains that its control unit 30 is coupled to the data center 20 server via a global computer network 12, which is described as the Internet. (Ex. 1005, 4:21-23, 4:61-63, FIG. 1.) When Wimsatt is modified by Johnson as discussed in claim 1, the control panel 101 in Wimsatt is coupled to the data center 20 server in the same manner – i.e., through the Internet.

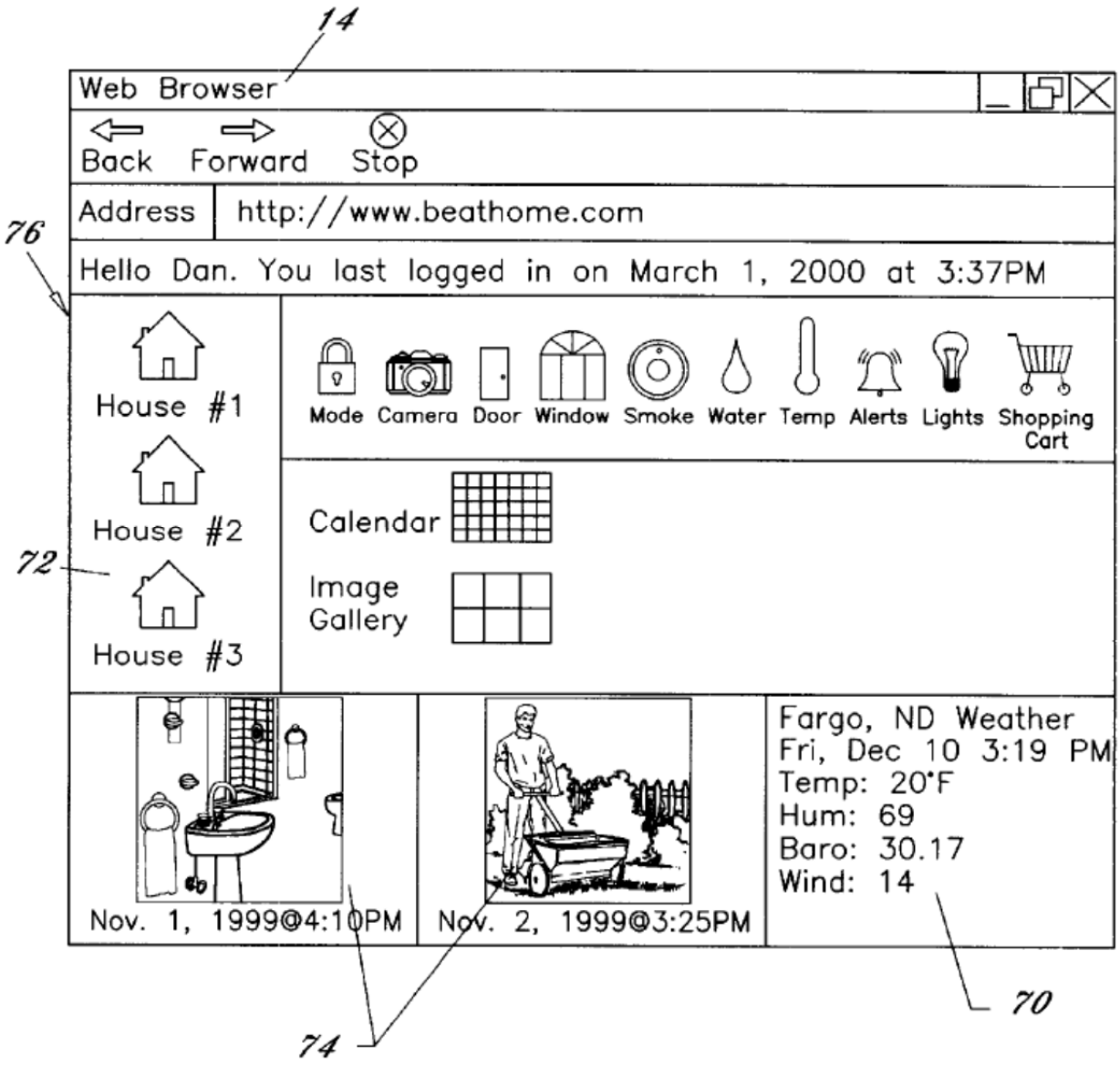
E. Dependent claim 5

5	The system of claim 1, comprising an interface coupled to the security network, wherein the interface allows control of the functions of the security network by a user.

127. Claim 5 is also disclosed by Wimsatt and Johnson. Johnson discloses

that a homeowner can access a web page that allows the homeowner to "monitor[] and control[]" aspects of the security system using that web page. (Ex. 1005, 4:30-36, 5:29-39, 6:35-59.) Johnson's web page is the claimed "interface." The security system (and its components) is part of the "security network" described in claim 1.

128. Figure 3 of Johnson (shown below) is an illustration of the web page. 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 communicate with and control the control panel 101 and the security system in the same manner. Thus, the web page 76 is communicatively coupled to the security network and allows the user to control functions of the security network.



129. A POSITA would be motivated to combine Johnson with Wimsatt for the reasons I already discussed with respect to claim element 1[e].

F. Dependent claim 6

6	The system of claim 1, comprising a portal coupled to the gateway, wherein the portal provides access to the communications and the functions of the security network via remote client devices.

130. Wimsatt and Johnson disclose claim 6. The web page 76 illustrated above in Figure 3 of Johnson is provided by a web browser 14, which is the claimed "portal." As similarly discussed in connection with claim 5, through the web browser 14, the web page allows a homeowner to "monitor[] and control[]" aspects of the security system using that web page. (Ex. 1005, 4:30-36, 5:29-39, 6:35-59.) Because these components are part of the "security network", the web browser 14 provides the user with access (via the web page) to the communications and functions of the security network. The web browser 14 in Johnson is coupled to the home's control unit 30 via the global network 12 and the data center 20 server. (*See, e.g.*, Ex. 1005, FIG. 1, 4:15-39.) And, the homeowner in Johnson is able to access the web page via the browser 14 using a remotely located computer, "wireless PDA", and/or "web-connected phones and pagers." (i.e., the claimed "remote client devices"). (*See, e.g.*, Ex. 1005, FIG. 5, Abstract ("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"), FIG. 1 (illustrating that the "user's computer" is remote from the home where the control unit 30 and control devices 40 are located), 4:30-36, 5:29-39, 6:35-59.)

131. When Wimsatt is modified by Johnson, the homeowner in Wimsatt

would be able to remotely access the control panel 101 in Wimsatt and control the controlled devices in the "security network" using the web page provided in Johnson. The motivations to combine Wimsatt, Johnson and Severson for claim 6 are the same as for claim 1.

G. Dependent claim 7

7	The system of claim 6, comprising an interface coupled to the security network, wherein the interface allows control of the functions of the security network from the remote client devices.

132. Claim 7 is substantively identical to claim 5 except for its dependency on claim 6 and it adds that the interface allows control "from the remote client devices." As discussed in claim 6, users can access the web page 76 (i.e., the claimed "interface") through the web browser 14 (i.e., the claimed "portal") using a remotely located computer, "wireless PDA", and/or "web-connected phones and pagers." (i.e., the claimed "remote client devices"). Thus, Wimsatt and Johnson disclose claim 7 for the same reasons discussed in claims 5 and 6.

H. Dependent claim 8

8	The system of claim 6, wherein the remote client devices include one or more of personal computers, personal digital assistants, cellular telephones, and mobile computing devices.

133. As discussed, Johnson discloses that the homeowner can access the web page via a computer, which is the claimed "personal computer". (Ex. 1005, 3:24-27, 3:40-43, 4:30-33, 6:36-38, 7:30-32.)

I. Dependent claim 9

9	The system of claim 1, wherein the gateway including the connection management component automatically discovers the security system components.

134. For the same reasons I discussed for claim element 1[d], which recites in part "the connection management component … automatically discovering the security system components," claim 9 is rendered obvious by Wimsatt, Johnson and Severson. As also discussed in that section, the CMC is a module within the gateway and thus the gateway necessarily automatically discovers the security system components when the CMC discovers them.

J. Dependent claim 12

12	The system of claim 1, wherein the gateway including the connection management component automatically establishes and controls the communications with the security system components.

135. For the same reasons I discussed for claim element 1[d], which recites in part "the connection management component … automatically discovering the security system components," claim 12 is rendered obvious by Wimsatt, Johnson and Severson. Wimsatt also discloses that, as a result of the discovery process, the control panel 101 is "programmed to support" the discovered devices and receives "full access" to those devices. (Ex. 1004, ¶ 0045.) A POSITA would understand that automatic discovery of the security system components includes establishing and controlling the communications with such components. As discussed, the

CMC is a module within the gateway and thus the gateway necessarily automatically establishes and controls communications with the security system components when the CMC discovers them.

K. Dependent claim 13

13	The system of claim 1, wherein the gateway including the connection management component automatically establishes a coupling with the security system including the security system components.

136. For the same reasons I discussed for claim elements 1[b] and 1[c], which recite in part "the connection management component … automatically establishing a wireless coupling with a security system" (element 1[b]) and "the security system including security system components" (element 1[c]), claim 13 is rendered obvious by Wimsatt, Johnson and Severson. As also discussed in that section, the CMC is a module within the gateway and thus the gateway necessarily automatically establishes a coupling with the security system when the CMC couples to it.

L. Dependent claim 14

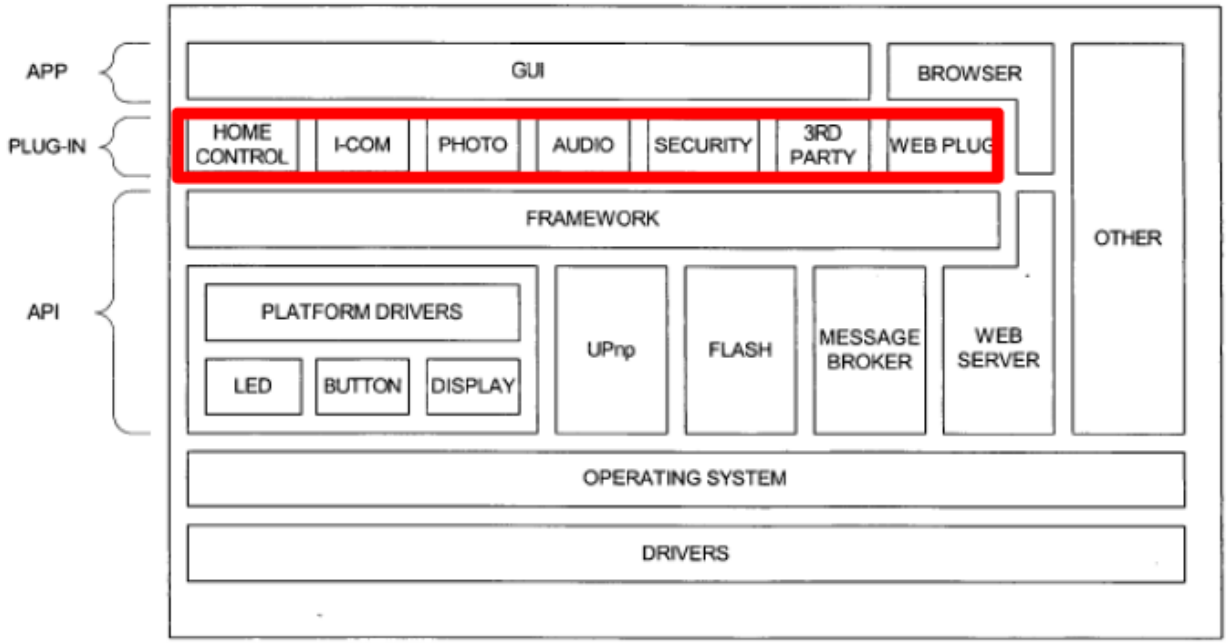
14	The system of claim 1, wherein the gateway includes a rules component that manages rules of interaction between the gateway and the security system components.

137. The "rules component" is just a description for software functionality. The Wimsatt system also has software in it that performs the same functions but has not specifically been named. The only valid way to compare software is by its

functionality. This sentiment about software functionality applies to all aspects of the gateway / controller software. To reiterate the only valid way to compare software of this type (custom embedded systems) is by comparing functionality.

138. The ‘619 patent appears to suggest that Automation engine 308 is an example of a “rules component” as it is described as “manag[ing] the user-defined rules of interaction between the different devices (e.g., when door opens turn on the light).” (Ex. 1001, 13:3-8.) Wimsatt describes an identical operation for the security plug-in.

139. Claim 14 is disclosed by Wimsatt and Johnson. The claimed “rules component” is collectively formed by the plug-ins shown below in annotated Figure 3 of Wimsatt, which are stored at and processed by the control panel 101.



140. Wimsatt discloses that the security plug-in in particular "may monitor [the] status of a home security system and when an anomaly is detected, activate the audio and home control plug-ins to provide information and/or alerts to users." (Ex. 1004, ¶ 0059; *see also, id.*, ¶¶ 0058, 0061.) The audio and home control plug-ins are described in Wimsatt as controlling the home's audio equipment 123 and the home's lighting system 113, respectively. (*Id.*, FIG. 1, ¶¶ 0056, 0058.) An alert received at the security plug-in therefore results in that plug-in activating the home's audio equipment 123 and the home's lighting system 113 (e.g., sounding an alarm and/or turning on the lights). Thus, the security plug-in includes the rules for determining how the control panel 101 and the other networked devices respond when the security system (and its sensors) alerts the control panel 101 to a

particular situation. In my opinion, it would be obvious to a POSITA that each plug-in includes its own set of rules for managing how the control panel 101 interacts and communicates with corresponding devices, and vice versa.

M. Dependent claim 15

15	The system of claim 1, wherein the gateway includes a device connect component that includes definitions of the security system components.

141. The plug-ins in Wimsatt also collectively form the claimed "device connect component". The '619 patent states that "DeviceConnect 310 includes definitions of all supported devices (e.g., cameras, security panels, sensors, etc.) using **standardized plug-in architecture**." (Ex. 1001, 13:9-19 (emphasis added).) This is exactly what Wimsatt discloses for its plug-ins. (Ex. 1004, ¶¶ 0057-0059.)

142. Although Wimsatt does not explicitly disclose that its plug-ins include definitions for the security system's sensors (i.e., the claimed "security system components"), this would be obvious to implement into the security plug-in in view of Severson. Severson discloses that sensor information (including sensor name, alert level) is learned into the controller. (*See, e.g.*, Ex. 1006, 23:60-67, Tables 4 and 5.) When Wimsatt is modified by Severson, the control panel 101 would include this sensor information. This information (or "definition") would be included in and/or used by the security plug-in in Wimsatt to support interaction between the control panel 101 and the sensors. The motivations for combining

Severson with Wimsatt and Johnson here are the same as discussed for claim 1.

N. 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.

143. 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*."

144. 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.

145. 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. Normal telephone conversations and communications take place in the voice band (under 4 KHz). DSL is completely separate from the normal phone communications and uses much higher frequencies and band width. In the home

when DSL is installed, it is also necessary to add blocking filters to keep the DSL from interfering with regular phone conversation and vice versa.

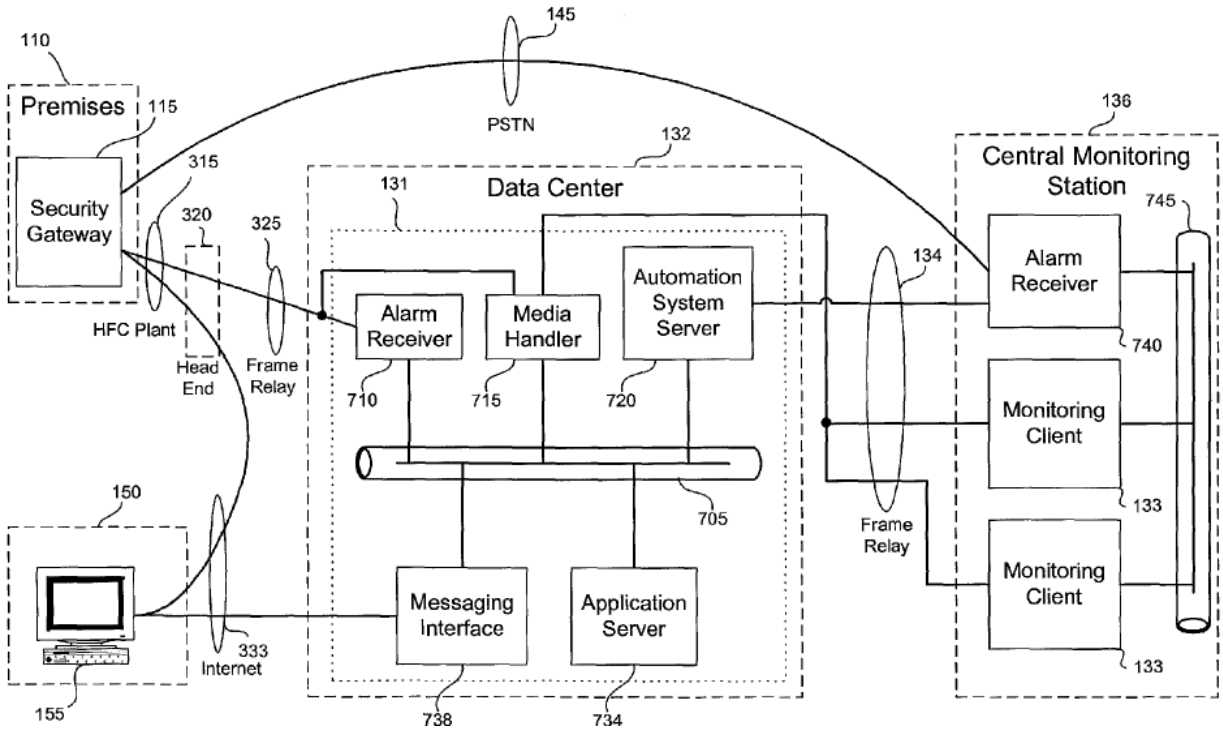
146. In my opinion, it would have been obvious to combine Wimsatt with Johnson and Severson so that both the security system and the control panel 101 in Wimsatt are capable of contacting a security agency (or central monitoring station). A POSITA would have understood the benefit of having two devices capable of contacting a security agency on different communication channels. 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. It was common practice to provide redundancy and alternate communications channels for security systems.

O. Dependent claim 17

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.

147. 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.)



148. 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.

149. In my opinion, 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. 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.

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

P. Dependent claim 18

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.

151. 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 2.

Q. Dependent claim 19

19	The system of claim 16, wherein the secondary communication link includes a broadband coupling.

152. As I discussed for claim 16, the claimed "secondary communication link" is formed by a DSL channel. It is well known that DSL technologies are broadband. Broadband refers to the band width of the channel. In order to support higher data rates the band width of the channel need to be increased or made broader. DSL provides much higher data rates than regular dial up hence it requires a much wider or broader channel. Broadband is a catch all phrase for high speed internet. The two most common broadband services offered the homeowner are DSL and Cable Modem. Thus, claim 19 is rendered obvious by Wimsatt in view of Johnson and Severson.

R. Dependent claim 20

20	The system of claim 16, wherein the secondary communication link

	includes a General Packet Radio Service (GPRS) coupling.

153. It is well known that GPRS communications are a type of mobile communication. Naidoo discloses that is 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.

154. Anthony discloses a security system that allows continuous remote monitoring and analysis. (Ex. 1007, ¶ 38.) Audiovisual signals and other signals from the system can be transmitted via general packet radio service ("GPRS"), which is a mobile communication mode.

155. 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. 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. Using a cellular data network such as GPRS removes the problem of the telephone line being cut. Thieves actively look

for and cut the telephone line before entering as they know that alarm systems normally use just the regular phone line to call for help. GPRS is cloud like in nature which makes it very quick and easy to communicate through.

S. Dependent claim 21

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.

156. 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.

157. In my opinion, 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). 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.

158. 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.

159. 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). 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.

T. Dependent claim 22

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.

160. 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.

U. Dependent claim 23

23	The system of claim 16, wherein the gateway receives control data for control of the security system components from remote client devices via the secondary communication link.

161. As I discussed for claims 5 to 7, 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 the security system (and its components) to modify the setting. (Ex. 1005, 7:47-8:5, 6:61-7:4.) This "command" is the claimed "control data." As explained throughout, the control panel 101 communicates with the data center 20 server via the Internet, which is the claimed "secondary communication link." 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.)

V. Dependent claim 24

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

162. 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.)

W. Dependent claim 25

25	The system of claim 24, wherein the gateway including the connection management component automatically discovers the network devices.

163. As discussed in connection with claim element 1[d], Wimsatt discloses that the CMC (which is part of the control panel 101) automatically discovers controlled devices within its network. (Ex. 1004, ¶ 0045.) Because security cameras (i.e., the claimed "network devices) are controlled devices, Wimsatt discloses automatically discovering the security cameras via the control panel's CMC. (Ex. 1004, ¶ 0040.) Thus, claim 25 is rendered obvious under Ground 1.

X. Dependent claim 26

26	The system of claim 24, wherein the gateway including the connection management component automatically installs the network devices in the security network.

164. The discovery process described in Wimsatt includes automatically installing the discovered devices into the control panel 101 and thus into the security network. For example, Wimsatt discloses that, as a result of the discovery process, the control panel 101 is "programmed to support" the discovered devices (e.g., an IP camera 109) and receives "full access" to those devices. (Ex. 1004, ¶ 0045.) The discovered / installed security camera is thus operational on the security network via the control panel 101. As discussed with respect to claim 1, the control panel's CMC performs this discovery process. Claim 26 is therefore rendered obvious under Ground 1.

Y. Dependent claim 27

27	The system of claim 24, wherein the gateway including the connection management component automatically configures the network devices for operation in the security network.

165. As I just discussed for claim 26, the discovery process described in Wimsatt includes automatically installing the discovered devices into the control panel 101 and thus into the security network such that the devices operate within the security network. For example, Wimsatt discloses that, as a result of the discovery process, the control panel 101 is "programmed to support" the

discovered devices (e.g., an IP camera 109) and receives "full access" to those devices. (Ex. 1004, ¶ 0045.) The discovered / installed security cameras are thus operational on the security network via the control panel 101. As discussed with respect to claim 1, the control panel's CMC performs this discovery, installation and configuration process. A POSITA would not install devices without having them configured to operate with the system. Claim 27 is therefore rendered obvious under Ground 1.

Z. Dependent claim 28

28	The system of claim 24, wherein the gateway controls communications between the network devices, the security system components, and the security server.

166. As previously discussed, when Wimsatt is modified by Johnson, the control panel 101 is the "middle man" between the remotely located data center 20 server and the home-based network devices (e.g., security cameras) / security system components (e.g., sensors). (Ex. 1005, FIG. 1; Ex. 1004, FIG. 1.) Nowhere does Johnson disclose that controlled devices communicate directly to the data center 20 server; rather, all communications must come from the control unit 30 (or control panel 101 in Wimsatt). (Ex. 1005, 7:16-8:5.) Thus, when Wimsatt is modified by Johnson, the control panel 101 "controls communications" per claim 28.

AA. Dependent claim 29

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.

167. 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).)

168. 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.

169. 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). 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. As also discussed for claim 16, the combined system discloses a plurality of different communication links, such as DSL, telephone line, Internet, etc.

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

BB. Dependent claim 30

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.

171. 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.)

CC. Dependent claim 31

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.

172. 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.

DD. 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.

173. 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.

EE. Dependent claim 33

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.

174. 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.

FF. Dependent claim 34

34	The system of claim 32, wherein the secondary communication link includes a broadband coupling.

175. As discussed for claims 16 and 32, the claimed "secondary communication link" is formed by a DSL channel. It is well known that DSL technologies are broadband. Broadband refers to the band width of the channel. In order to support higher data rates the band width of the channel need to be

increased or made broader. DSL provides much higher data rates than regular dial up hence it requires a much wider or broader channel. Broadband is a catch all phrase for high speed internet. The two most common broadband services offered the homeowner are DSL and Cable Modem. Thus, claim 34 is rendered obvious by Wimsatt in view of Johnson and Severson.

GG. Dependent claim 35

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

176. 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.

HH. Dependent claim 36

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.

177. 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

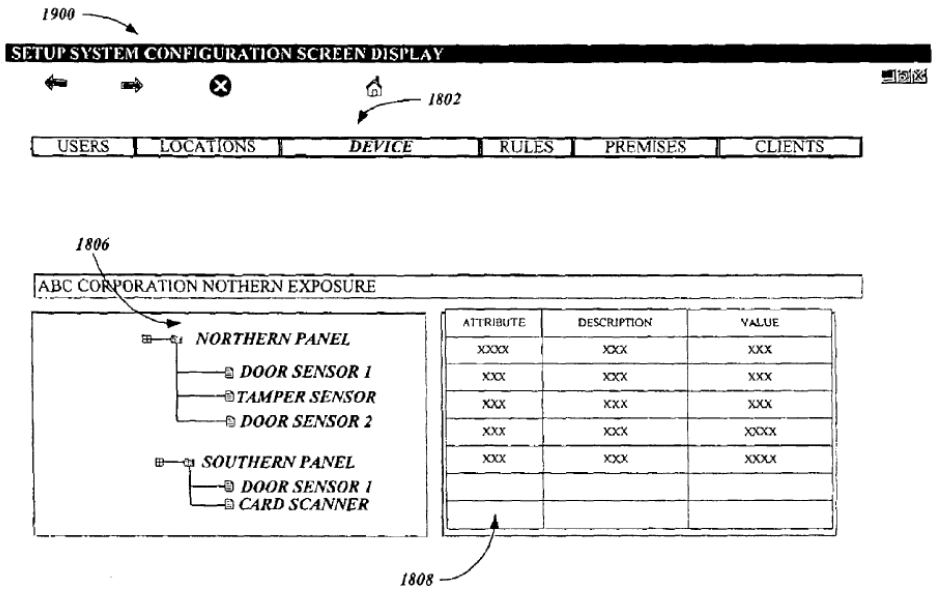
condition, **which may include alarm video**." (Ex. 1007, ¶¶ 0070-0071 (emphasis added).) This video comes from one of the network devices of Wimsatt. Thus, for the same reasons discussed in claim 21, claim 36 is rendered obvious under Ground 1.

II. Dependent claims 37 and 38

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.

178. 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. 15B, 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. 13, 14A-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. It would be easy to modify a component or devices properties to effectively make it useless which is the same result as just deleting it.



179. 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.)

180. In my opinion, 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. 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

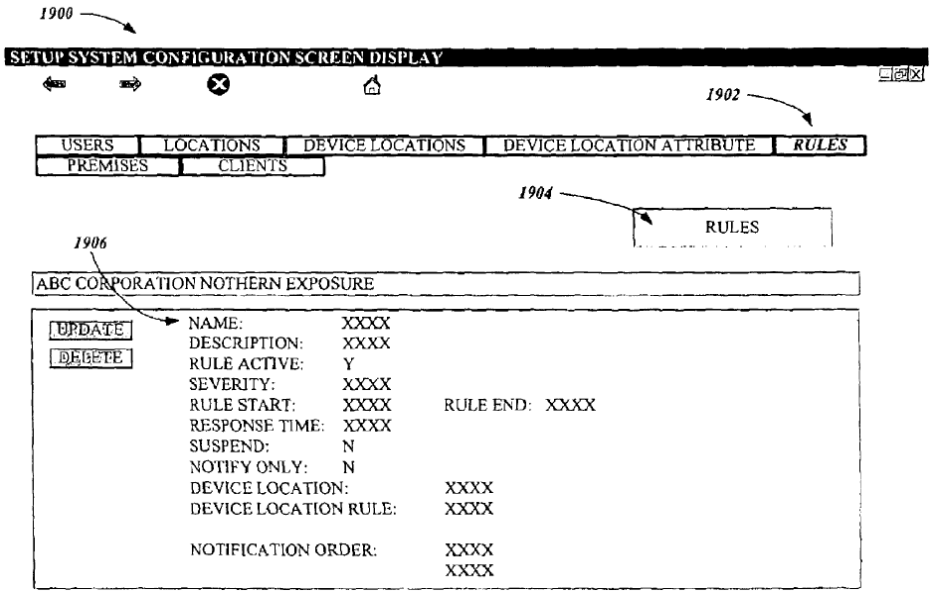
of the data center 20 server as well as allow the user to further customize his home security system. A POSITA would understand that these device connections are "couplings" between the control panel 101 and the network devices because adding a device to the system necessarily requires that the device is coupled to the control panel 101 for operation as part of the system.

181. 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.

JJ. Dependent claim 39

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

182. 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.)



183. 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.

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

185. In my opinion, 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. The rationale and motivations to combine these prior art references discussed for claims 37 and 38 also apply here.

KK. Dependent claim 40

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

186. 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, 7:47-5.) 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.)

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

LL. Dependent claim 41

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.

188. 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, 7:47-5.) 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.)

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

MM. Dependent claim 42

42	The system of claim 24, wherein the security server manages communications with the network devices.

190. Johnson discloses that the data center 20 server sends a "connect" command to the control unit 30 when it wants to communicate with the unit 30. (Ex. 1005, 7:17-28, 7:47-8:5.) If the unit 30 is online, then it establishes a direct secure connection with the server and can communicate data from its controlled devices with the server. (*Id.* 7:17-28, 7:47-8:5, 5:40-52.) For example, if a homeowner, via the server, requests a live video feed from one of its security cameras, then the server would connect with the control unit 30 and request that video feed. In turn, the control unit 30 would connect to the security camera to get the video feed. Because the server in Johnson manages communications between

itself and the control unit 30 and the control unit 30 communicates with its controlled devices, the server therefore manages communications with the cameras via the control unit 30. When Johnson is combined with Wimsatt, the data center 20 server in Johnson connects with the control panel 101 in Wimsatt to perform the same functions and manage connections in the same way. Thus, claim 42 is rendered obvious.

NN. Dependent claims 43 and 44

43	The system of claim 24, wherein the network device is an Internet Protocol device.
44	The system of claim 24, wherein the network device is a camera.

191. The security cameras in Wimsatt can be IP cameras 109 different from those located in the local network. (Ex. 1004, FIG. 1, ¶¶ 0038, 0040, 0072.) Thus, claims 43 and 44 are rendered obvious.

OO. Dependent claim 45

45	The system of claim 24, wherein the network device is a touchscreen.

192. Wimsatt discloses that the control panel 101 is connected to other panels 101 via hub 103 or wireless communication (panels 107). (Ex. 1004, ¶¶ 0035-0037.) It would be obvious to include one of these other panels 101/107 as a network device.

PP. Dependent claim 46

46	The system of claim 24, wherein the network device is a device

	controller that controls an attached device.

193. Claim 46 is rendered obvious by Wimsatt. The claimed "network device" is satisfied by any device that is included in the home automation network of Wimsatt. Figure 1 of Wimsatt illustrates a number of network devices, including a lighting control subsystem 113. Wimsatt explains that this subsystem 113 interface comprises a "control device", which is the claimed "device controller." (Ex. 1004, ¶ 0039.) As shown in the below, this control device is coupled to the home's lighting devices (e.g., lamps). (*Compare to* Ex. 1001, 15:21-26, 22:47-52, 22:63-23:3.)

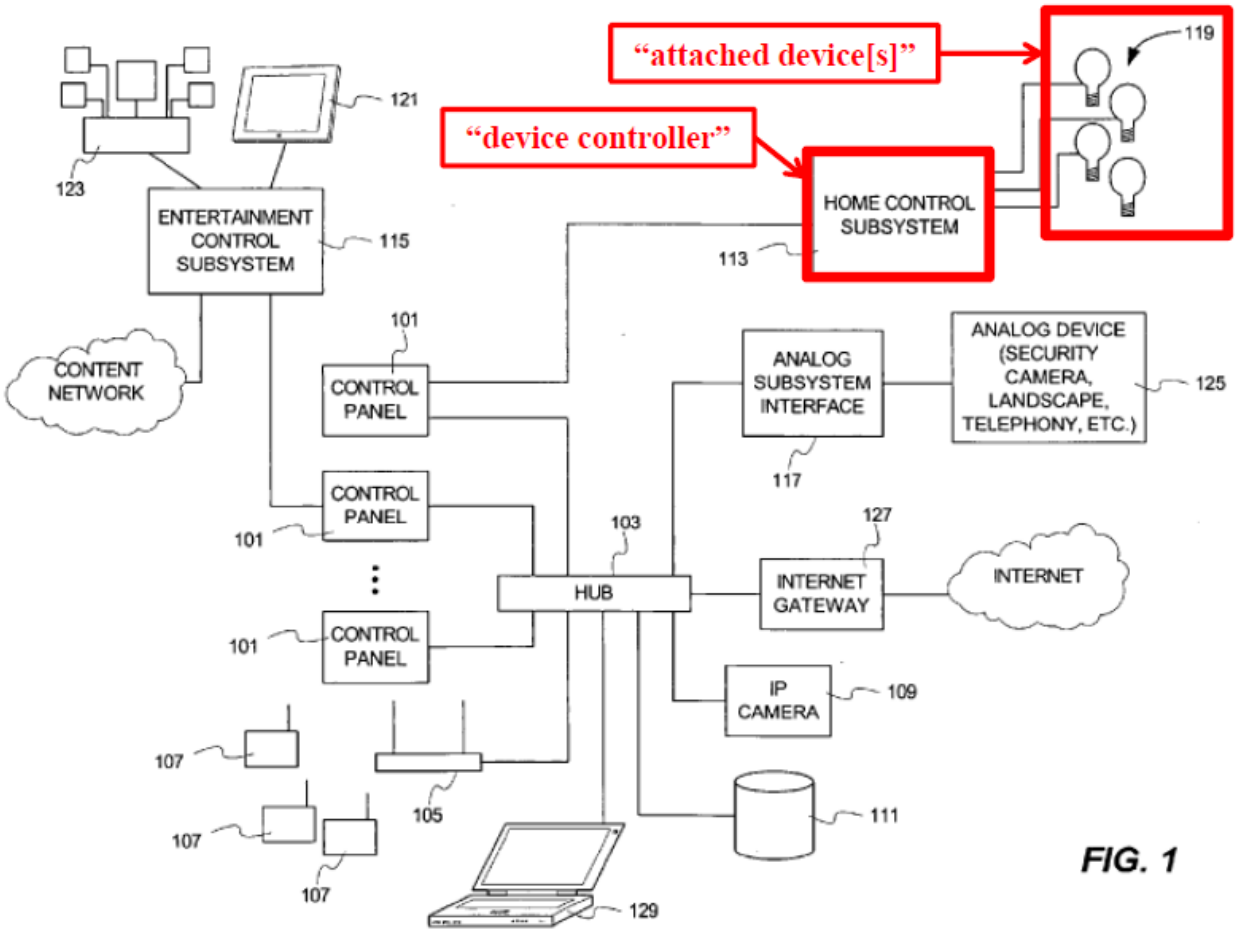


FIG. 1

QQ. Dependent claim 47

47	The system of claim 24, wherein the network device is a sensor.

194. As discussed for claim 1, Wimsatt discloses the claimed "network device" as an environmental sensor. (Ex. 1004, FIG. 1, ¶ 0038.) Thus, claim 47 is rendered obvious.

RR. Dependent claim 48

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

195. 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. Simply removing all of a user's rights would have the same effect as terminating a user.

196. 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. 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.

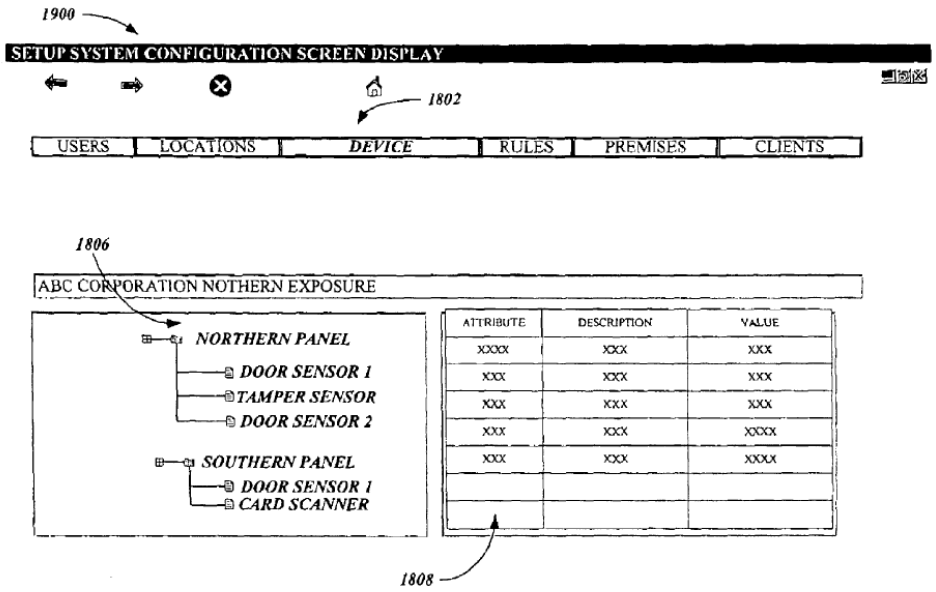
197. Alexander, Wimsatt, Johnson and Severson disclose similar integrated home monitoring systems and control panels. Thus, a POSITA would be motivated to combine the references to enhance their respective functionalities by providing this element in combination with those of claim 1.

SS. Dependent claims 49 and 50

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.

198. 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. 15B, 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. 13, 14A-18, 16:25-17:9, 11:13-17.) Although it does not describe deleting a monitoring device from the system, in my opinion, it would be obvious to a POSITA that "modifying" a device could include deleting it. It would be easy to modify a component or devices properties to effectively make it useless which is the same result as just deleting it.



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.)

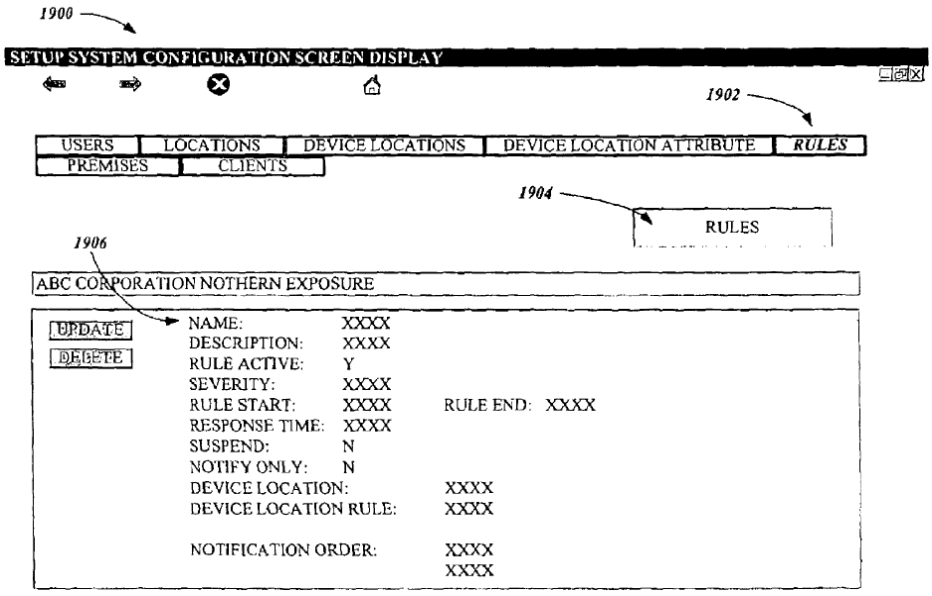
It would be obvious to combine Alexander with Wimsatt, Johnson and Severson so that the data center 20 server in Johnson is capable of performing the same functions described in Alexander through its control page 76, thereby predictably resulting in enhanced functionality of the data center 20 server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

simplification of device installation. 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.

TT. Dependent claim 51

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

199. 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.)



200. 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.

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

UU. Dependent claim 52

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

201. 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, 7:47-5.) 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.)

202. 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. 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. This would allow a user to access older data using the control page 76, if needed. Other

rationales and motivations to combine these references are discussed in connection with claim 48, 37 and 38 and apply here.

VV. Dependent claim 53

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.

203. 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, 7:47-5.) 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.)

204. 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.

205. 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.

WW. Dependent claim 54

54	The system of claim 1, wherein the security server manages communications with the security system components.

206. Johnson discloses that the data center 20 server sends a "connect" command to the control unit 30 when it wants to communicate with the unit 30. (Ex. 1005, 7:17-28, 7:47-8:5.) If the unit 30 is online, then it establishes a direct secure connection with the server and can communicate data from its controlled devices with the server. (*Id.* 7:17-28, 7:47-8:5, 5:40-52.) For example, if a homeowner, via the server, requests a live video feed from one of its IP cameras, then the server would connect with the control unit 30 and request that video feed. In turn, the control unit 30 would connect to the IP camera to get the video feed. A similar process is used to communicate with sensors. Because the server in Johnson manages communications between itself and the control unit 30 and the control unit 30 communicates with its controlled devices, the server therefore manages communications with the security system sensors and cameras via the control unit 30. When Johnson is combined with Wimsatt, the data center 20 server

in Johnson connects with the control panel 101 in Wimsatt to perform the same functions and manage connections in the same way. Thus, claim 54 is rendered obvious.

XX. Dependent claim 55

55	The system of claim 1, wherein the security server generates and transfers notifications to remote client devices, the notifications comprising event data.

207. Wimsatt and Johnson disclose claim 55. Johnson explains: "when a condition within the home reaches a warning level (i.e., **an 'event'**) … the control unit 30 sends an alert to the data center 20 through the global computer network 12." (Ex. 1005, 7:32-36 (emphasis added); *see also, id.*, FIG. 6, 5:63-67.) In response to this alert, "the control unit 30 may notify the data center 20 which can then **notify the homeowner of the condition** via e-mail, pager, web page, by direct telephone call or other communication means." (*Id.*, 6:2-6 (emphasis added); *see also, id.*, 7:42-46.) The cell phone, pager and/or computer receiving the notification via email or web page 74 in Johnson are "remote client devices." (*Id.*, FIG. 5 (illustrating that these remote devices are connected to the home via global computer network 12.)

208. When Wimsatt is modified by Johnson, the control panel 101 is connected to the data center 20 server that performs the same functions described

above. The same motivations to combine Wimsatt with Johnson and Severson for claim 1 apply here. In addition, a POSITA would understand the benefit of connecting the control panel 101 to the data center 20 server in Johnson because the connection would enhance the functionality of the control panel 101 and provide the homeowner with up-to-date notifications regarding the state of their property. This is especially important when security breaches occur within a home because immediate action might be needed.

YY. Dependent claim 56

56	The system of claim 55, wherein the notifications include one or more of short message service messages and electronic mail messages.

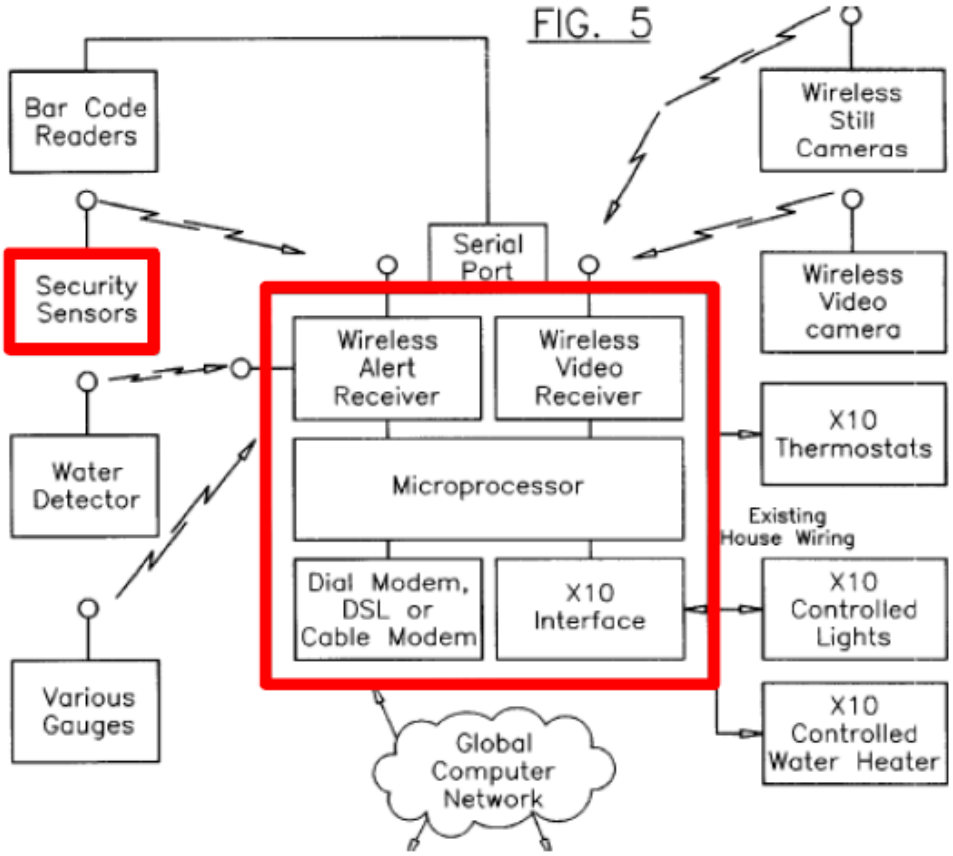
209. As discussed with respect to claim 55, the data center 20 server in Johnson notifies the homeowner via "e-mail" (i.e., electronic mail). Thus, claim 56 is rendered obvious.

ZZ. Dependent claim 57

57	The system of claim 55, wherein the event data is event data of the security system components.

210. When discussing "alerts" (or "events"), Johnson discloses that the alert (or event) can result from a security condition such as a home intrusion. (Ex. 1005, 5:54-67.) An alert of this nature would originate with the security sensors. This is shown below in annotated, excerpted Figure 5 of Johnson, which illustrates the "security sensors" sending an alert signal to the control unit 30. (*See also*, *id.*,

Ex. 1005, 5:54-62.) When Wimsatt is modified by Johnson, a POSITA would understand that the security sensors of the security system in Wimsatt would function similarly to those described in Johnson. Thus, claim 57 is rendered obvious.



AAA. Dependent claim 58

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.

211. 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.

212. 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.)

213. 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. 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. 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.

BBB. Dependent claim 59

59	The system of claim 1, wherein the security system components include one or more of sensors, cameras, input/output (I/O) devices, and accessory controllers.

214. As discussed for claim 1, a POSITA would have understood that the security system in Wimsatt includes a plurality of sensors. Wimsatt also discloses that its security system includes security cameras. (Ex. 1004, FIG. 1 (item 125, labeled "security camera"), ¶¶ 0040, 0075.) Furthermore, as also discussed for claim 1, Johnson discloses "security sensors." (*See*, Ex. 1005, FIG. 5.) Thus, claim 59 is rendered obvious.

CCC. Independent claim 60

215. As will be demonstrated in the following sections, the language of independent claim 60 is substantially identical to the language of independent claim 1.

1. Preamble: "A security network comprising"

216. Wimsatt in view of Johnson and Severson discloses a security network for the reasons that follow.

2. Claim elements 60[a] to 60[d]

217. As illustrated in the below chart, claim elements 60[a] to 60[d] are substantively identical to claim elements 1[a] to 1[e]. Thus, for the same reasons discussed above for claim elements 1[a] to 1[e], Wimsatt in view of Johnson and Severson discloses claim elements 60[a] to 60[d].

	Claim 1		Claim 60
1[a]	a gateway located at a first location	60[a]	a gateway including a connection management component located at a first location and automatically establishing a wireless coupling with a security system installed at the first location
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		
1[c]	the security system including security system components	60[b]	the security system including security system components,
1[d]	wherein the connection management component forms a security network by automatically discovering the	60[c]	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		security system components and integrating communications and functions of the security system components into the security network
1[e]	a security server at a second location different from the first location, wherein the security server is coupled to the gateway	60[d]	a security server at a second location different from the first location

3. Claim element 60[e]: "wherein the security server is coupled to the gateway and includes a plurality of security network applications"

218. For the same reasons discussed above for claim element 1[e], Wimsatt in view of Johnson and Severson discloses "the security server is coupled to the gateway." With respect to the latter recitation in claim element 60[e], the '619 patent provides details regarding Service Management clients that manage the operation of the overall service, including running applications to handle certain tasks such as provisioning, service monitoring, customer support and reporting. Johnson discloses that the data center 20 handles the same tasks. (Ex. 1005, col. 5, l. 54 – col. 6, l. 11.)

219. Such applications are also disclosed as the Operating System (OS) in Wimsatt. (Ex. 1004, FIG. 3.) It is well known the function of an OS on any computer is to dynamically provision processes and data. Wimsatt discloses that panel 101 includes "variants of a personal computer (PC) architecture to take

advantage of price and performance features." (Ex. 1004, ¶ 0034.) This passage clearly suggests that the panel's OS can function in the same manner as PC, including the provisioning features. Those provisioning features would obviously be applied to the applications and other content stored at panel 101. Thus, Wimsatt in view of Johnson and Severson teach claim element 60[e].

4. Claim elements 60[f]-60[i]

220. As illustrated in the below chart, claim elements 60[f] to 60[h] are identical to claim elements 1[f] to 1[h]. Thus, for the same reasons discussed above for claim elements 1[f] to 1[h], Wimsatt in view of Johnson discloses claim elements 60[f] to 60[h].

	Claim 1		Claim 60
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	60[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
1[g]	wherein the gateway generates processed data by processing at the gateway the security data, the device data, and the remote data	60[g]	wherein the gateway generates processed data by processing at the gateway the security data, the device data, and the remote data,
1[h]	wherein the gateway determines a state change of the security	60[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		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.

DDD. Independent claim 61

221. As will be demonstrated in the following sections, the language of independent claim 61 is substantially identical to the language of independent claims 1 and 60.

1. Preamble: "A security network comprising"

222. Wimsatt in view of Johnson and Severson discloses a security network for the reasons that follow.

2. Claim element 61[a]: "a gateway including a connection management component located at a first location"

223. Claim element 61[a] is identical to claim element 60[a], which is substantively identical to claim element 1[a]. Thus, for the same reasons discussed for claim elements 60[a] and 1[a], claim element 61[a] is rendered obvious by Wimsatt in view of Johnson and Severson.

3. Claim element 61[b]: "a wireless coupling between the gateway and a security system installed at the first location"

224. This claim element is substantively identical to claim element 1[b], which recites "a connection management component coupled to the gateway and

automatically establishing a wireless coupling with a security system installed at the first location." As discussed in that section, the "connection management component" is a software module within the control panel 101 in Wimsatt and the control panel 101 can be a wireless control panel 107. Thus, for the same reasons discussed for claim element 1[b], Wimsatt in view of Johnson and Severson disclose claim element 61[b].

4. Claim elements 61[c]-61[g]

225. As illustrated in the below chart, claim elements 61[c] to 61[g] are identical to claim elements 1[b]-1[d] and 1[f]-1[h], except for the underlined language which is discussed after the chart. Thus, for the same reasons discussed above for claim elements 1[b]-1[d] and 1[f]-1[h], Wimsatt in view of Johnson discloses claim elements 61[c] to 61[g].

	Claim 1		**Claim 61**
1[c]	the security system including security system components	61[c]	wherein the security system includes security system components <u>that are proprietary to the security system</u>,
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	61[d]	the connection management component automatically establishing the wireless coupling with the security system components and forming a security network by

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		automatically discovering the security system components and integrating communications and functions of the security system components into the security network,
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	61[e]	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 <u>from a remote network at a second location different from the first location</u>,
1[g]	wherein the gateway generates processed data by processing at the gateway the security data, the device data, and the remote data	61[f]	wherein the gateway generates processed data by processing at the gateway the security data, the device data, and the remote data,
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	61[g]	wherein the gateway determines a state change of the security system using the processed data and maintains objects at the remote network using the processed data, wherein the objects correspond to the security system components and the plurality of network devices; and

226. With respect to the underlined language in claim element 61[c], which recites "security system components <u>that are proprietary to the security system</u>,"

Wimsatt explains that its system "may be adapted to handle special-purpose and proprietary controlled devices and subsystems." (Ex. 1004, ¶ 0023.) As such, a POSITA would have understood that the entire controlled device – i.e., the entire security system, including the sensors of the security system – could be proprietary. Thus, Wimsatt and Johnson disclose this limitation.

227. With respect to the underlined language in claim element 61[e], which recites "remote data from a remote network at a second location different from the first location," the remote network corresponds to the network within which the data center 20 server in Johnson resides. This network is remote from the location of the home where the control panel 101 and its controlled devices reside. Thus, claim element 61[e] is substantively identical to claim element 1[f] and is rendered obvious for the same reasons discussed in claim element 1[f] and related sections discussing the data center 20 server.

5. Claim element 61[h]: "an interface coupled to the gateway, the interface providing communications with the security network and control of the functions of the security network from a remote client device"

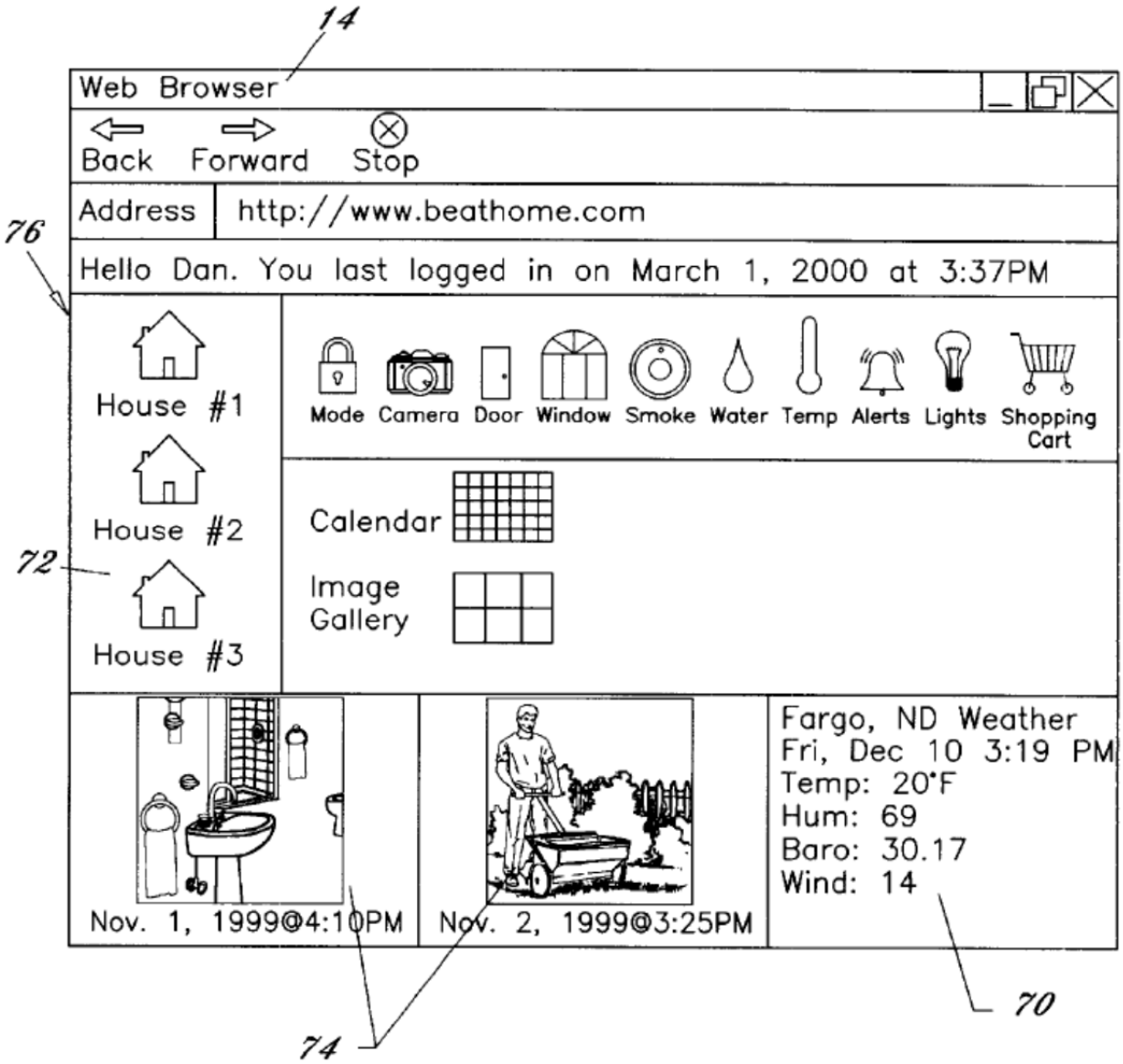
228. Wimsatt and Johnson disclose this limitation. For example, Johnson discloses that a homeowner can access a web page from a computer located outside the home or building. (*See, e.g.*, Ex. 1005, Abstract ("An Internet based home communications system for allowing a homeowner to monitor and control various

features of their home from a distant location via a global computer network"), FIG. 1 (illustrating that the "user's computer" is remote from the home where the control unit 30 and control devices 40 are located), 4:30-36, 5:29-39, 6:35-59.) Johnson's web page is the claimed "interface" and the homeowner's computer is the claimed "remote client device".

229. The web page in Johnson allows the homeowner to "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.) These components are all part of the "security network".

230. Figure 3 of Johnson (shown below) is an illustration of the web page. 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 (or building administrator) is able to remotely communicate with and control the control panel 101 and the controlled devices in the same manner. Thus,

the web page 76 is communicatively coupled to the control panel 101 via the data center 20 server.



231. A POSITA would have understood that the icons illustrated on the above web page represent particular controlled devices located within the home in Wimsatt. For example, the icon labeled "camera" corresponds to the IP cameras

109, and the icons labeled "door" and "window" correspond to door sensors and window sensors, respectively. Thus, Wimsatt in view of Johnson disclose this limitation. A POSITA would be motivated to combine Johnson with Wimsatt for the reasons already discussed with respect to claim 1.

232. The grounds discussed in claims 5-7 are applicable to this claim element as well.

EEE. Dependent claim 62

62	The system of claim 1, wherein a component of the gateway controls dynamic updating and replacing of the operating system of the security system on the gateway.

233. As discussed above, Wimsatt discloses an Operating System (OS). (Ex. 1004, FIG. 3.) Wimsatt discloses that panel 101 includes "variants of a personal computer (PC) architecture to take advantage of price and performance features." (Ex. 1004, ¶ 0034.) This passage clearly suggests that the panel's OS can function in the same manner as PC, including updating and replacing the OS. Such capability is well known to a POSITA.

VII. NO SECONDARY CONSIDERATIONS OF NON-OBVIOUSNESS EXIST

234. I am unaware of any evidence of secondary indicia of non-obviousness for the '619 patent.

VIII. CONCLUSION

235. I reserve the right to offer opinions relevant to the invalidity of the '619 patent claims at issue and/or offer testimony in support of the Declaration.

236. In signing this Declaration, I recognize that the Declaration will be filed as evidence in a contested case before the Patent Trial and Appeal Board of the United States Patent and Trademark Office. I also recognize that I may be subject to cross-examination in the case. If required, I will appear for cross-examination at the appropriate time.

237. I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true, and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under 18 U.S.C. § 1001.

Dated: SEP 30th, 2016

Respectfully submitted,

James Parker