

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

MOBOTIX CORP.,
Petitioner,

v.

e-WATCH, INC.,
Patent Owner.

Case IPR2013-00255
Patent 6,970,183

Before JAMESON LEE, MICHAEL W. KIM, and
GEORGIANNA W. BRADEN, *Administrative Patent Judges*.

BRADEN, *Administrative Patent Judge*.

FINAL WRITTEN DECISION
35 U.S.C. § 318(a) and 37 C.F.R. § 42.73

I. INTRODUCTION

A. Background

Mobotix Corporation (“Petitioner”) filed a Corrected Petition requesting *inter partes* review of claims 1–25 and 32–34 of U.S. Patent No. 6,970,183 (Ex. 1001, “the ’183 patent”) pursuant to 35 U.S.C. §§ 311–319. Paper 4. e-Watch, Inc. (“Patent Owner”) filed a Preliminary Response. Paper 10. On October 25, 2013, we instituted an *inter partes* review of claims 1–25 and 32–34 on less than all of the grounds of unpatentability alleged in the Petition. Paper 11 (“Dec. to Inst.”). After institution of trial, the Patent Owner filed a Patent Owner Response (Paper 17, “PO Resp.”), to which Petitioner filed a Reply (Paper 20). An oral argument was not held.

The Board has jurisdiction under 35 U.S.C. § 6(c). In this final written decision, issued pursuant to 35 U.S.C. § 318(a) and 37 C.F.R. § 42.73, we determine Petitioner has shown by a preponderance of the evidence that all challenged claims, claims 1–25 and 32–34, are unpatentable.

B. The ’183 Patent

The ’183 patent describes a full service, multi-media surveillance system capable of a wide range of monitoring techniques using digital network architecture. Ex. 1001, 3:46–48. According to the ’183 patent, the surveillance system includes “a combination of megapixel digital camera capability, with full-motion video surveillance,” and “a network including network components and appliances.” *Id.* at 3:40–43. Such network component and appliances include wiring, workstations, and servers. *Id.* at 3:43–44. The system may use wired and wireless appliances and sensors. *Id.* at 4:4–5. The surveillance system may be dispersed geographically with

various wide area carriers. *Id.* at Abstract, 3:40-45. The surveillance system is adapted for transmitting event data, video and/or image monitoring information, audio signals, and other sensor and detector data over significant distances. *Id.* at 4:43-52. The data is transmitted digitally over a LAN, wireless LAN, Intranet, or Internet. *Id.* at 4:48-50. The data may be used for automatic assessment and response, including dispatch of response personnel. *Id.* at 4:50-52. For example, GPS dispatching may be used to locate and alert personnel, as well as to indicate the location of an event. *Id.* at Abstract, 4:1-10.

Figure 1 of the '183 patent is reproduced below:

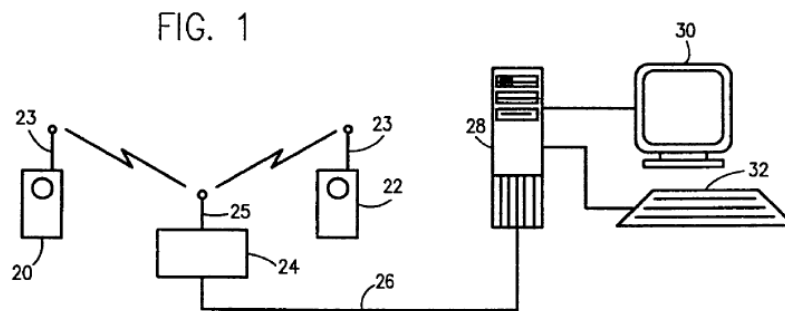


Figure 1 illustrates one embodiment of the multi-media surveillance system described in the '183 patent.

Figure 1 shows video and/or image signals captured by cameras 20, 22 converted to an RF signal. Ex. 1001, 16:58-64. Cameras 20, 22 are connected to antenna 23 for transmitting the RF signal to receiver 24. Ex. 1001, 16:58-62. Receiver 24 is connected to network 26 at a location convenient for receiving the RF signal from cameras 20, 22. *Id.* at 16:62-64. The RF signals transmitted by cameras 20, 22 to receiver 24 are then transmitted to monitor station 28 via network 26. *Id.* at 16:64-66. Monitor station 28 is generally a CPU where the raw data signals generated by

cameras 20, 22 and/or transmitted by receiver 24 are processed for display at monitor 30. *Id.* at 17:1-7.

Figure 6 of the '183 patent is reproduced below:

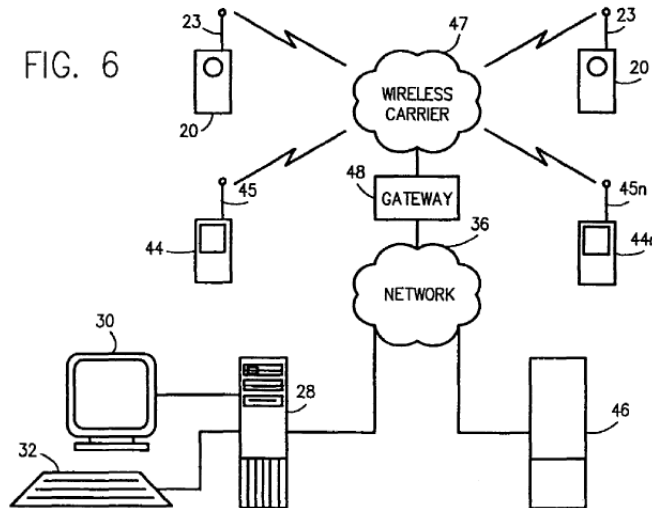


Figure 6 illustrates one embodiment of the multi-media surveillance system described in the '183 patent.

According to the embodiment of Figure 6, wireless mobile monitors 20, 44-44n are connected to any one of various wireless common carriers 47. Ex. 1001, 18: 35-51. Carriers 47 can transmit data directly to network 36, such as the Internet, via an ISP or private gateway 48. Ex. 1001, 17:30-35. Such a connection of monitors 44-44n to carriers 47 allows the system to have monitoring “capability over a larger geographic area that is greater than can be provided by a wireless LAN.” *Id.* at 18:32-35.

C. Illustrative Claims

Of challenged claims 1-25 and 32-34, claims 1, 18, and 25 are independent and are reproduced below.

1. A comprehensive, IP network compatible, multimedia surveillance and security system comprising a plurality of sensor appliances adapted to connected to a network based server for monitoring, logging, and transmitting data to the server in order to permit comprehensive surveillance of a predetermined area, the system comprising:
 - a. a conventional security sensor which is activated by the occurrence of an activating event and upon activation generates a signal;
 - b. a convertor for converting the conventional sensor signal into a network compatible signal and adapted for sending the converted signal via the network to the server;
 - c. a surveillance sensor appliance controlled by the server for monitoring an area and generating a signal indicating a condition in the monitored area in a programmed response mode controlled by the server, whereby the server receives and logs data transmitted by both the conventional sensor and the sensor appliance.
18. A comprehensive, IP network to a network based server for monitoring, logging, and transmitting data to the server in order to permit comprehensive surveillance of a predetermined area, the system comprising:
 - a. a multi-function image sensor appliance adapted for generating an image signal representing the visual condition of a monitored zone of operation, the image signal comprising both still frame image data and motion video image data;
 - b. a transmitter for sending image data to the server.
25. A comprehensive, IP network compatible, multimedia surveillance and security system comprising a plurality of sensor appliances adapted to connected to a network based server for monitoring, logging, and transmitting data to the server in order to permit comprehensive surveillance of a predetermined area, the system comprising:
 - a. a plurality surveillance sensor appliances controlled by the server for monitoring an area and generating a data signal

- indicating a condition in the monitored area controlled by the server, whereby the server receives and logs signal data;
- b. each sensor appliance adapted for transmitting the generated signal;
 - c. a network for communicating the plurality of sensor appliances with a central server;
 - d. the central server adapted for collecting and managing the data transmitted by the plurality of sensor appliances.

D. Prior Art References Alleged to Support Unpatentability

The following prior art references were asserted in the instituted grounds:

Ely	WO 97/40624	Oct. 30, 1997	Ex. 1004
Kogane	US 6,323,897 B1	Nov. 27, 2001	Ex. 1007
Fernandez	US 6,697,103 B1	Feb. 24, 2004	Ex. 1008

Takuya Imaide, *An MPEG Camera with Tapeless Video Recording*, Digest of Technical Paper Int'l Conf. on Consumer Elect. Appl. Phys. 1322, 342-343 (1997). Ex. 1009

Guntis Barzdins, *Wireless Internet Access in Latvia*, May 7, 1999, available at <http://web.archive.org/web/19990507062257/http://lucilia.ebc.ee/~enok/radiolink/HTMLDocument.html>. Ex. 1010

E. Grounds of Unpatentability Instituted for Trial

The following table summarizes the challenges to patentability that were instituted for *inter partes* review:

Claim	Grounds	Reference(s)
Claims 1–9, 12–17, 25, and 32	§ 103	Ely and Fernandez
Claims 10, 11, and 18–23	§ 103	Ely, Fernandez, and Imaide

Claim	Grounds	Reference(s)
Claim 24	§ 103	Ely, Fernandez, and Barzdins
Claims 25 and 33	§ 102	Kogane
Claims 32 and 34	§ 103	Kogane and Fernandez

II. ANALYSIS

A. Claim Construction

In an *inter partes* review, claim terms in an unexpired patent are given their broadest reasonable construction in light of the specification of the patent in which they appear. 37 C.F.R. § 42.100(b). Claim terms also are given their ordinary and customary meaning, as would be understood by one of ordinary skill in the art in the context of the entire disclosure. *In re Translogic Tech, Inc.*, 504 F.3d 1249, 1257 (Fed. Cir. 2007).

If an inventor acts as his or her own lexicographer, the definition must be set forth in the specification with reasonable clarity, deliberateness, and precision. *Renishaw PLC v. Marposs Societa' per Azioni*, 158 F.3d 1243, 1249 (Fed. Cir. 1998). Neither Petitioner nor Patent Owner contends that the specification of the '183 patent, as filed, coined a new meaning for any term, different from the ordinary recognized meaning for any term.

1. “Surveillance Sensor Appliance”

Independent claims 1, 18, and 25 of the '183 patent each recite “surveillance sensor appliance.” Petitioner contends “surveillance sensor appliance” indicates more than just a sensor, and should be construed as a

“sensor appliance.” Pet. 6 (citing Ex. 1001, 5:7, 5:39–43, 12:1-2, 15:53, 32:33–34).

The specification teaches that the disclosed surveillance system permits a security provider to have access to “sensor appliances.” Ex. 1001, 4:36–37. According to the specification, a “sensor appliance” may include multiple different sensors. *Id.* at 6:9–13 (“a plurality of sensor units, which may include at least one video image appliance sensor and/or at least one audio appliance sensor and/or at least one motion appliance sensor. . . .”); *see, e.g., id.* at 5:7 (“multiple sensors and appliances may be accommodated. . . .”). The specification indicates that a “surveillance sensor appliance” may be connected to a network. *Id.* at 20:21–26, 32:25–36, Fig. 1. This connection may be either hardwired or wireless. *Id.* A sensor appliance monitors conditions, such as temperature and smoke, and events, such as motion detection and contact closure. Ex. 1001, 5:39–50, 7:50–55. The specification further teaches that any number of devices can be a “surveillance sensor appliance,” for example, a camera, an audio monitor, or a thermostat that monitors static, unchanging conditions in an area. *Id.* at 15:53–56, 20:21–26, 32:30–36, claims 8–17, Fig. 1–3. Therefore, considering the specification as a whole, we determine that the broadest reasonable interpretation of “surveillance sensor appliance” is “a device that contains at least one sensor for monitoring conditions or events in an area.”

2. “Multi-Function Image Sensor Appliance”

Independent claim 18 recites “multi-function image sensor appliance.” This claim further recites that “a multi-function image sensor appliance” is “adapted for generating an image signal representing the visual condition of

a monitored zone of operation, the image signal comprising both still frame image data and motion video image data.” Ex. 1001, 46:59–63.

According to Petitioner, “multi-function image sensor appliance” should be construed as “an image sensor appliance that can generate more than one type of image signal.” Pet. 6 (citing Ex. 1012 at 7).

The specification states the following concerning imaging functions: “real-time streaming video can be combined with the still image layering scheme with the gap after the still image [filled] with streaming video data, and where desired, other data.” Ex. 1001, 38:9–12. Thus, the specification, both in the claim and elsewhere, discloses that a multi-function image sensor appliance can generate “an image signal” where the image signal comprises more than one type of data.

Given the disclosures of the ’183 patent, “multi-function image sensor appliance” is construed to mean “a sensor appliance capable of generating an image signal comprising more than one type of data.”

3. *“Surveillance sensor appliance controlled by the server for monitoring an area and generating a signal indicating a condition in the monitored area in a programmed response mode controlled by the server.”*

Petitioner contends that “[a] surveillance sensor appliance controlled by the server for monitoring an area and generating a signal indicating a condition in the monitored area in a programmed response mode controlled by the server,” as recited in independent claim 1, indicates that the surveillance sensor appliance is configured to monitor an area and to generate a signal indicating a condition in the monitored area. Pet. 6 (citing Ex. 1012, 6–7). According to Petitioner, the surveillance sensor appliance is controlled by the server, indicating that the surveillance sensor appliance can

receive and respond to signals from the server. *Id.* at 6–7. Essentially, Petitioner repeats the claim language found in claims 1 and 25. We agree with Petitioner that the claim language has a plain meaning and requires no special construction.

4. “*Comprehensive, IP network compatible, multimedia surveillance and security system*”

Independent claims 1, 18, and 25 of the ’183 patent each recite the following preamble: “[a] comprehensive, IP network compatible, multimedia surveillance and security system.” Petitioner contends the preamble of each independent claim should not be given patentable weight. Pet. 6, 10–11, 39, 45. Petitioner further contends that the preamble language regarding “comprehensive, IP network compatible, multimedia surveillance and security system” neither expressly nor implicitly defines claimed subject matter. Pet. 10-11. Neither of Petitioner’s contentions requires discussion, because the preamble does not set forth any claim feature that is not already included in the body of the claim.

B. Principles of Law

To prevail in its challenges to the patentability of the claims, the petitioner must establish facts supporting its challenges by a preponderance of the evidence. 35 U.S.C. § 316(e); 37 C.F.R. § 42.1(d). A claim is unpatentable under 35 U.S.C. § 103(a) if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. *KSR Int’l Co. v. Teleflex Inc.*, 550 U.S. 398, 406 (2007). To establish obviousness of a claimed invention, all the claim limitations must be taught or suggested by the prior art. *See CFMT, Inc. v. Yieldup Int’l Corp.*, 349

F.3d 1333, 1342 (Fed. Cir. 2003); *In re Royka*, 490 F.2d 981, 985 (CCPA 1974). A patent claim composed of several elements, however, is not proved obvious merely by demonstrating that each of its elements was known, independently, in the prior art. *KSR Int’l Co.*, 550 U.S. at 419. In that regard, for an obviousness analysis it can be important to identify a reason that would have prompted one of skill in the art to combine prior art elements in the way the claimed invention does. *Id.* However, a precise teaching directed to the specific subject matter of a challenged claim is not necessary to establish obviousness. *Id.* Rather, obviousness must be gauged in view of common sense and the creativity of an ordinarily skilled artisan. *Id.* Moreover, obviousness can be established when the prior art itself would have suggested the claimed subject matter to a person of ordinary skill in the art. *In re Rinehart*, 531 F.2d 1048, 1051 (CCPA 1976).

We analyze the instituted grounds of unpatentability in accordance with the above-stated principles.

C. Claims 1–9, 12–17, 25, and 32 — Alleged Obviousness over Ely and Fernandez

Petitioner asserts claims 1-9, 12–17, 25, and 32 of the ’183 patent are unpatentable under 35 U.S.C. § 103(a) over Ely and Fernandez. Pet. 10–23, 25–26, 45–49.

1. Ely’s Disclosure

Ely describes a video surveillance system that includes a central control station and a plurality of video camera and sensors. Figure 2 of Ely is reproduced below:

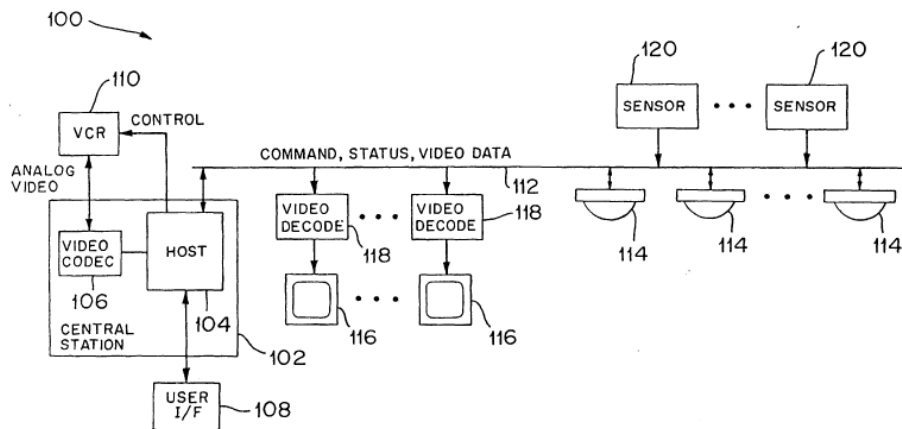


FIG. 2

Figure 2 illustrates one embodiment of the video surveillance system described in Ely.

According to the embodiment of Figure 2, a video surveillance system including local area network (LAN) 112, connects host computer 104 to other components of system 100, such as camera units 114, video monitors 116, and sensor devices 120. Ex. 1004, 9:5-18. Host computer 104 (which resides within central station 102) receives signals from sensors 120 and data from camera unit 114. *Id.* at 17:3-25.

Sensor devices 120 are of conventional types that detect, for example, unauthorized opening of doors, windows, and display cases and the like, and generate alarm signals indicative of these occurrences. Ex. 1004, 9:18-23. “[S]ensors 120 may also include conventional motion and/or heat sensing devices.” *Id.* Sensors 120 transmit signals via LAN 112 to host computer 104. *Id.* at 17:3-9. Host computer 104 then responds by sending an alarm command to certain predetermined camera units 114. *Id.*

Camera unit 114 is shown in Figure 3 of Ely, which is reproduced below:

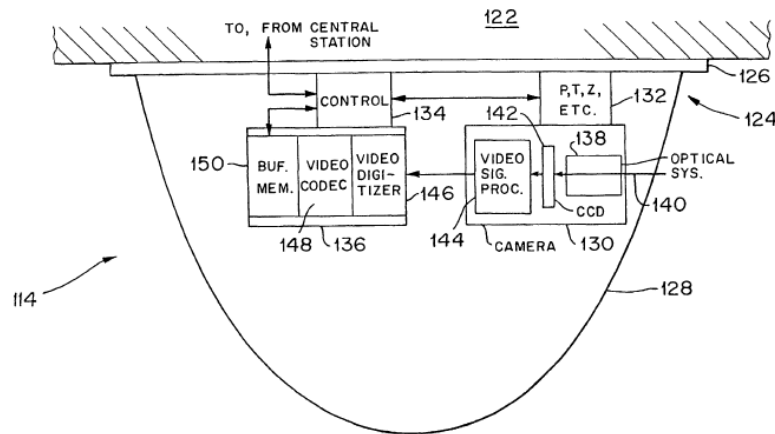


FIG. 3

Figure 3 illustrates a camera unit of the video surveillance system described in Ely.

Figure 3 illustrates camera unit 114 containing video camera 130, video signal processor 144, on-board buffer memory 150, and controller circuit 134. Ex. 1004, 10:15–19. Data from camera 130 is stored into buffer memory 150 and is transmitted (via controller 134) to host computer 104 of central station 102. *Id.* at 12:3–20, Fig. 4. Camera unit 114 may operate under the control of a stored program that is carried out by control circuit 134. *See, e.g., id.* at 12:3–8. Camera movements can be actuated automatically in response to an alarm signal. Ex. 1004, 2:5–9. Cameras can be controlled through commands (1) issued by the system host, (2) in response to pre-programmed surveillance routines, or (3) in response to operator input. *Id.* at 2:5–14. A data recorder (under the control of host computer 104) can record all data received via LAN 112, including live and buffered video data. *Id.* at 16:32–17:2.

2. Fernandez's Disclosure

Fernandez describes an integrated network for monitoring remote objects that includes an internet connection between (1) monitors (such as

cameras and GPS network detectors), (2) network servers, and (3) a database for storing object position movement. Ex. 1008, abstract. Figure 1 illustrates one embodiment of the system disclosed in Fernandez, and is reproduced below.

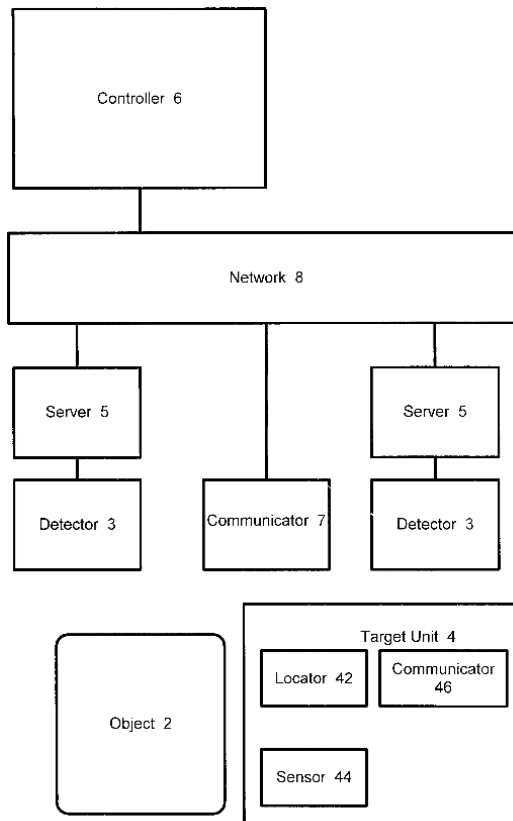


FIG. 1

Figure 1 illustrates one embodiment of the integrated monitoring network described in Fernandez.

Figure 1 shows controller 6 coupled to network 8 via a computer workstation or digital processing equipment. Ex. 1008, 2:23-26. Network 8 provides digital connection to the internet according to an internet protocol addressing scheme. *Id.* at 2:22-39, 3:16-17, 5:42-45. Network 8 further couples to server 5, sensor or detector 3, as well as communicator 7. *Id.* at 3:16-20. Communicator 7 communicates through a conventional or

wireless connection to one or more target units 4. *Id.* at 3:19–21. Target unit 4 is provided to move with and observe associated object 2.

Target unit 4 is a portable wireless communications device that determines the location and movement of object 2. *Ex.* 1008, 5:36–45. Target unit 4 senses and detects area condition, image, sound, etc. *Id.* at 8:1–5. Figure 2 from Fernandez is reproduced below:

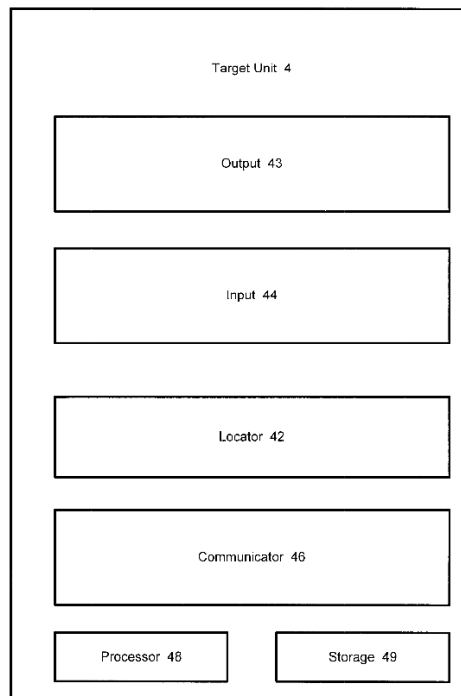


FIG. 2

Figure 2 illustrates a block diagram of target unit 4 from Fernandez.

Figure 2 shows communicator unit 46 included within target unit 4. *Ex.* 1008, 6:11–15. Communicator unit 46 uses a digital wireless transceiver to send and/or receive real-time or store-and-forwarded object data generated by input sensor 44. *Id.* at 6:30–32, 7:27–29. Processor 48 and memory 49, including operating system and web browser software, are also provided with target unit 4 for accessing and/or processing of data. *Id.* at 6:32–36. The data may be real-time object data received from input sensor

44 and accessible via server 5. *Id.* at 6:36–40. Input sensor 44 may include any optical, medical, or otherwise physical monitoring or observation device to provide real-time data sensed from monitored object 2. Ex. 1008, 6:16–23. Such devices may include one or more video cameras, active sensors, infra-red detectors, and microphones. *Id.*

The overall system of Fernandez includes a geographically or relatively fixed network of multiple sensors or detectors 3. Ex. 1008, 3:58–62, Fig. 1. Sensors or detectors 3 may each be accessible through Internet browsing interface, and may each be overlaid with a mobile set of target units 4 closely associated or attached to certain objects 2 for remote monitoring. *Id.* at 5:45–52. Sensor or detector 3 may be a digital imager, video capture device, motion detector, burglar alarm, smoke detector, thermostat, etc. *Id.* at 4:23–47. In certain instances, e.g., unauthorized home entry, sensed events may trigger other functionality, such as taking electronic photographs and/or notifying certain entities. *Id.* at 4:47–50. To that end, controller 6 may have a software tool that includes a dispatch generator, which can alert interested parties when there is an event that is monitored. *Id.* at 15:32–44.

3. Analysis

Petitioner contends that every limitation in claims 1-9, 12-17, 25, and 32 of the '183 patent is either taught or suggested by a combination of Ely and Fernandez. Pet. 10–23, 25–26, 45–49. In response, Patent Owner asserts Petitioner fails to provide *any* articulated reasoning to combine the prior art references to arrive at the claimed invention. PO Resp. 15–16. Petitioner, however, explicitly offered the following rationale to combine:

It would have been obvious to a person having ordinary skill in the art at the time of the invention to modify the surveillance network as taught by Ely with the surveillance network as taught by Fernandez because both references teach using known networks in the same way yielding predictable results. Such a substitution is well known, based on common sense, or the result of routine experimentation.

Pet. 26 (citing Ex. 1003 ¶ 41). We are persuaded by Petitioner’s reasoning, supported by Dr. Tal Lavian’s uncontested testimony, for why one of skill in art at the time the ’183 patent would have combined the teachings of Ely and Fernandez.

Patent Owner further contends the prior art fails to render the claims of the ’183 patent unpatentable, because the system in Ely does not support use of a network based server and does not have central storage for storing data from all cameras simultaneously. PO Resp. 7. Patent Owner’s contention is unpersuasive, because the ’183 patent specification’s description of a network based server encompasses the server disclosed in Ely. According to the specification of the ’183 patent, the key to identifying a network based server is (1) connection to the Internet, Intranet, or other wide area network (WAN) (Ex. 1001, 4:17–28, 5:5–7), and (2) providing a centralized location for data collection, logging functions, alarm detection, and other specialized functions (*id.* at 4:67-5:5). Ely teaches the use of host computer 104 at central control 102 with video data encoding/decoding device 106, and hardware and software required for a user interface. Ex. 1004, 9:5–10. A LAN connection is set up between camera unit 114, sensor unit 120, and host computer 104. *Id.* at 9:11–18, 12:3–13, Fig. 2. Petitioner’s expert witness, Dr. Lavian, testifies that the LAN is “a computer network located on a user’s premise within a limited geographic area.” Ex.

1003 ¶ 27. We are persuaded by Dr. Lavian’s unchallenged testimony regarding the definition of LAN. Accordingly, Ely’s host computer 104 with a LAN connection properly corresponds to the recited “network based server.”

Patent Owner’s contention also is unpersuasive in view of the combined teachings of Ely and Fernandez. Fernandez teaches the use of a network based server (Ex. 1008, 3:16–26) that provides digital storage (*id.* at abstract, 1:43–46, 9:10–25), and which receives and logs data from a plurality of sensor appliances (*id.* at 6:30–40, 7:27–29). Thus, the network based server and central storage elements of Fernandez meet the limitations of the challenged claims.

Patent Owner further contends that Ely fails to teach or suggest how a plurality of cameras and sensors are differentiated from one another to manage and independently collect discernible data from each camera. PO Resp. 12. The claims, however, do not require such differentiation between camera and sensors. Furthermore, Ely teaches that a plurality of cameras are differentiated, because video data may be routed from a *selected* camera, or a *selected* camera may be instructed not to transmit video data. Ex. 1004, 14:35–15:10. The system of Ely also contemplates the use of conventional split-screen techniques that include the use of video multiplexers, indicating the receipt of video data from multiple different camera units. *Id.*

Patent Owner then contends Ely does not disclose the ability to transmit all cameras simultaneously in or at near real time. PO Resp. 8. Rather, according to Patent Owner, Ely teaches that time slots are given to multiple cameras, or that individual cameras must be selected for transmission of data. *Id.* (citing Ex. 1004, 7:22, 8:38). The claims, however,

do not recite a “real-time” limitation. Moreover, Ely does disclose “real-time” transmission, as the contention of Patent Owner is based solely on one embodiment in Ely. Ely teaches in one embodiment that control circuit 134 of camera unit 114 transmits to central station 102 (via LAN 112) compressed video data that represents video signals *currently* being generated by camera 130. Ex. 1004, 12:9-13. Furthermore, Fernandez teaches that sensor unit 44, which includes video cameras, provides real-time object data. Ex. 1008, 6:16–32. As for simultaneous transmission from multiple cameras, Ely discloses the use of conventional split-screen techniques, including the use of video multiplexers, which would send and receive transmissions simultaneously from multiple cameras units 114. Ex. 1004, 15:36–16:3.

Patent Owner also contends Ely does not teach or suggest receiving and logging data from both the conventional sensors and surveillance sensor appliances, as recited in independent claim 1. PO Resp. 8. Ely does disclose (1) the use of a plurality of camera units 114, which are connected via LAN to a host computer 104 at a central station 102, and (2) sensor devices 120 that are of the conventional type. Ex. 1004, 9:18–23. Camera units 114 fall within the scope of the claim term “surveillance sensor appliances” as construed in Section II.A.1 of this Decision. Thus, we are persuaded that Ely teaches the use of conventional sensors and surveillance sensor appliances. Furthermore, Ely discloses that camera units 114 and sensor devices 120 transmit data via LAN 112 to host computer 104 at central station 102 (*id.* at 12:9–13), and that such data is stored in memory 150 (*id.* at 12:18–20), thereby teaching the receiving and logging of data from both types of sensors.

Patent Owner additionally contends that Ely fails to disclose a convertor for converting the conventional sensor signal into a network compatible signal, and for sending the converted signal via the network to the server. PO Resp. 12. The argument is unpersuasive, because Ely teaches that sensor devices 120 are connected via a LAN to host computer 104 (*id.* at 9:11–18, 12:3–13, Fig. 2), and that a signal indicative of an alarm condition is transmitted by sensor devices 120 via LAN 112 to host computer 104 at central station 102 (*id.* at 17:3–13, Fig. 2). In order for a signal to be transmitted by sensor devices 120 to LAN 112, the sensor signal must be converted into a LAN compatible signal. According to Petitioner, that indicates that Ely inherently teaches the use of a convertor to convert the conventional sensor signal from the sensor devices 120 into a [LAN] network compatible signal. Pet. 13–14 (citing Ex. 1003 ¶ 28); Reply 6 (citing Ex. 1003 ¶¶ 27, 28). We are persuaded by Petitioner’s reasoning, supported by the uncontested testimony of Dr. Lavian (Ex. 1003 ¶¶ 27, 28).

Patent Owner lastly contends that although Fernandez teaches a geographically fixed network of sensors, it fails to teach a software tool that includes a dispatch generator. PO Resp. 11. Patent Owner argues that it is improper hindsight analysis to speculate that Fernandez “may” include a dispatch generator. PO Resp. 11–12. Patent Owner’s contention is unpersuasive, because (1) claims 1–9, 12–17, and 25 do not require a dispatch generator, and (2) for claim 32, Patent Owner’s contention analyzes Fernandez in isolation. Fernandez should be read for what it teaches in combination with Ely, which, as explained below, discloses a network based server. Nonobviousness cannot be established by attacking the prior art references individually. *In re Merck & Co., Inc.*, 800 F.2d 1091, 1097 (Fed.

Cir. 1986). Patent Owner has not provided an explanation sufficient to overcome Petitioner’s argument and evidence as to why the combined teachings of Fernandez and Ely fall within the scope of the challenged claims.

Therefore, Petitioner has shown by a preponderance of the evidence that claims 1–9, 12–17, 25, and 32 are unpatentable over Ely and Fernandez.

D. Claims 10–11 and 18–23 — Alleged Obviousness over Ely, Fernandez, and Imaide

Petitioner alleges that claims 10–11 and 18–23 of the ’183 patent are unpatentable under 35 U.S.C. § 103(a) over Ely, Fernandez, and Imaide. Pet. 25–26, 39–42; Reply 8–11.

1. Imaide’s Disclosure

Imaide describes a compact MPEG camera that includes a PC card for tapeless video recording, and allows quick file access and easy connection to PCs. Ex. 1009, Abstract. Imaide further discloses the capturing and storage of video, audio, and still picture files without using tapes. *Id.* at Design Concept and Circuit Diagram.

2. Ely’s and Fernandez’s Disclosures

The disclosure of Ely and Fernandez are discussed in detail above in Sections II.B.1 and II.B.2.

3. Analysis

Petitioner contends that every limitation in claims 10–11 and 18–23 of the ’183 patent is either taught or suggested by a combination of Ely, Fernandez, and Imaide. Pet. 25–26, 39–42; Reply 8–11. According to Petitioner, one of skill in the art would have combined the teachings of the references, because at the time of the invention it would have been obvious

to modify the camera unit as taught by Ely with the camera as taught by Imaide. Petitioner asserts it was well-known in the art to substitute one camera for another camera in order to obtain predictable results. Pet. 21 (citing 1003 ¶ 52). Petitioner’s reasoning, supported by the unchallenged testimony of Dr. Lavian (Ex. 1003 ¶ 52), is persuasive.

Patent Owner disputes Petitioner’s contention that the challenged claims would have been obvious, because the prior art fails to teach several claim limitations. PO Resp. 7–8. First, according to Patent Owner, Ely neither teaches nor suggests use of a server to store digitized video data. *Id.* Patent Owner’s position is unpersuasive, however, because Ely’s host computer 104 with a LAN connection properly corresponds to the recited “network based server.” Ex. 1004, 9:5–10, 12:3–13, Fig. 2. Additionally, Fernandez teaches the use of a network based server (Ex. 1008, 3:16–26) that provides digital storage (*id.* at abstract, 1:43–46, 9:10–25), and which receives and logs data from a plurality of sensor appliances (*id.* at 6:30–40, 7:27–29).

Second, Patent Owner contends Ely fails to teach or suggest the use of a computer to display video data. PO Resp. 8. Ely discloses, however, the use of monitors 116 that are connected to either camera units 114 or to network 112. Ex. 1004, 9:23–32, Fig. 2. Ely then teaches that video data may be received by host 104 from camera unit 114 (by way of LAN 112) and then retransmitted by host 104 to selected monitor 116. *Id.* at 15:1–6. An artisan would understand that the video data is transmitted to monitor 116 for viewing thereon. *See, e.g.*, Ex. 1003 ¶¶ 26, 30–32.

Patent Owner further contends Ely fails to teach or suggest how a plurality of cameras and sensors are differentiated from one another to

manage and independently collect discernible data from each camera. PO Resp. 12. As discussed above, the claims, however, do not require such differentiation between camera and sensors. Furthermore, Ely teaches that differentiating between a plurality of cameras, because video data may be routed from a *selected* camera, or a *selected* camera may be instructed not to transmit video data. Ex. 1004, 14:35–15:10. Additionally, Fernandez teaches camera/sensor differentiation, because Fernandez states that instructions and/or modifications can be conveyed to target unit 4, for example to change, select, or adjust *particular* sensors 44. Ex. 1008, 6:54–58.

Regarding independent claim 18, Patent Owner contends Ely does not teach or suggest collection, storing, and retrieval of still frames, but rather that Ely only teaches recording video on a VCR, which are not still frames. PO Resp. 13. This contention is unpersuasive, because Ely discloses the use of a video codec that compresses video data in accordance with the H.261 standard. Ex. 1004, 11:18, 11:33. Dr. Lavian, Petitioner’s expert witness, opines that “[t]he ITU-T standard H.261 includes full motion video and the option of capturing still frame images because in H.261 digital video data is composed of multiple still frames and the ability to collect a signal frame is included as part of the standard.” Ex. 1003 ¶ 30. Dr. Lavian’s uncontested reasoning is persuasive. Furthermore, Fernandez discloses sensors that sense and transmit static and/or moving image signals to a server. Ex. 1008, 4:23–28. Additionally, Imaide teaches a sensor/camera adapted to capture both video data and still-frame images. Ex. 1009. We are persuaded by Petitioner’s position regarding the teachings of the asserted prior art.

Therefore, Petitioner has shown by a preponderance of the evidence

that claims 10–11 and 18–23 are unpatentable over Ely, Fernandez, and Imaide.

E. Claim 24 – Obvious over Ely, Fernandez, and Barzdins

Petitioner alleges that claim 24 of the '183 patent is unpatentable under 35 U.S.C. § 103(a) over Ely, Fernandez, and Barzdins. Pet. 24–25.

1. Barzdins's Disclosure

Barzdins describes data transmission using spread spectrum wireless LAN adapters adjusted for internet interconnections. Ex. 1010, 1–2.

2. Ely's and Fernandez's Disclosures

The disclosure of Ely and Fernandez are discussed in detail above in Sections II.B.1 and II.B.2.

3. Analysis

Dependent claim 24 requires that sensor appliances include a wireless transmitter and the server include a wireless receiver. Petitioner asserts that (i) Ely describes a surveillance security system including central station 102 (host computer 104) and camera units 114 (sensor appliances) (Ex. 1004, Fig. 2), (ii) Fernandez describes a surveillance security system including sensor appliance (target unit 4) comprising sensor unit 44 (e.g., video camera) and communicator 46 (wireless transmitter) (Ex. 1008, 3:17-22, 5:38-39, 6:30-39, Fig. 1), and (iii) Barzdins describes an IP compatible WLAN adapter (wireless transceiver) for a PC (Ex. 1010, 1). Pet. 24-25. Petitioner reasons it would have been obvious to a person of “skill in the art at the time of the invention to substitute the wireline connection of the central station (host computer) as taught by Ely with the wireless adapter (wireless receiver) of Barzdins, because both connections are” as follows: (i) well-known; (ii) commercially available; (iii) part of several ETSI

standards and FCC regulations; (iv) interchangeable; and (v) yield predictable results. Pet. at 25 (citing Ex. 1003 ¶ 49).

While Patent Owner does not address specifically claim 24, Patent Owner does contend generally that Petitioner fails to provide *any* articulated reasoning to combine the prior art to arrive at the claimed invention. PO Resp. 16. We are not persuaded by Patent Owner’s contention. To the contrary, we are persuaded by Petitioner’s position regarding the disclosures of the asserted prior art and the reasons why one of skill in the art would have combined the prior art teachings.

Therefore, we determine Petitioner has shown by a preponderance of the evidence that claim 24 is unpatentable over Ely, Fernandez, and Barzdins.

F. Claims 25, 33 – Anticipation by Kogane

Petitioner asserts that claims 25 and 33 of the ’183 patent are unpatentable under 35 U.S.C. § 102(b) over Kogane. Pet. 49–53; Reply 11–12.

1. Kogane’s Disclosure

Kogane describes a network surveillance video camera system that includes pivoting camera units, a data storing unit, a control server, and a monitor display all coupled to a network. Ex. 1007 Title, Abstract.

Figure 1 of Kogane is reproduced below:

FIG. 1

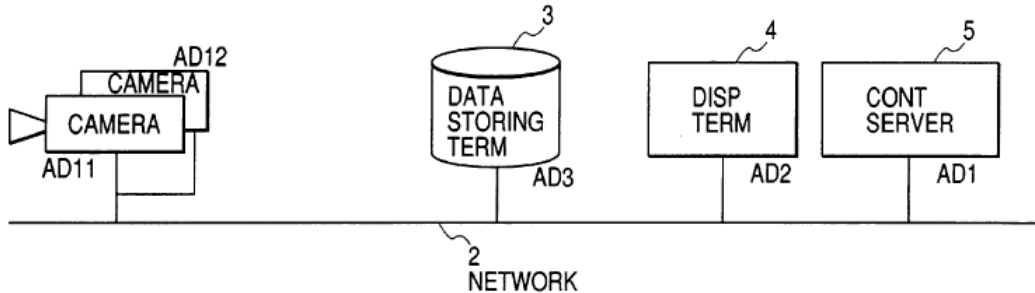


Figure 1 illustrates one embodiment of the network surveillance video camera system disclosed in Kogane.

Figure 1 shows the network surveillance video camera system, “including a plurality of camera units 1 having different (unique) addresses AD 11, AD12, . . . data storing terminal 3 having an address AD3, a display terminal having address AD2, and control server 5 having address AD1, which all are coupled to each other through network 2.” Ex. 1007, 3:40–46. When camera unit 1 is coupled to network 2, camera unit 1 communicates with control server 5 to receive its own address AD12 and address AD1 of control server 5. *Id.* at 37–40. Alternatively, control server 5 broadcasts a request for response to assign addresses when powered-on. *Id.* at 4:40–41.

Figure 3 of Kogane is reproduced below:

FIG. 3

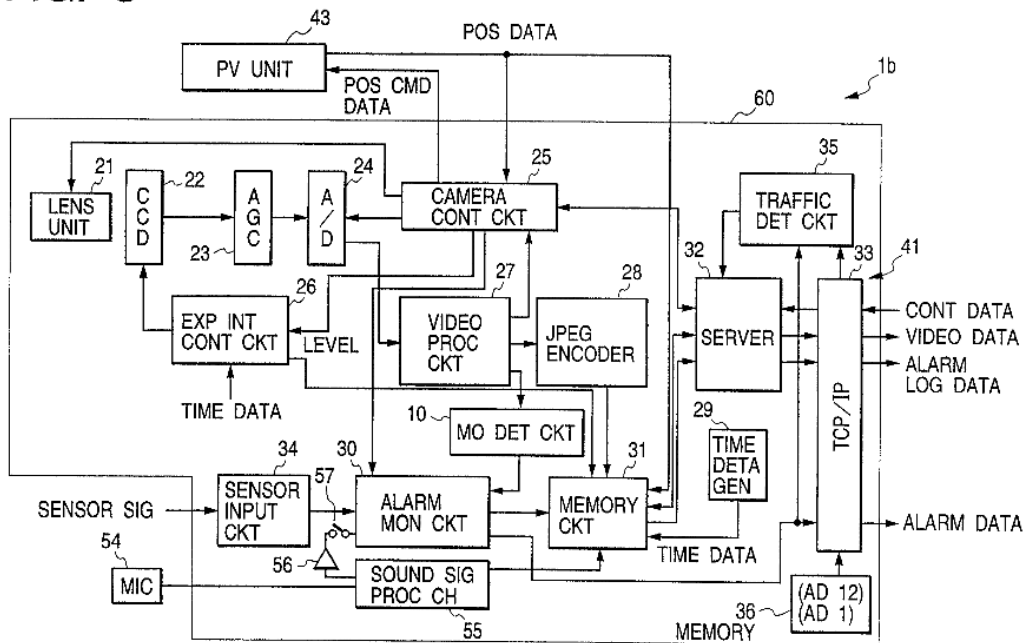


Figure 3 illustrates a camera unit disclosed in Kogane.

As shown in Figure 3, “alarm monitor circuit 30 is supplied with sensor signals from sensor input circuit 34, an output of the camera control circuit 25,” and “a motion detection signal from motion detection circuit 10.” Ex. 1007, 4:17–20. When motion detection circuit 10 detects motion in between consecutive frames of video data from video processing circuit 27, alarm monitoring circuit 30 generates alarm data to transmit to control server 5 through TCP/IP (transmission control protocol/internet protocol) circuit 33. *Id.* at 4:20–25. Moreover, when any sensor signals are inputted to sensor input circuit 34, alarm monitoring circuit 30 generates alarm data to transmit to control server 5 through TCP/IP circuit 33. *Id.* at 4:25–28. On the other hand, position data, time data, and alarm log data (e.g., alarm data, alarm type data, and the image of the video data regarding the alarm) are stored in

memory 31, and transmitted to control server 5 through server 32 and TCP/IP circuit 33. Ex. 1007, 4:28–33.

Control server 5 further includes a database for storing the following sets of video data from camera units 1 at occurrence of the alarm: alarm type data; time data; position data of pivoting unit 43; address data; and location data of camera unit 1. Ex. 1007, 6:4–8. Control server 5 receives a keyword from a keyboard to search the corresponding set of data in database 47. *Id.* at 6:8–10. When control server 5 receives the alarm data, the control server 5 receives alarm type data, time data, position data, and address data, and reads location data from location table 53 with the address data. *Id.* at 6:15–19. Control server 5 then “transmits the alarm data, alarm type data, time data, position data, address data, and the location data to display terminal 4 to display the data.” *Id.* at 6:19–21.

2. Analysis

Claim 25 is similar to independent claim 1, except that claim 25 does not recite a system comprising a conventional security sensor and a convertor. Rather, claim 25 recites a plurality of surveillance sensor appliance adapted to transmit a signal and a network for communicating between the sensor appliances and a central server. Petitioner contends that Kogane meets the claim limitations for independent claim 25. Pet. 49–50. According to Petitioner, the TCP/IP compatible multimedia surveillance and security system disclosed in Kogane uses a plurality of camera units 1a–1c that are connected to a network, thereby meeting the limitation of “plurality surveillance sensor appliance” recited in claim 25 of the ’183 patent. Pet. 50. Petitioner also contends Kogane meets the other limitations of claim 25, because camera units 1a–1c disclosed in Kogane receive commands and

requests from control server 5 (Ex. 1007, 3:48–52, 4:34–45), and transmit data across a network to control server 5, which then records the data in database 47 (*id.* at 4:51–64, 6:4–8). Pet. 50–51. We are persuaded by Petitioner’s contention.

Claim 33 depends from claim 25, and further requires “wherein the sensor appliance includes a location identifier component in the data signal.” Petitioner contends Kogane meets the limitations of claim 33, because Kogane teaches that alarm data is transmitted from camera unit 1 to control server 5, and that control server 5, after receiving the alarm data, looks up the location of sending camera unit 1 in location table 53 based on the address of sending camera unit 1 (*id.* at 6:15–21). Pet. 52–53. We are persuaded that Kogane teaches that the surveillance sensor appliance (i.e., camera unit 1) includes a location identifier in the data signal, thereby meeting the limitations of claim 33.

Patent Owner contends Kogane does not anticipate claims 25 and 33, because the Kogane server is used to control the camera image and video collection process, not the collection and management of transmitted data. PO Resp. 14 (citing Kogane at 3:66–4:4). According to Patent Owner, Kogane’s server 5 controls resolution, pan-tilt-zoom, frame-rate, and other such camera features. *Id.* (citing Kogane at 4:34–45). Patent Owner concludes that the control server of Kogane manages the way data is collected, not the way the collected data is managed. *Id.* We are not persuaded by Patent Owner’s position, because Kogane discloses a network surveillance video camera system (Ex. 1007 Title) that transmits data over TCP/IP circuit 33 to server 5 (Ex. 1007, 4:23–25), and server 5 includes a

data base for storing and management sets of the video data from camera units 1 (*id.* at 6:4–5).

Patent Owner also contends that Kogane does not teach a computer to display video. PO Resp. 10–11. We find Patent Owner’s contention unpersuasive, because (1) neither claim 25 nor claims 33 require a computer displaying video, and (2) Kogane discloses the use of display terminal 4, which includes display monitor 48. Ex. 1007 at 6:41–45. Transmitted data is displayed on display monitor 48. *Id.* at 6:48–51. Indeed, Kogane specifically teaches that an “operator can command which image is to be displayed.” *Id.* at 7:33–35.

Patent Owner lastly contends that Kogane fails to teach or suggest streaming motion video. PO Resp. 10. Neither claim 25 nor claims 33 requires streaming motion video. Accordingly, we are unpersuaded by Patent Owner’s contention.

Therefore, we determine Petitioner has shown by a preponderance of the evidence that claims 25 and 33 are unpatentable over Kogane.

G. Claims 32 and 34 – Obvious over Kogane and Fernandez

Petitioner asserts that claims 32 and 34 of the ’183 Patent are unpatentable under 35 U.S.C. § 103(a) over Kogane and Fernandez. Pet. 53–55; Reply 12–13.

1. Kogane’s and Fernandez’s Disclosures

The disclosure of Ely and Fernandez are discussed in detail above in Sections II.E.1 and II.B.2.

2. Analysis

Claim 32 depends from claim 25, and requires “the system further including a dispatch generator whereby the occurrence of a specified event generates a dispatch signal to a predetermined response team.” Ex. 1001, 23-26. Claim 34 depends from claim 33, and requires “wherein the system further includes a dispatch generator, whereby the occurrence of a specified event generates a dispatch signal to a predetermined response team based on location of the response team.” Ex. 1001, 29–32.

Petitioner contends the combination of Kogane and Fernandez meets the limitations of claims 32 and 34. Pet. 53–54. Specifically, Petitioner cites Kogane for describing a surveillance and security system comprising a network based server 5 and a central server 3 (Ex. 1007, Figs. 1 and 2), and Fernandez for teaching a security system comprising controller 6 with software tool 166 (dispatch generator) (Ex. 1008, 15:41-44). *Id.* Software tool 166 of Fernandez provides positional or directional functionality (dispatch signals) to alert authorities or other interested parties (predetermined response team) when an undesirable object or movement is monitored. *Id.* (citing Ex. 1008, 15:42-44; Fig. 3). According to Petitioner, it would have been obvious to a person having ordinary skill in the art at the time of the invention to modify the IP network compatible multimedia surveillance and security system as taught by Kogane with the dispatch generator as taught by Fernandez, because this is a known technique to improve similar devices in the same way since it is based on common sense or the result of routine experimentation. *Id.* at 54 (citing Ex. 1003 ¶ 73). We find Petitioner’s reasoning persuasive.

Patent Owner does not address the specific combination of Kogane and Fernandez. Instead, Patent Owner addresses the references separately, contending that (i) Kogane does not meet claims 32 and 34, because Kogane is directed to a JPEG system, which precludes the use of any motion video (PO Resp. 10), and (ii) Fernandez teaches a geographically fixed network of sensors, but fails to disclose a software tool that includes a dispatch generator (PO Resp. 11). According to Patent Owner, it is improper hindsight to speculate whether the system in Fernandez includes a dispatch generator. PO Resp. 11–12. Patent Owner’s contention is unpersuasive, because it attacks the prior art references individually, when the ground of unpatentability, as articulated by Petitioner, is based on the combined teachings of the Kogane and Fernandez. Nonobviousness cannot be established by attacking references individually when a challenge is predicated upon a combination of prior art disclosures. *See In re Merck & Co., Inc.*, 800 F.2d at 1097. Regardless, Patent Owner’s argument is unpersuasive, because (1) the use of motion video is not a required element in either claim 32 or 34, (2) as discussed above, Kogane does teach motion video, and (3) Fernandez teaches software tool 166 that functions as a dispatch generator by providing positional or directional functionality (dispatch signals) to alert authorities or other interested parties (predetermined response team) when an undesirable object or movement is monitored (Ex. 1008, 15:42–44; Fig.3).

Patent Owner further contends Kogane fails to disclose the use of a server as a management device for collecting and managing transmitted data. PO Resp. at 14–15. Again, Patent Owner fails to address the challenge as presented by Petitioner based on the combined teachings of Kogane and

Fernandez. Contrary to Patent Owner’s contention, Kogane does disclose a plurality of camera units 1a-1c that transmit data across a network to control server 5, which then records the data in database 47. Ex. 1007, 4:51–64, 6:4–8. Additionally, Fernandez teaches the use of a network based server (Ex. 1008, 3:16–26) that provides digital storage (*id.* at Abstract, 1:43–46, 9:10–25), and which receives and logs data from a plurality of sensor appliances (*id.* at 6:30–40, 7:27–29).

Therefore, we determine that Petitioner has shown by a preponderance of the evidence that claims 32 and 34 are unpatentable over Kogane and Fernandez.

III. CONCLUSION

We conclude Petitioner has shown by a preponderance of the evidence that:

- (1) claims 1–9, 12–17, 25, and 32 of the ’183 patent are unpatentable under 35 U.S.C. § 103(a) over Ely and Fernandez;
- (2) claims 10, 11, and 18–23 of the ’183 patent are unpatentable under 35 U.S.C. § 103(a) over Ely, Fernandez, and Imaide;
- (3) claim 24 of the ’183 patent is unpatentable under 35 U.S.C. § 103(a) over Ely, Fernandez, and Barzdins;
- (4) claims 25 and 33 of the ’183 patent are unpatentable under 35 U.S.C. § 102 as anticipated by Kogane; and
- (5) claims 32 and 34 of the ’183 patent are unpatentable under 35 U.S.C. § 103(a) over Kogane and Fernandez.

IV. ORDER

In consideration of the foregoing, it is hereby:

ORDERED that claims 1–25 and 32–34 of the '183 patent are unpatentable;

FURTHER ORDERED that because this is a final written decision, parties to the proceeding seeking judicial review of the decision must comply with the notice and service requirements of 37 C.F.R. § 90.2.

For PETITIONER:

Steven H. Slater
Michael Kucher
SLATER & MATSIL, L.L.P.
slater@slater-matsil.com
kucher@slater-matsil.com

For PATENT OWNER:

Robert C. Curfiss
bob@curfiss.com