Filed on behalf of Petitioner
By: Richard F. Giunta
Daniel T. Wehner
Randy J. Pritzker
WOLF, GREENFIELD & SACKS, P.C.
600 Atlantic Avenue
Boston, MA 02210
Tel: (617) 646-8000
Fax: (617) 646-8646
RGiunta-PTAB@wolfgreenfield.com

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

RPX Corporation

Petitioner

v.

MD Security Solutions, LLC

Patent Owner

Case No. TBD

Patent No. 7,864,983

DECLARATION OF TAL LAVIAN, PH.D.

TABLE OF CONTENTS

I, Tal Lavian, Ph.D., declare:

1. I have been retained by Petitioner RPX Corporation ("RPX"), to assess U.S. Patent No. 7,864,983 ("the '983 patent). I am being compensated for my time at a rate of $400 per hour, plus actual expenses. My compensation is not dependent in any way upon the outcome of RPX's petition.

I. PERSONAL AND PROFESSIONAL BACKGROUND

2. I have more than 27 years of professional experience. In 1987, I obtained a Bachelor of Science ("B.Sc.") in Mathematics and Computer Science from Tel Aviv University, Israel. In 1996, I obtained a Master's of Science ("M.Sc.") degree in Electrical Engineering also from Tel Aviv University. In 2006, I received a Ph.D. in Computer Science from the University of California at Berkeley.

3. I am employed by the University of California at Berkeley, and was appointed as a lecturer and Industry Fellow in the Center of Entrepreneurship and Technology ("CET") as part of UC Berkeley College of Engineering. I have been with the University of California at Berkeley since 2000 where I served as a Berkeley Industry Fellow, Lecturer, Visiting Scientist, Ph.D. Candidate, and Nortel's Scientist Liaison.

4. As an undergraduate and a Masters student in Tel Aviv University, I worked part time as a security officer and first respondent in a national oil and

gas repository. My duties included operating a control room with multiple security alarm systems, including many security cameras, different types of sensor technologies including motion sensors.

5. My Master's thesis was in the area of image processing. From 1987 until 1990, I worked for an Israeli startup (Shalev, Inc.). At that position, I developed image processing software for analysis of camera images from multiple angles. This included finding the exact shapes, borders and contours of objects.

6. From 1990 to 1993, I worked as a software engineer and team leader at Scitex Ltd., where I developed system and network communications tools. From 1994 to 1995, I worked as a software engineer and team leader for Aptel Communications, designing and developing mobile wireless devices and network software products.

7. From 1996 to 2007, I worked for Bay Networks and Nortel Networks. Bay Networks was in the business of making and selling computer network hardware and software. Nortel Networks acquired Bay Networks in 1998, and I continued to work at Nortel after the acquisition. Throughout my tenure at Bay and Nortel, I held positions including Principal Scientist, Principal Architect, Principal Engineer, Senior Software Engineer, and led the

development and research involving a number of networking technologies. I led the efforts of Java technologies at Bay network and Nortel Networks.

8. I am named as a co-inventor on more than 80 issued patents and I have co-authored more than 25 scientific publications, journal articles, and peer-reviewed papers. Furthermore, I am a Senior Member of the Institute of Electrical and Electronics Engineers ("IEEE").

9. I currently serve as a Co- Founder and Chief Technology Officer (CTO) of VisuMenu, Inc., where I design and develop architectures of visual IVR technologies for smartphones and wireless mobile devices in the area of network communications.

10. A detailed record of my professional qualifications, including a list of patents and academic and professional publications, is set forth in my curriculum vitae attached to this declaration as Exhibit 1011.

11. Prior to reviewing the '983 patent, I was well familiar with the subject matter described and claimed in the '983 patent. The '983 patent concerns a security system that includes one or more motion-activated cameras that records images in response to detecting motion and can be controlled by a handheld device, such as a cellular phone. (Ex. 1001 at 2:30-52;11:1-16) I am an expert in the field of home security systems and networking for connecting and controlling such systems.

II. MATERIALS REVIEWED AND CONSIDERED

12. In connection with my work on this matter, I have reviewed the '983 patent (Ex. 1001) as well as the other following documents:

EXHIBIT	DESCRIPTION
1001	U.S. Patent No. 7,864,983 ("the '983 patent")
1002	U.S. Patent Publication No. 2005/0267605 ("Lee")
1003	U.S. Patent No. 7,106,333 ("Milinusic")
1004	U.S. Patent No. 7,253,732 ("Osann")
1005	U.S. Patent Publication No. 2004/0120581 ("Ozer")
1006	U.S. Patent Publication No. 2007/0070185 ("Dy")
1007	U.S. Patent No. 7,463,145 ("Jentoft")
1008	Website: http://www.apple.com/pr/library/2001/10/16Apple-Powers-Up-Titanium-PowerBook-G4-with-New-G4-Processors.html
1009	Website: http://searchnetworking.techtarget.com/definition/terminal

III. LEVEL OF ORDINARY SKILL IN THE ART

13. For purposes of assessing whether prior art references disclose every element of a patent claim (thus "anticipating" the claim) and/or would have rendered the claimed invention obvious, I understand that the '983 patent and the prior art references must be assessed from the perspective of a person

having ordinary skill in the art ("POSA") to which the patent is related, based on the understanding of that person at the time of the invention date. I understand that a POSA is presumed to be aware of all pertinent prior art and the conventional wisdom in the art, and is a person having ordinary creativity. I have applied this standard throughout my declaration.

14. I have been asked to provide my opinion as to the state of the art in the field of security systems in the 2006 timeframe. I use the 2006 timeframe because the '983 patent claims priority on its face to applications filed in March and June of 2006. Whenever I offer an opinion below about the knowledge of a POSA, the manner in which a POSA would have understood the claims of the '983 patent, the manner in which a POSA would have understood the prior art, or what a POSA would have been led to do based on the prior art, I am referencing this timeframe (i.e., 2006). When I offer an opinion or explanation below about the teachings of the prior art and/or the claims of the '983 patent, I am explaining how the issue would have been viewed by a POSA in the 2006 timeframe, even if I do not say so specifically in each case. In my opinion, a POSA related to the '983 patent in the 2006 timeframe would have had at least a B.S. in Electrical Engineering, Computer Engineering or Computer Science or the equivalent, along with 2 years of working experience in image processing and/or developing telecommunications systems such as networked computer

systems. This person would have been capable of understanding and applying the prior art references discussed herein.

15. By 2006, I had received a Ph.D. in Computer Science with a focus on telecommunications, had received a Master's degree with a thesis focused on image processing, and had over 18 years of relevant professional experience. Therefore, I was a person of more than ordinary skill in the art during the relevant time period. However, I worked with many people who fit the characteristics of the POSA, and I am familiar with their level of skill. When developing the opinions set forth below, I assumed the perspective of a person having ordinary skill in the art, as set forth above.

IV. OVERVIEW OF THE '983 PATENT

16. The claims of the '983 patent relate to a security alarm system having one or more cameras and one or more motion detectors associated with and coupled to the camera(s) to activate the camera(s) when the motion detector(s) detect motion in a monitored area. The security system also includes a processor that receives commands from a handheld telecommunications unit, such as a cell phone, so that the system can be remotely controlled from the handheld telecommunications unit. The commands sent from the handheld telecommunications unit to the computer include a command for the processor to provide images captured by the camera(s) to the handheld telecommunications

unit. Some of the dependent claims describe other commands that the handheld telecommunications unit can send to the computer. Other dependent claims describe an image analysis process where images captured by the camera(s) are analyzed to identify objects in the images and perform actions based on the identified objects. As discussed further below, security systems with all of these features were well known before the '983 patent's filing date.

17. As discussed below, the claims of the '983 patent cover a security system and a method of operating a security alarm system having motion-activated cameras that can be controlled by a handheld telecommunications unit and include a number of other requirements. Systems and methods meeting all of the requirements of the claims were known to those of skill in the art before the '983 patent was filed. Both of the primary prior art references discussed below (i.e., Lee and Milinusic) provide an example of a security system that included motion-activated cameras controllable by a handheld telecommunications unit before the priority date of the '983 patent and meet or render obvious, alone or in combination with other references, all of the challenged claims.

V. SUMMARY OF THE '983 PATENT CLAIMS

18. The '983 patent (Ex. 1001)[1] describes and claims an alarm system

[1] Unless otherwise indicated, all citations in Section V are to Ex. 1001.

as described in Section IV above. I understand that each claim must be evaluated individually on its merits, and I have done so below. The ‘983 patent includes independent claims 1 and 11. The bracketed letters are added for purposes of cross reference.

1. An alarm system for protecting a structure, comprising:

[*A*] at least one motion detector arranged to have a field of view external of the structure and including an area proximate the structure;

[*B1*] at least one camera associated with and coupled to each of said at least one motion detector,

[*B2*] each of said at least one camera being arranged relative to the associated one of said at least one motion detector such that said camera has a field of view encompassing at least part of the field of view of the associated one of said at least one motion detector,

[*B3*] each of said at least one camera having a dormant state in which images are not obtained and an active state in which images are obtained and being activated into the active state when the associated one of said at least one motion detector detects motion;

[*C*] a processor coupled to said at least one camera and arranged to control said at least one camera and receive the image obtained by said at least one camera;

[*D*] a telecommunications module coupled to said processor, said telecommunications module being capable of communications over a telecommunications network; and

[*E*] a handheld telecommunications unit for transmitting commands for said processor via said telecommunications module to cause said processor to provide images to said telecommunications module to be transmitted to the telecommunications unit.

19. Independent claim 11 is a method claim that includes limitations similar to those in claim 1, with some differences noted below.

11. A method for protecting a structure, comprising:

[*A*] arranging a plurality of motion detectors on or around the structure, each in a position in which its field of view includes an area proximate the structure;

[*B1*] arranging a plurality of cameras on or around the structure, each camera being associated with one or more of the motion detectors

[*B2*] such that the camera has a field of view encompassing at least part of the field of view of any associated motion detector,

[*C*] providing a processor which controls the at least one camera and receives images obtained by the at least one camera;

[*D*] coupling a telecommunications module coupled to the processor, the telecommunications module being capable of communications over a telecommunications network; and

[*E*] transmitting commands from a handheld telecommunications unit to the processor via the

telecommunications module to cause the processor to provide images to the telecommunications module to be transmitted to the telecommunications unit.

20. Elements A, B1, and B2 recite typical components of a security system that includes one or more motion detectors and one or more cameras having a field of view that overlaps at least partially with the field of view of the motion detector(s). The specification of the '983 patent indicates that the motion detectors and the cameras both can be "standard, off-the-shelf components." (Ex. 1001: 7:19-21; 8:23-26). Element B3 recites functionality of the camera as being activated into an active state in which images are acquired when the motion detector detects motion. Motion-activated cameras for use in security systems were well-known prior to the relevant timeframe, as discussed in more detail below. Element B3 is absent from independent claim 11.

21. Elements C, D, and E recite typical components of a security system that can be controlled by a device over a telecommunications network. Element C (a processor) interfaces with the security system components such as the camera and the motion detector. Element D (a "telecommunications module") provides a communications interface between a handheld device and the processor. Element E (a "handheld telecommunications unit") sends and receives information to/from the processor via the telecommunications module.

22. I have been informed by counsel that a claim in a patent subject to *inter partes* review must be given its "broadest reasonable interpretation" (BRI)," consistent with the specification. I understand that a claim term explicitly defined in the specification of the patent should be interpreted in accordance with that definition. I further understand that a claim term that is not defined in the specification should be interpreted in accordance with its plain and ordinary meaning to a POSA at the time that the patent was filed if that plain and ordinary meaning is consistent with the specification. For example, I understand that the BRI of a claim term should be sufficiently broad to encompass any examples or embodiments of the term described in the specification. I apply the BRI standard in my analysis below.

23. "Structure" is not defined in the specification of the '983 patent. The specification provides several non-limiting examples of "premises or structure" such as a house, a warehouse, a boatyard, a business, a boat, or a land vehicle. (Ex. 1001 at 6:54-65). Thus, the BRI of the term "structure" includes at least the types of structures identified in the specification.

24. "Telecommunications network" is not defined in the specification of the '983 patent. The specification describes communications between the handheld telecommunications unit and the processor using a telephone network (Ex. 1001 at 11:23-30) or a computer network, such as the Internet (Ex. 1001 at

13:21-24). The plain and ordinary meaning of "telecommunications network" encompasses at least such networks. The BRI of "telecommunications network" to a POSA refers to a collection of nodes and links that enables the transmission of information between two computing entities, and encompasses at least telephone networks and computer networks, such as the Internet.

25. "Handheld telecommunications unit" is not defined in the specification of the '983 patent. The specification provides several examples of handheld telecommunication units including a cellular telephone, an iPod, a PDA, and a laptop computer. (Ex. 1001 at 6:2-6). Thus, the BRI of "handheld telecommunications unit" consistent with the specification includes at least those devices described as examples in the '983 patent specification.

26. "Silhouette" is not defined in the specification of the '983 patent. A silhouette generally refers to the shape or outline of an object. The specification describes derivation of a silhouette of an object as being based on a number of descriptors that are typical for the object (e.g., human body), or on other factors which can be used to distinguish, discriminate and/or differentiate the object from other types of objects (e.g., distinguishing animals from humans). (Ex. 1001 at 9:35-39). Thus, the BRI of "silhouette" consistent with the specification includes a representation of an object derived using at least the techniques described in the '983 patent specification.

VI. CLAIMS 1-20 ARE UNPATENTABLE IN LIGHT OF THE PRIOR ART IDENTIFIED IN RPX'S PETITION

27. I have been asked to provide my opinion concerning whether claims 1-20 of the '983 patent are unpatentable based on the prior art references identified in RPX's petition. The prior art references I reviewed include:

EXHIBIT	PRIOR ART REFERENCE
1002	U.S. Patent Publication No. 2005/0267605 ("Lee")
1003	U.S. Patent No. 7,106,333 ("Milinusic")
1004	U.S. Patent No. 7,253,732 ("Osann")
1005	U.S. Patent Publication No. 2004/0120581 ("Ozer")

28. I understand that in an *inter partes* review proceeding, claim terms should be given their broadest reasonable interpretation (BRI) consistent with the specification. In my analysis below and as discussed above, I apply that standard to the words and phrases of the challenged claims.

29. My opinions on the disclosure of each prior art reference, as relevant to the limitations of claims 1-20 of the '983 patent, are provided below. Claim charts with mappings from references to the claims of the '983 patent are attached for each of Grounds 1-4 as Appendices A-D, respectively, to this Declaration.

A. Ground 1: Claims 1-8, 11, and 18-20 of the '983 Patent Each Would have Been Obvious in View of Lee

30. According to the face of the document, Lee (Ex. 1002) is a U.S. patent application that published on December 1, 2005, from an application that was filed on January 6, 2005. I have been informed by counsel that it meets the requirements to be prior art to the '983 patent.

31. Lee describes a home entertainment security, surveillance, and automation control system that includes a main control unit, a plurality of remote devices, including a surveillance and security device ("S&S device"), and various user input devices capable of receiving a home user's commands (abstract, FIG. 1)[2]. Lee teaches that, in the 2005 timeframe, integrating audio and video devices into an existing home or building was complicated and costly due to the requirement to install new control wires. [0012]. The system of Lee uses RF/wireless communication and power line communication that is capable of transmitting various data via the power line without additional hardwire connections. [0066]-[0067].

32. The main control unit 100 of Lee is connected to remote devices (including S&S device 212) via a power line communication link 200 (FIG. 1). The main control unit 100 is configured to control the system and perform communication with one or more remote devices and user input devices via the

[2] Unless otherwise indicated, all citations in §A(¶¶30-86) are to Ex. 1002 (Lee).

power line communication link 200 or a wireless connection link. [0068]. Lee describes several types of user devices that can send control signals or control data to the main control unit 100. These user devices include a remote control 281, a cell phone 283, a wireless PDA 282, and a remote computer 291 that can communicate with main control unit 100 over the Internet. [0060];[0062]. The main control unit 100 controls the operation of remote devices, including S&S device 212, in response to commands received from one or more of the user devices. [0057]; [0107]; [0109].

33. The S&S device 212 is shown in more detail in FIG. 9 and includes one or more camera modules and one or more sensor modules. [0103]-[0104]. Each of the camera modules includes a camera 922, a sensor 923, and a camera interface 921. [0104]. Each of the sensor modules includes a sensor 931 and a sensor interface 932. [0104]. A house or building can be provided with a plurality of S&S devices 212 inside and outside the house/building to record information. [0105]; [0112]. Lee describes several modes in which the S&S device 212 may be set to operate, including an "ON mode," an "OFF mode," and an "INTERRUPT mode." [0107]. When the S&S device 212 is in "ON mode," the camera 922 is in a non-stop working state and in the "OFF mode" the camera is not working. [0107]. Lee describes that in "INTERRUPT mode," the camera will be on if a triggered signal is received from sensor 923. [0107]-[0108]. The

sensor 923 may trigger activation of the camera when, for example, presence of an intruder is detected by the sensor. [0108]; [0111]. Lee does not explicitly state that in "INTERRUPT mode" the camera is off (or "dormant") and not recording images prior to receiving a trigger signal, but a POSA would have understood that to be the case because otherwise, there would be no difference between Lee's "INTERRUPT mode" and Lee's "ON mode" in which images are recorded continuously.

34. The S&S device 212 can include any number of camera and sensor modules ([0105]), and numerous types of sensors including motion sensors. [0110].

35. Images acquired by the camera 922 are transmitted to the main control unit 100 via power line communication network 200. [0111]. The images may be watched live on an LCD display 50 (FIG. 1; [0084]; [0112]), stored on a mass storage module of the main control unit 100 ([0076]), and/or provided to remote computer 291 [0062]. When the S&S device 212 is triggered, information is sent to the main control unit 100 to alert the user of the event sensed by the S&S device 212 and the main control unit may automatically call the user's mobile telephone 283 if the user is not home. [0111]. The user may also monitor the system over the Internet. [0111].

36. After reviewing Lee and claims 1-8, 11, and 18-20 of the '983 patent, it is my opinion that every one of these claims would have been obvious to a POSA in view of Lee. The basis for my opinion and the details of my analysis are below.

i. Claim 1: "An alarm system for protecting a structure, comprising:"

37. Lee's system incorporates a surveillance and security ("S&S") device 212 that includes one or more camera modules 920 and one or more sensor modules 930. [0103]-[0104]. When the S&S device 212 has been triggered, the user can be alerted about the nature of the unusual event information sensed by the sensor(s) in the system in a number of ways, including via a text message, a live image sent to a display device 50, a telephone call to the user's mobile telephone if the user is not home, and/or via remote monitoring by the user over the Internet. [0111]. Accordingly, a POSA would have understood Lee's system to be an alarm system.

38. The camera modules 920 and sensor modules 930 are installed inside and outside of a house, which is a structure (see ¶23). Accordingly, Lee's system is an alarm system for protecting a structure.

a. "[*A*] at least one motion detector arranged to have a field of view external of the structure and including an area proximate the structure;"

39. Each of the camera modules 920 and sensor modules 930 in S&S device 212 includes a sensor. [0104]. The sensors include motion sensors. [0110]. The camera module(s) 920 and the sensor module(s) 930 may be installed outside a house as well as inside. [0105]. Lee describes that the purpose of the S&S device 212 is to monitor the house and detect intruders ("there is provided a security and surveillance device, including a plurality of sensors and cameras installed in correspondence to a place to be monitored for detecting information about [an] intruder." [0028]; "the sensor can send [a] trigger signal to the camera 922 when the presence of an intruder has been detected by the sensor and the sensor is triggered." [0108]). Lee is not explicit about where the camera modules 920 and sensor modules 930 of the S&S device 212 are placed outside the house and what field of view the motion detectors and cameras incorporated into the modules would have, but teaches that the modules should be "installed in the necessary sites inside and outside the house." [0105]. To achieve Lee's stated purpose of detecting the presence of an intruder and detecting information about an intruder ([0028]; [0108]), a POSA would have understood that "the necessary sites" to monitor include the areas proximate the access points to the house (e.g., doors and windows). Thus, it would have been

obvious to a POSA to implement a home installation of the Lee system by arranging motion sensors to have a field of view external of a structure (i.e., the house), and that the field of view would include areas proximate the structure (e.g., proximate doors and windows) to detect motion of any intruders seeking to enter the house.

b. "*[B1]* at least one camera associated with and coupled to each of said at least one motion detector,"

40. The S&S device 212 in Lee's system includes a plurality of camera modules 920 that each includes a surveillance camera 922 coupled to a sensor 923 (which may be a motion detector), and where the camera can be activated to record images when the motion detector is triggered. [0108]; [0110]-[0111]; FIG. 9. For example, Lee states, "the sensor can send [a] trigger signal to the camera 922 when the presence of an intruder has been detected by the sensor and the sensor is triggered." [0108]. Accordingly, a POSA would have understood that Lee discloses at least one camera associated with and coupled to at least the motion detector.

c. "*[B2]* each of said at least one camera being arranged relative to the associated one of said at least one motion detector such that said camera has a field of view encompassing at least part of the field of view of the associated one of said at least one motion detector,"

41. Lee does not explicitly state that the field of view of a camera 922 within a camera module 920 encompasses at least part of the field of view of at least one motion detector 923 that is within the same camera module 920 and associated with the camera 922. However, a POSA would have understood this to have been implicitly disclosed by Lee's description of a sensor (motion detector) 923 being disposed in the same module as the associated camera 922. ([0104]; FIG. 9), and by Lee's disclosure that cameras and motion detectors are "installed in correspondence to a place to be monitored for detecting information about [an] intruder." [0028]. A POSA would have understood that the camera and sensor in the same module "installed in correspondence to a **place to be monitored**" (emphasis added) would be arranged to monitor the same "place" by having fields of view that both encompass that "place."

42. Alternatively, even if a POSA would not have considered Lee to implicitly disclose that the camera 922 had a field of view that encompasses at least part of the field of view of its associated sensor 923 within a camera module 920, this would have been the obvious way a POSA would have implemented Lee's system. Lee indicates that cameras and motion detectors are

"installed in correspondence to a place to be monitored for detecting information about [an] intruder" ([0028]) and that "[g]enerally, the camera module 920, sensor module 930, and wireless module 940 are installed at necessary sites inside and outside the house." [0105]. To achieve Lee's stated purpose of detecting the presence of an intruder in a place and detecting information about an intruder in that place ([0028]; [0108]), and to implement the "INTERRUPT mode" where the camera is activated by a trigger signal from the motion detector ([0107]-[0111]), a POSA would have understood that the area monitored by the camera should include at least part of the area monitored by the sensor. Otherwise, the camera would not be able to capture images of the intruder detected by the motion detector. In addition, there would be no reason to activate the camera based upon an event (e.g., detected motion) if the camera cannot capture any information about the triggering event. Thus, it would have been obvious to a POSA to implement a home installation of the Lee system by arranging the camera 922 within a camera module 920 to have a field of view that encompasses at least part of the field of view of at least one motion detector 923 within the same camera module.

43. To further support my opinion that it would have been obvious to a POSA to implement Lee's system so that the camera 922 within a camera module had a field of view that encompasses at least part of the field of view of

the sensor 923 within the same module 920, I note that it was known prior to the relevant time period to have security systems that employ a camera activated by a motion detector, such that the field of view of the camera encompasses at least part of the field of view of the motion detector. (*see e.g.*, Ex. 1003 (Milinusic) at 5:51-59 ("Image capture [of an area] may be set to occur at predetermined times or upon the occurrence of predetermined occurrences, such as the detection of movement within the area being monitored by the sensor units 250 or 260."; Ex. 1007 (Jentoft) at 4:6-8 ("The motion sensor 20 and the camera 25 are positioned such that both devices have overlapping field of detection.").

d. "[*B3*] each of said at least one camera having a dormant state in which images are not obtained and an active state in which images are obtained and being activated into the active state when the associated one of said at least one motion detector detects motion;"

44. Lee describes several modes in which the S&S device 212 may be set to operate including an "ON mode," an "OFF mode," and an "INTERRUPT mode." [0107]. When the S&S device 212 is in "INTERRUPT mode," the camera is off unless and until a trigger signal is received indicating that the presence of an intruder has been detected by a sensor. [0107]-[0108]. The camera is said to be "activated" when the sensor 923 is triggered. [0111]. Although Lee does not explicitly state that when the system is in INTERRUPT mode the triggered "on" state of the camera is a state in which images are

obtained and that the camera is otherwise in an "off" state in which images are not obtained, a POSA would have understood that when the camera of Lee is "on" it is obtaining images, and when the camera of Lee is "off" it is not obtaining images. In addition to the common understanding to a POSA of what it would have meant for a camera to be on or off, this understanding is buttressed by Lee's explanation that when the device 212 is placed in "ON mode" the camera is in a non-stop working state, when the device 212 is placed in "OFF mode" the camera is not working ([0107]), and that when the security system "has been triggered" the S&S device 212 transmits video data to the main control unit 100. [0111].

45. Lee's system includes various types of sensors that may trigger the camera when the S&S device 212 is in "INTERRUPT mode," including motion sensors. [0110]. Lee does not explicitly state that in "INTERRUPT mode" the camera is off (or "dormant") and not recording images prior to receiving a trigger signal, but a POSA would have understood that to be the case because otherwise, there would be no difference between Lee's "INTERRUPT mode" and Lee's "ON mode" in which images are recorded continuously. Accordingly, when the sensor 923 is a motion sensor and the S&S device 212 is placed in "INTERRUPT mode," the camera 922 has a dormant state in which images are not obtained (e.g., when a trigger signal has not been received from the sensor),

and an active state in which images are obtained (e.g., when the trigger signal has been received from the sensor). The camera in "INTERRUPT mode" is activated into the active state when the motion sensor detects motion and sends a trigger signal to the camera. [0111].

e. "*[C]* a processor coupled to said at least one camera and arranged to control said at least one camera and receive the image obtained by said at least one camera;"

46. Lee's system includes a main control unit 100 that includes a microprocessor 150. [0069]. A POSA would have understood that a microprocessor is a processor as recited in the claims of the '983 patent. The microprocessor 150 is connected to a power line communication module 101 over a bus. [0069]. The power line communication module 101 is coupled to camera 922 via power line 200 and camera interface 921. (FIGS. 2 and 9). Accordingly, microprocessor 150 is coupled to camera 922.

47. The processor 150 is arranged to send control data via the power line communication network 200 to various aspects of S&S device 212 including camera 922 [0057]-[0058]; ("The power line communication interface module 101 is coupled to the bus and configured to transfer audio, video, sensor, and control data between the power line communication interface module and at least one of the plurality of remote devices, such as surveillance and security device over the power line communications link." [0083]); ("The interface

module receives control signals from the remote controller or the cell phone or a wireless PDA and then the microprocessor outputs a control signal to perform a desired function in response to the user signals." [0081]). The processor 150 can control the camera 922 in the camera module 920 to, for example, allow the user to select the "ON mode," "OFF mode," or "INTERRUPT mode" ([0107]) via the main control unit 100 and its processor 150. ([0071]; [0057]-[0058] ("a main control unit 100 that is capable of enabling a user to set, program, and control the system … and sending … the control data to at least one remote device" such as S&S device 212)).

48. Main control unit 100, including microprocessor 150, is also arranged to receive surveillance data (e.g., images) from the camera in S&S device 212. ("The camera can communicate with camera interface 921 and then the interface sends the image data and sensor data to the main control unit 100 via power line communication network." [0108]). Accordingly, a POSA would have understood that the main control unit 100 of Lee includes a processor (i.e., microprocessor 150) coupled to the camera (i.e., camera 922) and arranged to control the camera and receive an image obtained by the camera.

f. "*[D]* a telecommunications module coupled to said processor, said telecommunications module being capable of communications over a telecommunications network; and"

49. Lee's system includes a main control unit 100 having a microprocessor 150 and multiple types of communications interfaces to communicate with user input devices. (FIG. 1). The communications interfaces include an RF/wireless interface 190 ([0067]), a telephone line interface (e.g., Public Switched Telephone Network (PSTN) 292) ([0062]), and a computer network (e.g., local area network (LAN)/Internet 290) interface. FIG. 1;[0062]. Lee also discloses that there is an interface (not shown in FIG. 1) for connecting to the cell phone 283 and an interface (not shown in FIG. 1) for connecting to the PDA 282. [0060].

50. As discussed in ¶24 above, the BRI of the term "telecommunications network" encompasses the computer network (LAN/Internet) 290 described in Lee with which the main control unit 100 provides an interface. Lee also describes using a telephone network (e.g., the PSTN) to connect the main control unit 100 to input/output devices, including the computer 291. [0062]. Accordingly, a POSA would have understood that the main control unit 100 in the system of Lee includes one or more telecommunications modules coupled to the processor of the main control unit 100 and capable of communications over a telecommunications network.

g. "[*E*] a handheld telecommunications unit for transmitting commands for said processor via said telecommunications module to cause said processor to provide images to said telecommunications module to be transmitted to the telecommunications unit."

51. Lee's system includes multiple types of user input devices for sending control commands to main control unit 100, including wireless PDA 282, cell phone 283, and remote computer 29. [0059]; [0062]; FIG. 1. A user may program the system via on-screen program menus displayed on any of the user input devices. [0064]. Lee describes examples of commands that can be transmitted from the user input devices to the main control unit 100, including a command to set the main control unit 100 to a different mode, a command to switch the camera in S&S device 212 on or off, a command to place the camera in S&S device 212 in standby mode, and a command to turn the system on or off. [0060]; [0087].

52. As discussed above in ¶25, the BRI of "handheld telecommunications unit" in view of the specification of the '983 patent includes a laptop computer. Lee does not specify whether the remote computer 291 is a laptop computer. A POSA would have recognized that implementing remote computer 291 as a laptop computer was a viable and obvious choice. For example, laptop computers having Internet connectivity and display capabilities were well known before the relevant time period (*see e.g.*, Ex. 1008). Therefore,

the use of a laptop computer to implement the remote computer 291 would have been an obvious design choice to a POSA. Remote computer 291 is connected to the main control unit 100 over network 290 (e.g., the Internet) or PSTN network 292, both of which are telecommunications networks so that the remote computer 291 is coupled to the processor of the main control unit 100 via a telecommunication module ([0062]; FIG. 1). Remote computer 291 includes application software that enables the remote computer to both receive video data (which includes images) from the system and send control data to the system. [0062]. Because the main control unit 100 includes a microprocessor 150 and a telecommunications module ([0062]), a POSA would have understood that an obvious way to enable the remote computer 291 to send control data to the system and receive video data from the system would be by controlling the microprocessor 150 with the control data to send the requested video data to the telecommunications module for transmission to the remote computer 291. Accordingly, the remote computer 291 is a handheld communications unit that transmits commands to the main control unit 100 to provide images to the telecommunications module (e.g., Internet and/or PSTN interface) of the main control unit 100 to be transmitted to the remote computer 291.

53. A POSA would have also understood Lee's wireless PDA 282 and cell phone 283 to be handheld telecommunications devices. The wireless PDA

282 and cell phone 283 communicate with the main control unit 100 through interfaces that are not shown in FIG. 1. [0060]. Numerous types of interfaces for connecting cell phones to a security system were known, including connecting through a telecommunications network such as the PSTN. (*see e.g.*, Ex. 1006 (Dy) at [0014] ("a typical security system is shown for a residential location … each video camera produces a stream of continuous video that is wired back to a collection point 4 in the residence. The collection point 4 can be coupled to a telephone or other communications interface 5 that allows access to the public switched telephone network (PSTN) or any other type of wired or wireless network. A remote user 6 can command up display of video from any of the cameras 3 on a handheld telecommunications device 7, such as a cellular telephone by calling a particular telephone number, accessing a particular web-site or by any other access method."); Ex. 1006 (Dy) at [0019] ("In FIG. 2, a user sends commands from his cellular telephone 7 to the telephone interface 5 stating which camera or cameras he wishes to view. The telephone interface 5 sends a command to the collection point 4 via a processor that causes the correct video feed or feeds to be compressed and transmitted to the remote unit."); Ex. 1007 (Jentoft) at 3:18-30 ("a security system utilizes cameras to detect and identify intruders. The system includes an integrated camera/motion detector that is responsive to intrusion conditions … The intrusion sensors are activated

(armed) by a system user, using e.g., … a phone call with DTMF.")). Thus, a POSA would have considered connecting the cell phone 283 to the main control unit 100 of Lee via a telecommunications network (e.g., the PSTN) module to be an obvious way to implement the interface that Lee states is not shown explicitly. [0060]. Similarly, known interfaces for connecting a PDA to a security system included connection through a telecommunications system such as the Internet. (*see e.g.*, Ex. 1003 (Milinusic) at 2:63-65 ("A surveillance client 240 is provided and connected to the network 230"), Ex. 1003 (Milinusic) at 3:18-19 ("Network 230 may be a wide area network (WAN), such as, for example, the Internet"), Ex. 1003 (Milinusic) at 3:31-35 ("Surveillance client 240 may be implemented … as a personal digital assistant (PDA), such as a Palm Pilot.")). Thus, a POSA would have considered connecting the PDA 282 to the main control unit 100 via a telecommunications network (e.g., the Internet) module to be an obvious way to implement the interface that Lee states is not shown explicitly. [0060].

54. While Lee explicitly states that images ("video data") are transmitted to one type of user device that is used to access the system (i.e., computer 291), it does not explicitly state that images are transmitted to the other user devices, including the cell phone 283 and PDA 282. It would have been obvious to a POSA to transmit images to other types of user input devices

that include the ability to display images, including PDA 282 and cell phone 283. [0059]; FIG 1. It was known in the relevant timeframe to provide images to cell phones and PDAs. (*see e.g.*, Ex. 1006 (Dy) at abstract "A system and method for viewing video images from security systems on a remote handheld communications device like a cellular telephone."). Providing the user with the ability to not only control but also view images from any of the user devices capable of displaying images would have been an obvious design choice that would have provided the users of the Lee system with maximum flexibility in using the system.

ii. Claim 2: "The alarm system of claim 1, wherein said processor is coupled to said at least one motion detector and said telecommunications unit is also arranged to transmit commands for said processor to activate and deactivate said at least one motion detector."

55. Lee's system includes S&S device 212, which is controllable via user input devices such as remote controller 281, wireless PDA 282, cell phone 283, and remote computer 291. [0062]; [0064]; [0065]. A POSA would have appreciated that a user away from home would desire the ability to activate/deactivate S&S device 212 remotely using one of the user input devices to provide access to the home to housekeeping/maintenance personnel, children when they return home from school, etc., and that providing the user the ability to turn the device (including its motion detectors and cameras) on and off is the

most basic form of control for S&S device 212. Additionally, Lee describes sending command signals to change the setting mode of the S&S device 212 between ON, OFF, and INTERRUPT modes ([0107]). A command to set the S&S device 212 into ON or OFF mode is a command to deactivate the motion detector because the motion detector is not used to impact the turning on of the camera and is therefore not active in either the ON or OFF mode. Conversely, a command to set the S&S device 212 into INTERRUPT mode is a command to activate the motion detector because the motion detector is used to impact the turning on of the camera in INTERRUPT mode. In addition, it would have been obvious to a POSA to implement Lee's system to respond to commands to set the S&S device 212 to ON or OFF mode by turning off the motion detector entirely, because the motion detector is not being used when the S&S device 212 is in either of those modes and power consumed by the system can be reduced by not unnecessarily powering a motion detector that is not in use. In addition, among the functions of Lee's system that are controllable, a user can send command signals to turn on or off the entire system (not just the S&S device 212), which includes motion detectors. [0087]; [0110]. A POSA would have understood that turning on or off the system suggests that all components of the system, including any motion detectors included as part of S&S device 212, would be turned on or off, for example, to save power when the user turned the

system off. While the explanation of issuing commands is provided in connection with the remote controller 281, a POSA would have understood that such commands can be issued from any of the devices that Lee describes as having the ability to control the system, including the wireless PDA 282, cell phone 283, and remote computer 291. [0062]; [0064].

iii. Claim 3: "The alarm system of claim 1, wherein in said dormant state of each of said at least one camera, imaging by said camera is not performed and images are not obtained, each of said at least one camera being automatically activated from the dormant state into the active state when the associated one of said at least one motion detector detects motion in its field of view."

56. As discussed above in ¶44, Lee does not explicitly state that when the system is in "INTERRUPT mode" the triggered "on" state of the camera is a state in which images are obtained and that the camera is otherwise in an "off" state in which images are not obtained. However, a POSA would have understood that when the camera of Lee is "on" it is obtaining images, and when the camera of Lee is "off" it is not obtaining images. Additionally, a POSA would have understood that when the camera is "off" it is not performing imaging. In addition to the common understanding to a POSA of what it would have meant for a camera to be on or off, this understanding is buttressed by Lee's explanation that when the device 212 is placed in "ON mode" the camera is in a non-stop working state, when the device 212 is placed in "OFF mode" the

camera is not working ([0107]), and that when the security system "has been triggered" the S&S device 212 transmits video data to the main control unit 100. [0111].

57. Lee's system includes various types of sensors that may trigger the camera when the S&S device 212 is in "INTERRUPT mode," including motion sensors [0110]. When the sensor 923 is a motion sensor and the S&S device 212 is placed in "INTERRUPT mode," the camera 922 has a dormant state in which imaging by the camera is not performed and images are not obtained (e.g., when a trigger signal has not been received from the sensor), and an active state in which images are obtained (e.g., when the trigger signal has been received from the sensor). The camera in "INTERRUPT mode" is automatically activated from the dormant state into the active state when the motion sensor detects motion in its field of view and sends a trigger signal to the camera. [0111].

iv. Claim 4: "The alarm system of claim 1, wherein said telecommunications unit is one of a camera telephone, a cellular telephone and an Internet-enabled picture and/or video display device."

58. Lee's cell phone 283 is a telecommunications unit (see ¶¶51-53) and meets the requirement in claim 4 of a cellular telephone. [0059]. Remote computer 291 is also a telecommunications unit (see ¶¶51-53), communicates with the main control unit 100 via an "external Internet network" and has the ability to display pictures and video. [0062]. Accordingly, remote computer

291 is an Internet-enabled picture and/or video display device that also meets the requirement of claim 4. Finally, as discussed above in connection with limitation [E] of claim 1, it would have been obvious to a POSA to enable the PDA 282 to connect to the main control unit 100 via the Internet, so that the PDA 282 is also an Internet-enabled picture and/or video display device that meets the requirement of claim 4.

v. Claim 5: "The alarm system of claim 1, wherein said processor is arranged to receive, via said telecommunications module, one of a plurality of different code numbers from said telecommunications unit and control said at least one camera and said at least one motion detector in accordance with the received code number."

59. Lee describes sending control signals to the main control unit 100 from, among other devices, a cell phone 283, PDA 282, and remote computer 291. [0060]; [0062]. For example, Lee describes commands to control the S&S device 212. [0064]-[0065]. Lee also describes using a user device locally or via the Internet to change the setting mode of the S&S device 212 between ON, OFF, and INTERRUPT modes. [0107]. S&S device 212 includes a camera and a motion detector as discussed in connection with elements [A] and [B1] of claim 1. Changing the setting mode of the S&S device 212 controls both the camera (e.g., by turning it on or off) and the motion detector (e.g., by having it trigger activation of the camera in the INTERRUPT mode but not in the other modes). Lee also describes sending a command to turn on or off Lee's system,

which includes S&S device 212. [0087]. Turning on or off the system controls both the camera (e.g., by turning it on or off) and the motion detector (e.g., by turning it on or off). It would have been obvious to a POSA to power down all components of the system when turning the system of Lee off to reduce power consumption by components that are not being used. A POSA would have understood that a command to control S&S device 212, to set the mode of S&S device 212, and to turn on or off Lee's system are all commands that control the camera(s) and the motion detector(s) in the system. Lee does not explicitly describe that each of the commands sent to control the S&S device 212 are received by the processor in main control unit 100 as code numbers. Lee describes sending control signals to the main control unit 100 by pressing keys or buttons on a cell phone or wireless PDA. [0060]. A POSA would have understood that commands sent from any of Lee's devices including the cell phone 283, the PDA 282 or the remote computer 291 would include numbers, text, or some combination of numbers and text, and implementing the commands using code numbers for different commands would have been an obvious design choice. Accordingly, a POSA would have understood that it would have been obvious to implement a command sent from a user input device to change the mode of the S&S device 212 and a command sent from a user input device to turn on/off the system each using different code numbers to

control the camera(s) and the motion sensor(s) in the S&S device 212, that are received by the processor via a telecommunication module.

vi. Claim 6: "The alarm system of claim 5, wherein one of the code numbers is to cause said processor to cause images to be provided by said processor to said telecommunications module and transmitted to the telecommunications unit."

60. As discussed in ¶¶51-52, Lee's system includes a remote computer 291, which is a handheld communications unit that transmits commands to the main control unit 100 to provide images to the telecommunications module (e.g., Internet and/or PSTN interface) of the main control unit 100 to be transmitted to the remote computer 291. Additionally, a POSA would have considered connecting cell phone 283 or PDA 282 in Lee's system to the main control unit 100 via a telecommunications network (e.g., the Internet) module to be an obvious way to implement the interfaces that Lee states are not shown explicitly. [0060].

61. While Lee explicitly states that images ("video data") are transmitted to one type of user device that is used to access the system (i.e., computer 291), it does not explicitly state that images are transmitted to the other user devices, including the cell phone 283 and PDA 282. It would have been obvious to a POSA to transmit images to other types of user input devices that include the ability to display images, including PDA 282 and cell phone 283. [0059]; FIG 1. It was known in the relevant timeframe to provide images

to cell phones and PDAs (*see e.g.*, Ex. 1006 (Dy) at abstract "A system and method for viewing video images from security systems on a remote handheld communications device like a cellular telephone."). Providing the user with the ability to not only control but also view images from any of the user devices capable of displaying images would have been an obvious design choice that would have provided the users of the Lee system with maximum flexibility in using the system. A POSA would have further understood that such commands are implemented as code numbers. (see ¶59).

vii. Claim 7: "The alarm system of claim 5, wherein one of the code numbers is to cause said processor to direct said at least one camera to provide images to said processor and then cause the provided images to be forwarded by said processor to said telecommunications module and transmitted to the telecommunications unit."

62. As discussed in ¶¶51-52, Lee's system includes a remote computer 291, which is a handheld communications unit that transmits commands to the main control unit 100 to provide images to the telecommunications module (e.g., Internet and/or PSTN interface) of the main control unit 100 to be transmitted to the remote computer 291. Additionally, a POSA would have considered connecting cell phone 283 or PDA 282 in Lee's system to the main control unit 100 via a telecommunications network (e.g., the PSTN or the Internet) module to be an obvious way to implement the interfaces that Lee states are not shown explicitly. [0060].

63. While Lee explicitly states that images ("video data") are transmitted to one type of user device that is used to access the system (i.e., computer 291), it does not explicitly state that images are transmitted to the other user devices, including the cell phone 283 and PDA 282. It would have been obvious to a POSA to transmit images to other types of user input devices that include the ability to display images, including PDA 282 and cell phone 283. [0059]; FIG 1. It was known in the relevant timeframe to provide images to cell phones and PDAs (*see e.g.*, Ex. 1006 (Dy) at abstract "A system and method for viewing video images from security systems on a remote handheld communications device like a cellular telephone."). Providing the user with the ability to not only control but also view images from any of the user devices capable of displaying images would have been an obvious design choice that would have provided the users of the Lee system with maximum flexibility in using the system. A POSA would have further understood that the commands in Lee are implemented as code numbers. (see ¶59).

64. Additionally, in Lee, the commands (including code numbers) are transmitted from the user input devices to the main control unit processor. Lee describes using a user device locally or via the Internet to change the setting mode of the S&S device 212 between ON, OFF, and INTERRUPT modes. ([0087]; [0107]; [0160]). When the user device sends a command to set the

S&S device 212 to the "ON mode" the camera 922 is put into a "non-stop working state." [0107]. It would have been obvious to a POSA to provide at least one of the obtained images captured when the S&S device 212 is set to "ON mode" to the user device which issued the command to turn on the camera so as to enable the user who issued the "ON" command for a particular S&S device to see the images being collected from the S&S device after the device is on and recording images. One reason a POSA would have designed the system in this manner is to provide a visual confirmation to the requesting user that the S&S device for which the "ON" command was issued was indeed turned on. Providing the user with a live captured image from the S&S device 212 when the device was turned on would have been an obvious way to achieve that goal. Lee also describes that a user can watch live images on the LCD display to monitor the home or building by surveillance camera 922, or can monitor the system remotely over the Internet. [0111]-[0112]. While Lee explicitly states that images are transmitted live to one type of user device (i.e., LCD display 50), it does not explicitly state that images are transmitted live to the other user devices, including the cell phone 283, PDA 282, and remote computer 291. It would have been obvious to a POSA to transmit live images to other types of user input devices that include the ability to display images, including PDA 282, cell phone 283, and remote computer 291. [0059]; FIG 1. It was known in the

relevant timeframe to provide images to cell phones and PDAs, as discussed in ¶54. A POSA would have understood that Lee implicitly describes providing commands to allow the user to watch live images and monitor the system remotely over the Internet, and that such commands (code numbers) cause the processor to direct the camera(s) to provide live images to the processor and cause the processor to forward those images, via a telecommunications module, to any of the telecommunications units described by Lee (see ¶54). As described in Lee, the remote computer 291 includes software capable of sending control data to the system and receiving audio, video, and sensor data from the system. [0062].

viii. Claim 8: "The system of claim 1, wherein said at least one motion detector comprises a plurality of motion detectors, said at least one camera associated with said at least one motion detector being arranged to have a field of view overlapping a field of view of a plurality of said motion detectors."

65. S&S device 212 includes an unlimited number of modules - including camera module 920 and sensor modules 930 and 940 - that may be "installed in the necessary sites inside and outside the house." [0103]-[0105]. Some sensors (e.g., sensor 923) are associated with a camera in a common module (i.e., camera module 920), whereas other sensors (e.g., sensor 931) are not associated with a camera in a common module (i.e., sensor module 930). FIG. 9. Lee describes that surveillance cameras, such as 922, can be activated

when any of the sensors, such as sensor 923 is triggered. [0111]. A POSA would have understood that a camera with a wide field of view will have a wider field of view than most, if not all, motion detectors. A POSA would have further understood that, it would have been advantageous to include multiple motion detectors, each with a narrower field of view than the cameras, to detect motion at different areas in the camera's wider field of view, which would result in the field of view of the camera overlapping the fields of view of the plurality of motion detectors. A POSA would have understood that this would provide a benefit versus employing a 1:1 relationship between cameras and motion detectors as in some installations with a lot of area to monitor the system can use fewer cameras than would be required if a 1:1 relationship between cameras and motion detectors were used, thereby reducing the cost of the overall system. Accordingly, it would have been obvious to a POSA to implement Lee by including one or more cameras each having an overlapping field of view with multiple motion detectors.

ix. Claim 11: "A method for protecting a structure, comprising:"

66. Lee describes a method of protecting a structure by using a system that includes the S&S device 212 that includes one or more camera modules 920 and one or more sensor modules 930. [0103]-[0104]. The camera modules 920

and sensor modules 930 are installed inside and outside of a house, which is a structure (see ¶23).

a. "[*A*] arranging a plurality of motion detectors on or around the structure, each in a position in which its field of view includes an area proximate the structure;"

67. Each of the camera modules 920 and sensor modules 930 in S&S device 212 includes a sensor. [0104]. The sensors include motion sensors. [0110]. The camera module(s) 920 and the sensor module(s) may be installed outside a house as well as inside. [0105]. Lee describes that the purpose of the S&S device 212 is to monitor the house and detect intruders ("there is provided a security and surveillance device, including a plurality of sensors and cameras installed in correspondence to a place to be monitored for detecting information about [an] intruder." [0028]; "the sensor can send [a] trigger signal to the camera 922 when the presence of an intruder has been detected by the sensor and the sensor is triggered." [0108]). Lee is not explicit about where the camera modules 920 and sensor modules 930 of the S&S device 212 are placed and what field of view the motion detectors and cameras incorporated into the modules would have, but teaches that the modules should be "installed in the necessary sites inside and outside the house." [0105]. To achieve Lee's stated purpose of detecting the presence of an intruder and detecting information about an intruder ([0028]; [0108]), a POSA would have understood that "the necessary

sites" to monitor include the areas proximate the access points to the house (e.g., doors and windows). Thus, it would have been obvious to a POSA to implement a home installation of the Lee system by arranging motion sensors to have a field of view that includes an area proximate a structure (i.e., the house) to detect motion of any intruders seeking to enter the house, and to do so by arranging the motion detectors on or around the structure.

b. "[*B1*] arranging a plurality of cameras on or around the structure,"

68. The S&S device 212 in Lee's system includes a plurality of camera modules 920 that each includes a surveillance camera 922. [0108]; FIG. 9. Lee describes that the purpose of the S&S device 212 is to monitor the house and detect intruders ("there is provided a security and surveillance device, including a plurality of sensors and cameras installed in correspondence to a place to be monitored for detecting information about [an] intruder." [0028]; "the sensor can send [a] trigger signal to the camera 922 when the presence of an intruder has been detected by the sensor and the sensor is triggered." [0108]). Lee is not explicit about where the camera modules 920 and sensor modules 930 of the S&S device 212 are placed, but teaches that the modules should be "installed in the necessary sites inside and outside the house." [0105]. To achieve Lee's stated purpose of detecting the presence of an intruder and detecting information about an intruder ([0028]; [0108]), a POSA would have understood that "the

necessary sites" to monitor include the areas proximate the access points to the house (e.g., doors and windows). Thus, it would have been obvious to a POSA to implement a home installation of the Lee system by arranging the plurality of camera modules on or around a structure (i.e., the house) to capture images of any intruders seeking to enter the house.

c. "[*B2*] each camera being associated with one or more of the motion detectors such that the camera has a field of view encompassing at least part of the field of view of any associated motion detector,"

69. S&S device 212 includes motion sensors and cameras that can be activated when an associated motion sensor is triggered [0108]; [0110]-[0111]. For example, Lee states, "the sensor can send [a] trigger signal to the camera 922 when the presence of an intruder has been detected by the sensor and the sensor is triggered." [0108]. Accordingly, a POSA would have understood that Lee discloses each camera being associated with one or more motion detectors.

70. Lee does not explicitly state that the field of view of a camera 922 within a camera module 920 encompasses at least part of the field of view of any associated motion detector (e.g., motion detector 923) that is within the same camera module 920 and associated with the camera 922. However, a POSA would have understood this to have been implicitly disclosed by Lee's description of a sensor (motion detector) 923 being disposed in the same module as the associated camera 922. ([0104]; FIG. 9), and by Lee's disclosure that

cameras and motion detectors are "installed in correspondence to a place to be monitored for detecting information about [an] intruder." [0028]. A POSA would have understood that the camera and sensor in the same module "installed in correspondence to a **place to be monitored**" (emphasis added) would be arranged to monitor the same "place" by having fields of view that both encompass that "place."

71. Alternatively, even if a POSA would not have considered Lee to implicitly disclose that the camera 922 had a field of view that encompasses at least part of the field of view of its associated sensor 923 within a camera module 920, this would have been the obvious way a POSA would have implemented Lee's system. Lee indicates that cameras and motion detectors are "installed in correspondence to a place to be monitored for detecting information about [an] intruder" ([0028]) and that "[g]enerally, the camera module 920, sensor module 930, and wireless module 940 are installed at necessary sites inside and outside the house." [0105]. To achieve Lee's stated purpose of detecting the presence of an intruder in a place and detecting information about an intruder in that place ([0028]; [0108]), and to implement the "INTERRUPT mode" where the camera is activated by a trigger signal from the motion detector ([0107]-[0111]), a POSA would have understood that the area monitored by the camera should include at least part of the area monitored by the one or more

associated sensors. Otherwise, the camera would not be able to capture images of the intruder detected by the motion detector(s). In addition, there would be no reason to activate the camera based upon an event (e.g., detected motion) if the camera cannot capture any information about the triggering event. Thus, it would have been obvious to a POSA to implement a home installation of the Lee system by arranging the camera 922 within a camera module 920 to have a field of view that encompasses at least part of the field of view of at least one motion detector 923 within the same camera module.

72. To further support my opinion that it would have been obvious to a POSA to implement Lee's system so that the camera 922 within a camera module had a field of view that encompasses at least part of the field of view of the sensor 923 within the same module 920, I note that it was known prior to the relevant time period to have security systems that employ a camera activated by a motion detector, such that the field of view of such a camera encompasses at least part of the field of view of an associated motion detector. (*see e.g.*, Ex. 1003, (Milinusic) at 5:51-59 ("Image capture [of an area] may be set to occur at predetermined times or upon the occurrence of predetermined occurrences, such as the detection of movement within the area being monitored by the sensor units 250 or 260."; Ex. 1007 (Jentoft) at 4:6-8 ("The motion sensor 20 and the

camera 25 are positioned such that both devices have overlapping field of detection.").

d. "[*C*] providing a processor which controls the at least one camera and receives the image obtained by the at least one camera;"

73. Lee's system includes a main control unit 100 that includes a microprocessor 150. [0069]. A POSA would have understood that a microprocessor is a processor as recited in the claims of the '983 patent.

74. The processor 150 is arranged to send control data via the power line communication network 200 to various aspects of S&S device 212 including camera 922 [0057]-[0058]; ("The power line communication interface module 101 is coupled to the bus and configured to transfer audio, video, sensor, and control data between the power line communication interface module and at least one of the plurality of remote devices, such as surveillance and security device over the power line communications link." [0083]); ("The interface module receives control signals from the remote controller or the cell phone or a wireless PDA and then the microprocessor outputs a control signal to perform a desired function in response to the user signals." [0081]). The processor 150 can control the camera 922 in the camera module 920 to, for example, allow the user to select the "ON mode," "OFF mode," or "INTERRUPT mode" ([0107]) via the main control unit 100 and its processor 150. ([0071]; [0057]-[0058] ("a

main control unit 100 that is capable of enabling a user to set, program, and control the system … and sending … the control data to at least one remote device" such as S&S device 212)).

75. Main control unit 100, including microprocessor 150, is also arranged to receive surveillance data (e.g., images) from the camera in S&S device 212. ("The camera can communicate with camera interface 921 and then the interface sends the image data and sensor data to the main control unit 100 via power line communication network." [0108]). Accordingly, a POSA would have understood that the main control unit 100 of Lee includes a processor (i.e., microprocessor 150) arranged to control a camera (i.e., camera 922) and receive an image obtained by the camera.

e. "[*D*] coupling a telecommunications module coupled to the processor, the telecommunications module being capable of communications over a telecommunications network; and"

76. Lee's system includes a main control unit 100 having a microprocessor 150 and multiple types of communication interfaces to communicate with user input devices. (FIG. 1). The communications interfaces include an RF/wireless interface 190 ([0067]), a telephone line interface (e.g., Public Switched Telephone Network (PSTN) 292) ([0062]), and a computer network (e.g., local area network (LAN)/Internet 290) interface. FIG. 1; [0062]. Lee also discloses that there is an interface (not shown in FIG. 1) for connecting

to the cell phone 283 and an interface (not shown in FIG. 1) for connecting to the PDA 282. [0060].

77. As discussed in ¶24, the BRI of the term "telecommunications network" encompasses the computer network (LAN/Internet) 290 described in Lee with which the main control unit 100 provides an interface. Lee also describes using a telephone network (e.g., the PSTN) to connect the main control unit 100 to input/output devices, including the computer 291. [0062]. Accordingly, a POSA would have understood that the main control unit 100 in the system of Lee couples a telecommunications module to the processor of the main control unit 100 and that the telecommunications module is capable of communications over a telecommunications network.

f. "[*E*] transmitting commands from a handheld telecommunications unit to the processor via the telecommunications module to cause the processor to provide images to the telecommunications module to be transmitted to the telecommunications unit."

78. Lee's system includes multiple types of user input devices for sending control commands to main control unit 100, including wireless PDA 282, cell phone 283, and remote computer 291. [0059]; [0062]; FIG. 1. A user may program the system via on-screen program menus displayed on any of the user input devices. [0064]. Lee describes examples of commands that can be transmitted from the user input devices to the main control unit 100, including a

command to set the main control unit 100 to a different mode, a command to switch the camera in S&S device 212 on or off, a command to place the camera in S&S device 212 in standby mode, and a command to turn the system on or off. [0060]; [0087].

79. As discussed in ¶25, the BRI of "handheld telecommunications unit" in view of the specification of the '983 patent includes a laptop computer. Lee does not specify whether the remote computer 291 is a laptop computer. A POSA would have recognized that implementing remote computer 291 as a laptop computer would have been a viable and obvious choice. For example, laptop computers having Internet connectivity and display capabilities were well known before the relevant time period (*see e.g.*, Ex. 1008). Therefore, the use of a laptop computer to implement the remote computer 291 would have been an obvious design choice to a POSA. Remote computer 291 is connected to the main control unit 100 over network 290 (e.g., the Internet) or PSTN network 292, both of which are telecommunications networks so that the remote computer is coupled to the processor of the main control unit 100 via a telecommunication module. [0062]; FIG. 1. Remote computer 291 includes application software that enables the remote computer to both receive video data (which includes images) from the system and send control data to the system. [0062]. Accordingly, the remote computer 291 is a handheld communications

unit that transmits commands to the main control unit 100 to provide images to the telecommunications module (e.g., Internet and/or PSTN interface) of the main control unit 100 to be transmitted to the remote computer 291.

80. The PDA 282 and cell phone 283 communicate with the main control unit 100 through interfaces that are not shown in FIG. 1. [0060]. Numerous types of interfaces for connecting cell phones to a security system were known, including connecting through a telecommunications network such as the PSTN. (*see e.g.,* Ex. 1006 (Dy) at [0014] ("a typical security system is shown for a residential location … each video camera produces a stream of continuous video that is wired back to a collection point 4 in the residence. The collection point 4 can be coupled to a telephone or other communications interface 5 that allows access to the public switched telephone network (PSTN) or any other type of wired or wireless network. A remote user 6 can command up display of video from any of the cameras 3 on a handheld communications device 7, such as a cellular telephone by calling a particular telephone number, accessing a particular web-site or by any other access method."); Ex. 1006 (Dy) at [0019] ("In FIG. 2, a user sends commands from his cellular telephone 7 to the telephone interface 5 stating which camera or cameras he wishes to view. The telephone interface 5 sends a command to the collection point 4 via a processor that causes the correct video feed or feeds to be compressed and

transmitted to the remote unit."); Ex. 1007 (Jentoft) at 3:18-30 ("a security system utilizes cameras to detect and identify intruders. The system includes an integrated camera/motion detector that is responsive to intrusion conditions … The intrusion sensors are activated (armed) by a system user, using e.g., … a phone call with DTMF.")). Thus, a POSA would have considered connecting the cell phone 283 to the main control unit 100 of Lee via a telecommunications network (e.g., the PSTN) module to be an obvious way to implement the interface that Lee states is not shown explicitly. [0060]. Similarly, known interfaces for connecting a PDA to a security system included connection through a telecommunications system such as the Internet. (*see e.g.*, Ex. 1003 (Milinusic) at 2:63-65 ("A surveillance client 240 is provided and connected to the network 230"), Ex. 1003 (Milinusic) at 3:18-19 ("Network 230 may be a wide area network (WAN), such as, for example, the Internet"), Ex. 1003 (Milinusic) at 3:31-35 ("Surveillance client 240 may be implemented … as a personal digital assistant (PDA), such as a Palm Pilot.")). Thus, a POSA would have considered connecting the PDA 282 to the main control unit via a telecommunications network (e.g., the Internet) module to be an obvious way to implement the interface that Lee states is not shown explicitly. [0060].

81. While Lee explicitly states that images ("video data") are transmitted to one type of user device that is used to access the system (i.e.,

remote computer 291), it does not explicitly state that images are transmitted to the other user devices, including the cell phone 283 and PDA 282. It would have been obvious to a POSA to transmit images to other types of user input devices that include the ability to display images, including PDA 282 and cell phone 283. [0059]; FIG 1. It was known in the relevant timeframe to provide images to cell phones and PDAs (*see e.g.*, Ex. 1006 (Dy) at abstract "A system and method for viewing video images from security systems on a remote handheld communications device like a cellular telephone."). Providing the user with the ability to not only control but also view images from any of the user devices capable of displaying images would have been an obvious design choice that would have provided the users of the Lee system with maximum flexibility in using the system.

x. Claim 18: "The method of claim 11, further comprising programming the telecommunications module to receive commands from a handheld telecommunications unit over the telecommunications network to enable activation and deactivation of the motion detectors and cameras using the telecommunications unit."

82. Lee's system includes S&S device 212, which is controllable via user input devices such as remote controller 281, wireless PDA 282, cell phone 283, and remote computer 291. [0062]; [0064]. Among the functions of the system that are controllable, a user can send command signals to turn on or off the S&S device 212, which includes cameras and motion detectors. [0087];

[0110]. A POSA would have understood that a command to turn on or off S&S device 212 would turn on or off (i.e., activate/deactivate) all components of the S&S device 212 including any cameras and motion detectors included as part of S&S device 212. While the explanation of issuing commands is provided in connection with the remote controller 281, a POSA would have understood that such commands can be issued from any of the devices that Lee describes as having the ability to control the system, including the PDA 282, cell phone 283 and remote computer 291. [0062]; [0064]. A POSA would also have understood that because S&S device 212 is capable of received such commands from user input devices, that the telecommunications module in S&S device 212 was programmed to receive such commands.

xi. Claim 19: "The method of claim 11, wherein the processor is arranged to receive, via the telecommunications module, one of a plurality of different code numbers from the telecommunications unit and control the at least one camera and the at least one motion detector in accordance with the received code number."

83. Lee describes sending control signals to the main control unit 100 from, among other devices, a cell phone 283, wireless PDA 282, and remote computer 291. [0060]; [0062]. For example, Lee describes using a user device locally or via the Internet to change the setting mode of the S&S device 212 between ON, OFF, and INTERRUPT modes. [0107]. S&S device 212 includes a camera and a motion detector as discussed in connection with elements [A]

and [B1] of claim 11. Changing the setting mode of the S&S device 212 controls both the camera (e.g., by turning it on or off) and the motion detector (e.g., by having it trigger activation of the camera in the INTERRUPT mode but not in the other modes). Lee also describes sending a command to turn on or off Lee's system, which includes S&S device 212. [0087]. Turning on or off the system controls both the camera (e.g., by turning it on or off) and the motion detector (e.g., by turning it on or off). It would have been obvious to a POSA to power down all components of the system when turning the system of Lee off to reduce power consumption by components that are not being used. A POSA would have understood that it would have been obvious to implement the processor in the main control unit 100 to receive commands from the user input devices as code numbers. Lee describes sending control signals to the main control unit 100 by pressing keys or buttons on a cell phone or wireless PDA. [0060]. A POSA would have understood that commands sent from any of Lee's devices including the cell phone 283, the PDA 282 or the remote computer 291 would include numbers, text, or some combination of numbers and text, and implementing the commands using code numbers for different commands would have been an obvious design choice. Accordingly, a POSA would have understood that a command sent from a user input device to change the mode of the S&S device 212 and a command sent from a user input device to turn on/off

the system each includes one of a plurality of code numbers to control the camera(s) and the motion sensor(s) in the S&S device 212, and is received via a telecommunication module.

xii. Claim 20: "The method claim 19, wherein one of the code numbers is to cause the processor to cause images to be provided by the processor to the telecommunications module and transmitted to the telecommunications unit."

84. As discussed in ¶¶78-79, Lee's system includes a remote computer 291, which is a handheld communications unit that transmits commands to the main control unit 100 to provide images to the telecommunications module (e.g., Internet and/or PSTN interface) of the main control unit 100 to be transmitted to the remote computer 291. Additionally, a POSA would have considered connecting cell phone 283 or PDA 282 in Lee's system to the main control unit 100 via a telecommunications network (e.g., the Internet) module to be an obvious way to implement the interfaces that Lee states are not shown explicitly. [0060].

85. While Lee explicitly states that images ("video data") are transmitted to one type of user device that is used to access the system (i.e., computer 291), it does not explicitly state that images are transmitted to the other user devices, including the cell phone 283 and PDA 282. It would have been obvious to a POSA to transmit images to other types of user input devices that include the ability to display images, including PDA 282 and cell phone

283. [0059]; FIG 1. It was known in the relevant timeframe to provide images to cell phones and PDAs (*see e.g.*, Ex. 1006 (Dy) at abstract "A system and method for viewing video images from security systems on a remote handheld communications device like a cellular telephone."). Providing the user with the ability to not only control but also view images from any of the user devices capable of displaying images would have been an obvious design choice that would have provided the users of the Lee system with maximum flexibility in using the system.

86. As discussed in ¶78, Lee describes sending control signals to the main control unit 100 from, among other devices, a cell phone 283, wireless PDA 282, and remote computer 291. [0060]; [0062]. A POSA would have understood that it would have been obvious choice to implement the processor in the main control unit 100 to receive code numbers as commands from the user input that the main control unit processor can interpret to understand what command the user has selected. A POSA would have understood that commands sent from any of Lee's devices including the cell phone 283, the PDA 282 or the remote computer 291 would include numbers, text, or some combination of numbers and text, and implementing the commands using code numbers for different commands would have been an obvious design choice. Accordingly, a POSA would have understood that a command sent from a user

input device to request images be provided to the user input device includes one of a plurality of code numbers to cause microprocessor 150 of the main control unit 100 to cause images to be provided by the microprocessor to the telecommunications module and transmitted to the user input device.

B. Ground 2: Claims 9, 10, and 12-17 of the '983 Patent Each Would Have Been Obvious In View of Lee and Ozer

87. According to the face of the document, Ozer (Ex. 1005) is a U.S. patent that issued on April 3, 2007, from an application that was filed on August 27, 2003. I have been informed by counsel that it meets the requirements to be prior art to the '983 patent.

88. Ozer describes a system for detecting, recognizing, and analyzing people or other objects in security checkpoints, public-places, parking lots, or in similar environments under surveillance to detect the presence of certain objects of interest (e.g., people), and to identify their activities for security and other purposes in real-time. (Ex. 1005 (Ozer) at abstract). The system can be set up to identify several objects of interest including, humans and dogs, and to recognize a wide variety of activities. (Ex. 1005 (Ozer) at [0053]). The system builds a model of an object of interest for each video frame, and only tracks objects that fit the model of the user defined subject, such as a human or a dog. (Ex. 1005 (Ozer) at [0054]).

89. The object model for an object of interest is generated by segmenting the object in the image hierarchically into smaller parts and combining meaningful adjacent segments (Ex. 1005 (Ozer) at FIG. 5; 501), extracting contour points of the segmented regions of the object (Ex. 1005 (Ozer) at FIG. 5, 502), and fitting ellipses to the determined contours. (Ex. 1005 (Ozer) at [0062]). The object model is compared to a set of stored models to classify the object (Ex. 1005 (Ozer) at [0052]-[0053]; [0064]). Ozer refers to the model of the object for a frame of video as a silhouette, and can detect objects (such as a human body) by matching the object model with reference models. (Ex. 1005 (Ozer) at [0026]-[0027]; [0029]; [0034]; and [0064]).

90. After reviewing Lee and Ozer, and claims 9, 10, and 12-17 of the '983 patent, it is my opinion that every one of these claims would have been obvious to a POSA in view of Lee and Ozer. The basis for my opinion and the details of my analysis are below.

i. Claim 9: "The system of claim 1, wherein said processor is further arranged to derive a silhouette of any objects in the image, compare the silhouettes to a library of stored silhouettes having associated object identification to determine an exact or closest match of the derived silhouette to one of the stored silhouettes and retrieve the object identification associated with the exact or closest match, said processor being arranged to react to the detection of motion by said at least one motion detector based on the object identification."

91. Lee's surveillance camera 922 is activated when any of the sensors 923 (which can be a motion detector), is triggered. [0111][3]. When the system is triggered, S&S device 212 transmits video data to the main control unit 100 via power line communication network 200. [0111]. The user is alerted and a live image is shown on the user's LCD display device. [0111]. The main control unit 100 can also automatically call the user's mobile telephone, if the system is on and the user is not at home. [0111].

92. Lee's S&S device 212 includes one or more camera modules 920 and one or more sensor modules 930. [0103]-[0104]. When the S&S device 212 has been triggered, the user is alerted and a text message corresponding to the nature of the unusual event information sensed by the sensors in the system is sent to a display device 50 to inform the user which sensor was triggered. [0111]. Lee describes several modes in which the S&S device 212 may be set to operate including an "ON mode," an "OFF mode," and an "INTERRUPT

[3] Unless otherwise indicated, all citations in §B(¶¶87-109) are to Ex. 1002 (Lee).

mode." [0107]. When the S&S device 212 is in "INTERRUPT mode," the camera is off unless and until a trigger signal is received indicating that the presence of an intruder has been detected by a sensor [0107]-[0108].

93. Lee does not teach that object identification is performed before triggering an alert that notifies the user of an event [0111] or, when in "INTERRUPT mode," before generating a trigger signal to the camera indicating that the presence of an intruder has been detected. [0107]-[0108]. It would have been obvious to a POSA to modify the system of Lee to implement the object identification technique of Ozer to make the system more accurate by reducing the number of "false alarms" that may occur when the user is alerted and/or the camera is triggered in "INTERRUPT mode" by motion not caused by an object of interest (i.e., an intruder) but rather by other motion (e.g., a pet's movements), as specifically taught by Ozer. (Ex. 1005 (Ozer) at [0054]).

94. Ozer describes that it was known to compare objects in an image to silhouette templates to identify, among other objects, a human in the image being monitored. (Ex. 1005 (Ozer) at [0011]). The system of Ozer generates silhouettes of an object in an image to both classify objects (e.g., humans or dogs) in the image and to recognize a wide variety of activities. (Ex. 1005 (Ozer) at [0026]-[0027]; [0052]; [0053]-[0054]; [0064]). By identifying objects in the image, the system is more accurate because it rejects many elements in the

area being monitored that may be moving, but are not objects of interest. (Ex. 1005 (Ozer) at [0054]). Ozer's system determines an object model describing the shape of the object. (Ex. 1005 (Ozer) at [0061]-[0063]). As discussed above in ¶26, the BRI of "silhouette" includes at least a representation of the contours of an object derived based on a number of descriptors that are typical for the object (e.g., human body), or on other factors which can be used to distinguish, discriminate and/or differentiate objects, including distinguishing animals from humans. The object model of Ozer is derived using descriptors that are typical for a human body (e.g., hands head, torso). (Ex. 1005 (Ozer) at [0052]). A POSA would have understood that the object model of Ozer is a silhouette. Ozer describes using a graph matching process to compare the determined object model with a set of stored models. (Ex. 1005 (Ozer) at [0064]). A POSA would have understood Ozer's object model to be a silhouette (indeed Ozer specifically refers to it as such), and Ozer's identification of objects (such as a human body) by matching the object model with reference models to be determining a closest match between the derived silhouette of the object and a silhouette in the set of stored silhouettes. (Ex. 1005 (Ozer) at [0026]-[0027]; [0029]; [0034]; and [0064]).

95. It would have been obvious to a POSA to have modified the system of Lee to implement the object identification technique of Ozer that generates a

silhouette of an object in an image and compares the generated silhouette to a set of stored silhouettes to identify the object.

96. A POSA would have implemented the combined system by using the silhouette object identification technique of Ozer in Lee by having the processor in main control unit 100 of Lee identify the object (e.g., as human or not) that was detected as moving by the motion detector, and reacting to the detection of motion by the motion detector based on the object identification by generating an alert to the user of an event and/or triggering the camera in INTERRUPT mode when the object is determined to be a human, and by not doing so when the objected detected is not a human (e.g., a pet) to reduce false alarms as taught by Ozer. (Ex. 1005, (Ozer) at [0054]).

ii. Claim 10. The system of claim 9, wherein said at least one motion detector comprises a plurality of motion detectors and said at least one camera comprises a plurality of cameras, at least one of said cameras being associated exclusively with each of said motion detectors, at least two of said cameras are associated exclusively with each of said motion detectors or at least two of said cameras are associated non-exclusively with each of said motion detectors, wherein when at least two of said cameras are associated with one of said motion detectors, each of said at least two cameras has a dormant state in which imaging is not performed and images are not obtained and an active state in which images are obtained, said at least two cameras all being activated from the dormant state into the active state when the associated one of said motion detectors detects motion in its field of view such that said at least two cameras obtain images of the source of the motion detected by the associated one of said motion detectors, and said

processor being arranged to analyze images from said at least two cameras to determine depth information about a common object appearing in the images from said at least two cameras which may be the source of the motion, the depth information being used in the object identification being performed by the processor and indicating a distance between the structure and the object, said processor being arranged to react to the detection of motion by said at least one motion detector based on the object identification and based on the distance between the structure and the object."

97. The S&S device 212 of Lee includes a plurality of camera modules 920, each of which includes a camera 922 and a sensor 923 (which can be a motion detector). ([0104]; [0110]; [0111]; FIG. 9). Claim 10 recites three alternative ways in which a system including multiple cameras and motion detectors can be arranged, and requires that the claimed system meet one of these alternatives. A POSA would have understood that for claim 10 to be met by a system, only one of the alternatives need be present. I have been informed by counsel that this understanding is correct.

98. While the language in claim 10 is far from a model of clarity, I understand from counsel that it must be interpreted in view of the '983 specification, which describes three ways in which a plurality of cameras and motion detectors can be arranged. The first arrangement is that there is "a 1:1 correspondence or association between motion detectors and cameras, i.e., each motion detector has a single and exclusive camera whose field of view encompasses the field of view of the motion detector." (Ex. 1001 at 3:63-66). A

second arrangement involves a motion detector being associated with two or more cameras and being the "exclusive" motion detector for those cameras. (Ex. 1001 at 3:67-4:9). A third arrangement involves a camera being associated with two or more motion detectors so that it obtains an image when any of its associated detectors detects motion. (Ex. 1001 at 4:7-12). Claim 10 describes these three arrangements in the alternative, using the word "or," and requires a system that meets at least one of them.

99. Lee describes at least the first arrangement of multiple cameras and motion sensors where they have a 1:1 association. In Lee's system the camera 922 in a camera module 920 can be activated when an associated motion sensor 923 is triggered [0111]. Lee discloses an implementation in FIG. 9 in which camera modules 920 each includes a sensor (which can be a motion detector) 923 and an associated camera 922 in the same module. [0104]; [0111]; FIG. 9. A POSA would have understood Lee to disclose that the camera and sensor in the same module are associated exclusively in a 1:1 correspondence, or that this would have been an obvious way to implement what Lee discloses in FIG. 9 in the combination of Lee and Ozer.

100. Claim 10 includes additional limitations related to determining depth information about a common object appearing in images from at least two cameras "when at least two of said cameras are associated with one of said

motion detectors." These limitations do not apply to the first arrangement of cameras and motion detectors in a 1:1 correspondence which is shown in Lee and that I rely upon to demonstrate the obviousness of claim 10 over the combination of Lee and Ozer, and thus no further discussion of these limitations is necessary to demonstrate that claim 10 is obvious over the combination of Lee and Ozer. I have been informed by counsel that this understanding is correct.

iii. Claim 12: "The method of claim 11, wherein the processor further derives a silhouette of any objects in the image, compares the silhouettes to a library of stored silhouettes having associated object identification to determine an exact or closest match of the derived silhouette to one of the stored silhouettes and retrieves the object identification associated with the exact or closest match, further comprising generating a countermeasure to the detection of motion by the motion detectors based on the object identification when the object is identified as a potential threat to the structure."

101. See analysis of claim 9. As discussed therein, in the combination a POSA would have implemented, the combined system would use the silhouette object identification technique of Ozer in Lee by having the processor in main control unit 100 of Lee identify the object (e.g., as human or not) that was detected as moving by the motion detector, and reacting to the detection of motion by the motion detector based on the object identification by generating an alert to the user of an event and/or triggering the camera in "INTERRUPT mode" when the object is determined to be a human, and by not doing so when

the objected detected is not a human (e.g., a pet) to reduce false alarms as taught by Ozer. (Ex. 1005, (Ozer) at [0054]). The generation of an alert and the triggering of the camera in "INTERRUPT mode" are both countermeasures the system would generate when the object is identified as a potential threat (e.g., identified as potential intruder). As discussed above, the alert can include alerting the user and providing a live image to be shown on the user's LCD display device. [0111]. The alert can also include the main control unit 100 automatically calling the user's mobile telephone, if the system is on and the user is not at home. [0111]. These are consistent with the countermeasures described in the '983 patent which include "a message or warning is sent to a distant computer" or "the property owner's homepage ." (Ex. 1001 at 3:30-38).

iii. Claim 13: "The method of claim 12, wherein each camera is associated with only a single motion detector, each camera is associated with a plurality of motion detectors, or, multiple cameras are associated with each motion detector, wherein when a plurality of cameras are associated with one of the motion detectors, images from the plurality of cameras are analyzed by the processor to determined depth information about an object appearing in the images, the depth information being used in the object identification being performed by the processor."

102. The S&S device 212 of Lee includes a plurality of camera modules 920, each of which includes a camera 922 and a sensor 923 (which can be a motion detector). [0104]; [0110]; [0111]; FIG. 9. Claim 13 recites three alternative ways in which a system including cameras and motion detectors can

be arranged, and requires that the claimed system meet one of these three alternatives. A POSA would have understood that for claim 13 to be met by a system, only one of the alternatives in the list need be present. I have been informed by counsel that this understanding is correct.

103. The '983 specification describes three ways in which a plurality of cameras and motion detectors can be arranged. The first arrangement is that there is "a 1:1 correspondence or association between motion detectors and cameras, i.e., each motion detector has a single an exclusive camera whose field of view encompasses the field of view of the motion detector." (Ex. 1001 at 3:63-66). A second arrangement involves a motion detector being associated with two or more cameras and being the "exclusive" motion detector for those cameras. (Ex. 1001 at 3:67-4:9). A third arrangement involves a camera being associated with two or more motion detectors so that it obtains an image when any of its associated detectors detects motion. (Ex. 1001 at 4:7-12). Claim 13 describes these three arrangements in the alternative, using the word "or," and requires a system that meets at least one of them.

104. Lee describes at least the first arrangement of multiple cameras and motion detectors where they have a 1:1 association. In Lee's system, the camera 922 in a camera module 920 can be activated when an associated motion sensor 923 is triggered [0111]. Lee discloses an implementation in FIG. 9 in which

camera modules 920 each includes a sensor (which can be a motion detector) 923 and an associated camera 922 in the same module. ([0104]; [0111]; FIG. 9). A POSA would have understood Lee to disclose that the camera and sensor in the same module are associated exclusively in a 1:1 correspondence, or that this would have been an obvious way to implement what Lee discloses in FIG. 9 in the combination of Lee and Ozer.

105. Claim 13 includes additional limitations related to determining depth information about a common object appearing in images from a plurality of cameras "when a plurality of cameras are associated with one of the motion detectors." These limitations do not apply to the first arrangement of cameras and motion detectors in a 1:1 correspondence which is shown in Lee and that I rely upon to demonstrate the obviousness of claim 13 over the combination of Lee and Ozer, and thus no further discussion of these limitations is necessary to demonstrate that claim 13 is obvious over the combination of Lee and Ozer. I have been informed by counsel that this understanding is correct.

iv. Claim 14: "The method of claim 12, further comprising assigning a classification of "no threat" or "hostile" based on the object identification and/or the size of the object, the countermeasure being generated only when the classification is hostile."

106. As discussed in connection with claim 12, in the obvious combination of Lee and Ozer that a POSA would have implemented , the

combined system would use the silhouette object identification technique of Ozer in the system of Lee by having the processor in main control unit 100 of Lee identify the object (e.g., as human or not) that was detected as moving by the motion detector, and reacting to the detection of motion by the motion detector based on the object identification by generating an alert to the user of an event and/or triggering the camera in "INTERRUPT mode" when the object is determined to be a human, and by not doing so when the objected detected is not a human (e.g., a pet) to reduce false alarms as taught by Ozer. (Ex. 1005 (Ozer) at [0054]). The generation of an alert and the triggering of the camera in "INTERRUPT mode" are both countermeasures the system would generate when the object is identified as a potential threat or hostile (e.g., identified as a potential intruder) and would not generate when the object is classified as being no threat (e.g., a pet). As discussed above, the alert can include alerting the user and providing a live image to be shown on the user's LCD display device. [0111]. The alert can also include the main control unit 100 automatically calling the user's mobile telephone, if the system is on and the user is not at home. [0111]. These are consistent with the countermeasures described in the '983 patent which include "a message or warning is sent to a distant computer" or "the property owner's homepage ." (Ex. 1001 at 3:30-38).

v. Claim 15: "The method of claim 12, wherein the step of generating a countermeasure includes generate an audible

and/or visual alarm in proximity to the structure or generating at least one communication about the condition of the structure based on the object identification and forwarding the communication to a remote destination."

107. As discussed in connection with claim 14, in the obvious combination of Lee and Ozer that a POSA would have implemented , the combined system would use the silhouette object identification technique of Ozer in the system of Lee by having the processor in main control unit 100 of Lee identify the object (e.g., as human or not) that was detected as moving by the motion detector, and reacting to the detection of motion by the motion detector based on the object identification by generating an alert to the user of an event and/or triggering the camera in "INTERRUPT mode" when the object is determined to be a human, and by not doing so when the objected detected is not a human (e.g., a pet) to reduce false alarms as taught by Ozer. (Ex. 1005 (Ozer) at [0054]). The generation of an alert and the triggering of the camera in "INTERRUPT mode" are both countermeasures the system would take when the object is identified as a potential threat or hostile (e.g., identified as a potential intruder) and would not be generated when the object is classified as being no threat (e.g., a pet). As discussed above, the alert can include providing a live image to be shown on the user's LCD display device, which a POSA would have recognized is a visual alarm within the structure and therefore in proximity to the structure. [0111]. The alert can also include the main control unit 100

automatically calling the user's mobile telephone, if the system is on and the user is not at home, which a POSA would have recognized is a communication about the condition of the structure that is based on the object identification and is forwarded to a remote destination. [0111]. These actions are consistent with the countermeasures described in the '983 patent which include "a message or warning is sent to a distant computer" or "the property owner's homepage ." (Ex. 1001 at 3:30-38). Additionally, generating and forwarding a communication about the condition of a structure to a remote destination based on an object identification was well known prior to the relevant time period (*see e.g.*, Ex. 1004 (Osann) at 14:6-14 ("Given the inconvenience and expense of false alarms, the distributed video capability of this invention … could allow a Security Company or even the Police to view inside and around the home or building in the case of an alarm being set off, so that a "false alarm" condition can be determined without having to visit the location."); Ex. 1007 (Jentoft) at 5:6:13 ("The transceiver 60 further transmits signals including system status reports or recorded images via a telephone channel 70 or cable channel 75 to outside monitoring facilities … Outside monitoring facilities may include a private security company or a local law enforcement station.")).

vi. Claim 16: "The method of claim 15, wherein the remote destination is a police station, a fire station, a terminal monitored by an owner of the structure, or a private security station."

108. See analysis for claim 15. As described therein, the alert in the combined system of Lee and Ozer can include the main control unit 100 automatically calling the user's mobile telephone, if the system is on and the user is not at home. [0111]. The plain and ordinary meaning of "terminal" in the data communications field is "any device that terminates one end (sender or receiver) of a communicated signal." (Ex. 1009). A POSA would have understood that the user's mobile phone that can receive the alert signal in the combined system is a terminal. In addition, Lee teaches that an object of the Lee system is to allow the user to communicate and monitor the system via the Internet ([0021]) and shows that this may be done via a remote computer 291 that can receive video data from the system. [0062]; [0111]; FIG. 1. In the combined system of Lee and Ozer, a live image can be sent to the remote computer 291 (which a POSA would also have recognized as a terminal) over the Internet when an event occurs so that the user can monitor the system remotely over the web. [0111]. Additionally, forwarding a communication about the condition of a structure to a police station or a private security station based on an object identification was well known prior to the relevant time period (*see e.g.*, Ex. 1004 (Osann) at 14:6-14 ("Given the inconvenience and

expense of false alarms, the distributed video capability of this invention … could allow a Security Company or even the Police to view inside and around the home or building in the case of an alarm being set off, so that a "false alarm" condition can be determined without having to visit the location."); Ex. 1007 (Jentoft) at 5:6:13 ("The transceiver 60 further transmits signals including system status reports or recorded images via a telephone channel 70 or cable channel 75 to outside monitoring facilities … Outside monitoring facilities may include a private security company or a local law enforcement station.")), and it would have been obvious to a POSA to have such a communication sent in the combined system of Lee and Ozer so police or security personnel can be alerted and respond to a potential threat from an intruder if the user is not home or unwilling to investigate the potential threat on their own.

vi. Claim 17: "The method of claim 15, further comprising including one or more images obtained from the cameras or one or more images derived from the images obtained from the cameras in the communication being forwarded to the remote destination."

109. In the combined system, the communication forwarded to a remote destination can include live images from one or more cameras sent to the remote computer 291. (see analysis of claim 16). In addition, it would have been obvious to a POSA to implement the combined system by including sending to a remote destination an image from the camera showing the monitored area at the

time the event was detected as such systems were known. (*see e.g.*, Ex. 1004 (Osann) at 14:6-14 ("Given the inconvenience and expense of false alarms, the distributed video capability of this invention … could allow a Security Company or even the Police to view inside and around the home or building in the case of an alarm being set off, so that a "false alarm" condition can be determined without having to visit the location."); Ex. 1007 (Jentoft) at 5:6:13 ("The transceiver 60 further transmits signals including system status reports or recorded images via a telephone channel 70 or cable channel 75 to outside monitoring facilities … Outside monitoring facilities may include a private security company or a local law enforcement station.")).

C. Ground 3: Claims 1-8, 11, and 18-20 of the '983 Patent are Obvious in view of Milinusic and Osann

110. According to the face of the document, Milinusic (Ex. 1003) is a U.S. patent that issued on September 12, 2006, from an application that was filed on February 19, 2002. I have been informed by counsel that it meets the requirements to be prior art to the '983 patent.

111. Milinusic describes a surveillance system 100 that includes a surveillance server 210, a surveillance client 240, and multiple sensor units 250, 260, 270 all connected via a network, which is labeled 230 in FIG. 2 and labeled

130 in the other figures. (2:61-67; FIG. 2; FIG. 4).[4] Network 230 may be a wide area network (WAN), such as the Internet, or a local area network (LAN). (3:18-19). Each of the sensor units 250, 260, 270 is connected to the network 230 via a wired or wireless interface. (3:20-22). One or more of sensor units 250, 260, and 270 may be cameras, such as a digital camera or a video camera. (3:47-49). Sensor units 250, 260 and 270 may also be configured as a sensing device such as a motion detector. (3:51-55). The sensor units 250, 260, and 270 are configured to collect surveillance data by detecting predetermined conditions or occurrences and generating and outputting surveillance data representative of the detected conditions or occurrences. (3:41-45). The collected surveillance data may be transmitted from the sensor units 250, 260, 270 to surveillance server 210 via the network 230. (3:46-47). Surveillance data transmitted to surveillance server 210 includes image data output by camera units 250, 260. (6:20-32). The surveillance server 210 incorporates the received surveillance data into a database 220. (3:61-64). The database 220 may be stored on a memory device connected to surveillance server 210 or a memory device that is connected to the network 230 and accessible to the surveillance server 210 via network 230. (3:6-10).

[4] Unless otherwise indicated, all citations in §C(¶¶110-159) are to Ex. 1003 (Milinusic).

112. Surveillance server 210 includes a central processing unit (CPU) 360, storage memory 365 for storing data, and an input/output (I/O) interface 375 provided for interfacing with associated input and output devices including the network. (4:14-23; FIG. 4). CPU 360 is configured to control operation of the surveillance server 210 so that surveillance data may be received from the various sensor units 250, 260, 270 and incorporated into the surveillance database 220. (4:25-29). CPU 360 is also configured to retrieve and distribute surveillance data to a requesting surveillance client 240. (4:29-32).

113. Surveillance client 240 may be implemented as a general purpose computer, a personal computer or a personal data assistant (PDA), such as a Palm Pilot. (3:31-35). Surveillance client 240 is configured to allow a user to retrieve surveillance data by issuing a request to surveillance server 210. (3:35-38). Surveillance client 240 is also configured to allow a user to control or adjust specified sensor units 250, 260, 270 by issuing requests to the surveillance server 210, which transmits the requests to the specified sensor units. (3:37-41).

114. Sensor units 250, 260 may be configured to monitor a predetermined area, such as a warehouse interior area. (5:51-52; 6:59-67). Cameras 451, 452, and 461 are configured to capture an image of the area and objects within the area and to generate and output image data representative of the area/objects. (5:52-56; FIG. 4). Image capture may be set to occur at

predetermined times or upon the occurrence of predetermined occurrences, such as the detection of movement within the area being monitored by the sensor units 250 and 260. (5:56-59). The sensor units 250, 260 and the cameras 451, 452, and 461 may be supported and positioned by gimbals mounted to a support device such as a concrete wall, building, or other structure capable of providing support. (6:33-42).

115. According to the face of the document, Osann (Ex. 1004) is a U.S. patent that issued on August 7, 2007, from an application that was filed on December 7, 2004. I have been informed by counsel that it meets the requirements to be prior art to the '983 patent.

116. Osann describes a system that enables a user to deal with an intrusion into their home without having to personally confront the intruder. (Ex. 1004 (Osann) at abstract). The system is implemented in a home or building and incorporates a plurality of Energy Monitoring And Control (EMAC) points located at electrical junction box power access locations such as wall switch assembly 4 and power plug receptacle assembly 5. (Ex. 1004 (Osann) at 9:17-25; FIG. 1). An EMAC point includes an energy sensing capability and a digital communications circuit enabling communication with a central intelligence device such as a local personal computer (PC) 9 or Residential Gateway residing in the same building. (Ex. 1004 (Osann) at 9:26-

30). EMAC points may be located exterior of a home or building (e.g., connected to a light mounted on an exterior wall of a home or building). (Ex. 1004 (Osann) at 25:55-57; FIG. 28). A junction box extension unit 82 including a motion detector 85, a video camera 86, and a communication circuit capable of sending digital information to and from any remote device by way of the electrical power line at the junction box may be added between the exterior electrical junction box 83 and the exterior light 87. (Ex. 1004 (Osann) at 25:57-64; FIG. 28). Video information captured by the camera is digitized, compressed, and sent over the powerline communication link. (Ex. 1004 (Osann) at 25:64-65).

117. After reviewing Milinusic, Osann, and claims 1-8, 11, and 18-20 of the '983 patent, it is my opinion that every one of these claims would have been obvious to a POSA in view of Milinusic and Osann. Milinusic and Osann together disclose every limitation of the claims, and a POSA would have had reasons to put together the collective teachings of these references to result in a combination that meets all the limitations of each of these claims. The basis for my opinion and the details of my analysis are below.

i. Claim 1: "An alarm system for protecting a structure, comprising:"

118. Milinusic describes a surveillance system 100 that includes cameras and sensors to detect conditions (e.g., motion) and can be used to monitor a

predetermined area which can include a warehouse, which is a structure. (6:59-67). Milinusic also describes conventional systems as being deficient in not being able to determine information about an intruder. (1:37-44). A POSA would have understood that the surveillance system of Milinusic would be effective in monitoring a structure such as a warehouse, home or building for events such as an intruder, and would have understood that this would be among the primary uses for Milinusic's system. In addition, Osann describes providing a video surveillance and motion detection system to protect a home or building, which would have provided further motivation for a POSA to use the Milinusic system to protect a structure. (Ex. 1004 (Osann) at 25:55-60; FIG. 28). Additional motivation for this use of the Milinusic system is provided by the well-known use of camera and motion detector systems to protect a structure (*see e.g.*, Ex. 1002 (Lee) at [0105] ("Generally, the camera module 920, sensor module 930, and wireless module 940 are installed at the necessary sites inside and outside the house."), Ex. 1007 (Jentoft) at 1:14-16 ("The present invention is directed to a security arrangement and method for monitoring the inside of a facility or residence."), Ex. 1006 (Dy) at [0007] ("The present invention relates to a security system with video cameras that provide video surveillance of a predetermined residential or commercial area.")).

119. Milinusic teaches that the system can detect predetermined conditions, generate surveillance data representative of the detected condition and distribute surveillance data to a surveillance client based upon predetermined distribution criteria. (3:3-5; 3:64-4:1; 4:30-34). A POSA would have understood that the distribution of data to a client device upon detection of a condition is an alarm that notifies the client device of the condition, and that the condition may be detection of an intruder. Thus, a POSA would have understood that Milinusic discloses an alarm system. In addition, Osann explicitly describes generating an alarm upon the occurrence of an event such as detecting an intruder (Ex. 1004 (Osann) at 14:4-20) which would have provided further motivation for a POSA to have the Milinusic system generate an alarm upon detection of a condition such as an intruder. Additional motivation for having the Milinusic system generate an alarm is provided by the well-known generation of alarms from systems that use cameras and motion detectors to protect a structure (*see e.g.*, Ex. 1002 (Lee) at [0111] ("When the security system has been triggered …[t]he user is alerted and a text message corresponding to the nature of the unusual event information sensed by the sensors in the system is sent to a display device 50 to inform the user which sensor was triggered"), Ex. 1007 (Jentoft) at 6:55-60 ("The motion detector 22 detects the intruder walking toward the bed which triggers the camera to turn

"on" and begin recording the intruder's movements. In one embodiment, the security system may sound an alarm to scare the intruder into halting the unwanted activity")).

a. "[*A*] at least one motion detector arranged to have a field of view external of the structure and including an area proximate the structure;"

120. Milinusic's surveillance system 100 includes a plurality of sensor units 250, 260, 270 configured to collect surveillance data by detecting predetermined conditions or occurrences. (3:41-45; 5:24-64; FIG. 2; FIG. 4). Any of sensor units 250, 260, and 270 may be configured as a motion detector. (3:51-55). Milinusic describes configuring sensor units 250 and 260 to monitor a predetermined area, such as a warehouse interior area. (5:51-60; 6:59-67). Milinusic does not explicitly state that the predetermined area that may be monitored by the sensor units 250, 260 may be an area external of and proximate the structure. Milinusic describes conventional systems as being deficient in not being able to determine information about an intruder. (1:37-44). A POSA would have understood that the surveillance system of Milinusic would be effective in monitoring a structure such as a warehouse, home or building for events such as an intruder. To detect the presence of an intruder and detecting information about an intruder (1:37-44), a POSA would have understood that it would be desirable to monitor the areas proximate the access points to the house

(e.g., doors and windows). Thus, it would have been obvious to a POSA to use the Milinusic system to protect a structure (e.g., building or home) by arranging motion sensors (and cameras) to have a field of view external of the structure, and that the field of view would include areas proximate the structure (e.g., proximate doors and windows) to detect motion of any intruders seeking to enter the structure.

121. In addition, Osann describes providing video surveillance and motion detection devices at the exterior of a home or building. (Ex. 1004 (Osann) at 25:55-60; FIG. 28). A POSA would have been further motivated by this teaching in Osann to arrange the sensor units 250, 260 of Milinusic to have a field of view external a structure and including an area proximate the structure to detect intruders prior to their entry into the structure. Additional motivation for this arrangement of the motion detectors and cameras of the Milinusic system is provided by the well-known use of camera and motion detector systems to protect a structure by monitoring areas external to and proximate the structure (*see e.g.*, Ex. 1002 (Lee) at [0105] ("Generally, the camera module 920, sensor module 930, and wireless module 940 are installed at the necessary sites inside and outside the house.")).

b. "*[B1]* at least one camera associated with and coupled to each of said at least one motion detector,"

122. The sensor units 250, 260 and 270 in Milinusic's system may be cameras, such as a digital camera or a video camera configured to be responsive to, for example, the visible light spectrum or infrared radiation (IR). (3:47-51). FIG. 2 of Milinusic shows the sensor units 250, 260 and 270 connected to network 230. FIG. 4 shows sensor unit 250 as including cameras 451 and 452 and sensor unit 260 as including camera 461. (5:24-43). Surveillance data output from cameras 451, 452 and 461 is transmitted to data acquisition units 472, 474 and 476, respectively, and in turn transferred over the network 130 to surveillance server 210. (6:26-32). The camera in any of sensor units 250, 260, and 270 that includes a camera may be coupled to the motion detector in any sensor unit configured as a motion detector (3:51-55) via the network (230 in FIG. 2 and 130 in FIG. 4).

123. Additionally, Milinusic describes cameras 451, 452 (within sensor unit 250) and 461 (within sensor unit 260) as being configured to capture an image of an area upon the occurrence of predetermined occurrences such as the detection of movement with the area being monitored by sensor units 250, 260, which a POSA would recognize requires a motion detector coupled to the camera. (5:51-59). Thus, Milinusic teaches that the cameras 451, 452, and 461 each may be coupled to a motion detector that monitors the same area as the

camera. Milinusic does not explicitly state whether the sensor units 250, 260 include the motion detectors within the same sensor units as the cameras, or whether the motion detectors are provided in separate sensor units coupled to the cameras via the network. A POSA would have understood that either option would have been an obvious design choice, and that either option would include a motion detector coupled to the camera. A POSA would have also understood that providing the motion detectors within the same sensor unit as the associated camera was a known configuration that would provide the advantage of an integrated unit that provided the ability to capture surveillance data with a camera and to trigger the image capture with a motion detector monitoring the same area (*see e.g.*, Ex. 1002 (Lee) at [0104] ("camera module 920 comprises a cameras interface 921, a sensor 923, and a camera 922"), Ex. 1007 (Jentoft) at 3:52-55 ("A base unit 35 … integrates a motion sensor 20, a camera 25, a data processor 30, and a communication interface 15.")).

c. "*[B2]* each of said at least one camera being arranged relative to the associated one of said at least one motion detector such that said camera has a field of view encompassing at least part of the field of view of the associated one of said at least one motion detector,"

124. As discussed above for element [B1] of claim 1, Milinusic describes sensor units 250 and 260 as being arranged to monitor a predetermined area with the cameras 451, 452 (sensor unit 250) and 461 (sensor unit 260) being

arranged to capture images of the area they monitor. (5:51-55). Sensor units 250, 260 may be configured to include motion detectors. (3:51-55). Milinusic also describes image capture being set to occur upon the occurrence of predetermined occurrences, such as the detection of movement within the area being monitored by the sensor unit. (5:56-59). A POSA would have understood Milinusic as teaching that a motion detector (whether within the same sensor unit 250, 260 or a different sensor unit) and cameras 451, 452 or 461 are arranged to monitor the same area, meaning that each of these cameras has a field of view encompassing at least part of the field of view of an associated motion detector.

d. "[*B3*] each of said at least one camera having a dormant state in which images are not obtained and an active state in which images are obtained and being activated into the active state when the associated one of said at least one motion detector detects motion;"

125. Milinusic describes cameras 451, 452, and 461 being configured to capture an image of an area and the objects within the area and to generate output image data representative of the area/objects. (5:52-55). Milinusic describes setting image capture by the cameras to occur upon the detection of movement in an area being monitored by the sensor units 250 and 260. (5:55-59). Milinusic does not explicitly state that cameras 451, 452, and 461 are off (or "dormant") and not recording images prior to detecting movement when the

cameras are set to capture an image upon detection of movement, but a POSA would have understood that to be the case because otherwise, Milinusic would not have made a distinction between capturing images at predetermined times or upon the detection of movement. (5:55-59). A POSA would have further understood that movement is detected in Milinusic by a motion detector. (3:50-55). Accordingly, a POSA would have understood that when the cameras are set to capture an image upon the detection of movement in an area being monitored by a sensor unit, that the camera would have a dormant state in which images are not obtained (i.e., when motion is not detected in the area), and an active state in which images are obtained (i.e., when motion is detected in the area), and that the camera would be activated into the active state when the associated motion detector monitoring the area detects motion.

e. "*[C]* a processor coupled to said at least one camera and arranged to control said at least one camera and receive the image obtained by said at least one camera;"

126. Surveillance server 210 includes a central processing unit (CPU) 360. (4:14-16). A POSA would have understood that CPU 360 is a processor. CPU 360 is shown as being coupled to the network (230 in FIG. 2 and 130 in FIGs. 3-4) via local interface 370 and I/O processor 375. (FIG. 3). The surveillance server 210 (including its processor 360) is coupled to the sensor units 250 and 260 via the network (230 in FIG. 2 and 130 in FIGs. 3-4). (2:61-

67). Sensor units 250 and 260 may include cameras (3:47-51; 5:23-42). Accordingly, CPU 360 is coupled to at least one camera (e.g., in sensor units 250 and 260) via the network.

127. Milinusic's surveillance server 210 receives requests from surveillance client 240 to control or adjust specified sensor units. (3:37-40). Surveillance server 210 transmits the requests to the specified sensor units 250, 260, 270 upon receiving the requests from the surveillance client 240. (3:40-41). A POSA would have understood that the CPU 360 of the surveillance server 210 is arranged to control a camera in a sensor unit by transmitting requests received from the surveillance client 240 to the camera over the network (130 or 230).

128. Additionally, the CPU 360 of surveillance server 210 in Milinusic's system is configured to control the operation of the server so that surveillance data may be received from the various sensor units. (4:25-30). The surveillance data may include video data or still image data received from sensor units 250, 260, 270. (3:10-13). A POSA would have understood that the CPU 360 is arranged to receive images obtained by the cameras in the sensor units.

f. "*[D]* a telecommunications module coupled to said processor, said telecommunications module being capable of communications over a telecommunications network; and"

129. Surveillance server 210 in Milinusic's system includes an input/output (I/O) processor 375 that provides an interface to the network.

(4:16-23; FIG. 3). I/O processor 375 is coupled to CPU 360 via local interface 370. (FIG. 3). Network (230 in FIG. 2 and 130 in FIGs. 3-4) is described as a wide area network (WAN) such as the Internet or a local area network (LAN). (3:18-19). The Internet (or any WAN) is a telecommunications network under the BRI of that term, as discussed above in ¶24. Accordingly, a POSA would have understood I/O processor 375 to be a telecommunications module coupled to the processor (i.e., CPU 360) and being capable of communications over a telecommunications network (i.e., network 130/230).

g. "[*E*] a handheld telecommunications unit for transmitting commands for said processor via said telecommunications module to cause said processor to provide images to said telecommunications module to be transmitted to the telecommunications unit."

130. Surveillance system 100 of Milinusic includes a surveillance client 240 connected to the network (130 or 230). (2:63-65; FIGs. 2 and 4). Milinusic describes that the surveillance client 240 may be, for example, a general purpose computer, a personal computer or a personal digital assistant (PDA), such as a Palm Pilot. (3:33-35). A PDA is described in the '983 patent as an example of a handheld telecommunications unit. (Ex. 1001 at 5:67-6:6; 11:31-35 – ("Thus, control over the activation and deactivation of the alarm system, as well as other adjustment to the alarm system, can now be performed using a handheld telecommunications unit 42, whether it is a cellular telephone or a camera

telephone or a similar unit, such as a PDA.")). Laptop computers are also described in the '983 patent as examples of a handheld telecommunications unit. (Ex. 1001 at 5:67-6:6). Thus, the personal computer and PDA described by Milinusic as examples of surveillance client 240 meet the BRI of a handheld telecommunications unit as described in ¶25 above.

131. Surveillance client 240 of Milinusic is configured to allow a user to retrieve surveillance data by issuing a request to surveillance server 210. (3:34-37). The surveillance data may include video data and still image data. (3:12-13). Accordingly, a POSA would have understood that surveillance client 240, implemented as a PDA or a personal computer, is a handheld telecommunications unit for transmitting commands for the processor (i.e., CPU 360 in surveillance server 210) via the telecommunications module (i.e., I/O processor 375) to cause the processor to provide images to the telecommunications module to be transmitted to surveillance client 240.

ii. Claim 2: "The alarm system of claim 1, wherein said processor is coupled to said at least one motion detector and said telecommunications unit is also arranged to transmit commands for said processor to activate and deactivate said at least one motion detector."

132. Surveillance server 210 of Milinusic includes a central processing unit (CPU) 360, which is a processor. (4:14-16). CPU 360 is connected to the network (130 or 230) via local interface 370 and I/O processor 375. (FIG. 3).

Sensor units (e.g., 250, 260, and 270) configured as motion detectors may also be connected to a network (130 or 230). (2:61-67; 3:51-55). Accordingly, CPU 360 is coupled to at least one motion detector via the network (130 or 230).

133. Surveillance client 240 is configured to control or adjust sensor units by issuing requests to surveillance server 210. (3:37-40). Milinusic does not explicitly describe surveillance client 240 being arranged to transmit commands to CPU 360 to activate or deactivate a motion detector. However, Milinusic teaches that the sensor units may be set to capture images at predetermined times or upon the detection of movement in the monitored area. (5:55-60). It would have been obvious to a POSA to implement surveillance client 240 to send a command to deactivate the motion detector monitoring an area when the camera monitoring that area is set to capture images at predetermined times rather than upon the detection of motion in the area, as the motion detector is not being used when the camera is on and power consumed by the system can be reduced by not unnecessarily powering a motion detector that is not in use. Additionally, it would have been obvious to a POSA to provide the ability for the user to send commands from a user input device to activate and deactivate the security system (including the motion detectors) so that the system can be controlled remotely to turn it off and on as the user desires. This capability to remotely turn on and off a surveillance system with

cameras and motion detectors was known in the art (*see e.g.*, Ex. 1002 (Lee) at [0087] ("The system 10 receives user command signals from the remote controller 281 to control at least one of the plurality of remote devices or the system 10 … the user may program the system to turn on or off the system using the remote controller.")) and a POSA would have understood the benefits of providing that capability in the Milinusic system (e.g., to allow a user to remotely turn off the system before cleaning people enter the building and then turn it back on after they depart).

iii. Claim 3: "The alarm system of claim 1, wherein in said dormant state of each of said at least one camera, imaging by said camera is not performed and images are not obtained, each of said at least one camera being automatically activated from the dormant state into the active state when the associated one of said at least one motion detector detects motion in its field of view."

134. As discussed in ¶125, Milinusic describes cameras 451, 452, and 461 being configured to capture an image of an area and the objects within the area and to generate an output image data representative of the area/objects. (5:52-55). Milinusic describes setting image capture by the cameras to occur upon the detection of movement in an area being monitored by the sensor units 250 and 260. (5:55-59). A POSA would have understood that movement is detected in Milinusic by a motion detector (3:50-55), and that when the cameras are set to capture an image upon the detection of movement in an area being

monitored by a sensor unit, that the camera would have a dormant state in which imaging by the camera is not performed and images are not obtained (i.e., when motion is not detected in the area), and an active state in which images are obtained (i.e., when motion is detected in the area), and that the camera would be automatically activated into the active state when the associated motion detector monitoring the area detects motion.

iv. Claim 4: "The alarm system of claim 1, wherein said telecommunications unit is one of a camera telephone, a cellular telephone and an Internet-enabled picture and/or video display device."

135. Surveillance client 240 may be implemented as a general purpose computer, a personal computer, or a PDA, such as a Palm Pilot. (3:31-35). Surveillance client 240 is connected to surveillance server 210 via the network (130 or 230), which may be a wide area network (WAN) such as the Internet. (3:18-19; FIG. 2; FIG. 4). Milinusic describes surveillance server 210 being configured to retrieve and distribute surveillance data (e.g., video data or still image data) to a requesting surveillance client. (3:12-13; 3:64-66). Accordingly, a POSA would have understood that a computer or PDA implementing surveillance client 240 is an Internet-enabled picture and/or video display device.

136. In addition, it was known in the relevant timeframe to remotely control and receive images from a surveillance system via a cell phone (*see e.g.*,,

Ex. 1006 (Dy) at abstract "A system and method for viewing video images from security systems on a remote handheld communications device like a cellular telephone."; Ex. 1006 (Dy) at [0007] "The present invention can also include hand-held mobile communication device remote from the control point that receives transmission signals from the communications interface device, selects particular video cameras from which the user wants to view images, and displays video images from at least one of the selected video cameras."). It would have been obvious to a POSA that a cell phone could operate just like a PDA in serving as a surveillance client 240 in the Milinusic system, and that using a cell phone would provide the advantage of connectivity even when an Internet connection was not available.

v. Claim 5: "The alarm system of claim 1, wherein said processor is arranged to receive, via said telecommunications module, one of a plurality of different code numbers from said telecommunications unit and control said at least one camera and said at least one motion detector in accordance with the received code number."

137. Surveillance client 240 is configured to control or adjust sensor units by issuing requests to surveillance server 210. (3:37-40). Surveillance client 240 and surveillance server 210 are connected via network 230, which is described as a wide area network (WAN), such as the Internet, or a local area network (LAN). (3:18-19; FIG. 2). Milinusic does not explicitly describe CPU 360 receiving one of a plurality of code numbers from surveillance client 240. A

POSA would have understood that commands sent from surveillance client 240 would include numbers, text, or some combination of numbers and text, and implementing the commands using code numbers for different commands would have been an obvious design choice. A POSA would have further understood that a plurality of code numbers would be used, each corresponding to different particular command input by a user into the surveillance client 240 to enable the surveillance server 210 to determine which of the specified sensor units to control and how to control the specified sensor unit.

138. As discussed above in connection with claim 2, it would have been obvious to a POSA that the ability Milinusic discloses for the surveillance client 240 to control or adjust sensor units includes the ability to control or adjust the components that can be included in a sensor unit, including motion detectors and cameras (3:37-40; 3:51-55; 5:51-55; FIG. 4), and that different command and control actions require different code numbers to identify the action desired by the user. In addition, Milinusic teaches that the sensor units may be set to capture images at predetermined times or upon the detection of movement in the monitored area, and a POSA would have understood that number codes can be provided to allow the camera to be controlled to configure it to capture images at predetermined times or upon the detection of movement in the monitored area. (5:55-60).

139. As discussed in connection with claim 2, it would have been obvious to a POSA to implement surveillance client 240 to send commands to activate/deactivate the motion detector monitoring an area when the camera monitoring that area is set to capture images at predetermined times rather than upon the detection of motion in the area, as the motion detector is not being used and power consumed by the system can be reduced by not unnecessarily powering a motion detector that is not in use. Additionally, it would have been obvious to a POSA to provide the ability for the user to send commands from the user input device to activate and deactivate the security system (including the motion detectors and cameras) so that the system can be controlled remotely to turn it off and on as the user desires. This capability to remotely turn on and off a surveillance system with cameras and motion detectors was known in the art (*see e.g.*, Ex. 1002 (Lee) at [0087] ("The system 10 receives user command signals from the remote controller 281 to control at least one of the plurality of remote devices or the system 10 … the user may program the system to turn on or off the system using the remote controller.")) and a POSA would have understood the benefits of providing that capability in the Milinusic system (e.g., to allow a user to remotely turn off the system before cleaning people enter the building and then turn it back on after they depart).

vi. Claim 6: "The alarm system of claim 5, wherein one of the code numbers is to cause said processor to cause images to

be provided by said processor to said telecommunications module and transmitted to the telecommunications unit."

140. As discussed in ¶131, surveillance client 240 of Milinusic is configured to allow a user to retrieve surveillance data by issuing a request to surveillance server 210. (3:34-37). The surveillance data may include video data and still image data. (3:12-13). Accordingly, a POSA would have understood that surveillance client 240, implemented as a PDA or a personal computer, is a handheld communications unit for transmitting commands for the processor (i.e., CPU 360 in surveillance server 210) via the telecommunications module (i.e., I/O processor 375) to cause the processor to provide images to the telecommunications module to be transmitted to surveillance client 240. A POSA would have further understood that such commands are implemented as code numbers. (see ¶137).

vii. Claim 7: "The alarm system of claim 5, wherein one of the code numbers is to cause said processor to direct said at least one camera to provide images to said processor and then cause the provided images to be forwarded by said processor to said telecommunications module and transmitted to the telecommunications unit."

141. Surveillance client 240 of Milinusic is configured to allow a user to retrieve surveillance data by issuing a request to surveillance server 210. (3:34-37). The surveillance data may include video data and still image data. (3:12-13). Accordingly, a POSA would have understood that surveillance client 240,

implemented as a PDA or a personal computer, is a handheld communications unit for transmitting commands to the processor (i.e., CPU 360 in surveillance server 210), via the telecommunications module (i.e., I/O processor 375), to cause the processor to provide images to the telecommunications module to be transmitted to the surveillance client 240. (see ¶131). A POSA would have further understood that such commands are implemented as code numbers. (see ¶137). Milinusic also describes that video data may be provided by the surveillance system 100 for presentation in a streaming format. (2:56-57). Milinusic does not explicitly describe that surveillance client 240 is configured to allow a user to issue a request to surveillance server 210 to provide video data from a camera (e.g., camera 451, 452, or 461) in a streaming format. It would have been obvious to a POSA to configure Milinusic's system to implement such a command to enable a user to control the system to provide the streaming capability that Milinusic explicitly describes. A POSA would have understood that a command to provide video data from a camera in a streaming format is a command to direct the camera to provide live images to the processor and then cause the provided live images to be forwarded by the processor to said telecommunications module and transmitted to the user input device when the user input device includes the ability to display images. Surveillance systems that provided the ability to access live images from the system via a remote

telecommunications device were known. (*see e.g.*, Ex. 1002 (Lee) at [0111-0112].

viii. Claim 8: "The system of claim 1, wherein said at least one motion detector comprises a plurality of motion detectors, said at least one camera associated with said at least one motion detector being arranged to have a field of view overlapping a field of view of a plurality of said motion detectors."

142. Milinusic's surveillance system 100 includes a plurality of sensor units 250, 260, 270 that may be configured as cameras and motion detectors. (2:59-3:2; 3:47-56). Milinusic teaches that cameras having wide-angle optics may be used to allow for viewing and/or capture of a wide field of view. (5:27-30). Milinusic also teaches the use of cameras having telephoto optics to allow for close-up monitoring and/or capture of an area from a greater distance. (5:34-37). A POSA would have understood that zooming in or out by "close-up monitoring" means narrowing and widening the field of view. Milinusic also describes image capture by the camera being set to occur upon detection of movement within the area being monitored by sensor units 250, 260. (5:51-59). A POSA would have understood that a camera with a wide field of view will have a wider field of view than most, if not all, motion detectors. A POSA would have further understood that, it would have been advantageous to include multiple motion detectors, each with a narrower field of view than the cameras, to detect motion at different areas in the camera's wider field of view, which

would result in the field of view of the camera overlapping the fields of view of the plurality of motion detectors. A POSA would have understood that this would provide a benefit versus employing a 1:1 relationship between cameras and motion detectors as in some installations with a lot of area to monitor the system can use fewer cameras than would be required if a 1:1 relationship between cameras and motion detectors were used, thereby reducing the cost of the overall system.

ix. Claim 11: "A method for protecting a structure, comprising:"

143. Milinusic describes a method of protecting a structure by using a surveillance system 100 that includes cameras and sensors to detect conditions (e.g., motion) and can be used to monitor a predetermined area which can include a warehouse or other structure. (6:59-67). Milinusic also describes conventional systems as being deficient in not being able to determine information about an intruder. (1:37-44). A POSA would have understood that the surveillance system of Milinusic would be effective in monitoring a structure such as a warehouse, home or building for events such as an intruder, and would have understood that this would be among the primary uses for Milinusic's system. In addition, Osann describes providing a video surveillance and motion detection system to protect a home or building, which would have provided further motivation for a POSA to use the Milinusic system to protect a structure.

(Ex. 1004 (Osann) at 25:55-60; FIG. 28). Additional motivation for this use of the Milinusic system is provided by the well-known use of camera and motion detector systems to protect a structure (*see e.g.*, Ex. 102 (Lee) at [0105] ("Generally, the camera module 920, sensor module 930, and wireless module 940 are installed at the necessary sites inside and outside the house."), Ex. 1007 (Jentoft) at 1:14-16 ("The present invention is directed to a security arrangement and method for monitoring the inside of a facility or residence."), Ex. 1006 (Dy) at [0007] ("The present invention relates to a security system with video cameras that provide video surveillance of a predetermined residential or commercial area.")).

a. "[*A*] arranging a plurality of motion detectors on or around the structure, each in a position in which its field of view includes an area proximate the structure;"

144. Milinusic's surveillance system 100 includes a plurality of sensor units 250, 260, 270 configured to collect surveillance data by detecting predetermined conditions or occurrences. (3:41-45; FIG. 2; FIG. 4; 5:24-64). Any of sensor units 250, 260, and 270 may be configured as a motion detector. (3:51-55). Milinusic describes configuring sensor units 250 and 260 to monitor a predetermined area, such as a warehouse interior area. (5:51-60; 6:59-67). Milinusic does not explicitly state where the sensor units 250 and 260 are placed to monitor the predetermined area or that the area monitored has a field of view

that includes an area proximate the structure. Milinusic describes conventional systems as being deficient in not being able to determine information about an intruder. (1:37-44). A POSA would have understood that the surveillance system of Milinusic would be effective in monitoring a structure such as a warehouse, home or building for events such as an intruder. To detect the presence of an intruder and detecting information about an intruder (1:37-44), a POSA would have understood that it would be desirable to monitor the areas proximate the access points to the house (e.g., doors and windows). Thus, it would have been obvious to a POSA to use the Milinusic system to protect a structure (e.g., building or home) by arranging motion sensors (and cameras) one or around the structure and to have a field of view that included areas proximate the structure (e.g., proximate doors and windows) to detect motion of any intruders seeking to enter the structure.

145. In addition, Osann describes mounting video surveillance and motion detection devices to the exterior of a home or building. ((Ex. 1004 (Osann), 25:55-60; FIG. 28). A POSA would have been further motivated by this teaching in Osann to arrange the sensor units 250, 260 of Milinusic on or around the structure to have a field of view including an area proximate the structure to detect intruders prior to their entry into the structure. Additional motivation for this arrangement of the motion detectors and cameras of the

Milinusic system is provided by the well-known use of camera and motion detector systems to protect a structure by monitoring areas proximate a structure (*see e.g.*, (Lee) at [0105] ("Generally, the camera module 920, sensor module 930, and wireless module 940 are installed at the necessary sites inside and outside the house.")).

b. "[*B1*] arranging a plurality of cameras on or around the structure,"

146. The sensor units 250, 260 and 270 may be cameras, such as a digital camera or a video camera configured to be responsive to, for example, the visible light spectrum or infrared radiation (IR). (3:47-51). FIG. 4 shows sensor unit 250 as including cameras 451 and 452 and sensor unit 260 as including camera 461. (5:24-43). Surveillance data output from cameras 451, 452 and 461 is transmitted to data acquisition units 472, 474 and 476, respectively, and in turn transferred over the network 130 to surveillance server 210. (6:26-32). Milinusic describes configuring sensor units 250 and 260 to monitor a predetermined area, such as a warehouse interior area. (5:51-60; 6:59-67). Milinusic does not explicitly state where the sensor units 250 and 260 are placed to monitor the predetermined area. Milinusic describes conventional systems as being deficient in not being able to determine information about an intruder. (1:37-44). A POSA would have understood that the surveillance system of Milinusic would be effective in monitoring a structure such as a warehouse,

home or building for events such as an intruder. To detect the presence of an intruder and detecting information about an intruder (1:37-44), a POSA would have understood that it would be desirable to arrange the plurality of cameras on or around the structure (i.e., the house) to capture images of any intruders seeking to enter the house.

c. "[*B2*] each camera being associated with one or more of the motion detectors such that the camera has a field of view encompassing at least part of the field of view of any associated motion detector,"

147. The sensor units 250, 260 and 270 may be cameras, such as a digital camera or a video camera configured to be responsive to, for example, the visible light spectrum or infrared radiation (IR). (3:47-51). The camera in any of sensor units 250, 260, and 270 that includes a camera is coupled to the motion detector in any sensor unit configured as a motion detector (3:51-55) via the network (230 in FIG. 2 and 130 in FIG. 4).

148. Additionally, Milinusic describes cameras 451, 452 (within sensor unit 250) and 461 (within sensor unit 260) as being configured to capture an image of an area upon the occurrence of predetermined occurrences such as the detection of movement with the area being monitored by sensor units 250, 260, which a POSA would recognize requires a motion detector coupled to the camera. (5:51-59). Thus, Milinusic teaches that the cameras 451, 452, and 461 each may be coupled to a motion detector that monitors the same area as the

camera. Accordingly, a POSA would have understood that Milinusic discloses each camera being associated with one or more motion detectors.

149. Milinusic also describes image capture being set to occur upon the occurrence of predetermined occurrences, such as the detection of movement within the area being monitored by the sensor unit. (5:56-59). A POSA would have understood Milinusic teaching that a motion detector (whether within the same sensor unit 250, 260 or a different sensor unit) and cameras 451, 452 or 461 are arranged to monitor the same area, meaning that each of these cameras has a field of view encompassing at least part of the field of view of an associated motion detector.

d. "[*C*] providing a processor which controls the at least one camera and receives the image obtained by the at least one camera;"

150. Surveillance server 210 includes a central processing unit (CPU) 360. (4:14-16). A POSA would have understood that CPU 360 is a processor. Milinusic's surveillance server 210 receives requests from surveillance client 240 to control or adjust specified sensor units. (3:37-40). Surveillance server 210 transmits the requests to the specified sensor units 250, 260, 270 upon receiving the requests from the surveillance client 240. (3:40-41). A POSA would have understood that the CPU 360 of the surveillance server 210 is

arranged to control a camera in a sensor unit by transmitting requests received from the surveillance client 240 to the camera over the network (130 or 230).

151. Additionally, the CPU 360 of surveillance server 210 in Milinusic's system is configured to control the operation of the server so that surveillance data may be received from the various sensor units. (4:25-30). The surveillance data may include video data or still image data received from sensor units 250, 260, 270. (3:10-13). A POSA would have understood that the CPU 360 is arranged to receive images obtained by the cameras in the sensor units.

e. "[*D*] coupling a telecommunications module coupled to the processor, the telecommunications module being capable of communications over a telecommunications network; and"

152. Surveillance server 210 in Milinusic's system includes an input/output (I/O) processor 375 that provides an interface to the network. (4:16-23; FIG. 3). I/O processor 375 is coupled to CPU 360 via local interface 370. (FIG. 3). Network (230 in FIG. 2 and 130 in FIGs. 3-4) is described as a wide area network (WAN) such as the Internet or a local area network (LAN). (3:18-19). The Internet (or any WAN) is a telecommunications network under the BRI of that term, as discussed above in ¶24. Accordingly, a POSA would have understood that the system of Milinusic couples a telecommunications module (i.e., I/O processor 375) to the processor (i.e., CPU 360) and that the

telecommunications module is capable of communications over a telecommunications network (i.e., network 130/230).

f. "[*E*] transmitting commands from a handheld telecommunications unit to the processor via the telecommunications module to cause the processor to provide images to the telecommunications module to be transmitted to the telecommunications unit."

153. Surveillance system 100 of Milinusic includes a surveillance client 240 connected to the network (130 or 230). (2:63-65; FIGs. 2 and 4). Milinusic describes that the surveillance client 240 may be, for example, a general purpose computer, a personal computer or a personal digital assistant (PDA), such as a Palm Pilot. (3:33-35). A PDA is described in the '983 patent as an example of a handheld telecommunications unit. (Ex. 1001 at 5:67-6:6; 11:31-35 ("Thus, control over the activation and deactivation of the alarm system, as well as other adjustment to the alarm system, can now be performed using a handheld telecommunications unit 42, whether it is a cellular telephone or a camera telephone or a similar unit, such as a PDA.")). Laptop computers are also described in the '983 patent as examples of a handheld telecommunications unit. (Ex. 1001 at 5:67-6:6). Thus, the personal computer and PDA described by Milinusic as examples of surveillance client 240 meet the BRI of a handheld telecommunications unit as described in ¶25.

154. Surveillance client 240 of Milinusic is configured to allow a user to retrieve surveillance data by issuing a request to surveillance server 210. (3:34-37). The surveillance data may include video data and still image data. (3:12-13). Accordingly, a POSA would have understood that the system of Milinusic transmits commands from surveillance client 240, implemented as a PDA or a personal computer, to the processor (i.e., CPU 360 in surveillance server 210) via the telecommunications module (i.e., I/O processor 375) to cause the processor to provide images to the telecommunications module to be transmitted to surveillance client 240.

x. Claim 18: "The method of claim 11, further comprising programming the telecommunications module to receive commands from a handheld telecommunications unit over the telecommunications network to enable activation and deactivation of the motion detectors and cameras using the telecommunications unit."

155. Surveillance server 210 of Milinusic includes a central processing unit (CPU) 360, which is a processor. (4:14-16). Surveillance client 240 is configured to control or adjust specified sensor units by issuing requests to surveillance server 210. (3:37-40). A POSA would have understood that the most basic control of a sensor unit is to turn the sensor unit on or off (i.e., activate or deactivate the sensor unit). Accordingly, it would have been obvious to implement a command to activate/deactivate motion detectors and cameras in Milinusic's system. Additionally, Milinusic teaches that the sensor units may be

set to capture images at predetermined times or upon the detection of movement in the monitored area. (5:55-60). It would have been obvious to a POSA to implement surveillance client 240 to send a command to deactivate the motion detector and the camera monitoring an area when the camera monitoring that area is set to capture images at predetermined times (i.e., not continuous capturing of images), as neither the camera nor the motion detector is being used when images are not being captured (i.e., not at the predetermined times) and power consumed by the system can be reduced by not unnecessarily powering devices that are not in use. Additionally, it would have been obvious to a POSA to provide the ability for the user to send commands from a user input device to activate and deactivate the security system (including the motion detectors and the cameras) so that the system can be controlled remotely to turn it off and on as the user desires. This capability to remotely turn on and off a surveillance system with cameras and motion detectors was known in the art (*see e.g.*, Ex. 1002 (Lee) [0087] ("The system 10 receives user command signals from the remote controller 281 to control at least one of the plurality of remote devices or the system 10 … the user may program the system to turn on or off the system using the remote controller.")) and a POSA would have understood the benefits of providing that capability in the Milinusic system (e.g., to allow a user to

remotely turn off the system before cleaning people enter the building and then turn it back on after they depart).

xi. Claim 19: "The method of claim 11, wherein the processor is arranged to receive, via the telecommunications module, one of a plurality of different code numbers from the telecommunications unit and control the at least one camera and the at least one motion detector in accordance with the received code number."

156. Surveillance client 240 is configured to control or adjust sensor units by issuing requests to surveillance server 210. (3:37-40). Surveillance client 240 and surveillance server 210 are connected via network 230, which is described as a wide area network (WAN), such as the Internet, or a local area network (LAN). (3:18-19; FIG. 2). Milinusic does not explicitly describe CPU 360 receiving one of a plurality of code numbers from surveillance client 240. A POSA would have understood that commands sent from surveillance client 240 would include numbers, text, or some combination of numbers and text, and implementing the commands using code numbers for different commands would have been an obvious design choice. A POSA would have further understood that a plurality of code numbers would be used, each corresponding to different particular command input by a user into the surveillance client 240 to enable the surveillance server 210 to determine which of the specified sensor units to control and how to control the specified sensor unit.

157. As discussed above in connection with claim 18, it would have been obvious to a POSA that the ability Milinusic discloses for the surveillance client 240 to control or adjust sensor units includes the ability to control or adjust the components that can be included in a sensor unit, including motion detectors and cameras (3:37-40; 3:51-55; 5:51-55; FIG. 4), and that different command and control actions require different code numbers to identify the action desired by the user. In addition, Milinusic teaches that the sensor units may be set to capture images at predetermined times or upon the detection of movement in the monitored area, and a POSA would have understood that code numbers can be provided to allow the camera to be controlled to configure it to capture images at predetermined times or upon the detection of movement in the monitored area. (5:55-60).

158. As discussed in connection with claim 18, it would have been obvious to a POSA to implement surveillance client 240 to send commands to activate/deactivate the motion detector and the camera monitoring an area when the camera monitoring that area is set to capture images at predetermined times as neither the motion detector nor the camera is being used when images are not being captured and power consumed by the system can be reduced by not unnecessarily powering devices that are not in use. Additionally, it would have been obvious to a POSA to provide the ability for the user to send commands

from the user input device to activate and deactivate the security system (including the motion detectors and cameras) so that the system can be controlled remotely to turn it off and on as the user desires. This capability to remotely turn on and off a surveillance system with cameras and motion detectors was known in the art (*see e.g.*, Ex. 1002 (Lee) at [0087] ("The system 10 receives user command signals from the remote controller 281 to control at least one of the plurality of remote devices or the system 10 … the user may program the system to turn on or off the system using the remote controller.")) and a POSA would have understood the benefits of providing that capability in the Milinusic system (e.g., to allow a user to remotely turn off the system before cleaning people enter the building and then turn it back on after they depart).

xii. Claim 20: "The method claim 19, wherein one of the code numbers is to cause the processor to cause images to be provided by the processor to the telecommunications module and transmitted to the telecommunications unit."

159. As discussed in ¶154, surveillance client 240 of Milinusic is configured to allow a user to retrieve surveillance data by issuing a request to surveillance server 210. (3:34-37). The surveillance data may include video data and still image data. (3:12-13). Accordingly, a POSA would have understood that surveillance client 240, implemented as a PDA or a personal computer, is a handheld communications unit for transmitting commands for the processor (i.e., CPU 360 in surveillance server 210) via the telecommunications module (i.e.,

I/O processor 375) to cause the processor to provide images to the telecommunications module to be transmitted to surveillance client 240. A POSA would have further understood that such commands are implemented as code numbers. (see ¶156).

D. Ground 4: Claims 9, 10, and 12-17 of the '983 Patent are Obvious in view of Milinusic, Osann, and Ozer.

160. As discussed above, I have been informed by counsel that Milinusic, Osann, and Ozer each meets the requirements to be prior art to the '983 patent.

161. After reviewing Milinusic, Osann, and Ozer, and claims 9, 10, and 12-17 of the '983 patent, it is my opinion that every one of these claims would have been obvious to a POSA in view of Milinusic, Osann, and Ozer. The basis for my opinion and the details of my analysis are below.

ii. Claim 9: "The system of claim 1, wherein said processor is further arranged to derive a silhouette of any objects in the image, compare the silhouettes to a library of stored silhouettes having associated object identification to determine an exact or closest match of the derived silhouette to one of the stored silhouettes and retrieve the object identification associated with the exact or closest match, said processor being arranged to react to the detection of motion by said at least one motion detector based on the object identification."

162. Milinusic teaches that the system can detect predetermined conditions, generate surveillance data representative of the detected condition

and distribute surveillance data to a surveillance client based upon predetermined distribution criteria. (3:3-5; 3:64-4:1; 4:30-34)[5]. A POSA would have understood that the distribution of data to a surveillance client upon detection of a condition is an alarm that notifies the client of the condition, and that the condition may be detection of an intruder. In addition, Osann explicitly describes generating an alarm upon the occurrence of an event such as detecting an intruder (Ex. 1004 (Osann) at 14:4-20), which would have provided further motivation for a POSA to have the Milinusic system generate an alarm upon detection of a condition such as an intruder.

163. The combination of Milinusic and Osann does not teach that object identification is performed before generating an alarm that notifies the user that an intruder has been detected. It would have been obvious to a POSA to modify the combined system of Milinusic and Osann to implement the object identification technique of Ozer to make the system more accurate by reducing the number of "false alarms" that may occur when the user is alerted by motion not caused by an object of interest (i.e., an intruder) but rather by other motion (e.g., a pet's movements), as specifically taught by Ozer. (Ex. 1005 (Ozer) at [0054]).

[5] Unless otherwise indicated, all citations in §D(¶¶160-179) are to Ex. 1003 (Milinusic).

164. Ozer describes that it was known to compare objects in an image to silhouette templates to identify, among other objects, a human in the image being monitored. (Ex. 1005 (Ozer) at [0011]). The system of Ozer generates silhouettes of an object in an image to both classify objects (e.g., humans or dogs) in the image and to recognize a wide variety of activities. (Ex. 1005 (Ozer) at [0026]-[0027]; [0052]; [0053]-[0054]; [0064]). By identifying objects in the image, the system is more accurate because it rejects many elements in the area being monitored that may be moving, but are not objects of interest. (Ex. 1005 (Ozer) at [0054]). Ozer's system determines an object model describing the shape of the object. (Ex. 1005 (Ozer) at [0061]-[0063]). As discussed above in ¶26, the BRI of "silhouette" includes at least a representation of the contours of an object derived based on a number of descriptors that are typical for the object (e.g., human body), or on other factors which can be used to distinguish, discriminate and/or differentiate different objects, including distinguishing animals from humans. The object model of Ozer is derived using descriptors that are typical for a human body (e.g., hands head, torso). (Ex. 1005 (Ozer) at [0052]). A POSA would have understood that the object model of Ozer is a silhouette. Ozer describes using a graph matching process to compare the determined object model with a set of stored models. (1005 (Ozer) at [0064]). A POSA would have understood Ozer's object model to be a silhouette (indeed

Ozer specifically refers to it as such), and Ozer's identification of objects (such as a human body) by matching the object model with reference models to be determining a closest match between the derived silhouette of the object and a silhouette in the set of stored silhouettes. (1005 (Ozer) at [0026]-[0027]; [0029]; [0034]; and [0064]).

165. It would have been obvious to a POSA to have modified the combined system of Milinusic and Osann to implement the object identification technique of Ozer that generates a silhouette of an object in an image and compares the generated silhouette to a set of stored silhouettes to identify the object.

166. A POSA would have implemented the combined system by using the silhouette object identification technique of Ozer in the combined Milinusic/Osann system by having the CPU 360 in surveillance server 210 of Milinusic identify the object (e.g., as human or not) that was detected as moving by the motion detector, and reacting to the detection of motion by the motion detector based on the object identification by distributing data to surveillance client 240 or generating another type of alarm upon the occurrence of an event when the object is determined to be a human, and by not doing so when the objected detected is not a human (e.g., a pet) to reduce false alarms as taught by Ozer. (Ex. 1005, (Ozer) at [0054]).

ii. Claim 10. The system of claim 9, wherein said at least one motion detector comprises a plurality of motion detectors and said at least one camera comprises a plurality of cameras, at least one of said cameras being associated exclusively with each of said motion detectors, at least two of said cameras are associated exclusively with each of said motion detectors or at least two of said cameras are associated non-exclusively with each of said motion detectors, wherein when at least two of said cameras are associated with one of said motion detectors, each of said at least two cameras has a dormant state in which imaging is not performed and images are not obtained and an active state in which images are obtained, said at least two cameras all being activated from the dormant state into the active state when the associated one of said motion detectors detects motion in its field of view such that said at least two cameras obtain images of the source of the motion detected by the associated one of said motion detectors, and said processor being arranged to analyze images from said at least two cameras to determine depth information about a common object appearing in the images from said at least two cameras which may be the source of the motion, the depth information being used in the object identification being performed by the processor and indicating a distance between the structure and the object, said processor being arranged to react to the detection of motion by said at least one motion detector based on the object identification and based on the distance between the structure and the object."

167. Milinusic's surveillance system 100 includes a plurality of sensor units 250, 260, 270 configured to collect surveillance data by detecting predetermined conditions or occurrences. (3:41-45; 5:24-64; FIG. 2; FIG. 4). FIG. 4 shows sensor unit 250 as including cameras 451 and 452 and sensor unit 260 as including camera 461. (5:24-43). The camera in any of sensor units 250, 260, and 270 that includes a camera may be coupled to the motion detector in

any sensor unit configured as a motion detector. (3:51-55). Claim 10 recites three alternative ways in which a system including multiple cameras and motion detectors can be arranged, and requires that the claimed system meet one of these alternatives. A POSA would have understood that for claim 10 to be met by a system, only one of the alternatives need be present. I have been informed by counsel that this understanding is correct.

168. While the language in claim 10 is far from a model of clarity, I understand from counsel that it must be interpreted in view of the '983 specification, which describes three ways in which a plurality of cameras and motion detectors can be arranged. The first arrangement is that there is "a 1:1 correspondence or association between motion detectors and cameras, i.e., each motion detector has a single and exclusive camera whose field of view encompasses the field of view of the motion detector." (Ex. 1001 at 3:63-66). A second arrangement involves a motion detector being associated with two or more cameras and being the "exclusive" motion detector for those cameras. (Ex. 1001 at 3:67-4:9). A third arrangement involves a camera being associated with two or more motion detectors so that it obtains an image when any of its associated detectors detects motion. (Ex. 1001 at 4:7-12). Claim 10 describes these three arrangements in the alternative, using the word "or," and requires a system that meets at least one of them.

169. Milinusic does not explicitly state whether the sensor units 250, 260 include the motion detectors within the same sensor units as the cameras, or whether the motion detectors are provided in separate sensor units coupled to the cameras via the network. A POSA would have understood that either option would be an obvious design choice, and that either option would include a motion detector coupled to the camera. Additionally, Osann explicitly shows an integrated unit that includes a camera and a sensor associated exclusively in a 1:1 correspondence. (Ex. 1004 (Osann) at 15:58-60; FIG. 28 ("extension unit 82 has both motion detector 85 and video camera 86 attached and also includes a circuit for controlling exterior light 87.")). It would have been obvious to a POSA to arrange a camera and motion detector in Milinusic's system in a 1:1 correspondence in an integrated unit as taught by Osann to provide the ability to capture surveillance data with a camera and to trigger the image capture with a motion detector monitoring the same area.

170. Claim 10 includes additional limitations related to determining depth information about a common object appearing in images from at least two cameras "when at least two of said cameras are associated with one of said motion detectors." These limitations do not apply to the first arrangement of cameras and motion detectors in a 1:1 correspondence which is taught by the combined system of Milinusic and Osann and that I rely upon to demonstrate the

obviousness of claim 10 over the combination of Milinusic, Osann, and Ozer, and thus no further discussion of these limitations is necessary to demonstrate that claim 10 is obvious over the combination of Milinusic, Osann, and Ozer. I have been informed by counsel that this understanding is correct.

iii. Claim 12: "The method of claim 11, wherein the processor further derives a silhouette of any objects in the image, compares the silhouettes to a library of stored silhouettes having associated object identification to determine an exact or closest match of the derived silhouette to one of the stored silhouettes and retrieves the object identification associated with the exact or closest match, further comprising generating a countermeasure to the detection of motion by the motion detectors based on the object identification when the object is identified as a potential threat to the structure."

171. See analysis of claim 9. As discussed therein, in the combination a POSA would have implemented, the combined system would use the silhouette object identification technique of Ozer in the combined system of Milinusic and Osann by having the CPU 360 in surveillance server 210 of Milinusic identify the object (e.g., as human or not) that was detected as moving by the motion detector, and reacting to the detection of motion by the motion detector based on the object identification by distributing data to surveillance client 240 or generating another type of alarm upon the occurrence of an event when the object is determined to be a human, and by not doing so when the objected detected is not a human (e.g., a pet) to reduce false alarms as taught by Ozer.

(Ex. 1005 (Ozer) at [0054]). The generation of an alert and the triggering of the camera to capture an image of a monitored area upon the detection of movement in the area are both countermeasures the system would generate when the object is identified as a potential threat (e.g., identified as potential intruder). As discussed above, the alert can include distribution of data to a client device upon detection of a condition as taught by Milinusic (3:3-5; 3:64-4:1; 4:30-34) and generating an alarm upon the occurrence of an event such as detecting an intruder as taught by Osann (Ex. 1004 (Osann) at 14:4-20). These are consistent with the countermeasures described in the '983 patent which include "a message or warning is sent to a distant computer" or "the property owner's homepage ." (Ex. 1001 at 3:30-38).

iii. Claim 13: "The method of claim 12, wherein each camera is associated with only a single motion detector, each camera is associated with a plurality of motion detectors, or, multiple cameras are associated with each motion detector, wherein when a plurality of cameras are associated with one of the motion detectors, images from the plurality of cameras are analyzed by the processor to determined depth information about an object appearing in the images, the depth information being used in the object identification being performed by the processor."

172. Milinusic's surveillance system 100 includes a plurality of sensor units 250, 260, 270 configured to collect surveillance data by detecting predetermined conditions or occurrences. (3:41-45; 5:24-64; FIG. 2; FIG. 4). FIG. 4 shows sensor unit 250 as including cameras 451 and 452 and sensor unit

260 as including camera 461. (5:24-43). The camera in any of sensor units 250, 260, and 270 that includes a camera may be coupled to the motion detector in any sensor unit configured as a motion detector (3:51-55) via the network (230 in FIG. 2 and 130 in FIG. 4). Claim 13 recites three alternative ways in which a system including cameras and motion detectors can be arranged, and requires that the claimed system meet one of these three alternatives. A POSA would have understood that for claim 13 to be met by a system, only one of the alternatives in the list need be present. I have been informed by counsel that this understanding is correct.

173. The '983 specification describes three ways in which a plurality of cameras and motion detectors can be arranged. The first arrangement is that there is "a 1:1 correspondence or association between motion detectors and cameras, i.e., each motion detector has a single an exclusive camera whose field of view encompasses the field of view of the motion detector." (Ex. 1001 at 3:63-66). A second arrangement involves a motion detector being associated with two or more cameras and being the "exclusive" motion detector for those cameras. (Ex. 1001 at 3:67-4:9). A third arrangement involves a camera being associated with two or more motion detectors so that it obtains an image when any of its associated detectors detects motion. (Ex. 1001 at 4:7-12). Claim 13

describes these three arrangements in the alternative, using the word "or," and requires a system that meets at least one of them.

174. Milinusic does not explicitly state whether the sensor units 250, 260 include the motion detectors within the same sensor units as the cameras, or whether the motion detectors are provided in separate sensor units coupled to the cameras via the network. A POSA would have understood that either option would be an obvious design choice, and that either option would include a motion detector coupled to the camera. Additionally, Osann explicitly shows an integrated unit that includes a camera and a sensor associated exclusively in a 1:1 correspondence. (Ex. 1004 (Osann) at 15:58-60 ("extension unit 82 has both motion detector 85 and video camera 86 attached and also includes a circuit for controlling exterior light 87.")). It would have been obvious to a POSA to arrange a camera and motion detector in Milinusic's system in a 1:1 correspondence in an integrated unit as taught by Osann to provide the ability to capture surveillance data with a camera and to trigger the image capture with a motion detector monitoring the same area.

175. Claim 13 includes additional limitations related to determining depth information about a common object appearing in images from at least two cameras "when at least two of said cameras are associated with one of said motion detectors." These limitations do not apply to the first arrangement of

cameras and motion detectors in a 1:1 correspondence which is taught by the combined system of Milinusic and Osann and that I rely upon to demonstrate the obviousness of claim 10 over the combination of Milinusic, Osann, and Ozer, and thus no further discussion of these limitations is necessary to demonstrate that claim 13 is obvious over the combination of Milinusic, Osann, and Ozer. I have been informed by counsel that this understanding is correct.

iv. Claim 14: "The method of claim 12, further comprising assigning a classification of "no threat" or "hostile" based on the object identification and/or the size of the object, the countermeasure being generated only when the classification is hostile."

176. As discussed in connection with claim 9, in the obvious combination of Milinusic, Osann, and Ozer that a POSA would have implemented , the combined system would use the silhouette object identification technique of Ozer in the combined system of Milinusic and Osann by having the CPU 360 in surveillance server 210 of Milinusic identify the object (e.g., as human or not) that was detected as moving by the motion detector, and reacting to the detection of motion by the motion detector based on the object identification by distributing data to surveillance client 240 or generating another type of alarm upon the occurrence of an event when the object is determined to be a human, and by not doing so when the objected detected is not a human (e.g., a pet) to reduce false alarms as taught by Ozer.

(Ex. 1005, (Ozer) at [0054]). The generation of an alert and the triggering of the camera to capture an image of a monitored area upon the detection of movement in the area are both countermeasures the system generate when the object is identified as a potential threat or hostile (e.g., identified as a potential intruder) and would not generate when the object is classified as being no threat (e.g., a pet). As discussed above, the alert can include distribution of data to a client device upon detection of a condition as taught by Milinusic (3:3-5; 3:64-4:1; 4:30-34) and generating an alarm upon the occurrence of an event such as detecting an intruder as taught by Osann (Ex. 1004 (Osann) at 14:4-20). These are consistent with the countermeasures described in the '983 patent which include "a message or warning is sent to a distant computer" or "the property owner's homepage ." (Ex. 1001 at 3:30-38).

v. Claim 15: "The method of claim 12, wherein the step of generating a countermeasure includes generate an audible and/or visual alarm in proximity to the structure or generating at least one communication about the condition of the structure based on the object identification and forwarding the communication to a remote destination."

177. As discussed in connection with claim 14, in the obvious combination of Milinusic, Osann, and Ozer that a POSA would have implemented, the combined system would use the silhouette object identification technique of Ozer in the combined system of Milinusic/Osann by having the CPU 360 in surveillance server 210 of Milinusic identify the object (e.g., as

human or not) that was detected as moving by the motion detector, and reacting to the detection of motion by the motion detector based on the object identification by distributing data to surveillance client 240 or generating another type of alarm upon the occurrence of an event when the object is determined to be a human, and by not doing so when the objected detected is not a human (e.g., a pet) to reduce false alarms as taught by Ozer. (Ex. 1005, (Ozer) at [0054]). The generation of an alert and the triggering of the camera to capture an image of a monitored area upon the detection of movement in the area are both countermeasures the system generate when the object is identified as a potential threat or hostile (e.g., identified as a potential intruder) and would not generate when the object is classified as being no threat (e.g., a pet). As discussed above, the alert can include distribution of data to a client device upon detection of a condition as taught by Milinusic (3:3-5; 3:64-4:1; 4:30-34) and generating an alarm upon the occurrence of an event such as detecting an intruder as taught by Osann (Ex. 1004 (Osann) at 14:4-20). In particular, Osann describes that video may be transmitted to a security company or the police, which is a remote location (Ex. 1004 (Osann) at 14:6-14 ("Given the inconvenience and expense of false alarms, the distributed video capability of this invention … could allow a Security Company or even the Police to view inside and around the home or building in the case of an alarm being set off, so

that a "false alarm" condition can be determined without having to visit the location.")). It would have been obvious to a POSA to have such a communication sent in the combined system of Milinusic, Osann, and Ozer so police or security personnel can be alerted and respond to a potential threat from an intruder if the user is not home or unwilling to investigate the potential threat on their own.

vi. Claim 16: "The method of claim 15, wherein the remote destination is a police station, a first station, a terminal monitored by an owner of the structure, or a private security station."

178. See analysis for claim 15. As described therein, the alert in the combined system of Milinusic, Osann, and Ozer can include the CPU 360 in surveillance server 210 of Milinusic identifying the object (e.g., as human or not) that was detected as moving by the motion detector, and reacting to the detection of motion by the motion detector based on the object identification by transmitting video to a remote location which is a security company or the police. (Ex. 1004 (Osann) at 14:6-14 ("Given the inconvenience and expense of false alarms, the distributed video capability of this invention … could allow a Security Company or even the Police to view inside and around the home or building in the case of an alarm being set off, so that a "false alarm" condition can be determined without having to visit the location.")). Additionally, as discussed in connection with claim 15, Milinusic describes distributing data to a

surveillance client 240 when an event is detected. A POSA would have understood surveillance client 240 to be a terminal monitored by the owner of the structure under the plain and ordinary meaning of "terminal" as "any device that terminates one end (sender or receiver) of a communicated signal." (Ex. 1009).

vi. Claim 17: "The method of claim 15, further comprising including one or more images obtained from the cameras or one or more images derived from the images obtained from the cameras in the communication being forwarded to the remote destination."

179. In the combined system, the communication forwarded to a remote destination can include video data (i.e., images) from one or more cameras. (Ex. 1004 (Osann) at 14:6-14 ("Given the inconvenience and expense of false alarms, the distributed video capability of this invention … could allow a Security Company or even the Police to view inside and around the home or building in the case of an alarm being set off, so that a "false alarm" condition can be determined without having to visit the location.")).

VII. SIGNATURE

180. I hereby declare that all statements made in this declaration of my own personal knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements are made with the knowledge that willful false statements and the like are punishable by fine, imprisonment, or both, under Section 1001 of Title 18 of the U.S. Code.

Executed on: 11/14/2015

Tal Lavian

11/14/2015

Tal Lavian, Ph.D.

Appendix A: Claim chart for U.S. 7,864,983 – Ground 1: Obviousness over Lee

‘983 CLAIMS	**LEE**
1. An alarm system for protecting a structure, comprising:	Surveillance and security device (“S&S device”) 212 includes a camera module 920 and sensor modules 930 and 940, which modules may be “installed in the necessary sites inside and outside the house.” [0103]-[0105]. When the S&S device 212 has been triggered, the user is alerted and a text message corresponding to the nature of the unusual event information sensed by the sensors in the system is sent to a display device 50 to inform the user which sensor was triggered. [0111].
[*A*] at least one motion detector arranged to have a field of view external of the structure and including an area proximate the structure;	Camera module 920 includes a sensor 923. [0104]. Sensor module 930 also includes a sensor 931 [0104]. The sensors include motion sensors. [0110]. The camera module(s) 920 and the sensor module(s) may be installed outside a house as well as inside. [0105]. A POSA would have arranged the motion sensors in modules 920 and 930 to each have a field a view external of the structure to include an area proximate the structure. (see obviousness analysis above this claim chart).
[*B1*] at least one camera associated with and coupled to each of said at least one motion detector,	S&S device 212 includes a plurality of camera modules 920 that each includes a surveillance camera 922 coupled to a sensor 923 (which may be a motion detector), and where the camera can be activated to record images when the motion detector is triggered. [0108]; [0110]-[0111]; FIG. 9.
[*B2*] each of said at least one camera being arranged relative to the associated one of said at least one motion detector such that said	S&S device 212 includes motion sensors and cameras that can be activated when an associated motion sensor is triggered [0111]. Camera module 920 includes a sensor (which can be a motion detector) 923 being disposed in the same module as the associated camera 922. ([0104]; FIG. 9). Cameras and motion detectors are “installed in

camera has a field of view encompassing at least part of the field of view of the associated one of said at least one motion detector,	correspondence to a place to be monitored for detecting information about [an] intruder." [0028]. A POSA would understand that the camera and sensor in the same module "installed in correspondence to a place to be monitored" would be arranged to monitor the same "place" by having fields of view that both encompass that "place." Alternatively, it was known to have overlapping fields of view between a camera and a motion detector that activates it, and a POSA would have arranged at least one of the cameras to have a field of view that encompasses at least part of the field of view of a motion detector that activates it. (see obviousness analysis above this claim chart).
[*B3*] each of said at least one camera having a dormant state in which images are not obtained and an active state in which images are obtained and being activated into the active state when the associated one of said at least one motion detector detects motion;	S&S device 212 can be set to operate in three different modes – an "ON mode," an "OFF mode," and an "INTERRUPT mode." [0107]. When S&S device 212 is in "INTERRUPT mode," the camera is off unless and until a trigger signal is received indicating that the presence of an intruder has been detected by a sensor [0107]-[0108]. The camera is said to be "activated" when the sensor 923 is triggered. [0111]. Video data is transmitted to a main control unit 100 when the security system has been triggered [0111]. A POSA would have understood that when the camera of Lee is "on" it is obtaining images, and when the camera of Lee is "off" it is not obtaining images. (see obviousness analysis above this claim chart).
[*C*] a processor coupled to said at least one camera and arranged to control said at least one camera and receive the	Main control unit 100 that includes a microprocessor 150. [0069]. The microprocessor 150 is connected to a power line communication module 101 over a bus. [0069]. Power line communication module 101 is coupled to camera 922 via power line 200 and camera

image obtained by said at least one camera;	interface 921 (FIGS. 2 and 9). Accordingly, microprocessor 150 is coupled to camera 922. Processor 150 is arranged to send control data via the power line communication network 200 to various aspects of S&S device 212 including camera 922 [0057]-[0058]. Processor 150 can control the camera 922 in the camera module 920 to, for example, allow the user to select the "ON mode," "OFF mode," or "INTERRUPT mode" ([0107]) via the main control unit 100 and its processor 150. ([0071]; [0057]-[0058]). Main control unit 100, including microprocessor 150, receives surveillance data (e.g., images) from the camera in S&S device 212. [0108].
[*D*] a telecommunications module coupled to said processor, said telecommunications module being capable of communications over a telecommunications network; and	Main control unit 100 has a microprocessor 150 and multiple types of communication interfaces to communicate with user input devices. (FIG. 1). The communications interfaces include an RF/wireless interface 190 ([0067]), a telephone line interface (e.g., Public Switched Telephone Network (PSTN) 292) ([0062]), and a computer network (e.g., local area network (LAN)/Internet 290) interface. (FIG. 1;[0062]). Lee also discloses that there is an interface (not shown in FIG. 1) for connecting to the cell phone 283 and an interface (not shown in FIG. 1) for connecting to the PDA 282. [0060].
[*E*] a handheld telecommunications unit for transmitting commands for said processor via said telecommunications module to cause said processor to provide images to said telecommunications	Lee describes several types of user input devices for sending control commands to main control unit 100 including wireless PDA 282, cell phone 283, and remote computer 291. [0059]. A user may program the system via on-screen program menus displayed on any of the user input devices. [0064]. Commands that can be transmitted from the user input devices to the main control unit 100, include a command to set the main control unit 100 to a different mode, a

module to be transmitted to the telecommunications unit.	command to switch the camera in S&S device 212 on or off, a command to place the camera in S&S device 212 in standby mode, and a command to turn the system on or off. [0060]; [0087]. Remote computer 291 is connected to the main control unit 100 over a network 290 (e.g., the Internet or PSTN), which are telecommunications networks. Remote computer 291includes application software that enables the remote computer to both receive video data from the system and send control data to the system. [0062]. Wireless PDA 282 and cell phone 283 communicate with the main control unit 100 through interfaces that are not shown in FIG. 1 of Lee. [0060]. It would have been obvious to a POSA to implement wireless PDA 282 and/or cell phone 283 transmit commands to cause the main control unit to transmit images to the wireless PDA 282 and/or cell phone 283. (see obviousness analysis above this claim chart).
2. The alarm system of claim 1, wherein said processor is coupled to said at least one motion detector and said telecommunications unit is also arranged to transmit commands for said processor to activate and deactivate said at least one motion detector.	S&S device 212 is controllable via user input devices such as remote controller 281, wireless PDA 282, cell phone 283, and remote computer 291. [0062]; [0064]; [0065]. A POSA would have understood that the most basic form of control for S&S device 212 is the ability to turn the device (including its motion detectors and cameras) on and off. (see obviousness analysis above this claim chart). Additionally, Lee describes sending command signals to change the setting mode of the S&S device 212 between ON, OFF, and INTERRUPT modes ([0107]), which controls the motion detector (e.g., by having it trigger activation of the camera in INTERRUPT mode but not in the other modes). Additionally, among the functions of the system that are controllable, a user can send command signals to turn on or off the S&S device 212, which includes motion

	detectors. [0087]; [0110]. A POSA would have understood that a command to turn on or off S&S device 212 would turn on or off (i.e., activate/deactivate) all components of the S&S device 212 including any motion detectors included as part of S&S device 212. (see obviousness analysis above this claim chart).
3. The alarm system of claim 1, wherein in said dormant state of each of said at least one camera, imaging by said camera is not performed and images are not obtained, each of said at least one camera being automatically activated from the dormant state into the active state when the associated one of said at least one motion detector detects motion in its field of view.	S&S device 212 can be set to operate in three different modes – an "ON mode," an "OFF mode," and an "INTERRUPT mode." [0107]. When S&S device 212 is in "INTERRUPT mode," the camera is off unless and until a trigger signal is received indicating that the presence of an intruder has been detected by a sensor [0107]-[0108]. The camera is said to be "activated" when the sensor 923 is triggered. [0111]. Video data is transmitted to a main control unit 100 when the security system has been triggered [0111]. A POSA would have understood that when the camera of Lee is when the camera of Lee is "off" imaging by the camera is not performed and it is not obtaining images. A POSA would have also understood that when the camera receives a trigger signal from an associated sensor the camera is automatically activated from the dormant state into the active state. (see obviousness analysis above this claim chart).
4. The alarm system of claim 1, wherein said telecommunications unit is one of a camera telephone, a cellular telephone and an Internet-enabled picture and/or video display device.	Cell phone 283 is a telecommunications unit (see claim 1[E]). [0059]. Alternatively, remote computer 291, is a telecommunications unit (see claim 1[E]), communicates with the main control unit 100 via an "external Internet network" and has the ability to display pictures and video. [0062]. Accordingly, remote computer 291 is an Internet-enabled picture and/or video display device.
5. The alarm system of claim 1, wherein said processor is	Control signals are sent to main control unit 100 from, among other devices, a cell phone 283, wireless PDA 282, and remote computer 291. [0060]; [0062]. The

arranged to receive, via said telecommunications module, one of a plurality of different code numbers from said telecommunications unit and control said at least one camera and said at least one motion detector in accordance with the received code number.	control signals include control signals for controlling S&S device 212. [0064-]-[0065]. A user device locally or via the Internet can be used to change the setting mode of S&S device 212 between ON, OFF, and INTERRUPT modes. [0107]. S&S device 212 includes a camera and a motion detector as discussed in connection with claim 1[A] and 1[B1]. Changing the setting mode of the S&S device 212 controls both the camera (e.g., by turning it on or off) and the motion detector (e.g., by having it trigger activation of the camera in the INTERRUPT mode but not in the other modes). A user device may also send a command to turn on or off Lee's system, which includes S&S device 212. [0087]. Turning on or off the system controls both the camera (e.g., by turning it on or off) and the motion detector (e.g., by turning it on or off). A POSA would have understood that a command sent from a user input device to control S&S device 212, to change the mode of the S&S device 212 and a command sent from a user input device to turn on/off the system includes one of a plurality of code numbers to control the camera(s) and the motion sensor(s) in the S&S device 212, and is received via a telecommunication module. (see obviousness analysis above this claim chart).
6. The alarm system of claim 5, wherein one of the code numbers is to cause said processor to cause images to be provided by said processor to said telecommunications module and transmitted to the telecommunications	Lee describes several types of user input devices for sending control commands to main control unit 100 including wireless PDA 282, cell phone 283, and remote computer 291. [0059]. It would have been obvious to a POSA to transmit images to any of the user input devices that include the ability to display images in response to a command from the user input device to provide the images. [0059]; FIG 1. A POSA would have further understood that such commands are implemented as code numbers. (see obviousness analysis above this claim chart).

unit.	
7. The alarm system of claim 5, wherein one of the code numbers is to cause said processor to direct said at least one camera to provide images to said processor and then cause the provided images to be forwarded by said processor to said telecommunications module and transmitted to the telecommunications unit.	Lee describes several types of user input devices for sending control commands to main control unit 100 including wireless PDA 282, cell phone 283, and remote computer 291. [0059]. A user device locally or via the Internet can be used to change the setting mode of the S&S device 212 between ON, OFF, and INTERRUPT modes. [0107]. When the user device sends a command to set the S&S device 212 to the "ON mode" the "camera 922 is on non-stop working state." [0107]. A user can watch live images on the LCD display to monitor the home or building by surveillance camera 922. [0112]. It would have been obvious to a POSA to transmit live images to a user input device that includes the ability to display images, including PDA 282 and cell phone 283 in response to a command to turn the S&S device 212 on. [0059]; FIG 1. A POSA would have further understood that such a command is implemented as code numbers. A POSA would have also understood that a command to turn the camera in S&S device 212 on is a command to direct the camera to provide live images to the processor and then cause the provided live images to be forwarded by the processor to said telecommunications module and transmitted to the user input device when the user input device includes the ability to display images. (see obviousness analysis above this claim chart).
8. The system of claim 1, wherein said at least one motion detector comprises a plurality of motion detectors, said at least one camera associated with said at least one motion detector being arranged	S&S device 212 includes an unlimited number of modules - including camera module 920 and sensor modules 930 and 940 - that may be "installed in the necessary sites inside and outside the house." [0103]-[0105]. Some sensors (e.g., sensor 923) are associated with a camera in a common module (i.e., camera module 920), whereas other sensors (e.g., sensor 931) are not

to have a field of view overlapping a field of view of a plurality of said motion detectors.	associated with a camera in a common module (i.e., sensor module 930). FIG. 9. Surveillance cameras, such as 922, can be activated when any of the sensors, such as sensor 923 is triggered. [0111]. It would have been obvious to a POSA to implement Lee by including one or more cameras each having an overlapping field of view with multiple motion detectors. (see obviousness analysis above this claim chart).
11. A method for protecting a structure, comprising:	S&S device 212 includes a camera module 920 and sensor modules 930 and 940, which modules may be "installed in the necessary sites inside and outside the house." [0103]-[0105].
[*A*] arranging a plurality of motion detectors on or around the structure, each in a position in which its field of view includes an area proximate the structure;	Camera module 920 includes a sensor 923. [0104]. Sensor module 930 also includes a sensor 931 [0104]. The sensors include motion sensors. [0110]. The camera module(s) 920 and the sensor module(s) may be installed outside a house as well as inside. [0105]. A POSA would have arranged the motion sensors in modules 920 and 930 to each have a field a view including an area proximate the structure. (see obviousness analysis above this claim chart).
[*B1*] arranging a plurality of cameras on or around the structure,	The system of Lee includes a plurality of camera modules 920 that each includes a surveillance camera 922. [0104]; FIG. 9. The camera module(s) 920 and the sensor module(s) may be installed outside a house as well as inside. [0105]. A POSA would have arranged the plurality of camera modules 920 on or around the house, which is a structure. (see obviousness analysis above this claim chart).
[*B2*] each camera being associated with one or	S&S device 212 includes motion sensors and cameras that can be activated when an associated motion sensor is

more of the motion detectors such that the camera has a field of view encompassing at least part of the field of view of any associated motion detector,	triggered [0111]. Camera module 920 includes a sensor (which can be a motion detector) 923 being disposed in the same module as the associated camera 922. ([0104]; FIG. 9). Cameras and motion detectors are "installed in correspondence to a place to be monitored for detecting information about [an] intruder." [0028]. A POSA would have understood that the camera and sensor in the same module "installed in correspondence to a place to be monitored" would be arranged to monitor the same "place" by having fields of view that both encompass that "place." Alternatively, it was known to have overlapping fields of view between a camera and a motion detector that activates it, and a POSA would have arranged at least one of the cameras to have a field of view that encompasses at least part of the field of view of a motion detector that activates it. (see obviousness analysis above this claim chart).
[*C*] providing a processor which controls the at least one camera and receives the image obtained by the at least one camera;	Main control unit 100 that includes a microprocessor 150. [0069]. Processor 150 is arranged to send control data via the power line communication network 200 to various aspects of S&S device 212 including camera 922 [0057]-[0058]. Processor 150 can control the camera 922 in the camera module 920 to, for example, allow the user to select the "ON mode," "OFF mode," or "INTERRUPT mode" ([0107]) via the main control unit 100 and its processor 150. ([0071]; [0057]-[0058]). Main control unit 100, including microprocessor 150, receives surveillance data (e.g., images) from the camera in S&S device 212. [0108].
[*D*] coupling a telecommunications module coupled to the processor, the telecommunications module being capable of communications	Main control unit 100 has a microprocessor 150 and multiple types of communication interfaces to communicate with user input devices. (FIG. 1). The communications interfaces include an RF/wireless interface 190 ([0067]), a telephone line interface (e.g., Public Switched Telephone Network (PSTN) 292) ([0062]), and a computer network (e.g., local area

over a telecommunications network; and	network (LAN)/Internet 290) interface. (FIG. 1;[0062]). Lee also discloses that there is an interface (not shown in FIG. 1) for connecting to the cell phone 283 and an interface (not shown in FIG. 1) for connecting to the PDA 282. [0060].
[*E*] transmitting commands from a handheld telecommunications unit to the processor via the telecommunications module to cause the processor to provide images to the telecommunications module to be transmitted to the telecommunications unit.	Lee describes several types of user input devices for sending control commands to main control unit 100 including wireless PDA 282, cell phone 283, and remote computer 291. [0059]. A user may program the system via on-screen program menus displayed on any of the user input devices. [0064]. Commands that can be transmitted from the user input devices to the main control unit 100, include a command to set the main control unit 100 to a different mode, a command to switch the camera in S&S device 212 on or off, a command to place the camera in S&S device 212 in standby mode, and a command to turn the system on or off. [0060]; [0087]. Remote computer 291 is connected to the main control unit 100 over a network 290 (e.g., the Internet or PSTN), which are telecommunications networks. Remote computer 291includes application software that enables the remote computer to both receive video data from the system and send control data to the system. [0062]. Wireless PDA 282 and cell phone 283 communicate with the main control unit 100 through interfaces that are not shown in FIG. 1 of Lee. [0060]. It would have been obvious to a POSA to implement wireless PDA 282 and/or cell phone 283 transmit commands to cause the main control unit to transmit images to the wireless PDA 282 and/or cell phone 283. (see obviousness analysis above this claim chart).
18. The method of claim 11, further	S&S device 212 is controllable via user input devices such as remote controller 281, wireless PDA 282, cell

comprising programming the telecommunications module to receive commands from a handheld telecommunications unit over the telecommunications network to enable activation and deactivation of the motion detectors and cameras using the telecommunications unit.	phone 283, and remote computer 291. [0062]; [0064]. Among the functions of the system that are controllable, a user can send command signals to turn on or off the S&S device 212, which includes motion detectors. [0087]; [0110]. A POSA would have understood that a command to turn on or off S&S device 212 would turn on or off (i.e., activate/deactivate) all components of the S&S device 212 including any motion detectors included as part of S&S device 212. (see obviousness analysis above this claim chart).
19. The method of claim 11, wherein the processor is arranged to receive, via the telecommunications module, one of a plurality of different code numbers from the telecommunications unit and control the at least one camera and the at least one motion detector in accordance with the received code number.	Control signals are sent to main control unit 100 from, among other devices, a cell phone 283, wireless PDA 282, and remote computer 291. [0060]; [0062]. A user device locally or via the Internet can be used to change the setting mode of S&S device 212 between ON, OFF, and INTERRUPT modes. [0107]. S&S device 212 includes a camera and a motion detector as discussed in connection with claim 1[A] and 1[B1]. Changing the setting mode of the S&S device 212 controls both the camera (e.g., by turning it on or off) and the motion detector (e.g., by having it trigger activation of the camera in the INTERRUPT mode but not in the other modes). A user device may also send a command to turn on or off Lee's system, which includes S&S device 212. [0087]. Turning on or off the system controls both the camera (e.g., by turning it on or off) and the motion detector (e.g., by turning it on or off). A POSA would have understood that a command sent from a user input device to change the mode of the S&S device 212 and a command sent from a user input device

	to turn on/off the system includes one of a plurality of code numbers to control the camera(s) and the motion sensor(s) in the S&S device 212, and is received via a telecommunication module. (see obviousness analysis above this claim chart).
20. The method claim 19, wherein one of the code numbers is to cause the processor to cause images to be provided by the processor to the telecommunications module and transmitted to the telecommunications unit.	Lee describes several types of user input devices for sending control commands to main control unit 100 including wireless PDA 282, cell phone 283, and remote computer 291. [0059]. It would have been obvious to a POSA to transmit images to any of the user input devices that include the ability to display images in response to a command from the user input device to provide the images. [0059]; FIG 1. A POSA would have further understood that such commands are implemented as code numbers. (see obviousness analysis above this claim chart).

Appendix B: Claim chart for U.S. 7,864,983 – Ground 2: Lee and Ozer (Claims 9, 10, 12-17)

‘983 CLAIMS	**LEE and OZER**
9. The system of claim 1, wherein said processor is further arranged to derive a silhouette of any objects in the image, compare the silhouettes to a library of stored silhouettes having associated object identification to determine an exact or closest match of the derived silhouette to one of the stored silhouettes and retrieve the object identification associated with the exact or closest match, said processor being arranged to react to the detection of motion by said at least one motion detector based on the object identification.	Surveillance camera 922 in Lee is activated when any of the sensors 923 (which can be a motion detector), is triggered. [0111]. When the system is triggered, the user is alerted and a text message corresponding to the nature of the unusual event information sensed by the sensors in the system is sent to a display device 50 to inform the user which sensor was triggered. [0111]. S&S device 212 may be set to operate in one of several modes including an “ON mode,” an “OFF mode,” and an “INTERRUPT mode.” [0107]. When the S&S device 212 is in “INTERRUPT mode,” the camera is off unless and until a trigger signal is received indicating that the presence of an intruder has been detected by a sensor [0107]-[0108]. Ozer describes comparing objects in an image to silhouette templates to identify, among other objects, a human in the image being monitored. [0011]. Ozer’s system generates silhouettes of an object in an image to both classify objects (e.g., humans or dogs) in the image and to recognize a wide variety of activities. [0026]-[0027]; [0052]; [0053]-[0054]; [0064]. By identifying objects in the image, the system is more accurate because it rejects many elements in the area being monitored that may be moving, but are not objects of interest. [0054]. Ozer’s system determines an object model describing the shape of the object being classified (e.g., human body), which is derived using descriptors that are typical for a human body (e.g., hands head, torso). [0052]; [0061]-[0063]. The object model is compared with a set of stored models to determine an exact or closest match. [0064]. In the combination, the system of Lee would implement the object detection technique of Ozer to make the generation of an alert and/or triggering of the camera in INTERRUPT mode be based on the object identification so that the alert can/or triggering may occur when the object is identified as a

	potential threat (e.g., intruder) but not when the object is identified as not being a potential threat. This would make the system more accurate by reducing the number of "false alarms" that may occur when the user is alerted and/or the camera is triggered in INTERRUPT mode by motion not caused by an object of interest (i.e., an intruder) but rather by other motion (e.g., a pet's movements). (see obviousness analysis above this claim chart).
10. The system of claim 9, wherein said at least one motion detector comprises a plurality of motion detectors and said at least one camera comprises a plurality of cameras, at least one of said cameras being associated exclusively with each of said motion detectors, at least two of said cameras are associated exclusively with each of said motion detectors or at least two of said cameras are associated non-exclusively with each of said motion detectors, wherein when at least two of said cameras are associated with one	The S&S device 212 of Lee includes a plurality of camera modules 920, each of which includes a camera 922 and a sensor 923 (which can be a motion detector). ([0104]; [0110]; [0111]; FIG. 9). Camera 922 in a camera module 920 can be activated when an associated motion sensor 923 is triggered [0111]. FIG. 9 shows that camera modules 920 each includes a sensor (which can be a motion detector) 923 and an associated camera 922 in the same module. ([0104]; [0111]; FIG. 9). A POSA would have understood Lee to disclose that the camera and sensor in the same module are associated exclusively (see obviousness analysis above this claim chart).

of said motion detectors, each of said at least two cameras has a dormant state in which imaging is not performed and images are not obtained and an active state in which images are obtained, said at least two cameras all being activated from the dormant state into the active state when the associated one of said motion detectors detects motion in its field of view such that said at least two cameras obtain images of the source of the motion detected by the associated one of said motion detectors, and said processor being arranged to analyze images from said at least two cameras to determine depth information about a common object appearing in the images from said at least two cameras	

which may be the source of the motion, the depth information being used in the object identification being performed by the processor and indicating a distance between the structure and the object, said processor being arranged to react to the detection of motion by said at least one motion detector based on the object identification and based on the distance between the structure and the object.	
12. The method of claim 11, wherein the processor further derives a silhouette of any objects in the image, compares the silhouettes to a library of stored silhouettes having associated object identification to determine an exact or closest match of the derived	Surveillance camera 922 in Lee is activated when any of the sensors 923 (which can be a motion detector), is triggered. [0111]. When the system is triggered countermeasures are generated including, the user is alerted and a text message corresponding to the nature of the unusual event information sensed by the sensors in the system is sent to a display device 50 to inform the user which sensor was triggered. [0111]. The countermeasures can also include the main control unit 100 automatically calling the user's mobile telephone, if the system is on and the user is not at home. [0111]. S&S device 212 may be set to operate in one of several modes including an "ON mode," an "OFF mode," and an "INTERRUPT mode." [0107]. When the S&S device 212 is in "INTERRUPT mode," the camera is off unless and until a trigger signal is received indicating that the presence of an

silhouette to one of the stored silhouettes and retrieves the object identification associated with the exact or closest match, further comprising generating a countermeasure to the detection of motion by the motion detectors based on the object identification when the object is identified as a potential threat to the structure.	intruder has been detected by a sensor [0107]-[0108]. Ozer describes comparing objects in an image to silhouette templates to identify, among other objects, a human in the image being monitored. [0011]. Ozer's system generates silhouettes of an object in an image to both classify objects (e.g., humans or dogs) in the image and to recognize a wide variety of activities. [0026]-[0027]; [0052]; [0053]-[0054]; [0064]. By identifying objects in the image, the system is more accurate because it rejects many elements in the area being monitored that may be moving, but are not objects of interest. [0054]. Ozer's system determines an object model describing the shape of the object being classified (e.g., human body), which is derived using descriptors that are typical for a human body (e.g., hands head, torso). [0052]; [0061]-[0063]. The object model is compared with a set of stored models to determine an exact or closest match. [0064]. In the combination, the system of Lee would implement the object detection technique of Ozer to make the generation of a countermeasure including an alert and/or triggering of the camera in INTERRUPT mode be based on the object identification so that the alert can/or triggering may occur when the object is identified as a potential threat (e.g., intruder) but not when the object is identified as not being a potential threat. This would make the system more accurate by reducing the number of "false alarms" that may occur when the user is alerted and/or the camera is triggered in INTERRUPT mode by motion not caused by an object of interest (i.e., an intruder) but rather by other motion (e.g., a pet's movements). (see obviousness analysis above this claim chart).
13. The method of claim 12, wherein each camera is associated with only a single	The S&S device 212 of Lee includes a plurality of camera modules 920, each of which includes a camera 922 and a sensor 923 (which can be a motion detector). ([0104]; [0110]; [0111]; FIG. 9). Camera 922 in camera module 920 can be activated when an associated motion sensor 923 is triggered [0111]. FIG. 9 shows that camera modules 920

motion detector, each camera is associated with a plurality of motion detectors, or, multiple cameras are associated with each motion detector, wherein when a plurality of cameras are associated with one of the motion detectors, images from the plurality of cameras are analyzed by the processor to determined depth information about an object appearing in the images, the depth information being used in the object identification being performed by the processor.	each includes a sensor (which can be a motion detector) 923 and an associated camera 922 in the same module. ([0104]; [0111]; FIG. 9). A POSA would have understood Lee to disclose that the camera and sensor in the same module are associated exclusively (see obviousness analysis above this claim chart).
14. The method of claim 12, further comprising assigning a classification of "no threat" or "hostile" based on the object identification and/or the size of the object, the countermeasure	See analysis of claims 9 and 12. In the combination, the system of Lee would implement the object detection technique of Ozer and generate a countermeasure (e.g., generate an alert, trigger the camera in INTERRUPT mode, call the user's mobile telephone) when the object is identified as a potential threat (e.g., identified as potential intruder) but not otherwise. [0111]. (see obviousness analysis above this claim chart).

being generated only when the classification is hostile.	
15. The method of claim 12, wherein the step of generating a countermeasure includes generate an audible and/or visual alarm in proximity to the structure or generating at least one communication about the condition of the structure based on the object identification and forwarding the communication to a remote destination.	The alert generated by Lee's system can include providing a live image to be shown on the user's LCD display device. ([0111]), which a POSA would have recognized as a visual alarm in proximity to the structure. (see obviousness analysis above this claim chart). The alert can also include the main control unit 100 automatically calling the user's mobile telephone, if the system is on and the user is not at home ([0111]), which a POSA would have recognized generating at least one communication about the condition of the structure based on the object identification and forwarding the communication to a remote destination. (see obviousness analysis above this claim chart). Additionally, in the obvious combination, a communication would be sent to alert police or a private security company monitoring the home (see obviousness analysis above this claim chart).
16. The method of claim 15, wherein the remote destination is a police station, a first station, a terminal monitored by an owner of the structure, or a private security station.	See analysis for claim 15. The alert in the combined system of Lee and Ozer can include the main control unit 100 automatically calling the user's mobile telephone. [0111]. In addition, Lee allows the user to communicate and monitor the system via the Internet [0021] and shows that this may be done via a remote computer 291 that can receive video data from the system. ([0062]; [0111]; FIG. 1). In the combination, a live image can be sent to the remote computer 291 over the Internet when an event occurs so that the user can monitor the system remotely over the web. [0111]. Additionally, in the obvious combination, a communication about the condition of a structure based on an object identification would be forwarded to a police station or a private security station (see obviousness analysis above this claim chart).
17. The method	In the combined system, the communication forwarded to a

of claim 15, further comprising including one or more images obtained from the cameras or one or more images derived from the images obtained from the cameras in the communication being forwarded to the remote destination.	remote destination can include live images from one or more cameras sent to the remote computer 291. (see analysis of claim 16). In addition, in the obvious combination, an image from the camera showing the monitored area at the time the event was detected would be sent to remote destination (see obviousness analysis above this claim chart).

Appendix C: Claim chart for U.S. 7,864,983 – Ground 3: Milinusic and Osann

'983 CLAIMS	**MILINUSIC AND OSANN**
1. An alarm system for protecting a structure, comprising:	Milinusic describes a surveillance system 100 to monitor predetermined areas which can include a warehouse (6:59-67), teaches that conventional systems are deficient in determining information about an intruder (1:37-44), and distributes surveillance data to a user when predetermined conditions are detected. (3:3-5; 3:64-4:1; 4:30-34). Osann provides video surveillance and motion detection to protect a home or building (25:55-60; Fig. 28) and generates an alarm upon detecting an intruder. (14:4-20). In the combination the system of Milinusic would be used to protect a structure and generate an alarm upon detected conditions such as detecting an intruder. (see obviousness analysis above this claim chart).
[*A*] at least one motion detector arranged to have a field of view external of the structure and including an area proximate the structure;	Milinusic's surveillance system includes sensor units (e.g., 250, 260, 270) that may be motion detectors. (3:41-45 and 51-55). Osann describes video surveillance cameras 86 and motion detectors 85 that monitor the exterior of a home (25:55-60; Fig. 28). In the combination, at least one motion detector of Milinusic is arranged to have a field of view external of the structure and including an area proximate the structure. (see obviousness analysis above this claim chart).
[*B1*] at least one camera associated with and coupled to each of said at least one motion detector,	Milinusic's surveillance system includes sensor units 250 and 260 that include cameras 451, 452 and 461 coupled to motion detectors so that they capture images upon the detection of movement in the areas they monitor. (3:47-51; 5:24-43 and 51-59). Cameras may be coupled to motion detectors in other sensor units via the network (130 or 230) (3:51-55; FIGs. 2 and 4) or include motion detectors in the same sensor units. (see obviousness analysis above this claim chart).
[*B2*] each of said at	Milinusic's sensor units 250 and 260 are arranged to monitor

least one camera being arranged relative to the associated one of said at least one motion detector such that said camera has a field of view encompassing at least part of the field of view of the associated one of said at least one motion detector,	a predetermined area, with cameras 451, 452, and 461 being arranged to capture an image of the area upon detection of movement within the area being monitored. (5:51-55 and 56-59). Sensor units 250 and 260 may be configured as a motion detector. (3:51-55). In the combination, motion detectors (e.g., in sensor units 250, 260 or other sensor units) and cameras 451, 452, 461 are arranged to monitor the same predetermined area, so that at least one camera is arranged relative to at least one motion detector such that the camera has a field of view encompassing at least part of the field of view of the motion detector. (see obviousness analysis above this claim chart).
[*B3*] each of said at least one camera having a dormant state in which images are not obtained and an active state in which images are obtained and being activated into the active state when the associated one of said at least one motion detector detects motion;	Milinusic describes setting image capture by a camera to occur upon the occurrence of predetermined events such as the detection of movement in an area being monitored by the sensor units (e.g., motion detectors). (5:51-59).
[*C*] a processor coupled to said at least one camera and arranged to control said at least one camera and receive the image obtained by said at least one camera;	Milinusic's system 100 includes a surveillance server 210 coupled to cameras 451, 452 (in sensor unit 250) and 461 (in sensor unit 260) via network 230, and sensor units 250, 260, and 270, each of which is also connected to network 130. (FIG. 4; 2:61-67; 3:47-51; 5:23-42). Surveillance server 210 includes a central processing unit (CPU) 360 (4:14-16) coupled to the cameras via the network (130 or 230). (FIG. 3). Surveillance server 210 is arranged to transmit control

	information to the sensor units 250 and 260 in response to requests from a surveillance client 240 (3:37-41). The CPU 360 is configured to control the operation of the server 210 so that surveillance data (e.g., images) may be received from the various sensor units (e.g., a camera). (3:12-15; 4:25-30).
[*D*] a telecommunications module coupled to said processor, said telecommunications module being capable of communications over a telecommunications network; and	Milinusic's server 210 includes an input/output (I/O) processor 375 that provides an interface to the network (130 or 230), which may be a WAN such as the Internet. (3:18-19; 4:16-23; FIG. 3). I/O processor 375 is coupled to CPU 360 via local interface 370. (FIG. 3). I/O processor 375 is a telecommunications module capable of communications over a telecommunications network (i.e., network 130).
[*E*] a handheld telecommunications unit for transmitting commands for said processor via said telecommunications module to cause said processor to provide images to said telecommunications module to be transmitted to the telecommunications unit.	Milinusic's system 100 includes a surveillance client 240 connected to network 230. (2:63-65). Surveillance client may be a personal computer or a personal digital assistant (PDA). (3:33-35). The surveillance client 240 is configured to allow a user to retrieve surveillance data from the surveillance server 210 by issuing a request to surveillance server 210. (3:31-37). The surveillance data may include video data and still image data. (3:12-13). The CPU 360 is configured to control the operation of the server 210 so that surveillance data (e.g., images) may be received from the various sensor units (e.g., a camera). (3:12-15; 4:25-30).
2. The alarm system of claim 1, wherein said processor is coupled to said at	Milinusic's server 210 and sensor units (e.g., 250, 260, and 270) that may be configured as motion detectors are all connected to the same network (130 or 230). (2:61-67; 3:51-55). Surveillance server 210 includes CPU 360. (4:14-16). .

least one motion detector and said telecommunications unit is also arranged to transmit commands for said processor to activate and deactivate said at least one motion detector.	Surveillance client 240, which may be a PDA or personal computer, is configured to control or adjust specified sensor units by issuing requests to surveillance server 210 that are then transmitted to the specified sensor unit. (3:33-40). In the combination, a handheld telecommunications device (surveillance client 240) transmits commands to server 210 to activate and deactivate a motion detector. (see obviousness analysis above this claim chart).
3. The alarm system of claim 1, wherein in said dormant state of each of said at least one camera, imaging by said camera is not performed and images are not obtained, each of said at least one camera being automatically activated from the dormant state into the active state when the associated one of said at least one motion detector detects motion in its field of view.	Milinusic describes setting image capture by a camera to occur upon the occurrence of predetermined events such as the detection of movement in an area being monitored by the sensor units (e.g., motion detectors). (5:51-59).
4. The alarm system of claim 1, wherein said telecommunications unit is one of a camera telephone, a cellular telephone	Milinusic's surveillance client 240 may be a personal computer or a personal data assistant (PDA). (3:31-35) and may be coupled to the surveillance server 210 via a network (130 or 230) that includes the Internet. (3:18-19). In the obvious combination the surveillance client may also be a cellular telephone. (see obviousness analysis above this claim chart).

and an Internet-enabled picture and/or video display device.	
5. The alarm system of claim 1, wherein said processor is arranged to receive, via said telecommunications module, one of a plurality of different code numbers from said telecommunications unit and control said at least one camera and said at least one motion detector in accordance with the received code number.	Milinusic's surveillance client 240 is configured to control or adjust specified sensor units by issuing requests to surveillance server 210. (3:37-40). Surveillance client 240 and surveillance server 210 are connected by network 230, which may be a wide area network (e.g., the Internet) or a local area network. (3:18-19; Fig. 2). In the combination, the CPU 360 in surveillance server 210 receives from surveillance clients 240, over the network (130 or 230), a plurality of code numbers to control cameras and motion detectors in sensor units (e.g., 250, 260, 270). (see obviousness analysis above this claim chart).
6. The alarm system of claim 5, wherein one of the code numbers is to cause said processor to cause images to be provided by said processor to said telecommunications module and transmitted to the telecommunications unit.	Milinusic's surveillance client 240 is configured to allow a user to retrieve surveillance data from the surveillance server 210 by issuing a request to surveillance server 210. (3:31-37). The surveillance data may include video data and still image data. (3:12-13). The CPU 360 is configured to control the operation of the server 210 so that surveillance data (e.g., images) may be received from the various sensor units (e.g., a camera). (3:12-15; 4:25-30). In the obvious combination, the CPU 360 in surveillance server 210 receives from surveillance clients 240, over the network (130 or 230), a code number to cause the CPU 360 to be provided by CPU 360 to the telecommunications module and transmitted to the surveillance client 240. (see obviousness analysis above this claim chart).
7. The alarm system of claim 5,	Milinusic's surveillance client 240 is configured to allow a user to retrieve surveillance data from the surveillance server

wherein one of the code numbers is to cause said processor to direct said at least one camera to provide images to said processor and then cause the provided images to be forwarded by said processor to said telecommunications module and transmitted to the telecommunications unit.	210 by issuing a request to surveillance server 210. (3:31-37). The surveillance data may include video data and still image data. (3:12-13). The CPU 360 is configured to control the operation of the server 210 so that surveillance data (e.g., images) may be received from the various sensor units (e.g., a camera). (3:12-15; 4:25-30). Additionally, Milinusic describes surveillance server 210 being configured to retrieve and distribute surveillance data to a requesting surveillance client 240. (4:30-32). Milinusic also describes that video data may be provided by the surveillance system 100 for presentation in a streaming format. (2:56-57). In the combination, surveillance client 240 would implement a command to enable a user to view live images recorded by the camera in a streaming format. A POSA would have understood that a command to provide video data from a camera in a streaming format is a command to direct the camera to provide live images to the processor and then cause the provided live images to be forwarded by the processor to said telecommunications module and transmitted to the user input device when the user input device includes the ability to display images. (see also the obviousness analysis above this claim chart for claim 5).
8. The system of claim 1, wherein said at least one motion detector comprises a plurality of motion detectors, said at least one camera associated with said at least one motion detector being arranged to have a field of view overlapping a field of view of a	Milinusic's system 100 includes a plurality of cameras and motion detectors (2:59-3:2; 3:47-56; FIG. 2; FIG. 4). Cameras may have a wide field of view, be configured to monitor a predetermined area, and capture images upon detection of movement within the area being monitored. (5:27-30 and 51-59). In the obvious combination, at least one camera would have a field of view that overlaps a field of view of a plurality of motion detectors. (see obviousness analysis above this claim chart).

plurality of said motion detectors.	
11. A method for protecting a structure, comprising:	Milinusic describes a surveillance system 100 to monitor predetermined areas which can include a warehouse (6:59-67), teaches that conventional systems are deficient in determining information about an intruder (1:37-44), and distributes surveillance data to a user when predetermined conditions are detected. (3:3-5; 3:64-4:1; 4:30-34). Osann provides video surveillance and motion detection to protect a home or building (25:55-60; Fig. 28). In the combination the system of Milinusic would be used to protect a structure. (see obviousness analysis above this claim chart).
[*A*] arranging a plurality of motion detectors on or around the structure, each in a position in which its field of view includes an area proximate the structure;	Milinusic's surveillance system includes sensor units (e.g., 250, 260, 270) that may be motion detectors. (3:41-45 and 51-55). Osann describes video surveillance cameras 86 and motion detectors 85 that monitor the exterior of a home (25:55-60; Fig. 28). In the combination, the motion detectors of Milinusic are arranged on or around the structure, each in a position in which its field of view includes an area proximate the structure. (see obviousness analysis above this claim chart).
[*B1*] arranging a plurality of cameras on or around the structure,	Milinusic's surveillance system includes sensor units 250 and 260 that include cameras 451, 452 and 461 coupled to motion detectors so that they capture images upon the detection of movement in the areas they monitor. (3:47-51; 5:24-43 and 51-59). Osann describes video surveillance cameras 86 and motion detectors 85 that monitor the exterior of a home (25:55-60; Fig. 28). In the combination, the cameras of Milinusic are arranged on or around the structure. (see obviousness analysis above this claim chart).
[*B2*] each camera	Milinusic's sensor units 250 and 260 are arranged to monitor

being associated with one or more of the motion detectors such that the camera has a field of view encompassing at least part of the field of view of any associated motion detector,	a predetermined area, with cameras 451, 452, and 461 being arranged to capture an image of the area upon detection of movement within the area being monitored. (5:51-55 and 56-59). Sensor units 250 and 260 may be configured as a motion detector. (3:51-55). In the combination, motion detectors (e.g., in sensor units 250, 260 or other sensor units) and cameras 451, 452, 461 are arranged to monitor the same predetermined area, so that each camera is associated with one or more motion detectors such that the camera has a field of view encompassing at least part of the field of view of the associated motion detector. (see obviousness analysis above this claim chart).
[*C*] providing a processor which controls the at least one camera and receives the image obtained by the at least one camera;	Milinusic's system 100 includes a surveillance server 210 including a central processing unit (CPU) 360 (4:14-16). Surveillance server 210 is arranged to transmit control information to the sensor units 250 and 260 in response to requests from a surveillance client 240 (3:37-41). The CPU 360 is configured to control the operation of the server 210 so that surveillance data (e.g., images) may be received from the various sensor units (e.g., a camera). (3:12-15; 4:25-30).
[*D*] coupling a telecommunications module coupled to the processor, the telecommunications module being capable of communications over a telecommunications network; and	Milinusic's server 210 includes an input/output (I/O) processor 375 that provides an interface to the network (130 or 230), which may be a WAN such as the Internet. (3:18-19; 4:16-23; FIG. 3). I/O processor 375 is coupled to CPU 360 via local interface 370. (FIG. 3). I/O processor 375 is a telecommunications module capable of communications over a telecommunications network (i.e., network 130).
[*E*] transmitting commands from a handheld	Milinusic's system 100 includes a surveillance client 240 connected to network 230. (2:63-65). Surveillance client may be a personal computer or a personal digital assistant

telecommunications unit to the processor via the telecommunications module to cause the processor to provide images to the telecommunications module to be transmitted to the telecommunications unit.	(PDA). (3:33-35). Surveillance client 240 is configured to allow a user to retrieve surveillance data from the surveillance server 210 by issuing a request to surveillance server 210. (3:31-37). The surveillance data may include video data and still image data. (3:12-13). The CPU 360 is configured to control the operation of the server 210 so that surveillance data (e.g., images) may be received from the various sensor units (e.g., a camera). (3:12-15; 4:25-30).
18. The method of claim 11, further comprising programming the telecommunications module to receive commands from a handheld telecommunications unit over the telecommunications network to enable activation and deactivation of the motion detectors and cameras using the telecommunications unit.	Milinusic's server 210 and sensor units (e.g., 250, 260, and 270) that may be configured as motion detectors are all connected to the same network (130 or 230). (2:61-67; 3:51-55). Surveillance server 210 includes CPU 360. (4:14-16). . Surveillance client 240, which may be a PDA or personal computer, is configured to control or adjust specified sensor units by issuing requests to surveillance server 210 that are then transmitted to the specified sensor unit. (3:33-40). In the combination, a handheld telecommunications device (surveillance client 240) transmits commands to server 210 to activate and deactivate motion detectors and cameras. (see obviousness analysis above this claim chart).
19. The method of claim 11, wherein the processor is arranged to receive, via the telecommunications module, one of a	Milinusic's surveillance client 240 is configured to control or adjust specified sensor units by issuing requests to surveillance server 210. (3:37-40). Surveillance client 240 and surveillance server 210 are connected by network 230, which may be a wide area network (e.g., the Internet) or a local area network. (3:18-19; Fig. 2). In the combination, the CPU 360 in surveillance server 210 receives from surveillance clients 240, over the network (130 or 230), a

plurality of different code numbers from the telecommunications unit and control the at least one camera and the at least one motion detector in accordance with the received code number.	plurality of code numbers to control cameras and motion detectors in sensor units (e.g., 250, 260, 270). (see obviousness analysis above this claim chart).
20. The method claim 19, wherein one of the code numbers is to cause the processor to cause images to be provided by the processor to the telecommunications module and transmitted to the telecommunications unit.	Surveillance client 240 is configured to allow a user to retrieve surveillance data from the surveillance server 210 by issuing a request to surveillance server 210. (3:31-37). The surveillance data may include video data and still image data. (3:12-13). The CPU 360 is configured to control the operation of the server 210 so that surveillance data (e.g., images) may be received from the various sensor units (e.g., a camera). (3:12-15; 4:25-30). In the combination, the CPU 360 in surveillance server 210 receives from surveillance clients 240, over the network (130 or 230), a code number to cause CPU 360 to cause images to be provided by CPU 360 to the telecommunications module and transmitted to the surveillance client 240. (see obviousness analysis above this claim chart).

Appendix D: Claim chart for U.S. 7,864,983 – Ground 4: Milinusic, Osann and Ozer (Claims 9, 10, 12-17)

'983 CLAIMS	**MILINUSIC, OSANN and OZER**
9. The system of claim 1, wherein said processor is further arranged to derive a silhouette of any objects in the image, compare the silhouettes to a library of stored silhouettes having associated object identification to determine an exact or closest match of the derived silhouette to one of the stored silhouettes and retrieve the object identification associated with the exact or closest match, said processor being arranged to react to the detection of motion by said at least one motion detector based on the object identification.	Milinusic's system can detect predetermined conditions, generate surveillance data representative of the detected condition and distribute surveillance data to a surveillance client based upon predetermined distribution criteria. (3:3-5; 3:64-4:1; 4:30-34). Osann describes generating an alarm upon the occurrence of an event such as detecting an intruder (14:4-20). Ozer compares objects in an image to silhouette templates to determine an exact or closest match and thereby identify, among other objects, a human in the image being monitored. [0011]; [0064]. Ozer's system generates silhouettes of an object in an image to both classify objects (e.g., humans or dogs) in the image and to recognize a wide variety of activities. [0026]-[0027]; [0052]; [0053]-[0054]; [0064]. By identifying objects in the image, the system is more accurate because it rejects many elements in the area being monitored that may be moving, but are not objects of interest. [0054]. Ozer's system determines an object model describing the shape of the object, which is derived using descriptors that are typical for the object (e.g., for a human body). [0052]; [0061]-[0063]. In the combination, the system of Milinusic/Osann would implement the object detection technique of Ozer to generate an alert or alarm only when the object that was detected is classified as an object of interest (e.g., intruder) to make the system more accurate by reducing the number of "false alarms" that may occur when the user is alerted and/or the camera is triggered by motion not caused by an object of interest (i.e., an intruder) but rather by other motion (e.g., a pet's movements). (see obviousness analysis above this claim chart).
10. The system of claim 9, wherein said at least one motion detector	Milinusic's surveillance system 100 includes a plurality of sensor units 250, 260, 270 configured to collect surveillance data by detecting predetermined conditions or occurrences including the detecting of movement in a monitored area.

comprises a plurality of motion detectors and said at least one camera comprises a plurality of cameras, at least one of said cameras being associated exclusively with each of said motion detectors, at least two of said cameras are associated exclusively with each of said motion detectors or at least two of said cameras are associated non-exclusively with each of said motion detectors, wherein when at least two of said cameras are associated with one of said motion detectors, each of said at least two cameras has a dormant state in which imaging is not performed and images are not obtained and an active state in which images are obtained, said at least two cameras	(3:41-45; FIG. 2; FIG. 4; 5:24-64). FIG. 4 shows sensor unit 250 as including cameras 451 and 452 and sensor unit 260 as including camera 461. (5:24-43). The camera in any of sensor units 250, 260, and 270 that includes a camera may be coupled to the motion detector in any sensor unit configured as a motion detector (3:51-55) via the network (230 in FIG. 2 and 130 in FIG. 4). FIG. 28 of Osann shows an integrated unit that includes a camera and a sensor associated exclusively in a 1:1 correspondence. In the combination, at least one of the Milinusic cameras is associated exclusively in a 1:1 relationship with one of the Milinusic motion detectors (see obviousness analysis above this claim chart).

all being activated from the dormant state into the active state when the associated one of said motion detectors detects motion in its field of view such that said at least two cameras obtain images of the source of the motion detected by the associated one of said motion detectors, and said processor being arranged to analyze images from said at least two cameras to determine depth information about a common object appearing in the images from said at least two cameras which may be the source of the motion, the depth information being used in the object identification being performed by the processor and indicating a distance between the structure and the object, said processor being	

arranged to react to the detection of motion by said at least one motion detector based on the object identification and based on the distance between the structure and the object.	
12. The method of claim 11, wherein the processor further derives a silhouette of any objects in the image, compares the silhouettes to a library of stored silhouettes having associated object identification to determine an exact or closest match of the derived silhouette to one of the stored silhouettes and retrieves the object identification associated with the exact or closest match, further comprising generating a countermeasure to the detection of motion by the	Milinusic teaches that the system can detect predetermined conditions, generate surveillance data representative of the detected condition and distribute surveillance data to a surveillance client based upon predetermined distribution criteria. (3:3-5; 3:64-4:1; 4:30-34). Osann describes generating an alarm upon the occurrence of an event such as detecting an intruder (14:4-20). Ozer compares objects in an image to silhouette templates to determine an exact or closest match and thereby identify, among other objects, a human in the image being monitored. [0011]; [0064]. Ozer's system generates silhouettes of an object in an image to both classify objects (e.g., humans or dogs) in the image and to recognize a wide variety of activities. [0026]-[0027]; [0052]; [0053]-[0054]; [0064]. By identifying objects in the image, the system is more accurate because it rejects many elements in the area being monitored that may be moving, but are not objects of interest. [0054]. Ozer's system determines an object model describing the shape of the object, which is derived using descriptors that are typical for the object (e.g., for a human body). [0052]; [0061]-[0063]. In the combination, the system of Milinusic/Osann would implement the object detection technique of Ozer and generate one or more countermeasures (e.g., the generation of an alert (e.g., alarm) and/or the triggering of the camera to capture an image of a monitored area) upon the detection of movement in the area only when the object is identified as a potential threat (e.g., intruder), and would not take countermeasures when the object is not identified as a

motion detectors based on the object identification when the object is identified as a potential threat to the structure.	potential threat. (see obviousness analysis above this claim chart)
13. The method of claim 12, wherein each camera is associated with only a single motion detector, each camera is associated with a plurality of motion detectors, or, multiple cameras are associated with each motion detector, wherein when a plurality of cameras are associated with one of the motion detectors, images from the plurality of cameras are analyzed by the processor to determined depth information about an object appearing in the images, the depth information being used in the object identification being performed by the	Milinusic's surveillance system 100 includes a plurality of sensor units 250, 260, 270 configured to collect surveillance data by detecting predetermined conditions or occurrences including the detecting of movement in a monitored area. (3:41-45; FIG. 2; FIG. 4; 5:24-64). FIG. 4 shows sensor unit 250 as including cameras 451 and 452 and sensor unit 260 as including camera 461. (5:24-43). The camera in any of sensor units 250, 260, and 270 that includes a camera may be coupled to the motion detector in any sensor unit configured as a motion detector (3:51-55) via the network (230 in FIG. 2 and 130 in FIG. 4). FIG. 28 of Osann shows an integrated unit that includes a camera and a sensor associated exclusively in a 1:1 correspondence. In the combination, at least one of the Milinusic cameras is associated exclusively in a 1:1 relationship with one of the Milinusic motion detectors (see obviousness analysis above this claim chart).

processor.	
14. The method of claim 12, further comprising assigning a classification of "no threat" or "hostile" based on the object identification and/or the size of the object, the countermeasure being generated only when the classification is hostile.	See analysis of claims 9 and 12. The combined system of Milinusic/Osann generates countermeasures (e.g., generates surveillance data representative of the detected condition and distribute surveillance data to a surveillance client based upon predetermined distribution criteria and/or generates an alarm) upon the occurrence of an event such as detecting movement in a monitored area. In the combination, the combined system of Milinusic/Osann would implement the object detection technique of Ozer and the generation of a countermeasure (e.g., generating an alarm or triggering of the camera to capture an image of a monitored and distributing surveillance data) based upon the detection of movement in the area would take place only when the object is identified as a potential threat (e.g., identified as potential intruder). (see obviousness analysis above this claim chart).
15. The method of claim 12, wherein the step of generating a countermeasure includes generate an audible and/or visual alarm in proximity to the structure or generating at least one communication about the condition of the structure based on the object identification and forwarding the communication to a remote destination.	Milinusic describes distributing data to a client device upon detection of a condition (3:3-5; 3:64-4:1; 4:30-34). Osann describes transmitting video to a remote destination such as a security company or the police upon the occurrence of an event such as detecting an intruder. (14:4-20). In the combination, the system would have generated at least one communication about the condition of the structure based on the object identification and forwarded the communication to a remote destination. (see obviousness analysis above this claim chart).
16. The method of claim 15, wherein the remote	See analysis for claim 15. The alert in the combined system of Milinusic, Osann, and Ozer can include transmitting video to a remote destination such as a security company or the

destination is a police station, a first station, a terminal monitored by an owner of the structure, or a private security station.	police upon the occurrence of an event such as detecting an intruder. (Ex. 1004 (Osann) at 14:4-20). (see obviousness analysis above this claim chart).
17. The method of claim 15, further comprising including one or more images obtained from the cameras or one or more images derived from the images obtained from the cameras in the communication being forwarded to the remote destination.	See analysis for claim 15. In the combined system, the communication forwarded to a remote destination can include video (e.g., images) obtained from the cameras in the combined system. (see obviousness analysis above this claim chart).