Declaration of Tal Lavian in Support of Petition for *inter partes* review of U.S. Patent No. 6,975,220

Mail Stop Inter Parties Review

Attn: Patent Trial and Appeal Board
Commissioner for Patents
PO Box 1450
Alexandria, VA 22313-1450

Commissioner:

I, Tal Lavian, declare as follows:

1. I have been retained on behalf of Mobotix Corporation for the above-captioned *inter partes* review proceeding, involving U.S. Patent No. 6,975,220 ("the '220 Patent").
2. I have reviewed and am familiar with the specification of the '220 Patent (filed on April 10, 2000; issued on December 13, 2005).
3. I have reviewed the following:
   a. U.S. Patent No. 6,930,709 to Creamer et al. ("Creamer")
   b. U.S. Patent No. 6,697,103 to Fernandez ("Fernandez")
   c. U.S. Provisional Patent Application No. 60-051489 to Thomas et al. ("Thomas")
   d. UK Patent GB 2325548 to Nabavi ("Nabavi")
   e. U.S. Patent No. 5,495,288 to Broady et al. ("Broady")
   f. U.S. Patent No. 5,019,803 to Maram ("Maram")

g. U.S. Patent No. 5,229,850 to Toyoshima ("Toyoshima")

h. U.S. Patent No. 6,359,647 to Sengupta et al. ("Sengupta")

i. Axis 240 User's Manual (Revision 1.4, Dated November 1998, hereinafter "Axis 240").

4. I have been asked to provide my technical review, analysis, insights, and opinions regarding the above-noted references that form the basis for the grounds for rejection set forth in the Petition for *inter partes* review of the '220 Patent.

Contents

I. Qualifications 5
II. Person of Ordinary Skill in the Art 7
III. Background of the Art 7
IV. Background of the '220 Patent 13
V. Application of Creamer, Creamer in View of Fernandez, and Thomas in View of Fernandez to the '220 Patent Claims 13
A. Overview Of Referenced Art 14
B. Creamer 19
Imaging Device Activated By Controller Upon Event Signal 20
Transmission Upon Event Signal 26
Imaging Device Covering The Area Where Trigger Device Is Located 28
Website 31
Authorized Entity 33
Detecting Event In A Premises 35
Lamp 35
C. Creamer in View of Fernandez 36
Website 38
Detecting Event In A Premises 40
Imaging Device Covering The Area Where Trigger Device Is Located 41
Integrating Various Sensor Components 42
Beam Sensor 43
Broken Glass Detector 44
Fire Detector 45
Microphone 46
Maintenance Detector 47
Unique Identifiers for Sensors 48
D. Thomas in view of Fernandez 51
Image Device Activated Upon Event Signal 55
Website 57
Unique Identifiers For Sensors 61
Lamp 62
Maintenance Detector 63
Integrating Various Sensor Components 65
Broken Glass Detector 66

Fire Detector 67
Microphone 68

I. Qualifications

5. I possess the knowledge, skills, experience, training and the education to form an expert opinion and testimony in this case. My Curriculum Vitae, including a listing of academic/professional publications and patents, is set forth in MOB1004.

6. My academic background includes a Ph.D. in Computer Science, received from the University of California at Berkeley, a Master of Science ("M.Sc.") degree in Electrical Engineering, and a Bachelor of Science, ("B.Sc.") degree in Mathematics and Computer Science from Tel Aviv University. My Ph.D. Dissertation was entitled: "Lambda Data Grid: Communications Architecture in Support of Grid Computing."

7. I currently serve as a Center for Entrepreneurship and Technology (CET) Industry Fellow and Lecturer at University of California Berkeley's College of Engineering. At U.C. Berkeley, I have studied network services, telecommunications systems and software, communications infrastructure and data centers. I have also served as the scientific liaison between U.C. Berkeley and Nortel Research Lab.

8. Since 2006, I have also served as the Principal Scientist at Innovations IP, based in Sunnyvale, CA, providing consulting and research services

in areas including network communications, telecommunications and internet software technologies.

9. From 1996-2007, I worked at Nortel Research Lab, holding the positions of Principal Scientist, Principal Architect, Principal Engineer, and Senior Software Engineer. At Nortel, I also served as Principal Investigator for several US Department of Defense (DARPA) projects concerning network communications. In addition, I led a project on networking computation for the United States Air Force Research Lab (AFRL). I also led a network communications research project for an undisclosed US Federal Agency, as well as several other research projects concerning communications networks.

10. While at Nortel, I received the Top Talent Award and the Top Inventors Award.

11. Prior to my work at Nortel, I worked at Bay Networks; Bay Networks was later acquired by Nortel Networks. At Bay Networks, I held various scientific and research roles including working in the CTO Office in the fields of computer networking and Internet technologies. Prior to my work at Bay Networks, I worked as a software engineer for Aptel Communications, a start-up company developing wireless spread

spectrum Personal-Communication-Network (PCN) and Personal-Communication-System (PCS) technologies.

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

II. Person of Ordinary Skill in the Art

13. A person of ordinary skill in the art with regard to the '220 Patent would have a Bachelor's degree in Computer Science, Electrical Engineering or a related field, or at least 3 years of experience in the network communications field. A person of ordinary skill in the art would be familiar with transmission of voice, data and video images using internet communications and websites. The '220 Patent, 1:5-9.

III. Background of the Art

14. Networking technologies have been adopted by surveillance systems to allow observation from a distance. Thus, surveillance devices such as cameras, microphones, and sensors are often connected to communication networks for transmission of detected information for review, analysis, control or storage.

15. The ’220 Patent itself describes some prior art in the Background Information Section:

> “[s]ystems for detecting and reporting intrusions and other types of events including but not limited to fire and medical emergencies are well known in the prior art. A typical system for securing and protecting the occupants of a premises, such as a home or an office building for example.” The ’220 Patent, 1:16-20.

16. The ’220 Patent also includes a Figure (FIG. 1) (reproduced below) showing a prior art surveillance system 11 including various prior art sensors/detectors connected to a system controller 21. The detected intrusion can be sent to a central monitor 31 via an auto dialer and modem 29 shown in FIG. 1. The ‘220 Patent, 1:35-2:24. According to the ’220 Patent, the various sensors/detectors that had been incorporated in the prior art network surveillance systems include temperature or other maintenance function sensors 12 (i.e. low heating fuel sensors), entry point sensors 13, motion sensors 15, beam sensors 17, fire/smoke detector 18, audio detectors 19, broken glass detector 20. The ’220 Patent, 5:35-52 and FIG. 1.

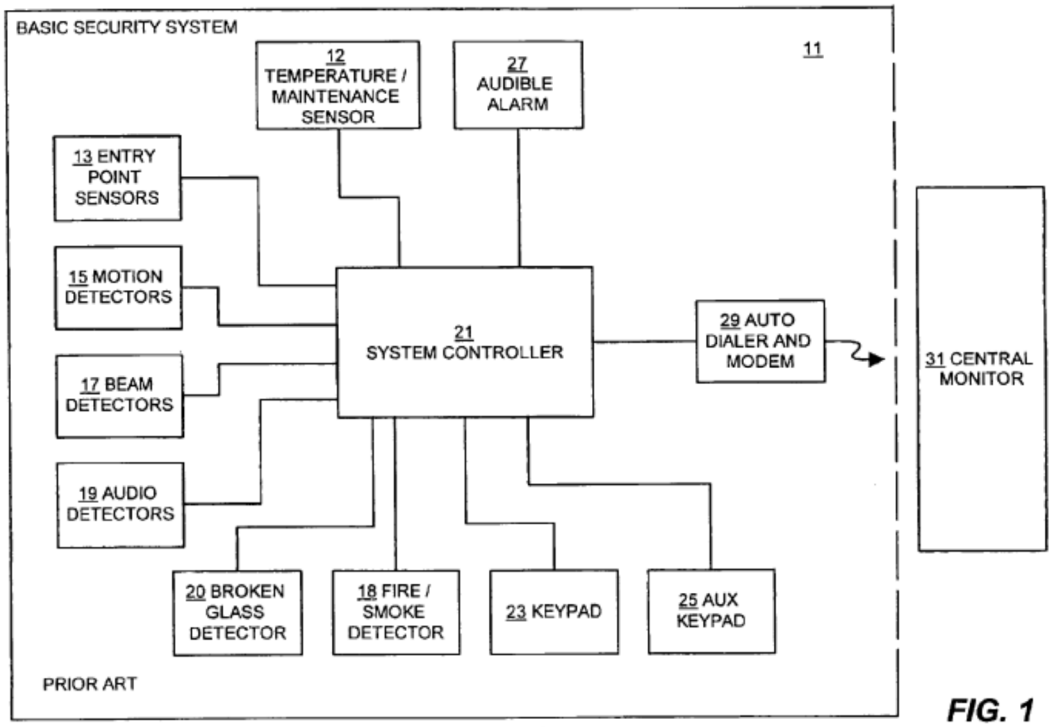


FIG. 1

17. FIG. 2 of the ’220 Patent (reproduced below) shows another prior art security system using video surveillance 32 that the ’220 Patent indicates “may be used by itself or in conjunction with the basic security system 11 [of FIG. 1] for home or commercial use.” The ’220 Patent, 6:25-30. The prior art security system using video surveillance 32 includes a set of video cameras 33 a-n for capturing video signals that are transmitted to a video monitor 39 for remote review by security personnel. As acknowledged by the ’220 Patent, use of a video recorder 41 to store video images for allowing review of the event after it has occurred was also known by the time of filing the ’220 Patent application. The ’220 Patent, 6:30-47.

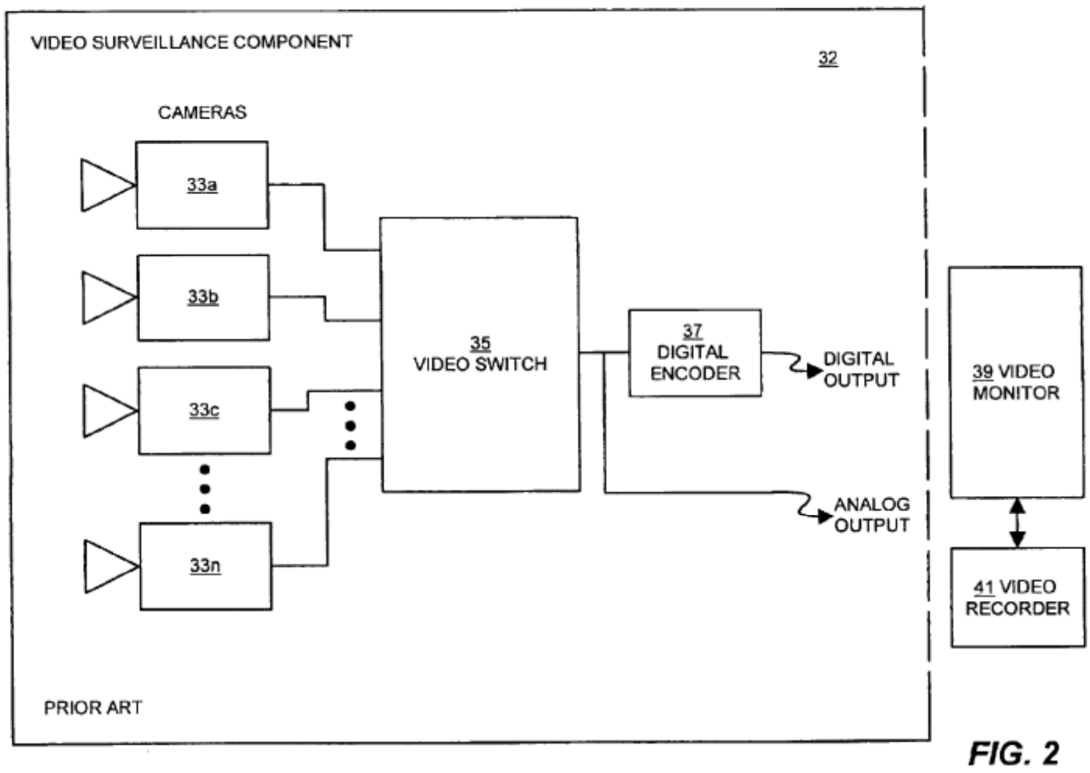


FIG. 2

18. By the mid-1990's, surveillance systems networked to allow remote viewing and monitor using an internet browser had also been known and commercialized. For instance, Axis Communications introduced ThinServer™ Devices, each of which is essentially a network server with built-in Web server that allows an authorized user to access and manage connected devices (e.g., cameras) via any standard Web browser. *See, e.g.,* Axis 240 User's Manual (Revision 1.4, Dated November 1998, "Axis 240") at 3.

19. A device connected to the network will contain a network interface that includes, or is, a port with a port number or identifier accessible by other connected devices in the network. Multiple devices in a network

surveillance system may have individual network interfaces connected to the network directly, or they may be coupled together to a single network interface that is responsible for data communication over the network. The Axis 240 Network Camera Server is an example ThinServer™ Device that functions as a network interface to connect one or more video cameras to an Ethernet network. The Axis 240 Network Camera Server includes built-in webs server and provides interactive surveillance and remote monitoring. Images captured by the connected cameras are transmitted over the local network or Internet and are accessed by users through a Web browser. *See, e.g.,* Axis 240 at 7.

20. Typically, network-connected devices in the same communication network use a common communication protocol to facilitate communication. TCP/IP (Transmission Control Protocol/Internetworking Protocol) is a well-known, widely adopted network protocol. TCP/IP is a stack of protocols that includes multiple layers of sub-protocols. The TCP/IP protocol includes Internet Protocol (IP) for the Internetwork Layer (also called the Internet, or network layer), which interconnects devices on different networks.

21. IP is a packet communication protocol based on IP datagrams. IP datagrams are packages of data with source and destination addresses (also known as IP address).

22. Destination addresses allow for the routing of packets between devices and networks connected to on the Internet. Each network-connected device has a unique IP address for identification and addressing during network communications. Any device communicating with others using IP protocol would need a unique IP address to do so.

23. The metric "bandwidth", measured in Hertz, refers to the capacity or rate of a network connection of a communication link. Other metrics, such as data rate (measured in bits per second) can also quantify the capacity of a communication link.

24. Bandwidth can be a valuable, limited resource affecting the quality of service (data rate, latency, etc.) delivered by a network. To effectively use available bandwidth, network surveillance systems may be designed to limit the amount of data transmission over the network.

25. For example, data compression techniques may be used to reduce the amount of data transmitted over the network for remote monitoring. Certain event data may only be delivered if triggered by an event (e.g. alarm or user request). Depending on system's resources and design

choices, data content and delivery may be modified to remain within bandwidth constraints.

IV. Background of the ’220 Patent

26. The ’220 Patent discloses a system for detecting an event within a premises and for providing data, such as live or recorded video and audio, regarding said event to a web site. The event may be an unauthorized entry to the premises, a fire, or a maintenance malfunction within the premises. The ’220 Patent, Abstract.

27. Upon detection of the event, a camera and other data-gathering devices are activated; then, the data from these devices is transmitted to a website. Said website can be accessed by authorized users for monitoring the event in real time or as a recording. The ’220 Patent, Abstract, 4:8-11, and 4:19-27.

V. Application of Creamer, Creamer in View of Fernandez, and Thomas in View of Fernandez to the ’220 Patent Claims

28. It is my opinion, upon review of the art, that Creamer in view of Fernandez, and Thomas in view of Fernandez teach the claims of the ’220 Patent which are relevant to this examination. I discuss, in detail, my reasoning below.

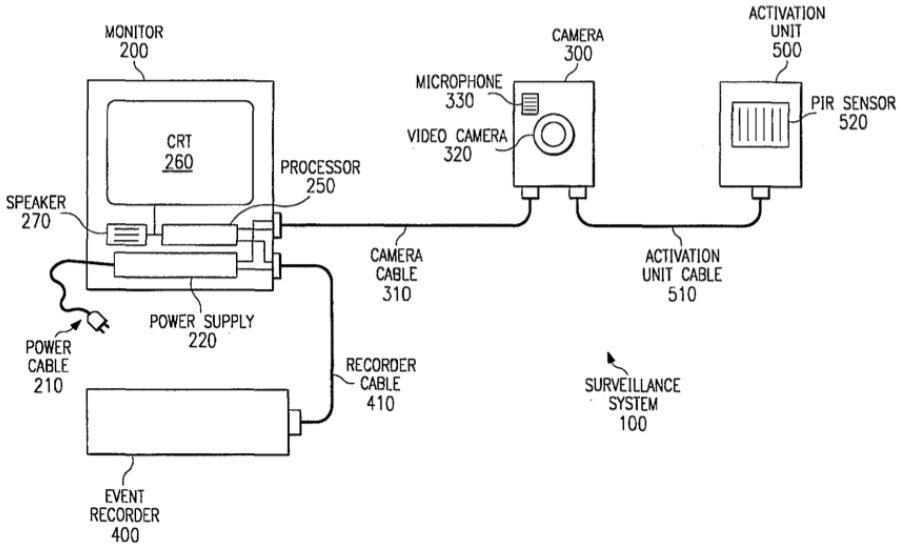
29. In my discussion, I reference Broady, Maram, Toyoshima, and

Sengupta. An overview of these references is provided below.

A. Overview Of Referenced Art

30. U.S. Patent No. 5,495,288 to Broady et al. ("Broady") filed Feb. 27, 1996 teaches a monitoring system whose sensors trigger activation of a camera connected to a monitoring system. Broady teaches that the entire system is turned off (and thus, not recording any video frames) until it is triggered. Once a sensor triggers the system, the camera will start monitoring video and recording. Broady, Abstract, FIG. 1.

> "When the activation unit detects a condition for which the surveillance system is to record, the activation unit sends an activation signal through the activation unit cable, camera, and camera cable to the monitor. A processor in the monitor sends a command to the event recorder over the recorder cable to record the video and audio signals generated by the camera, which are also sent to the event recorder over the recorder cable." (Broady Abstract)



Broady FIG.1

31. U.S. Patent No. 5,019,803 to Maram ("Maram") filed Dec. 2, 1988 teaches a detection system for homes and offices that uses a passive infrared detector and wireless radio to transmit a signal upon detection, or when the system is low on batteries. Maram, Abstract and FIGURE 1A.

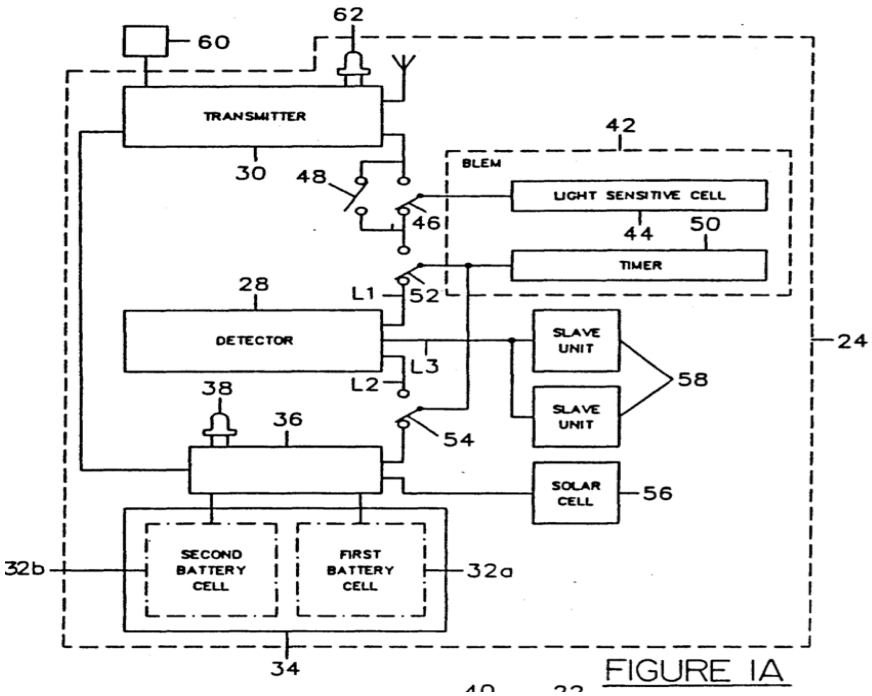
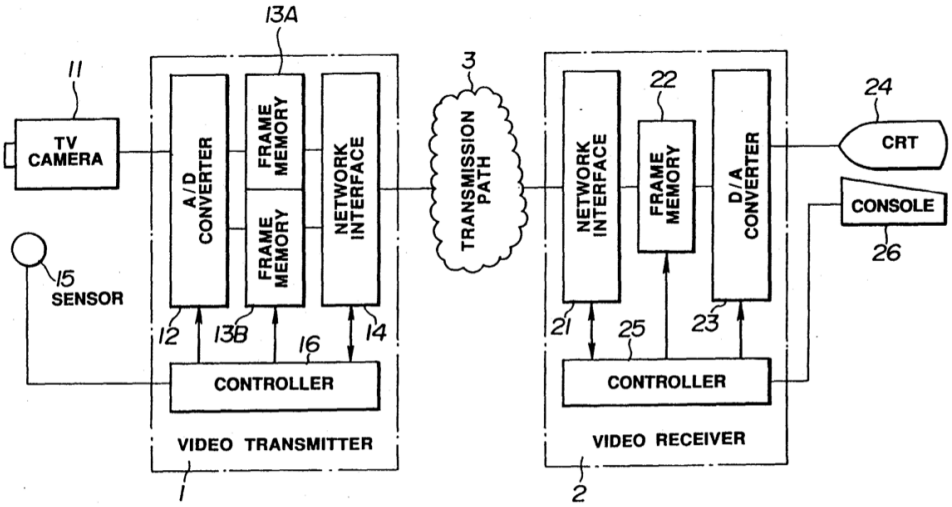
32. 

FIGURE IA

33. U.S. Patent No. 5,229,850 to Toyoshima ("Toyoshima") filed Jul. 29, 1991 teaches a system where a "communication path is established, only when monitoring a video signal on an object is required". Toyoshima, Abstract. The system's video recorder is activated due to sensor activation. Because of potential time delays in the activation of the communication subsystem, Toyoshima discloses that the video subsystem stores the data in video memory until such time that it can be forwarded to the monitoring system, marked as "video receiver" in FIG. 1.

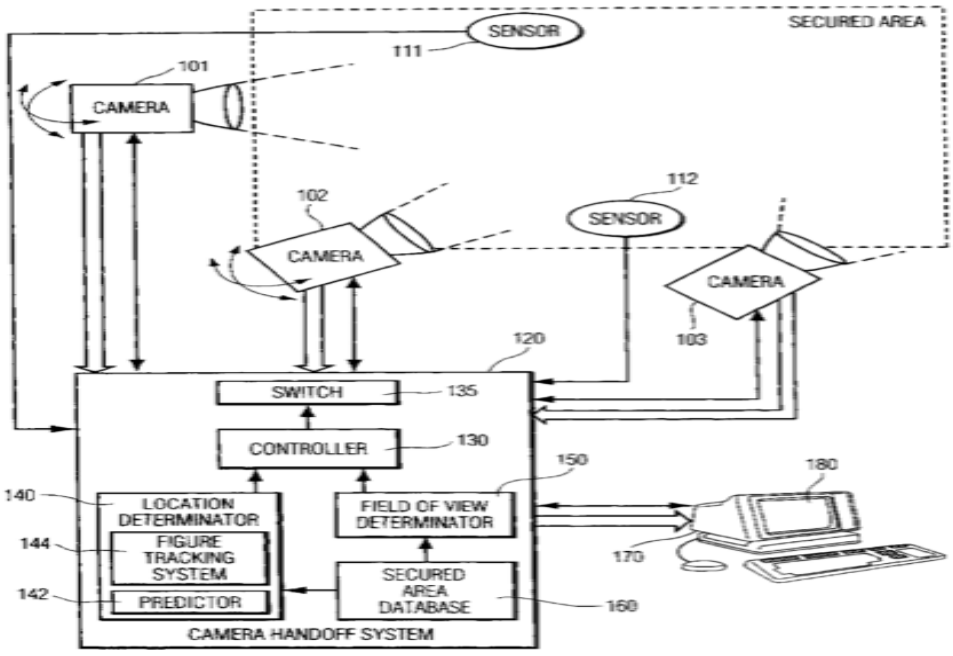
FIG.1



34. U.S. Patent No. 6,359,647 to Sengupta et al. (hereinafter "Sengupta") filed Aug. 7, 1998 teaches a system of multiple video cameras that figuratively follows an intruder to a facility. The system activates alternate cameras based on sensors that tell it where the intruder is located at any given time. Sengupta, Abstract. The Abstract is instructive:

> "The invention provides for the automation of a multiple camera system based upon the location of a target object in a displayed camera image. The preferred system provides a nearly continuous display of a figure as the figure moves about throughout multiple cameras' potential fields of view. When the figure approaches the bounds of a selected camera's field of view, the system

determines which other camera's potential field of view contains the figure, and adjusts that other camera's actual field of view to contain the figure. When the figure is at the bounds of the selected camera's field of view, the system automatically selects the other camera. The system also contains predictive location determination algorithms. By assessing the movement of the figure, the system selects and adjusts the next camera based upon the predicted subsequent location of the figure." (Sengupta, Abstract)



Sangupta FIG 1

B. Creamer

35. Creamer teaches the following:

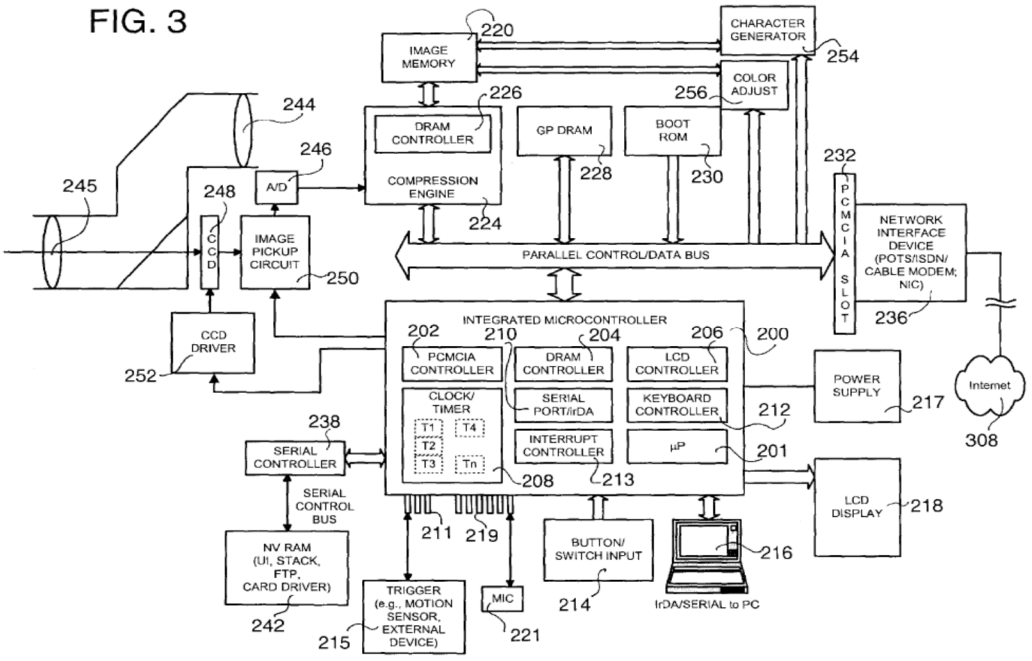
    a. an integrated Internet camera for capturing digital images,

    b. transmitting real-time and stored digital images to the Internet,

    c. and permitting authorized user accesses to said digital images via the Internet. Creamer, Abstract and 2:48-51.

36. The camera can be used in connection with security, child care monitoring, and surveillance. Creamer, 33:39-42. Creamer does not limit the use and clearly addresses, at a high level, the uses described in '220. Creamer, 10:36-38, 11:7-9, and FIG. 3. As can be seen in the excerpted figure below, the integrated Internet camera (1) includes an image-forming optical system (245), an image pickup (248), an image pickup circuit (250), a microcontroller (200), and a network interface device (236) communicably linked to the Internet (308).

FIG. 3



37. The camera (1) is connected to a number of triggering devices (215) such as motion sensors or trip switches for detecting events such as unauthorized entry. The triggering devices (215) send event signals to the microcontroller (200). Creamer, 7:14-24 and FIG. 3.

Imaging Device Activated By Controller Upon Event Signal

38. Creamer discloses that the triggering of the trigger devices causes activation of the camera and initiates transfer of digital image files. Creamer, 5:12-18. Claim 72 of Creamer teaches that the microcontroller activates the imaging device to initiate image capture and image transmission in response to a trigger event:

"72. The integrated network-capable camera according to

> claim 64, further comprising a trigger device linked to said microcontroller, wherein said microcontroller initiates an image capture and transfer of the digital image files to the destination computer, in response to triggering of said trigger device." (Creamer, Claim 72)

39. In fact, a person of ordinary skill in the art at the time of filing the application for the '220 Patent (a "POSITA") would readily appreciate that, in terms of design choices, the imaging devices would either be "always on" or activated "on-demand." Activating an imaging device "on-demand" upon a sensor signal was a known design choice in the art by the time of filing the '220 Patent application.

Broady

40. For example, Broady explicitly discloses that, when a passive infrared (PIR) sensor senses a condition for activating the surveillance system, an activation unit sends an activation signal to the camera. *See, e.g.,* Broady, 3:12-23.

> "The activation unit 500 contains a sensor, such as apassive infrared (PIR) sensor 520, for detecting a condition for which the surveillance system 100 requires activation. Although the present embodiment illustrates the use of thePIR sensor 520, other sensors, such as glass

break detectors, motion detectors, open circuit sensors, closed circuit sensors, or the like, can be used in place thereof. When the PIR sensor 520 senses a condition for activating the surveillance system 100, the *activation unit 500 sends an activation signal to the camera 300* through the activation unit cable 510. *The camera 300, in tum, sends the activation signal to the monitor* 200 through the camera cable 310." (Broady, 3:12-23, emphasis added)

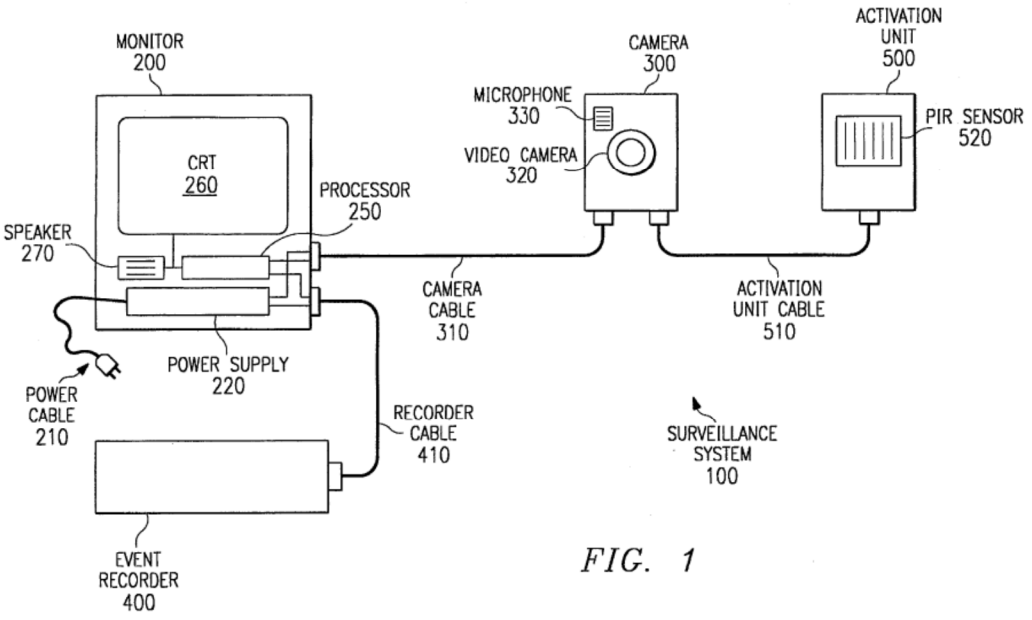


FIG. 1

U.S. Patent Feb. 27, 1996 Sheet 1 of 3 5,495,288

"A processor 250 in the monitor 200 receives the activation signal from camera cable 310. Upon receiving the activation signal, the processor 250 *sends the video signals and audio signals from the camera 300 to the event recorder 400*, and a command for the event recorder 400 to record the video and audio signals

generated by the camera 300." ." (Broady, 3:24-28, emphasis added)

"Although the processor 250 is illustrated herein as being a part of the monitor 200, the processor 250 can be a separate component from the monitor 200, *or a part of any other component in the surveillance system 100*, such as the event recorder 400." (Broady, 3:29-38, emphasis added)

"Although the surveillance system 100 of FIG. 1 is illustrated with only one camera 300, *it is possible to have a plurality of cameras 300 connected to the monitor, with each camera 300 connected to an activation unit* 500." (Broady, 3:45-49, emphasis added)

"When the *activation unit detects a condition* for which the surveillance system is to record, the *activation unit sends an activation signal* through the activation unit cable, camera, and camera cable to the monitor." (Broady, Abstract, emphasis added)

"REMOTE ACTIVATED SUVEILLANCE SYSTEM "(Broady, Title)

Sengupta

41. As another example, Sengupta discloses automatic camera handoff security systems that automatically select and thus activate a camera to track a target point when an alarm condition is sensed. *See, e.g.,* Senguputa, Title, 2:43-49, and 3:31-32.

> "AUTOMATED CAMERA HANDOFF SYSTEM FOR FIGURE TRACKING IN A MULTIPLE CAMERA SYSTEM" (Sengupta, Title)
>
> "In another embodiment, the selection of a target is also automated. Security systems often automatically select a camera associated with an alarm, for the presentation of a view of the alarmed area to the operator. By associating a target point with each alarm, for example the *entry way of a door having an alarm, the system can automatically select and adjust the camera associated with the alarm to contain that target point,* and identify the target as those portions of so the image which exhibit movement. Thereafter, the system will track the target, as discussed above." (Sengupta 2:43-49, emphasis added)
>
> "The optional alarm sensors 111, 112 provide for *automatic camera selection when an alarm condition is sensed*. Each alarm sensor has one or more cameras associated with it; when the alarm is activated, an associated camera is selected and adjusted to a

predefined line of sight and the view is displayed on the screen 180 for the operator's further assessment and subsequent security actions." (Sengupta, 3:31-36, emphasis added)

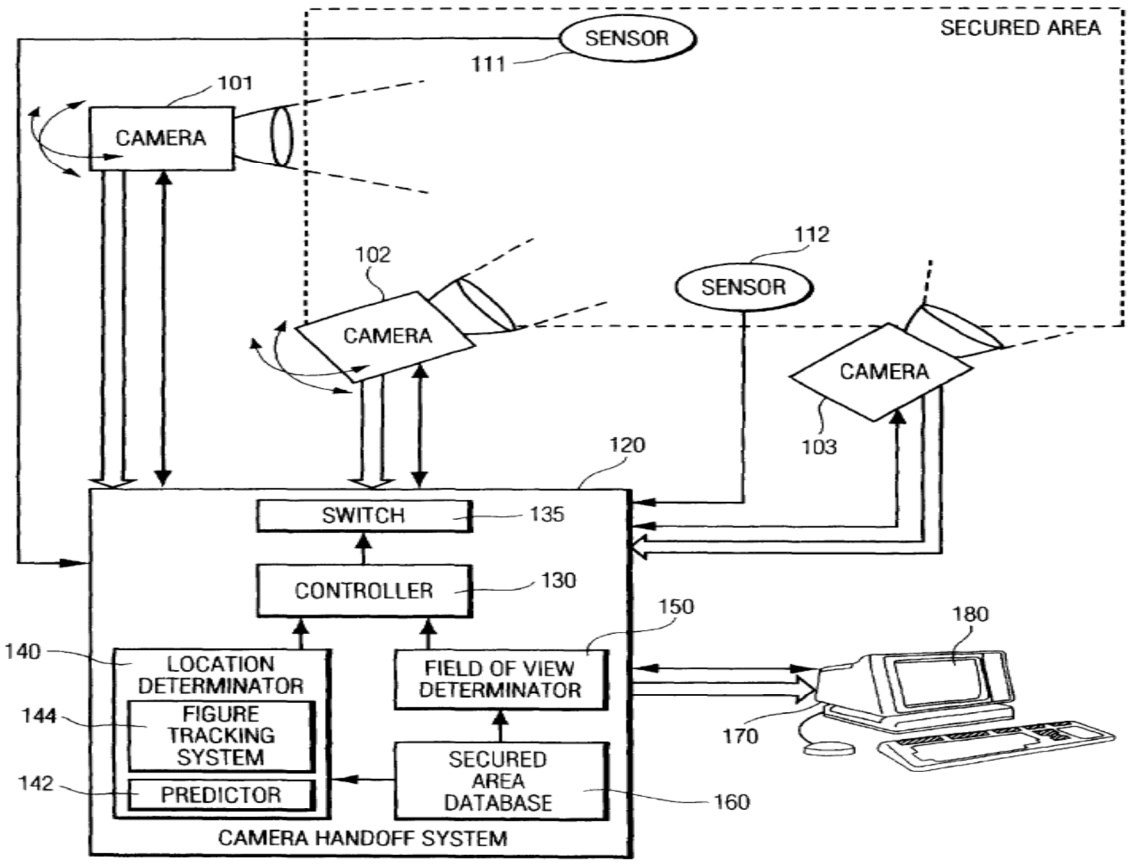


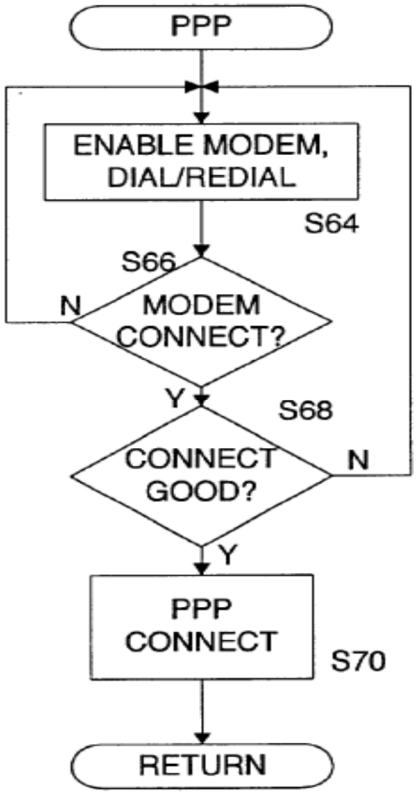
FIG. 1

Sengupta FIG.1

42. Therefore, it would have been obvious to a POSITA to implement the "on-demand" design to activate (e.g., turn on and/or begin signal transmission) the camera by the controller upon receiving the signal from the particular sensor.

Transmission Upon Event Signal

43. In addition to the explicit disclosure (in claim 72) of sensor triggering activating the integrated and network capable camera, sending digital images to the destination computer, Creamer, further discloses a dial-up connection mode of the camera. Creamer, 14:49-51.



44. In FIG. 12 (excerpted above), Creamer teaches how the dial-up connection is made when the camera uses a modem as the network interface. *See also* associated text of FIG. 12 and 19:63-67.

45. A POSITA reading about the "dial-up" connection of Creamer would

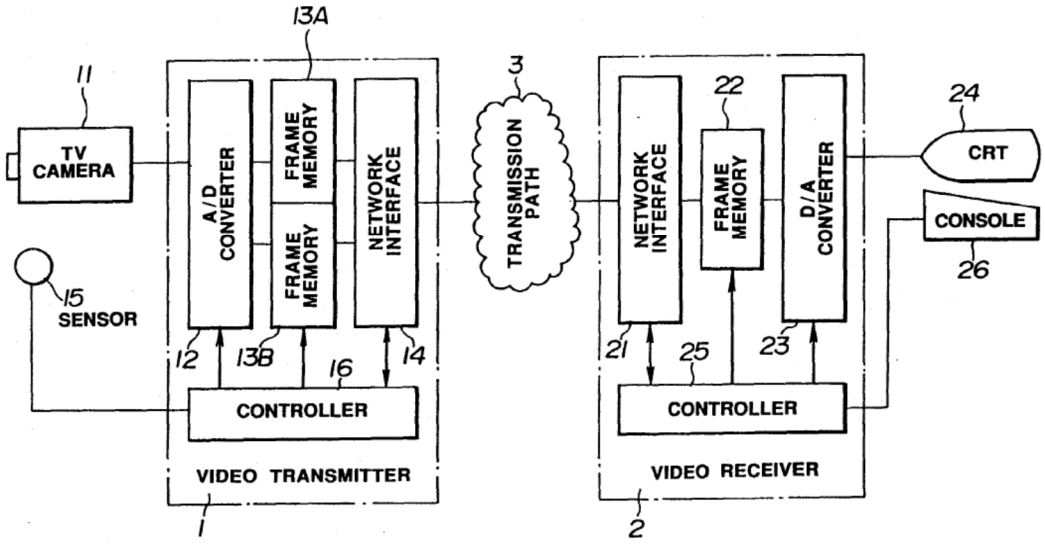
understand that the reference to an upload indication is a reference to the transmission activation signal from the controller that triggers the transmission of the event data after detection of the event to establish the dialup connection.

46. Such an understanding is consistent with the Specification of the ’220 Patent, which itself does not explicitly recite the claimed “transmission activation signal,” but instead discloses that the “transmitter 319 is typically a [digital subscriber line, DSL] modem.” The ’220 Patent, 8:3-10. A DSL modem can connect to the Internet through a dial-up connection, such as the dial-up connection disclosed in Creamer. A dial-up connection uses a modem over a twisted-pair phone line, like a DSL connection.

47. In fact, by the time of filing the ’220 Patent application, triggering data transmission upon detecting an event in network surveillance systems was a known technique.

48. For example, Toyoshima discloses a video monitoring system networked via an ISDN network for transmitting a video signal immediately following the occurrence of an event. Toyoshima, Title, 1:56-59, and FIG. 1.

FIG.1



49. As can be seen in FIG. 1 (excerpted above), Toyashima discloses that the video transmitter (1) acquires and transmits video signal in response to a detection signal from sensor (15) indicative of an abnormal event. Toyoshima, FIG.1, 5:61-67.

Imaging Device Covering The Area Where Trigger Device Is Located

50. A POSITA reviewing Creamer would understand Creamer to disclose that the referenced image capture would be from an imaging device covering the area where the trigger device is located, because it is the area nearest to, or covered by, the device that is triggered that is most relevant.

51. This is particularly true in the case of a motion detector being triggered,

as claimed in claim 74 of Creamer: it is important to see what person (or animal) triggered the motion detector; because the person (or animal) that triggered the motion detector would be located in the area covered by the motion detector, it is only logical that the respective imaging device should cover the same area as covered by the motion detector.

52. This known feature is disclosed, for instance, in UK patent GB 2325548 to Nabavi ("Nabavi") filed May 21, 1997, which discloses a security alarm system including a contact switch and an infra-red motion detector located in a room. See excerpts below:

> "Figure 1 shows a security alarm system in which an alarm controller 1 includes one or more input means 2 and an output means 3. The input means 2 are connected to various sensors or detectors which detect breaches of security of, for example, a home. Two types of detectors are shown, a contact switch 4, which would typically be fitted to a door or window for detecting whether or not the door or window is open, and an infrared motion detector 5 which would normally be fitted in an upper comer of a room, hall or landing for detecting movement within that room. A low-cost television camera 6 could be placed in a room, positioned so as to observe activity in that room. The camera could be positioned so as to observe garages, stables, sheds or even the outside of a house." Nabavi, 3:12-20.

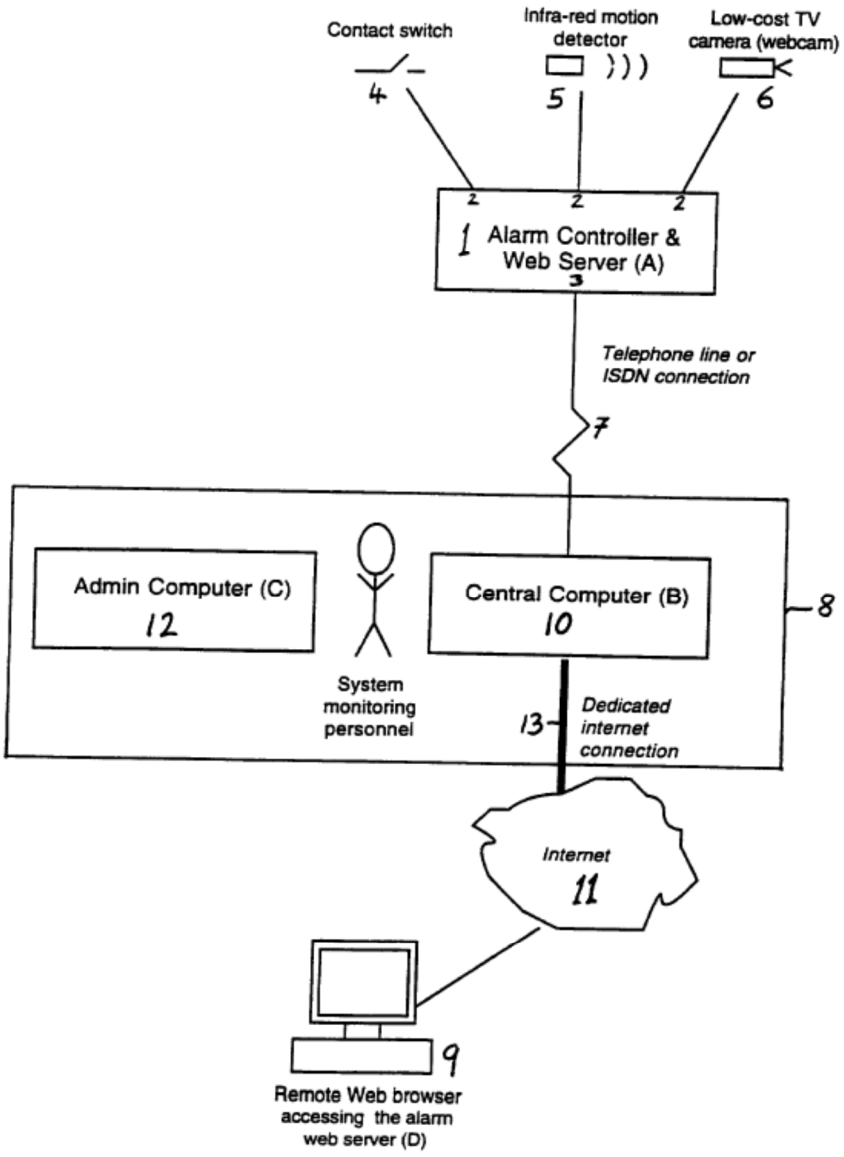


Figure 1: How the alarm controller/web server links via the Security Centre to the internet and hence to the remote user

53. Nabavi further specifies that the security alarm system includes one or more cameras placed in said room, positioned to cover the area where the contact switch and the infra-red motion detector are located, so as to observe activity in that room. Nabavi, 3:12-20 and Figure 1.

Website

54. Figures 4A and 4B of Creamer show that the camera is connected to the Internet (308), via Internet Service Provider (ISP) 304 in FIG. 4A or an intranet server 316 in FIG. 4B. The Internet is coupled to multiple personal computers (310) associated with Web browsers.

FIG. 4A

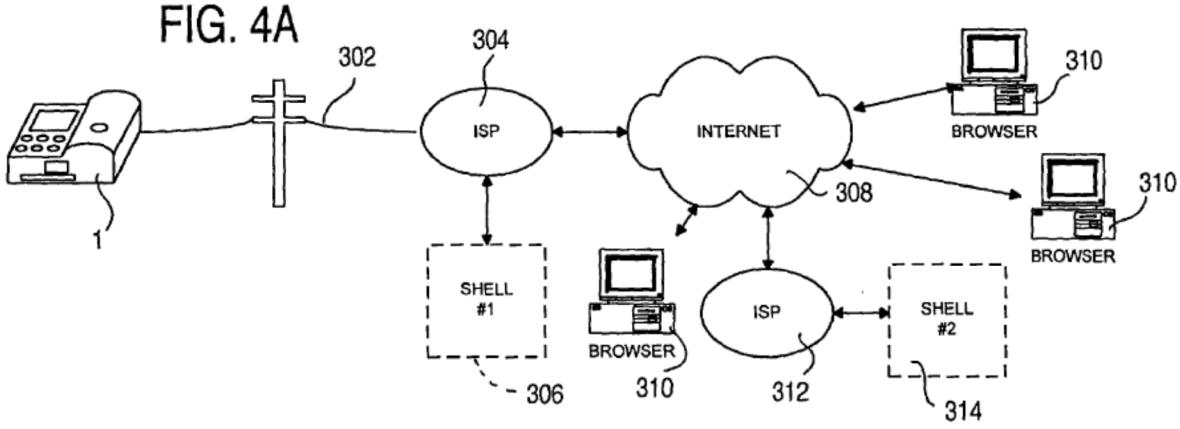
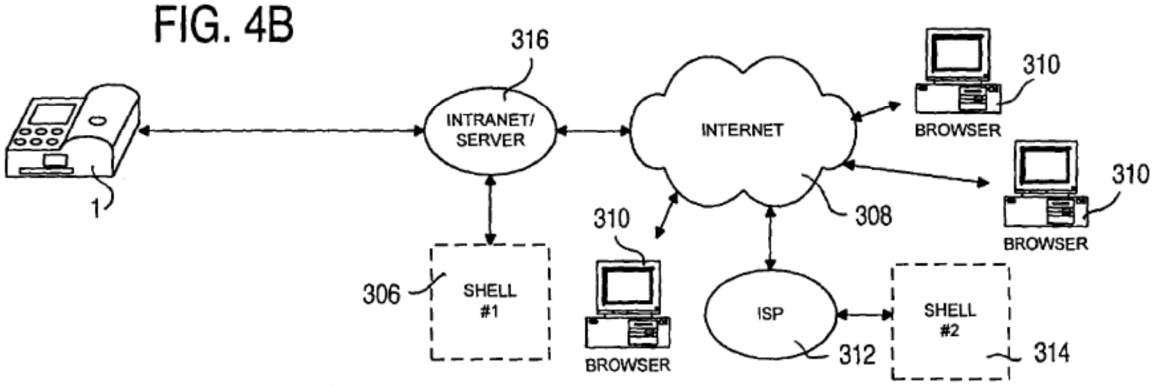


FIG. 4B



55. Creamer discloses that the integrated Internet camera (1) can access a shell account (306) that provides access to a user directory in which the user may store HTML files and other files necessary to create and allow access to a Web page. Creamer, 11:56- 12:4.

56. HTML (HyperText Markup Language) is the primary markup language for creating web pages and other information that can be displayed in a web browser.

57. Creamer further discloses that the user directory stores compressed image files referenced by, or linked to, the Web page and viewable by any remote user using an accessing device such as a personal computer (310) equipped with a Web browser linked to the Internet (308). Creamer, 12:5-9. Creamer also makes clear reference to the "World Wide Web" (a hypertext-driven global multimedia system, hereinafter the "Web"). Creamer, 1: 22-23.

58. A "website" can refer to a computer system that has a recognized domain name and runs a Web server for publishing and providing access to a group of related webpages on the Web. In this context, a website can include a web-based front end (e.g., server-based applications such as web pages) and a backend (e.g., a computer system having a domain name and running a web server) that includes or is connected to varying hardware to augment the server's functionality and connectivity (e.g., initiate phone call). Publically accessible websites collectively constitute the World Wide Web.

59. Sometimes, the terms "website" and "web page" are used

interchangeably. In this context, a website can include a set of related web pages and is hosted by a web server (e.g., a computer system) for access through a web browser.

60. Regardless, it would have been obvious to a POSITA that, although Creamer does not use the term "website," Creamer's references to a Web page, and access to the Web page using a computer 310 equipped with a Web browser linked to the Internet (Creamer, 12:5-9), the Internet Service Provider (ISP) 304 and intranet server 316 (Creamer, FIGS. 4A-4B), and the domain name server (DNS) (Creamer, 14:42-46), are references to a website that publishes said Web page by a computer system having a domain name and a web server.

Authorized Entity

61. Creamer teaches that the digital images captured and transferred by the camera (1) to the Internet are available to any authorized user on the Internet. Creamer, Abstract, 2:55-59 and 3:45-59.

62. Creamer further discloses a network authentication device for providing network login authentication for connecting to the predetermined Internet address via the network interface device. In this manner, the integrated Internet camera may access and transmit files to networks having security and authorization provisions. Creamer, 4:25-31.

Creamer's security and authorization provisions, and the login authentication mechanism, clearly indicate that the digital images are accessible to "authorized entities".

63. Creamer further discloses that the camera (1) can be used in entertainment, advertising, education, security, traffic monitoring, weather monitoring, child care monitoring, surveillance, and general consumer applications. Creamer, 33:39-42.

64. In view of the Creamer disclosures regarding camera use as well as his disclosures regarding security a POSITA would conclude that an authorized entity (who can access the Web page and viewing event data captured by the integrated Internet camera) could be one of the following:

a. a central monitor (e.g., in traffic monitoring and weather monitoring applications);

b. a property owner (e.g., in entertainment, education, and security applications);

c. police personnel (e.g., in security and surveillance applications);

d. fire personnel (e.g., in security and surveillance applications);

e. or emergency medical personnel (e.g., in child care monitoring applications in hospitals).

Detecting Event In A Premises

65. Many, if not most, classrooms and child care facilities are located inside a premises. In view of Creamer's disclosed camera use in education and child care monitoring (Creamer, 33:39-43), a POSITA would understand that the integrated Internet camera (1) of Creamer would be used for detecting events in a premises.

Lamp

66. Creamer discloses that triggerable devices (e.g., lighting, an alarm, etc.) can be connected to at least two input trigger ports (211a) and one output trigger port (211b) and they thus would be coupled to the microcontroller (200). Creamer, 32:47-61 and FIG. 3 (reproduced above in ¶ 36). Creamer discloses that "local lighting" can be linked to image captures, and activated to accompany the image captures. Creamer, 32:60-61.

67. A POSITA reviewing Creamer would conclude that the local lighting described in Creamer could be a lamp (a well-known, commonly used lighting device on various premises) or any other known lighting device, such as a spotlight, floodlight or infrared light. A POSITA would conclude that this light would be activated while the video camera is operating to enable the camera to record the event if, for example, it is

dark or there is low light.

C. Creamer in View of Fernandez

68. Creamer teaches the features described in ¶¶ 35-67.

69. Fernandez discloses a surveillance system that includes a network (hardwired or wireless) for monitoring and processing remote and/or local moveable objects. Fernandez, 1:33-36. The integrated network includes the following:

a. cameras that detect objects and generate an image signal,

b. a browser interface that displays objects and detectors,

c. and an Internet that provides selectable connection between a system controller and various cameras according to object positions. Fernandez, Abstract.

70. Fernandez further discloses a detector (3) and a sensor unit (44), which may be the same type of device. Fernandez, 3:22-25 and 6:16-29. While the detector and/or sensor unit may be a video camera, Fernandez discloses that they may also be a non-imaging sensor, including a microphone, a temperature sensor, a smoke detector, etc. Fernandez, 4:35-50 and 6:16-29.

71. Because both Creamer and Fernandez teach using similar components (cameras, other forms of sensors, and detectors) applied to the same type

of system (a surveillance systems that uses the Internet to allow authorized users to remotely view images and other data on a website), a POSITA would be motivated to combine Creamer and Fernandez; such a combination would yield known or predictable results, based on the knowledge of a POSITA.

72. For example, a POSITA would be motivated to add to or modify the triggering devices of the integrated Internet camera system taught by Creamer with any of the detectors and triggering devices as taught by Fernandez (e.g., as in Claims 2-10 and 16-19) as the sensor/triggering devices are commonly incorporated components of a network surveillance system. Combining components of two known surveillance systems, each of them networked to allow remote viewing using an internet browser, into a single network surveillance system according to known methods would be well within the capabilities of a POSITA and have resulted in known, predictable results to a POSITA.

73. Additionally, Fernandez discloses a number of known techniques used in surveillance systems networked for use with the Internet, such as the following:

a. using the network surveillance system to detect events in a premise and activate an imaging device of the network surveillance system

upon a signal from a sensor located in an area covered by the imaging device (as in Claims 1, 7 and 25);

b. supporting continuous or dynamic audio/video streaming of the event data via the Internet to authorized users (as in Claims 11 and 12);

c. providing and transmitting unique identifiers for each of the sensors over the network (as in Claim 13);

d. and allowing various authorized entities to access the event data from a website over the network (as in Claims 14 and 20-28).

74. A POSITA would be capable of applying the known techniques of network surveillance systems as taught by Fernandez to the integrated Internet camera system as taught by Creamer; the result of this application would have been predictable to a POSITA.

Website

75. Fernandez expressly uses the term "website" and frequently references to it. For example, Fernandez discloses:

> accessing real-time object data or other contextual information available or accessible via public or private IP address or other ***website*** associated with or supported by one or more detector 3-server 5 coupled pair, (Fernandez, 3:51-54, emphasis added).

> accessed object data or other contextual information may

be obtained by one or more monitoring user controller 6 through network 8 and one or more conventional or proprietary wired or wireless communicator 7 coupled thereto for communicating with one or more target units 4 as well, preferably via public or private IP address or other ***website*** associated with or supported by one or more target unit 4 (Fernandez, 5:22-29, emphasis added).

Preferably, browser software functions according to commercially available browser product such as, e.g., Netscape Navigator or Microsoft Explorer, or any other functionally equivalent means for accessing Internet, intranet or other ***conventional or proprietary LAN/WAN website***, network node or IP address. (Fernandez, 8:62-67, emphasis added).

a controller comprising a browser software interface for accessing a ***website*** comprising remote real-time object data associated with the remote object and displaying the remote object data on a screen,

(Fernandez, 22:7-11, emphasis added).

76. As such, the teaching of "website" by Creamer would have been even more apparent to a POSITA reviewing Creamer with knowledge of Fernandez, in view of Fernandez's explicit references and ample description of a "website". Alternatively, it would have been obvious to

a POSITA to incorporate the "website" as taught by Fernandez into the integrated Internet camera as taught by Creamer, for example, to allow "accessing real-time object data or other contextual information available or accessible via [the] website" as taught by Fernandez.

Detecting Event In A Premises

77. Fernandez teaches the integrated surveillance network used for detecting an event in a premises, for example, by placing the sensory and positional detectors along elevators, buildings, restrooms, classrooms, hotel, offices, hospitals, prisons, storage warehouses, churches, stores, and virtually any other practical location of monitorable human or animal activity. Fernandez, 19:35-41.

78. Not only would a POSITA reviewing Creamer use the camera taught by Creamer for detecting an event in a premises, a POSITA would have also been motivated to use the camera taught by Creamer to monitor and detect events in a premises in view of the teaching of Fernandez, as such a usage would have yielded known, predictable results, based on the knowledge of a POSITA. Furthermore, the '220 Patent acknowledges that prior art systems were used to detect events in a premises: "[s]ystems for detecting and reporting intrusions…are well known in the prior art... for securing and protecting the occupants of a premises." The

’220 Patent, 1:16-19.

Imaging Device Covering The Area Where Trigger Device Is Located

79. Fernandez discloses that the detectors (3) may be digital imagers or video capture devices (Fernandez, 4:23-28) or they may be implemented to sense state and other signals from motion detectors, burglar alarms, door or window open/close detectors (Fernandez 4:43-50).

80. Fernandez teaches that in the case of unauthorized home entry, such sensed state or signal may trigger other functionality, such as taking electronic photographs and/or notifying certain entities. Fernandez, 4:43-50.

81. Fernandez further discloses that the image device captures event data and tracks the object/event detected at a particular sensor that is in an area covered by the particular imaging device. Fernandez, 4:57-61.

82. Therefore, Fernandez teaches use of cameras covering the area where motion detectors are triggered so as to observe and track the object. It would have been obvious to a POSITA reviewing Fernandez, to implement the Creamer system so as to activate a camera for image capture in the area covered by the imaging device, for example, in order to track the event detected by the trigger device that is located in the coverage area of the image device.

Integrating Various Sensor Components

83. Fernandez discloses that the detector (3) and sensor (44) include a variety of sensing and measuring devices (e.g., motion detector, burglar alarm, door or window open/close detector, smoke detector, thermostat, etc.). Fernandez, 4:43-50.

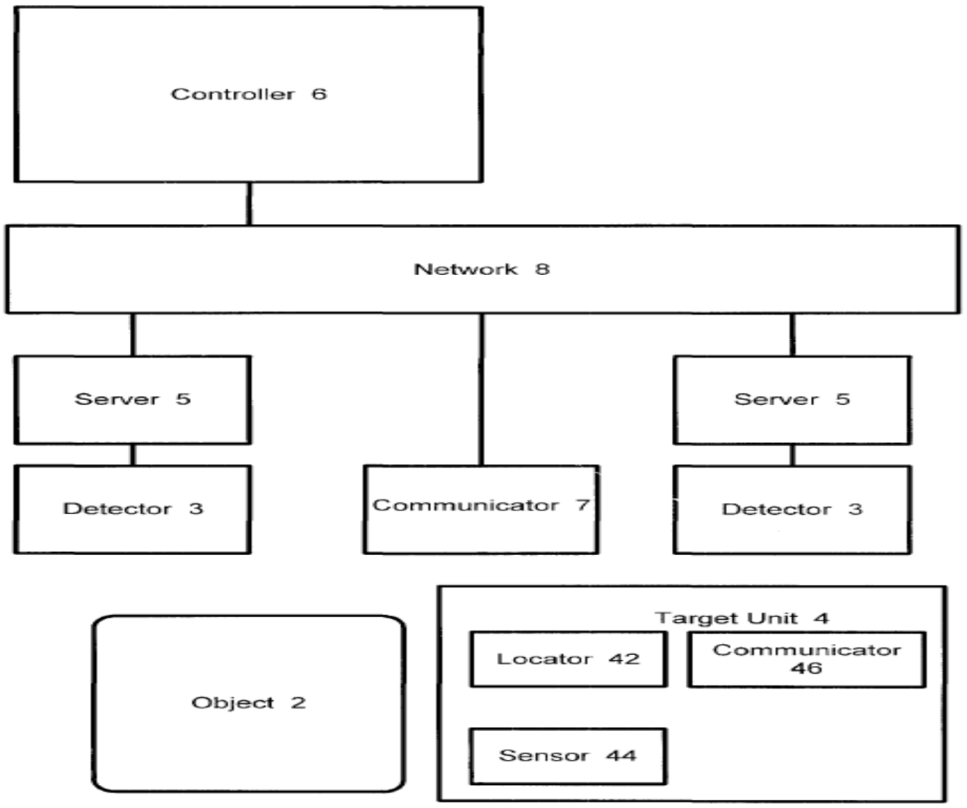


FIG. 1

84. Fernandez teaches coupling the detector (3) to the server (5) that is further connected to the network (8). Fernandez, 3:17-57 and FIG.1. These various detectors and sensors are thus integrated into the surveillance system and networked, e.g., based on Internet and TCP/IP protocol (Fernandez, 3:43-57), to allow remote access and viewing of

statuses and information captured by the various detectors and sensors.

85. It would have been obvious to a POSITA to integrate any of the sensor components in the network surveillance system as taught by Fernandez into the integrated Internet camera system taught by Creamer. Such a combination would have been well within the capabilities of a POSITA and would have yielded known, predictable results to a POSITA.

86. In fact, the ’220 Patent itself acknowledges that, by the time of filing the ’220 Patent application, prior art surveillance systems had incorporated various sensors/detectors including temperature or other maintenance function sensors 12, entry point sensors 13, motion sensors 15, beam sensors 17, fire/smoke detector 18, audio detectors 19, broken glass detector 20 as components of a network surveillance system. The ’220 Patent, 5:35-52 and FIG. 1.

Beam Sensor

87. Fernandez discloses that detectors (3) may be implemented as a fixed motion detector that activates in response to object movement to sensing a state of unauthorized home entry. Fernandez, 4:43-50 and 12:35-36.

88. It would have been obvious to a POSITA reading about use of a “motion detector” in Fernandez along with a broad range of other detectors in the “unauthorized home entry” detection system of Fernandez that a beam

detector could be used as detector (3) in addition to, or in lieu of, a motion detector to detect unauthorized movement in a passageway and be an integral component of the network surveillance system.

89. In fact, integrating a beam detector into network surveillance systems was a known technique by the time of filing the ’220 Patent application.

90. For example, Thomas discloses a beam sensor as an example sensor component of a surveillance system that is networked to allow remote monitoring and reviewing of event data using an Internet browser. (*See, e.g.,* Thomas at Page 1, 3rd paragraph). In addition, the ’220 Patent shows beam sensors 17 as a component of a prior art security system 11. The ’220 Patent, 5:46-48 and FIG. 1.

Broken Glass Detector

91. Fernandez discloses a “door or window open/close detector.” Fernandez, 4:45-46.

92. It would have been obvious to a POSITA reading about the use of a “burglar alarm, door or window open/close detector” along with a broad range of other detectors in the “unauthorized home entry” detection system of Fernandez, that a broken glass detector could be used as a detector (3) in addition to, or in lieu of, a door or window open/close detector.

93. In fact, by the time of filing the ’220 Patent application, incorporating broken glass detectors in surveillance systems was a known technique. For example, Broady discloses broken glass detectors as an example sensor component for a remote activated surveillance system. Broady, 3:16 and Title. In addition, the ’220 Patent shows broken glass detector 20 as a component of a prior art security system 11. The ’220 Patent, 5:51-52 and FIG. 1.

Fire Detector

94. Fernandez discloses a “smoke detector.” (*See, e.g.,* Fernandez, 4:46).

95. It is well known that a smoke detector is a form of a fire detector because a smoke detector typically detects smoke, heat, or an open flame, as an indicator of a fire.

96. It would have been obvious to a POSITA reading about use of a “smoke detector” in Fernandez along with a broad range of other detectors in the “unauthorized home entry” (Fernandez, 4:48) detection system of Fernandez, that a fire/flame detector could be used as detector (3) in addition to, or in lieu of, a smoke detector to detect fires and/or open flames.

97. In fact, systems by the time of filing the ’220 Patent application, incorporating a fire/flame detector with surveillance system was a

known technique. For example, Maram discloses "fire detectors" as example components of another surveillance system networked to a main station control unit through wire connectors for detection of unauthorized intrusion into homes, offices, etc. Maram, 1:8-24. In addition, the '220 Patent shows fire/smoke detector 18 as a component of a prior art security system 11. The '220 Patent, 5:49 and FIG. 1.

Microphone

98. Fernandez discloses that sensor unit (44) may include one or more video cameras and microphones to provide real-time object data, such as audio and/or video signals. *See, e.g.,* Fernandez, 6:16-20.

99. Fernandez further discloses that video and/or audio information may be pre-recorded or delivered from current "live" broadcast or transmission. Fernandez, 11:33-35.

100. In view of the reference to audio and video signals in Fernandez, it would have been obvious to a POSITA reviewing Fernandez that a microphone could be included as part of the imaging device to provide audio signals, as taught by Fernandez.

101. In fact, incorporating a microphone into an imaging device was known in the art by the time of filing the '220 Patent application. For example, Broady explicitly discloses a camera that includes a video camera and a

microphone for generating video and audio signals from an area under surveillance by the surveillance system. Broady, 3:3-5. In addition, the '220 Patent shows fire/smoke detector 18 as a component of a prior art security system 11. The '220 Patent, 5:49 and FIG. 1.

Maintenance Detector

102. Fernandez discloses a maintenance detector such as a "thermostat" (*See, e.g.,* Fernandez, 4:46) for detecting an event that is a premises maintenance malfunction, such as high temperatures due to failure of an a/c system.

103. Fernandez also discloses detecting a premises maintenance malfunction by conducting a ping test upon one or more associated detectors to recognize current conditions or states and reveal defective or unresponsive detectors. Fernandez, 19:18-26.

104. In addition, the '220 Patent shows temperature or other maintenance function sensors 12 (i.e. low heating fuel sensors) as a component of a prior art security system 11. The '220 Patent, 5:35-38 and FIG. 1.

105. Claim 7 of the '220 Patent recites "…a maintenance detector for detecting ***an*** event that is a premises maintenance malfunction" instead of "***the*** event" as in Claim 1. I have been informed that use of "an" in front of the term "event" suggests that this is an event in addition to the

event that is the subject of Claim 1.

106. Nevertheless, to the extent that "an event that is a premises maintenance malfunction" is interpreted to be "**the** event detected at a particular at least one sensor wherein the imaging device is activated by the controller upon receiving the signal from the particular sensor that is in an area covered by a particular imaging device," and "the event data captured by the imaging device upon receiving a transmission activation signal from the controller after detection of **the** event," it would have been obvious to a POSITA to add to or modify the trigger device of Creamer to include the malfunction detector (e.g., thermostat) as taught by Fernandez such that the camera of Creamer initiates an image capture and transfer of the digital image files to the destination shell account in response to triggering (e.g., the premises maintenance malfunction, such as high temperatures due to failure of an a/c system or detecting a defective or unresponsive detector) of the trigger device. Creamer, 5:12-18 and Claims 72 and 74.

Unique Identifiers for Sensors

107. Fernandez discloses that processor (48) transmits object data from sensor (44) to a pre-configured webpage site (Fernandez, 6:50-52) and

the data from sensor (44) includes identifiers associated with detectors (Fernandez, 10:5-12).

108. Thus, Fernandez makes clear that each at least one sensor has an associated identification code that is transmitted to the website with the event data.

109. Fernandez discloses that sensor unit (44) may include multiple sensors (e.g., one or more video cameras, an active sensor, infra-red detector, microphone, or other optical, medical, or otherwise physical monitoring or observation device to provide real-time object data). Fernandez, 6:16-20.

> "Sensor unit 44 may include one or more video cameras, active sensor, infra-red detector, microphone, or other optical, medical, or otherwise physical monitoring or observation device to provide real-time object data, such as audio and/or video signals, or other electronically detectable frequency signal, such as infra-red, or other analog or digital electrical signal sensed from monitored object 2 depending on nature of object and kind of monitoring desired." (Fernandez 6:16-20)

110. So it would have been obvious to a POSITA reviewing Fernandez that each of the sensors could have a unique associated identification code

that is transmitted to the website with the event data so that the specific sensor providing the information reflected on the website regarding respective events can be properly identified at the website.

111. A POSITA reviewing Fernandez would understand that the unique identification code can allow an authorized accessing entity to determine the type of event that has occurred. For example, the authorized accessing entity can determine an unauthorized home entry based on the identification code and the event data associated with the motion sensor or active sensor. Fernandez, 4:43-50[1].

> "Alternately in facility monitoring application, detectors 3 may be implemented to sense state and other measurement signals from motion detector, burglar alarm,

[1] Fernandez discloses "detector 3 may provide substantially equivalent input functionality of sensor 44" (Fernandez, 3:24-26) and "the detector 3 may be implemented be implemented to sense state and other measurement signals from motion detector, burglar alarm, door or window open/close detector, smoke detector, thermostat, phone answering machine, or other electrical home appliance. In certain instances, e.g., unauthorized home entry, such sensed state may trigger other functionality, such as taking electronic photograph and/or notifying certain entities." (Fernandez, 4:43-50.)

> door or window open/close detector, smoke detector, thermostat, phone answering machine, or other electrical home appliance. In certain instances, e.g., unauthorized home entry, such sensed state may trigger other functionality, such as taking electronic photograph and/or notifying certain entities." (Fernandez 4:43-50)

112. Based on the unique identification codes and the event data associated with the multiple sensors, the authorized accessing entity can also identify which sensor (e.g., among video cameras, active sensor, infra-red detector, microphone, or other devices) detected the event.

113. In addition, Fernandez discloses that there can be multiple detectors and multiple video cameras, e.g., Fernandez, FIG. 1 (reproduced above in ¶ 83) and 6:16-20.

114. A POSITA would understand that each of the multiple video cameras can have a unique identification code that is transmitted with the corresponding image signals captured by the video cameras to the website for real-time review. Based on the identification codes, the authorized accessing entity can determine which cameras are providing the imaged data to the web site.

D. Thomas in view of Fernandez

115. Fernandez teaches the features described in ¶¶ 69-114.

116. Thomas discloses systems for remote monitoring and control over a computer network, for example in connection with surveillance and security systems. *See, e.g.,* Thomas at page 1, first paragraph.

117. At one end of Thomas' system, a remote user can monitor the surveillance system using a graphical user interface (GUI) showing a Web page. The GUI can show images from the on-site image sensors and security system statuses detected by various sensors.

118. FIG. 16 of Thomas shows one of several disclosed user interfaces. The GUI window (1600) of FIG. 16 shows the status of various detecting devices of an alarm system, including door sensors, motion sensors, cameras, and switches.

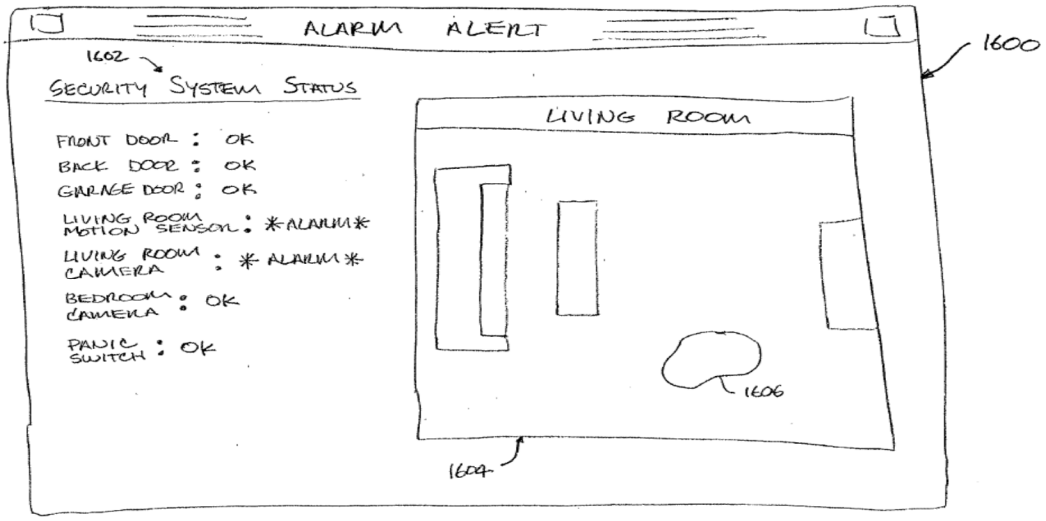


FIG. 16

119. The GUI window (1600) also includes an image viewer (1604) for displaying an image or series of images related to the alarm conditions,

for example, in a living room. Thomas, paragraph bridging pages 16 and 17.

120. FIG. 6 of Thomas shows a plurality of cameras (604) connected to an image controller (602).

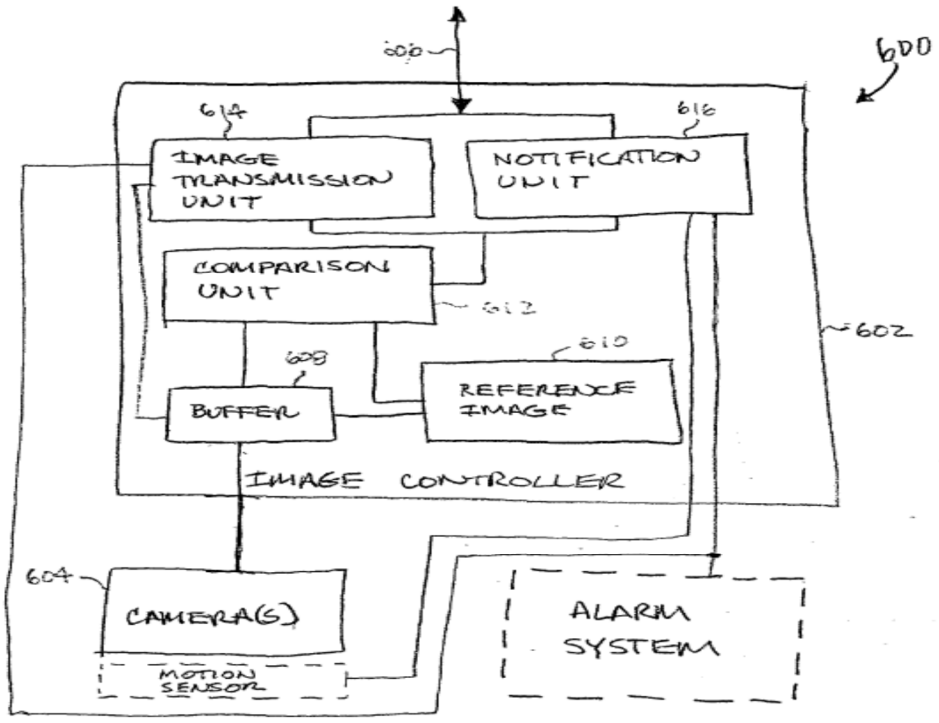


FIG. 6

121. An alarm system and motion sensor are connected to the notification unit (616) of the image controller (602). The controller (602), in turn, is connected to the Internet (104) via link (606), over which images and data are transmitted. Thomas, page 8, second full paragraph.

122. Because both Thomas and Fernandez teach using similar components (cameras, other forms of sensors, and detectors) in similar technologies

(surveillance systems that use the Internet to allow authorized users to remotely view images and other data on a Website), a POSITA would have been motivated to combine Thomas and Fernandez, as such combination would have yielded known, predictable results.

123. For example, a POSITA would be motivated to add to or modify the alarm system devices of the remote monitoring and control system taught by Thomas with any of the detectors and sensors as taught by Fernandez (e.g., as in Claims 2, 3, 5-10 and 16-19) as the detectors and sensor are commonly incorporated components of a network surveillance system.

124. Combining components of two known surveillance systems, each of them networked to allow remote viewing using an internet browser, into a single network surveillance system according to known methods would have resulted in known, predictable results to a POSITA and would have been well within the capabilities of a POSITA.

125. Additionally, Fernandez discloses a number of known techniques used in surveillance systems networked for use with the Internet, such as the following:

a. activating an imaging device of the network surveillance system upon a signal from a sensor located in an area covered by the imaging

device (e.g., as in Claims 1, 7 and 25),

b. providing continuous or dynamic audio/video streaming of the event data via the Internet to authorized users (e.g., as in Claims 11 and 12),

c. and allowing various authorized entities to access the event data from a website over a network (e.g., as in Claims 14 and 20-28).

126. A POSITA would have been capable of applying the known techniques in the network surveillance system as taught by Fernandez to the remote monitoring and control system taught by Thomas and the results would have been predictable to a POSITA.

Image Device Activated Upon Event Signal

127. While Thomas does not specifically disclose that "the imaging device is activated by the controller upon receiving the signal from the particular sensor," controller activation of a particular imaging device upon receipt of a trigger event signal would be an obvious design choice, as the imaging devices would either be "always on" or activated "on-demand." In fact, activating an imaging device "on-demand" upon a sensor signal was a known design choice in the art by the time of filing the '220 Patent application. See also discussion in ¶¶ 39-40 of this declaration. Accordingly, it would have been obvious to a POSITA to implement the "on-demand" design to activate the camera of the remote monitoring

and control system taught by Thomas when the alarm system or motion sensor detects an alarm condition.

128. Fernandez teaches that the detector (3), including an imaging device (video camera, Fernandez, 4:23-28), is coupled to the controller (6) in FIG. 1 (reproduced above in ¶ 83).

129. The imaging device can be controlled to focus, tilt, pan, etc., as well as to observe and track common objects, obtaining various comparative surveillance data. Fernandez, 4:57-61.

> "Optionally, detectors 3 may be coupled to control mechanism for adjusting detector operation, such as focus, tilt, pan, focus, etc., as well as means for causing multiple neighboring detectors to observe and track common object or object set, thereby obtaining various comparative surveillance data." (Fernandez, 4:56-61)

130. Fernandez further discloses that the imaging device is activated by the controller upon receiving the signal from the detectors (3) (motion detector, burglar alarm, door or window open/close detector) when they sense states such as unauthorized home entry; the activated imaging device then takes electronic photographs. Fernandez, 4:43-50.

> "Alternately in facility monitoring application, detectors 3 may be implemented to sense state and other measurement signals from motion detector, burglar alarm,

> door or window open/close detector, smoke detector, thermostat, phone answering machine, or other electrical home appliance. In certain instances, e.g., unauthorized home entry, such sensed state may trigger other functionality, such as taking electronic photograph and/or notifying certain entities." (Fernandez 4:43-50)

131. Though it would have been obvious to a POSITA to implement the "on-demand" design feature of Thomas to activate the camera upon an alarm condition detected by the alarm system, it would also have been obvious for a POSITA to modify the remote monitoring and control system taught by Thomas to activate the camera by a controller upon receiving a sensor signal as taught by Fernandez. Implementing such a known technique or design choice to the image device of the network surveillance system would have yielded known, predictable results, and have been within the capability of a POSITA.

Website

132. A "website" can refer to a computer system that has a recognized domain name and runs a Web server for publishing and providing access to a group of related webpages on the Web. In this context, a website can include a web-based front end (e.g., server-based applications such as web pages) and a backend (e.g., a computer system having a domain

name and running a web server) that includes or is connected to varying hardware to augment the server's functionality and connectivity (e.g., initiate phone call). Publically accessible websites collectively constitute the World Wide Web.

133. Sometimes, the terms "website" and "web page" are used interchangeably. In this context, a website can include a set of related web pages and is hosted by a web server (e.g., a computer system) for access through a web browser.

134. Thomas discloses that the image is transmitted to a hosting Internet server; the interested user is then able to view the image by accessing the Internet server via a web browser application program. Thomas at page 9, 1st partial paragraph.

> "In one embodiment, the image can be transmitted as a file transfer over the Internet 104 and the interested person can be notified by pager. In another embodiment, the image can be transmitted to a hosting Internet server, and the interested user is then able to view the image by accessing the Internet server via a web browser application program. In still another embodiment, the transmission of the image and its notification for the interested user can both be performed by sending an electronic mail message to the interested person, where the electronic mail message includes a textual, visual or

> audio notification and may have the image being transmitted as an attachment to the electronic mail message. The attached image is thereafter able to be remotely viewed by the interested user by a variety of approaches. One approach is for the attached image to be launchable (automatically or manually) into a viewer. Another approach is for the interested user to start an application program which is able to display the image(s)." (Thomas at page 9, 1st partial paragraph.)

135. Thomas further discloses that the user may log on to the Internet (104) and access the GUI window (1500) through a browser. Thomas at 16, 2nd paragraph and FIG. 15.

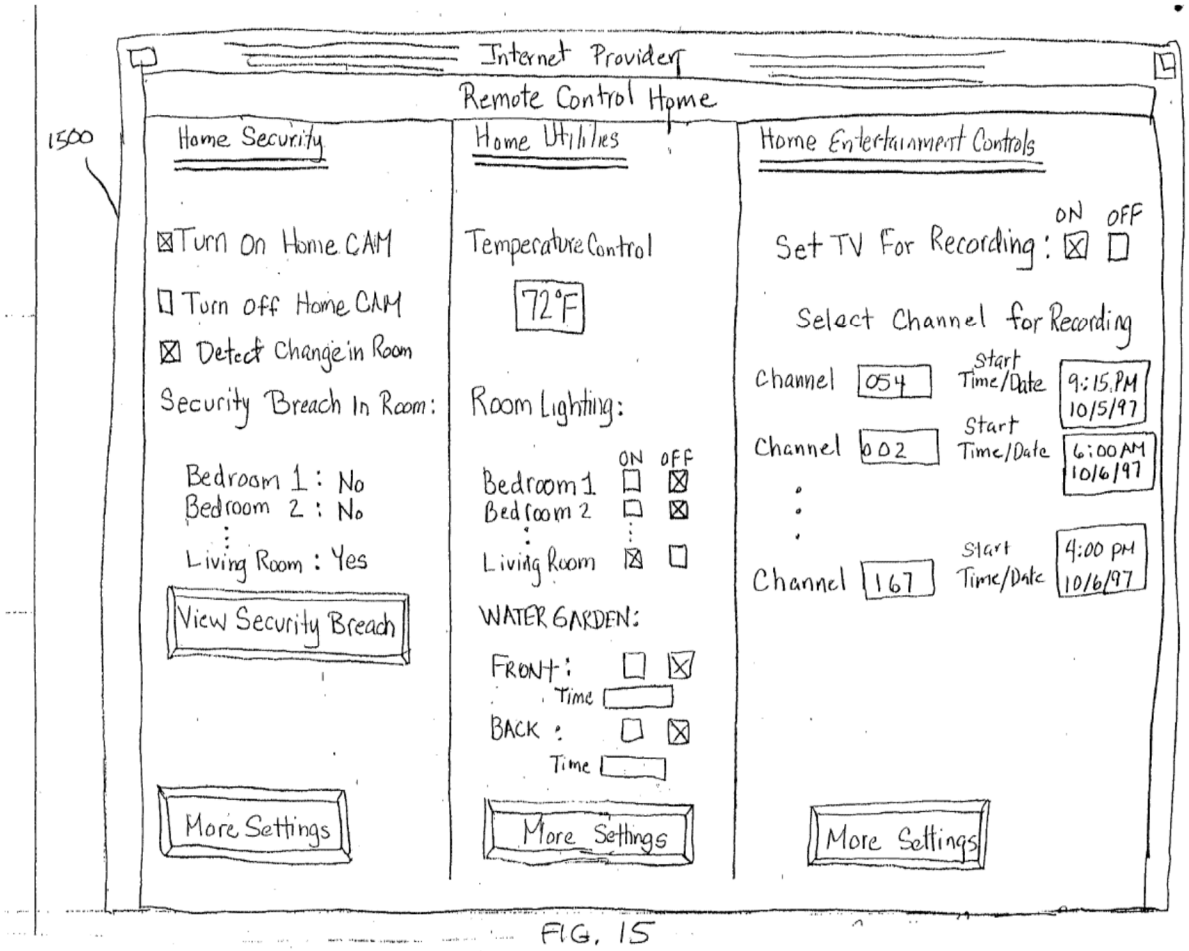


FIG. 15

136. Therefore, a POSITA reviewing Thomas would understand that the references to, among other things, "hosting Internet server" and "web browser application program" would be a reference to a website that publishes said Web page by a computer system having a domain name and a web server.

137. Furthermore, Fernandez expressly uses the term "website" and frequently references to it as set forth more fully in ¶ 75 of this declaration.

138. As such, the teaching of "website" by Thomas would have been more apparent for a POSITA in view of Fernandez's explicit references and ample description. Alternatively, it would have been obvious to a POSITA to incorporate the "website" as taught by Fernandez into the remote monitoring and control as taught by Thomas, for example, to allow "accessing real-time object data or other contextual information available or accessible via [the] website" as taught by Fernandez.

Unique Identifiers For Sensors

139. Thomas shows the statuses of multiple sensors placed in different locations in the displayed GUI windows for users to view through a website. *See, e.g.,* Thomas, FIGS. 15 and 16 (reproduced above in ¶¶ 135 and 118, respectively).

140. For example, FIG. 16 shows sensors at front door, back door, garage door, living room motion sensor, panic switch, etc. To properly distinguish and display the statues of each of these sensors on the GUI at the website, it would have been obvious to a POSITA that each of the multiple sensors has a unique associated identification code that is transmitted to the website.

141. In the example shown in FIG.16, at least the identification codes and event data associated with the living room motion sensor and living

room camera can allow an authorized entity to determine the type of event (e.g., "alarm") and the particular sensors detecting the event (e.g., the living room motion sensor and camera).

142. In addition, the identification code and event data associated with the living room camera (e.g., shown in the image viewer (1604)) can allow the authorized entity to determine that the living room camera is the imaging device providing imaged data to the web site.

Lamp

143. Thomas discloses that the GUI window (1500) at the website can provide the user with a variety of utility controls including controls for lighting of selected rooms. Thomas at page 16, 2nd paragraph and FIG. 15. The user can request the control to turn-on certain lights. *See, e.g.*, Thomas at page 13, 3rd paragraph.

144. It would have been obvious to a POSITA reviewing Thomas that lighting of selected rooms can be provided by a lamp (a known, commonly used lighting device) such that the lamp is coupled to the controller and is activated in order to enable the video camera to record the event, for example, in a living room, if the room is dark or there is low light.

Maintenance Detector

145. Thomas discloses maintenance detectors that can provide status information, including a malfunction status, of premises maintenance such heating, cooling, sprinkler system, and the like. Thomas, pg. 12, last paragraph.

> "The remote request processing 1000 begins by displaying 1002 a status request form on a display for the remote computer. Next, the user of the remote computer completes 1004 the status request form so as to indicate the particular information appliances that status information is desired. For example, the user may request status information for an alarm system, VCR, digital TV programming or other home entertainment controls, home utilities including lighting, heating, cooling, sprinkler system, and the like. The completed status request form is then sent 1006 to a local computer. (Thomas, pg. 12, last paragraph.)

146. The maintenance detector can be, for example, a temperature sensor for detecting an event that is a premises maintenance malfunction, such as high temperatures due to failure of an a/c system, since the GUI window of the surveillance system in FIG. 15 shows a "Temperature Control" and a temperature of "72°F."

147. Thomas further discloses that the user may request the control to adjust

the temperature to 60 degrees F (i.e., configure a set point or a specific range for the temperature sensor). *See, e.g.,* Thomas at pg. 13, 3rd paragraph. The temperature sensor can determine that the temperature within the premises has moved outside the specified range.

148. In addition, the ’220 Patent shows temperature or other maintenance function sensors 12 (i.e. low heating fuel sensors) as a component of a prior art security system 11. The ’220 Patent, 5:35-38 and FIG. 1

149. To the extent that “**an** event that is a premises maintenance malfunction” recited in Claim 7 of the ’220 Patent is interpreted to be “**the** event detected at a particular at least one sensor wherein the imaging device is activated by the controller upon receiving the signal from the particular sensor that is in an area covered by a particular imaging device” and “the event data captured by the imaging device upon receiving a transmission activation signal from the controller after detection of **the** event” in Claim 1 of the ’220 Patent, Thomas discloses that the transmitter is triggered by an alarm condition to forward the image and alarm status information over the network to the website. *See, e.g.,* Thomas at pg. 21, Claim 26.

150. Thus, a POSITA reviewing Thomas would understand that the premises maintenance malfunction detected by the maintenance detector (e.g.,

high temperatures due to failure of an a/c system by the thermostat) can be an alarm condition that activates the camera and triggers the transmitter to transmit the event data over the network to the website.

Integrating Various Sensor Components

151. Fernandez discloses that the detector (3) and sensor (44) include a variety of sensing and measuring devices (e.g., motion detector, burglar alarm, door or window open/close detector, smoke detector, thermostat, etc.). Fernandez, 4:43-50.

152. Fernandez teaches coupling the detector (3) to the server (5) that is further connected to the network (8). Fernandez, 3:17-57 and FIG.1. These various detectors and sensors are thus integrated into the surveillance system networked, e.g., based on Internet and TCP/IP protocol (Fernandez, 3:43-57), to allow remote access and viewing of statuses and information captured by the various detectors and sensors.

153. It would have been obvious to a POSITA to integrate any of the sensor components in the network surveillance system as taught by Fernandez into the remote monitoring and control taught by Thomas. Such a combination would have yielded known, predictable results to a POSITA and well within the capabilities of a POSITA.

154. In fact, the ’220 Patent itself acknowledges that, by the time of filing the

’220 Patent application, prior art surveillance systems had incorporated various sensors/detectors including temperature or other maintenance function sensors 12, entry point sensors 13, motion sensors 15, beam sensors 17, fire/smoke detector 18, audio detectors 19, broken glass detector 20 as components of a network surveillance system. The ’220 Patent, 5:35-52 and FIG. 1

Broken Glass Detector

155. Fernandez discloses a “door or window open/close detector.” *See, e.g.*, Fernandez, 4:45-46.

156. It would have been obvious to a POSITA reading about use of a “burglar alarm, door or window open/close detector” along with a broad range of other detectors in the “unauthorized home entry” detection system of Fernandez, that a broken glass detector could be used as a detector 3 in addition to, or in lieu of, a door or window open/close detector to be an integral component of a network surveillance system.

157. In fact, it was known to incorporate a broken glass detector in surveillance systems by the time of filing the ’220 Patent application.

158. For example, Broady discloses broken glass detectors as an example sensor component for a remote activated surveillance system. Broady, 3:16 and Title. In addition, the ’220 Patent shows broken glass detector

20 as a component of a prior art security system 11. The ’220 Patent, 5:51-52 and FIG. 1.

Fire Detector

159. Fernandez discloses a “smoke detector.” (*See, e.g.,* Fernandez, 4:46).

160. It is well known that a smoke detector is a form of a fire detector because the smoke detector typically detects smoke as an indicator of fire.

161. It would have been obvious to a POSITA reading about use of a “smoke detector” in Fernandez along with a broad range of other detectors in the “unauthorized home entry” (Fernandez, 4:48) detection system of Fernandez, that a fire/flame detector could be used as a detector 3 in addition to, or in lieu of, a smoke detector to detect fires and/or open flames to be an integral component of a network surveillance system.

162. In fact, it was known to incorporate a fire/flame detector in surveillance systems by the time of filing the ’220 Patent application.

163. For example, Maram discloses “fire detectors” as example components of detector units connected to main station control unit through wire connectors for detection of unauthorized intrusion into homes, offices, etc. Maram, 1:8-24. In addition, the ’220 Patent shows fire/smoke detector 18 as a component of a prior art security system 11. The ’220

Patent, 5:49 and FIG. 1

Microphone

164. Fernandez discloses that sensor unit 44 may include one or more video cameras and microphone to provide real-time object data, such as audio and/or video signals. *See, e.g.,* Fernandez, 6:16-20.

165. Fernandez further discloses that video and/or audio information which may be pre-recorded or delivered from current "live" broadcast or transmission. Fernandez, 11:33-35.

166. In view of the reference to audio and video signals in Fernandez, it would have been obvious to a POSITA reviewing Fernandez that a microphone could be included as part of the imaging device to provide audio signals, as taught by Fernandez. In fact, it was known to incorporate a microphone into an imaging device by the time of filing the '220 Patent application.

For example, Broady explicitly discloses a camera that includes a video camera and a microphone for generating video and audio signals of an area under surveillance by the surveillance system. Broady, 3:3-5.

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

Executed this 17 day of Oct, 2014 in Sunnyvale, CA.

Date: Oct, 17 - 2014

Tal Lavian

Dr. Tal Lavian