IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Applicants:	G.T. Barker et al.	Attorney Docket No.:	116340
Application No.:	09/825,506	Art Unit: 2143 / Confirmation No.:	2007
Filed:	April 3, 2001	Examiner:	J.E. Avellino

Title: SYSTEM AND METHOD FOR PROVIDING CONFIGURABLE SECURITY MONITORING UTILIZING AN INTEGRATED INFORMATION SYSTEM

APPELLANTS' APPEAL BRIEF

Seattle, Washington

December 9, 2008

TO THE COMMISSIONER FOR PATENTS:

This Appeal Brief is filed in support of the Notice of Appeal filed on June 9, 2008, appealing the Examiner's final rejection, dated January 10, 2008, of pending Claims 1, 4, 5, 7-36, 38-50, and 52-58. Claims 4, 5, 7-36, 38-50, and 52-58 were rejected under 35 U.S.C. §103(a) as being unpatentable over Baxter (United States Patent No. 6,023,223), in view of Horon (United States Patent No. 6,229,429).

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS[PLLC]
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100

TABLE OF CONTENTS

		Page
I.	REAL PARTY IN INTEREST	1
II.	RELATED APPEALS AND INTERFERENCES	2
III.	STATUS OF CLAIMS	3
IV.	STATUS OF AMENDMENTS	4
V.	SUMMARY OF CLAIMED SUBJECT MATTER	5
VI.	GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL	10
VII.	ARGUMENT	11
	Ground 1: Whether Claims 1, 4-5, 7-36, 38-50, and 52-68 are legally obvious under 35 U.S.C. § 103(a) over Baxter in view of Horon.	11
	Independent Claim 1	12
	Claim 4	18
	Claim 5	19
	Claim 8	19
	Claim 14	20
	Claim 15	20
	Claim 16	21
	Claim 17	21
	Claim 20	22
	Claim 21	22
	Claim 22	23
	Claim 23	23
	Claim 24	23

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS[PLLC]
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100

Claim 25 24
Claim 27 25
Claim 28 25
Claim 29 26
Claim 30 26
Independent Claim 34 27
Claim 35 29
Claim 36 29
Claim 38 29
Claim 39 30
Claim 40 30
Claim 41 30
Claim 44 31
Independent Claim 48 31
Claim 52 32
Claim 53 33
Claim 54 33
Claim 55 33
VIII. CLAIMS APPENDIX 35
IX. EVIDENCE APPENDIX 46
X. RELATED PROCEEDINGS APPENDIX 47

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS[PLLC]
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100

I. REAL PARTY IN INTEREST

The real party in interest is VIG Acquisitions Ltd., L.L.C., of Wilmington, Delaware.

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS[PLLC]
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100

II. RELATED APPEALS AND INTERFERENCES

Appellants are not aware of any prior or pending appeals, judicial proceedings, or interferences that may be related to, directly affect or be affected by, or have a bearing on the decision of the Board of Appeals and Interferences (hereinafter the "Board") in the pending appeal.

III. STATUS OF CLAIMS

Claims 1, 4, 5, 7-36, 38-50, and 52-58 are rejected and on appeal.

Claims 2-3, 6, 37, and 51 have been canceled.

EX2009 - Page 6 of 51
IPR2023-00419
Motorola Solutions, Inc. v. Applied Capital, Inc.

IV. STATUS OF AMENDMENTS

Upon information and belief, there are no outstanding amendments filed subsequent to the final Office Action of January 10, 2008.

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS[PLLC]
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100

V. SUMMARY OF CLAIMED SUBJECT MATTER

In the summary below, the page and line numbers correspond to the page and line numbers of the application as filed. However, the references to the detailed description made herein are merely provided as an aid in understanding of the claimed subject matter. Accordingly, the locations referenced in the detailed description are merely exemplary embodiments of the disclosed subject matter and should not be construed as limiting.

With regard to Claim 1, a method for processing monitoring device data in an integrated information system that includes a central server in communication with two or more geographically distinct sites is provided. (FIGURE 1; FIGURE 2; FIGURE 3; FIGURE 4; page 4, lines 11-27; page 7, lines 22-31; page 9, line 34, to page 10, line 24; page 12, lines 4-25; page 13, lines 29-34; page 22, line 19, to page 23, line 22.) Monitoring device data corresponding to two monitoring devices with at least one monitoring device at each geographically distinct site and the monitoring device data is obtained continuously from the two or more geographically distinct sites. (FIGURE 2; FIGURE 4; FIGURE 5; page 4, lines 25-27; page 7, lines 32-34; page 8, lines 6-18; page 11, lines 22-26; page 12, lines 3-31; page 13, lines 8-9; page 21, lines 12-13.) One or more monitoring rules are obtained that correspond to the at least one monitoring device and establish the threshold monitoring device data that define a rule violation. (FIGURE 6; page 4, lines 27-29; page 14, lines 13-27; page 15, line 30, to page 18, line 3). Further, obtaining the one or more rules includes: obtaining asset rules if the monitoring device data is characterized as asset data; obtaining resource rules if the monitoring device data is characterized as resource data; and obtaining device rules if the monitoring device data is characterized as event data. (FIGURE 6; FIGURE 7A; FIGURE 7B; page 11, line 26, to page 12, line 2; page 12, line 26, to page 13, line 8; page 15, line 30, to page 16, line 7; page 16, lines 13-16; page 17, lines 3-23; page 20, lines 7-35; page 21, lines 12-26.) The monitoring

device data is processed at the central server according to the monitoring rules to determine whether a rule violation that identifies a combination of thresholds for each of the two monitoring devices has occurred. (FIGURE 6; FIGURE 7A; FIGURE 7B; page 4, lines 27-30; page 11, lines 11-13; page 13, lines 9-16; page 14, lines 12-27; page 15, line 30, to page 18, line 3; page 20, lines 7-35.) The monitoring device data is processed according to the rules including determining whether the monitoring device data exceeds thresholds of security information indicative of whether unauthorized access to a premises has occurred. (FIGURE 6; FIGURE 7A; FIGURE 7B; page 4, lines 27-30; page 14, lines 12, to page 15, line 2; page 16, line 7, to page 18, line 3; page 20, lines 7-35; page 21, line 1, to page 22, line 8.) An output corresponding to the processing of the monitoring device is generated indicating whether a rule violation has occurred. (FIGURE 6; FIGURE 7A; FIGURE 7B; page 13, lines 17-26; page 15, lines 2-24; page 16, line 26, to page 17, line 2; page 17, line 28, to page 18, line 3; page 20, lines 19-22; page 21, line 33, to page 22, line 18.) The monitoring data is characterized as asset data, resource data, or event data (page 12, lines 29-31). The asset data includes data from an identifiable object that is not capable of independent action (page 12, lines 31-35). The resource data includes data from an object capable of independent action (page 12, line 35, to page 13, line 3). Event data includes data from a device having a defined state (page 13, lines 4-7).

With regard to Claim 34, a system for implementing an integrated information system is provided (FIGURE 1; FIGURE 2; FIGURE 3; page 4, line 33, to page 5, line 5). One or more monitoring devices corresponding to two or more geographically distinct sites are organized according to geographic criteria and operable to continuously transmit monitoring device data (FIGURE 2; FIGURE 4; FIGURE 5; page 4, lines 25-27; page 4, line 34, to page 5, line 2; page 7, lines 22-31; page 8, lines 6-18; page 9, line 34, to page 10, line 24; page 11, lines 22-26; page 12, line 3, to page 13, line 9; page 21, lines 12-13; page 22, line 19, to page 23, line 22.) A

central processing server is operable to continuously obtain the monitoring device data from at least one monitoring device at each of the two or more geographically distinct sites. (FIGURE 2; FIGURE 4; FIGURE 5; page 4, lines 25-27; page 4, line 34, to page 5, line 2; page 7, lines 22-31; page 8, lines 6-18; page 9, line 34, to page 10, line 24; page 11, lines 22-26; page 12, line 3, to page 13, line 9; page 21, lines 12-13; page 22, line 19, to page 23, line 22.) The central processing server processes the monitoring device data according to one or more device rules that correspond to the one or more monitoring devices organized according to geographic criteria and generates an output that corresponds to the processing and reflects the results of processing the monitoring device data according to the rules. (FIGURE 6; FIGURE 7A; FIGURE 7B; page 4, lines 27-30; page 5, lines 2-12; page 11, lines 11-13; page 13, lines 9-26; page 14, lines 12-27; page 15, line 2, to page 18, line 3; page 20, lines 7-35; page 21, line 33, to page 22, line 18.) The processing of monitoring device data by the central processing server includes determining whether the monitoring device data exceeds thresholds of security information indicative of whether an unauthorized access to a premises has occurred. (Page 4, lines 27-30; page 5, lines 2-12; page 15, lines 1-17; page 21, line 1, to page 22, line 8.) The processing of the monitoring device data performed by the central processing server includes several additional steps. The monitoring device data is characterized as asset data, resource data, or event data. (FIGURE 6; FIGURE 7A; FIGURE 7B; page 11, line 26, to page 12, line 2; page 12, line 26, to page 13, line 8; page 15, line 30, to page 16, line 7; page 16, lines 13-16; page 17, lines 3-23; page 20, lines 7-35; page 21, lines 12-26.) If the monitoring device data is characterized as asset data that is from an identifiable object incapable of independent action, asset rules are obtained. (FIGURE 7A; page 12, lines 31-35; page 15, lines 31-34.) If the monitoring device data is characterized as resource data from an object capable of independent action, resource rules are obtained. (FIGURE 7B; page 12, line 35, to page 13, line 3; page 17, lines 8-11.) If the

monitoring device data is characterized as event data from a device having a defined state, device rules are obtained. (FIGURE 6; page 13, lines 4-7.) The monitoring device rules identify a combination of thresholds for the monitoring device data that define a rule violation. (Page 4, lines 27-30.)

With regard to Claim 48, a system for implementing an integrated information system is provided. (FIGURE 1; FIGURE 2; FIGURE 3; page 4, line 33. to page 5, line 5.) One or more monitoring devices are operable to continuously transmit monitoring device data from two or more geographically distinct sites organized according to geographic criteria. (Figure 2; FIGURE 4; FIGURE 5; page 4, lines 25-27; page 4, line 34, to page 5, line 2; page 7, lines 22-31; page 8, lines 6-18; page 9, line 34, to page 10, line 24; page 11, lines 22-26; page 12, line 3, to page 13, line 9; page 21, lines 12-13; page 22, line 19, to page 23, line 22.) A central processing means continuously obtains monitoring device data from one or more monitoring devices, processes the monitoring device data according to one or more monitoring device rules corresponding to one or more monitoring devices organized according to geographic criteria, and generates outputs that correspond to the processing and reflect the results of processing the monitoring device data according to the rules. (FIGURE 2; FIGURE 4; FIGURE 5; page 4, lines 25-27; page 4, line 34, to page 5, line 2; page 7, lines 22-31; page 8, lines 6-18; page 9, line 34, to page 10, line 24; page 11, lines 22-26; page 12, line 3, to page 13, line 9; page 21, lines 12-13; page 22, line 19, to page 23, line 22.) The processing of monitoring device data performed by the processing means includes determining whether the monitoring device data exceeds thresholds of security information indicative of whether an unauthorized access to a premises has occurred. (Page 4, lines 27-30; page 5, lines 2-12; page 15, lines 1-17; page 21, line 1, to page 22, line 8). The processing of the monitoring device data performed by the central processing means includes several steps. The monitoring device data is characterized as asset

data, resource data, or event data. (FIGURE 6; FIGURE 7A; Figure 7B; page 11, line 26, to page 12, line 2; page 12, line 26, to page 13, line 8; page 15, line 30, to page 16, line 7; page 16, lines 13-16; page 17, lines 3-23; page 20, lines 7-35; page 21, lines 12-26.) If the monitoring device data is characterized as asset data that is from an identifiable object incapable of independent action, asset rules are obtained. (FIGURE 7A; page 12, 31-35; page 15, lines 31-34.) If the monitoring device data is characterized as resource data from an object capable of independent action, resource rules are obtained. (FIGURE 7B; page 12, line 35, to page 13, line 3; page 17, lines 8-11.) If the monitoring device data is characterized as event data from a device having a defined state, device rules are obtained. (FIGURE 6; page 13, lines 4-7.) The monitoring device rules identify a combination of thresholds for the monitoring device data that define a rule violation. (Page 4, lines 27-30.)

EX2009 - Page 12 of 51
IPR2023-00419
Motorola Solutions, Inc. v. Applied Capital, Inc.

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Claims 1, 4-5, 7-36, 38-50, and 52-58 were rejected under 35 U.S.C. §103(a) as being unpatentable over Baxter (United States Patent Number 6,023,223), in view of Horon (United States Patent Number 6,229,429). In view of these rejections, the ground presented for appeal is as follows:

Ground 1: Whether Claims 1, 4-5, 7-36, 38-50, and 52-68 are legally obvious under 35 U.S.C. § 103(a) over Baxter in view of Horon.

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS PLLC
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100

VII. ARGUMENT

In *KSR International Co. v. Teleflex Inc.*, 550 U.S. __, 82 U.S.P.Q.2d 1385, 1395-97 (2007), the Supreme Court instructed that a claim rejection under 35 U.S.C. § 103 must include a clear articulation of the reason(s) why the claimed invention would have been obvious in view of the prior art. See also M.P.E.P. § 2143 and *In re Kahn*, 441 F.3d 977, 988 (Fed. Cir. 2006) ("Rejections on obviousness ground cannot be sustained by mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness.") Further, "[w]hen evaluating claims for obviousness under 35 U.S.C. § 103, all the limitations of the claims must be considered and given weight." See *Ex parte Grasselli*, 231 U.S.P.Q. 393 (Bd. App. 1983) aff'd mem. 738 F.2d 453 (Fed. Cir. 1984). See also M.P.E.P. § 2143.01(II). In addition, it is well established that a *prima facie* case of obviousness is only shown if the cited references, alone or in combination, teach or suggest each and every element recited in the claim. *In re Bell*, 991 F.2d 781 (Fed. Cir. 1993).

Appellants respectfully submit that the Examiner has failed to provide a clear articulation of the reasons why the claimed invention is legally obvious in view of Baxter in view of Horon. Appellants further submit that the Examiner has failed to determine correctly the scope and contents of the prior art and also to properly assess the difference between the references and the claimed invention.

Ground 1: Whether Claims 1, 4-5, 7-36, 38-50, and 52-68 are legally obvious under 35 U.S.C. § 103(a) over Baxter in view of Horon.

The Office Action rejected Claims 1, 4-5, 7-36, 38-50, and 52-68 as being unpatentable over Baxter in view of Horon. Appellants respectfully disagree and submit that neither Baxter nor Horon, alone or in combination, disclose or suggest each element of the independent claims.

Appellants further submit that neither Baxter nor Horon, alone or in combination, disclose or suggest additional patentable subject matter recited in the dependent claims.

Independent Claim 1

With regard to Claim 1, appellants submit that neither Baxter nor Horon disclose or suggest each and every element of Claim 1, nor would it have been obvious to a person of ordinary skill in the art to implement a method as claimed in Claim 1 in view of Baxter and Horon. Claim 1 recites:

> 1. In an integrated information system including a central server in communication with two or more geographically distinct sites, a method for processing monitoring device data, the method comprising:
>
> obtaining monitoring device data from the two or more geographically distinct sites, wherein the monitoring device data corresponds to two monitoring devices with at least one monitoring device at each geographically distinct site wherein the monitoring device data is obtained continuously;
>
> obtaining one or more monitoring rules corresponding to the at least one monitoring device, wherein the one or more rules establish the thresholds of monitoring device data that define a rule violation and wherein obtaining one or more rules includes:
>
> obtaining asset rules if the monitoring device data is characterized as asset data;
>
> obtaining resource rules if the monitoring device data is characterized as resource data; and
>
> obtaining device rules if the monitoring device data is characterized as event data;
>
> processing the monitoring device data at the central server according to the monitoring rules to determine whether a rule violation occurred wherein a rule violation identifies a combination of thresholds for each of the two monitoring devices;
>
> wherein processing the monitoring device data according to the rules includes determining whether the monitoring device data exceeds thresholds of security information indicative of whether an unauthorized access to a premises has occurred; and
>
> generating an output corresponding to the processing of the monitoring device data, wherein the output indicates whether a rule violation occurred;

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS PLLC
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100

characterizing the monitoring device data as asset data, resource data or event data;

wherein asset data includes data from an identifiable object that is not capable of independent action;

wherein resource data includes data from an object capable of independent action; and

wherein event data includes data from a device having a defined state.

Baxter is purportedly directed at a system and method for early warning detection and notification of environmental conditions. In this regard, Baxter uses a plurality of remotely located environmental sensors having a communication uplink to one or more Earth-orbiting satellites or other wireless transmission means. The environmental sensors periodically upload environmental condition data to a satellite. Then the satellite downloads the condition data to the database server where an interface provides access to the condition data through a network such as the Internet. The environmental conditions monitored by the system in Baxter include hydrocarbon concentrations, water temperature, wind speed, plate tectonics, atmospheric pressure, toxin concentrations, and the like. Additional applications may include tracking of animal migrations and densities, deforestation, polar ice cap activity, red tide, and other geological, biological, atmospheric, and oceanic conditions.

Yet, Baxter fails to teach or disclose all the elements of Claim 1. Regarding "obtaining monitoring device data from the two or more geographically distinct sites, wherein the monitoring device data corresponds to two monitoring devices with at least one monitoring device at each geographically distinct site wherein the monitoring device data is obtained continuously" for determining whether an unauthorized access to a premise has occurred, Baxter does not disclose this recitation of Claim 1. The Office Action asserts that Baxter discloses

EX2009 - Page 16 of 51
IPR2023-00419
Motorola Solutions, Inc. v. Applied Capital, Inc.

"obtain data in real time from the environmental sensors" and cites Col. 2, lines 55-67, of Baxter in support of that proposition. Appellants respectfully disagree. The cited portion of Baxter recites that "there is a need in the art for a global monitoring system that provides continuous real-time coverage of environmental conditions." However, the actual data of Baxter is obtained periodically. Indeed, Baxter explicitly states that the remote "sensors *periodically* upload environmental condition data to the satellite, the satellite downloads the condition data to the database server, the communication interface provides access to the condition data through the Internet." (Emphasis added.) Baxter at Col. 3, lines 14-19. Moreover, the Baxter reference explicitly indicates throughout the disclosure that data is periodically obtained and not obtained continuously as implied in the Office Action, stating:

> Thus, at periodic intervals, new data gathered by the satellites is emailed to the end-user for analysis. This method permits the end-user to create a personal archive of historical data for a particular query. (Baxter at Col. 5, lines 1-4.)
>
> Remotely located oil detection buoys in the Gulf of Mexico periodically relay hydrocarbon concentrations to orbiting satellites which then transmit the data to the web server. (Baxter at Col. 5, lines 16-20.)
>
> Remotely located sensors 15a-c may be pre-configured to periodically upload diagnostic information through the communications uplink. (Baxter at Col. 7, lines 44-48.)
>
> A communications interface between said database server and a data network wherein said sensors periodically upload environmental condition data. (Baxter at Col. 9, lines 11-15.)

Thus, it is quite clear that the data of Baxter is not being communicated continuously as recited in Claim 1. While periodically uploading environmental condition data to a satellite may have benefits when environmental conditions are being monitored, the system disclosed in

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS PLLC
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100

Baxter could not be applied to obtaining security data. When securing a facility, each moment can be of critical importance. By periodically uploading data, the Baxter system does not satisfy the time-sensitive requirements of a security monitoring system. In contrast to the system disclosed in Baxter, Claim 1 recites obtaining monitoring device data continuously.

Regarding "obtaining one or more monitoring rules corresponding to the at least one monitoring device, wherein the one or more rules establish the thresholds of monitoring device data that define a rule violation and wherein obtaining one or more rules includes: obtaining asset rules if the monitoring device data is characterized as asset data; obtaining resource rules if the monitoring device data is characterized as resource data; and obtaining device rules if the monitoring device data is characterized as event data," Baxter also fails to teach this recitation of Claim 1. The Office Action asserts that this recitation of Claim 1 is the same as "obtaining trigger conditions" and is disclosed at Col. 7, line 61, to Col. 8, line 21, of Baxter. Appellants respectfully disagree. Baxter purportedly allows a user to select a trigger condition to notify the user of the occurrence of some environmental condition. Baxter does not mention characterizing data that has been obtained and obtaining a specific type of rules based on the characterization as is recited in Claim 1.

The Examiner asserts that characterizing device data is disclosed because "incoming device data is characterized based on the type of device that sends the data, which inherently characterizes the data according to the characteristics of the data." However, the Examiner does not specify the portion of Baxter on which this assertion is based. As mentioned above, careful review of Baxter reveals nothing of characterizing monitoring device data. Appellants again note

that the Supreme Court requires a clear articulation of the reasons why an invention would be obvious in view of the prior art.

As conceded in the Office Action (page 4), Baxter fails to disclose that the rule violation determines an unauthorized access to a premises has occurred, or that the data can be characterized as resource or event data. Appellants agree with the Examiner in this regard. Careful review of Baxter fails to reveal anything that would teach, disclose, or even remotely suggest "wherein processing the monitoring device data according to the rules includes determining whether the monitoring device data exceeds thresholds of security information indicative of whether an unauthorized access to a premises has occurred," "characterizing the monitoring device data as asset data, resource data or event data," "wherein resource data includes data from an object capable of independent action," and "wherein event data includes data from a device having a defined state" as recited in Claim 1. However, the Examiner asserts that these and other recitations are taught by Horon. Appellants respectfully disagree. Horon, even if properly combinable with Baxter, which appellants deny, fails to remedy the deficiencies of Baxter.

Horon is purportedly directed toward a monitoring system that includes a monitoring station receiving messages from a variety of control panels in a uniform format. The system of Horon purportedly provides graphic capabilities for displaying a facility map with images representing the different devices and their locations. Horon purportedly allows changing a facility image in response to adding, removing, or relocating devices and advising an operator to add device images to a facility image. Thus, Horon is directed toward a system of graphically

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS PLLC
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100

representing the location of various devices within a location. In other words, Horon monitors the devices themselves and not the underlying activity the devices are installed to perform.

In contrast, Claim 1 recites a method for processing monitoring device data. Claim 1 does not merely locate devices as Horon does. The method of Claim 1 processes the monitoring device data obtained from the monitoring devices according to monitoring device rules. The Examiner asserts that Horon discloses a "plurality of sensors to determine if an unauthorized access to premises has occurred." This is in error. At Col. 1, lines 18-27, Horon briefly mentions that a system can include a variety of types of detectors. However, even the most broad reading of this portion of Horon would not teach "processing the monitoring device data according to the rules includes determining whether the monitoring device data exceeds thresholds of security information indicative of whether an unauthorized access to a premises has occurred" as recited in Claim 1. Careful review of Horon fails to reveal anything in the way of determining if an unauthorized access to premises has occurred.

Regarding "characterizing the monitoring device data as asset data, resource data or event data," "wherein resource data includes data from an object capable of independent action," and "wherein event data includes data from a device having a defined state," Horon also fails to disclose these recitations of Claim 1. Horon simply does not mention characterizing data. The Examiner asserts that these recitations of Claim 1 are taught at Col. 1, lines 15-26, and Col. 2, lines 18-35, of Horon. However, appellants have reviewed these portions of the reference carefully and find nothing to suggest these recitations of Claim 1. As mentioned above, Horon

merely mentions a number of possible device types. Horon does not identify data as resource data or event data. As a result, Horon fails to remedy the deficiencies of Baxter.

As noted above, the Supreme Court in KSR has specifically instructed that a 35 U.S.C. § 103(a) rejection requires a clear articulation of the reasons why the claimed invention would have been obvious. "When evaluating claims for obviousness under 35 U.S.C. § 103(a), ***all*** the limitations of the claims must be considered and given weight." See *Ex parte Grasselli*, 231 U.S.P.Q. 393 (Bd. App. 1983), *aff'd mem.* 738 F.2d 453 (Fed. Cir. 1984). (Emphasis added.) See also M.P.E.P. § 2143.01(II). In light of the above, appellants submit that Baxter and Horon, alone or in combination, fail to disclose or suggest each element of Claim 1. Accordingly, a proper *prima facie* case of obviousness has not been made. Appellants submit that the Board should overturn the 35 U.S.C. § 103(a) rejection of Claim 1.

Claims 4-5 and 7-33 depend either directly or indirectly from Claim 1 and are allowable for at least the same reasons as Claim 1 as well as for the additional subject matter they recite. For example, additional discussion of the patentability of Claims 4-5, 8, 14-17, 20-25, and 27-30 is provided as follows.

Claim 4

Claim 4 recites "wherein the monitoring device data is characterized as asset data and device data." The Examiner cited Horon, Col. 1, lines 15-26, as disclosing this limitation. Appellants respectfully disagree. This portion of the reference fails to even mention characterizing data. As discussed with respect to Claim 1, the cited reference fails to disclose characterizing monitoring device data. Further, Claim 4 recites characterizing the monitoring

device data as both asset and device data. Neither of the cited references disclose such a functionality.

In view of the above, and in addition to depending from an allowable independent claim, Claim 4 should be allowed.

Claim 5

Claim 5 recites "wherein the monitoring device data is characterized as resource data and device data." The Examiner cited Horon, Col. 1, lines 15-26, as disclosing this limitation. Appellants respectfully disagree. As discussed with respect to Claim 1, the cited reference fails to disclose characterizing monitoring device data. Further, Claim 5 recites characterizing the monitoring device data as both resource and device data. Neither of the cited references disclose such a functionality.

In view of the above, and in addition to depending from an allowable independent claim, Claim 5 should be allowed.

Claim 8

Claim 8 recites "wherein the monitoring device data is motion detection data and wherein the device rule threshold is the detection of motion." The Examiner asserts that Horon discloses this recitation at Col. 1, lines 15-26. Appellants respectfully disagree. Horon, at best, mentions a number of devices which include a motion detector. It does not mention monitoring device data is motion detection data, much less a device rule threshold being the detection of motion as recited in Claim 8. Indeed, a motion detector as recited in Horon is not the same as motion detection data nor the detection of motion being a device rule threshold.

In view of the above, and in addition to depending from an allowable independent claim, Claim 8 should be allowed.

Claim 14

Claim 14 recites "wherein generating an output corresponding to the processing of the monitoring device data includes generating a communication to one or more designated users, wherein generating the communication includes identifying a hierarchy that prioritizes the communication to the one or more designated users." The Examiner asserts that Horon discloses this recitation at Col. 1, lines 15-26. Appellants respectfully disagree. Careful review of this portion of Horon reveals nothing in the way of identifying a hierarchy that prioritizes the communication to one or more users. Neither of the cited references disclose such a functionality. The Examiner does not provide a clear articulation of how the above-cited portion of Horon discloses this recitation of Claim 14.

In view of the above, and in addition to depending from an allowable independent claim, Claim 14 should be allowed.

Claim 15

Claim 15 recites "wherein generating an output to one or more designated users includes: obtaining a schedule of preferred notification methods; and selecting a notification method from the schedule of notification methods." Appellants agree with the Examiner that such a functionality is not disclosed by either reference. However, the Examiner asserts that such functionality is well known and expected. Appellants respectfully disagree. The Examiner's position is purely speculative and not founded in any particular cited figure or passage. With the wide variety of communication methods and devices available, Claim 15 adds a significant functionality to the present application. The lack of such functionalities in the cited references only lends credence to appellants' position that the recitations of Claim 15 are not well known.

In view of the above, and in addition to depending from an allowable independent claim, Claim 15 should be allowed.

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS[PLLC]
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100

Claim 16

Claim 16 recites "wherein the schedule of preferred notification methods includes an indication of one or more preferred communication methods based on a time of day." Appellants agree with the Examiner that such a functionality is not disclosed by either reference. However, the Examiner asserts that such functionality is well known and expected. Appellants respectfully disagree. The Examiner's position is purely speculative and not founded in any particular cited figure or passage. Indeed, Claim 16 adds a significant functionality to the present application. The lack of such a functionality in the cited references only lends credence to appellants' position that the recitations of Claim 16 are not well known.

In view of the above, and in addition to depending from an allowable independent claim, Claim 16 should be allowed.

Claim 17

Claim 17 recites "wherein each designated user is associated with a schedule of preferred notification methods." Appellants agree with the Examiner that such a functionality is not disclosed by either reference. However, the Examiner asserts that such functionality is well known and expected. Appellants respectfully disagree. The Examiner's position is purely speculative and not founded in any particular cited figure or passage. With the wide variety of communication methods and devices available, Claim 17 adds a significant functionality to the present application. The lack of such functionalities in the cited references only lends credence to appellants' position that the recitations of Claim 17 are not well known.

In view of the above, and in addition to depending from an allowable independent claim, Claim 17 should be allowed.

Claim 20

Claim 20 recites "wherein the action includes activating a physical device within a monitored premises." Appellants agree with the Examiner that such a functionality is not disclosed by either reference. However, the Examiner asserts that such functionality is well known and expected. Appellants respectfully disagree. The Examiner's position is purely speculative and not founded in any particular cited figure or passage. Claim 20 adds a significant functionality to the present application. Activating physical devices aids the present invention in its overall purpose of monitoring a facility. The lack of such a functionality in the cited references only lends credence to appellants' position that the recitations of Claim 20 are not well known.

In view of the above, and in addition to depending from an allowable independent claim, Claim 20 should be allowed.

Claim 21

Claim 21 recites "wherein the physical device generates . . . an output in a tangible medium." Appellants agree with the Examiner that such a functionality is not disclosed by either reference. However, the Examiner asserts that such functionality is well known and expected. Appellants respectfully disagree. The Examiner's position is purely speculative and not founded in any particular cited figure or passage. Claim 21 adds a significant functionality to the present application. The use of physical devices aids the present invention in its overall purpose of securing a facility. The lack of such a functionality in the cited references only lends credence to appellants' position that the recitations of Claim 21 are not well known or expected.

In view of the above, and in addition to depending from an allowable independent claim, Claim 21 should be allowed.

Claim 22

Claim 22 recites "wherein the physical device is an audible alarm." Appellants agree with the Examiner that such a functionality is not disclosed by either reference. However, the Examiner asserts that such functionality is well known and expected. Appellants respectfully disagree. The Examiner's position is purely speculative and not founded in any particular cited figure or passage. Claim 22 adds a significant functionality to the present application. The use of an audible alarm aids the present invention in its overall purpose of securing a facility. The lack of such a functionality in the cited references only lends credence to appellant's position that the recitations of Claim 22 are not well known or expected.

In view of the above, and in addition to depending from an allowable independent claim, Claim 22 should be allowed.

Claim 23

Claim 23 recites "wherein the physical device is a microphone and speaker assembly." The Examiner asserts that this recitation of Claim 23 is taught by Baxter's recitation of a "telephone." Appellants respectfully disagree. A microphone and speaker assembly are not the same as a telephone. In addition, the Examiner has already conceded that the prior art references fail to teach the physical device of Claim 20, which Claim 23 depends from.

In view of the above, and in addition to depending from an allowable independent claim, Claim 23 should be allowed.

Claim 24

Claim 24 recites "wherein generating an output corresponding to the processing of the monitoring device data includes processing one or more additional monitoring device rules prior to generating an output." The Examiner asserts that Baxter discloses this recitation at Col. 4, lines 1-21, and Col. 7, line 61, to Col. 8, line 21. Appellants respectfully disagree. As referenced

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS PLLC
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100

above with respect to Claim 1, the cited references do not disclose monitoring device rules. The Examiner suggests that "using boolean operators, multiple thresholds are evaluated before generating an output" somehow teaches the recitation of Claim 24. Again, appellants respectfully disagree. Careful review of the cited portions of Baxter do not reveal a discussion of monitoring device rules, much less "generating an output corresponding to the processing of the monitoring device data includes processing one or more additional monitoring device rules prior to generating an output" as recited in Claim 24.

The Supreme Court is quite clear that a Section 103(a) rejection must be supported by a clear articulation of how the cited references disclose a claim. The Examiner has not provided a clear articulation of how the cited references teach the recitations of Claim 24.

In view of the above, and in addition to depending from an allowable independent claim, Claim 24 should be allowed.

Claim 25

Claim 25 recites "wherein the at least one monitoring device includes a network access monitor and wherein the monitoring device includes data identifying one or more users logged into a computer network." Appellants agree with the Examiner that such a functionality is not disclosed by either reference. However, the Examiner asserts that such functionality is well known and expected. Appellants respectfully disagree. The Examiner's position is purely speculative and not founded in any particular cited figure or passage. Claim 25 adds a number of significant functionalities to the present application. The use of a network access monitor and having data identifying users logged into a computer network aids the present invention in its overall purpose of securing a facility. The lack of such a functionality in the cited references only lends credence to appellants' position that the recitations of Claim 25 are not well known or expected.

In view of the above, and in addition to depending from an allowable independent claim, Claim 25 should be allowed.

Claim 27

Claim 27 recites "wherein the monitoring device data further includes data identifying a particular individual passing through the monitored data." Appellants agree with the Examiner that such a functionality is not disclosed by either reference. However, the Examiner asserts that such functionality is well known and expected. Appellants respectfully disagree. The Examiner's position is purely speculative and not founded in any particular cited figure or passage. Claim 27 adds an important functionality to the present invention. The identification of a particular individual passing through the monitored data aids the present invention in its overall purpose of securing a facility. The lack of such a functionality in the cited references only lends credence to appellants' position that the recitations of Claim 27 are not well known or expected.

In view of the above, and in addition to depending from an allowable independent claim, Claim 27 should be allowed.

Claim 28

Claim 28 recites "wherein the at least one monitoring device includes a number of monitoring devices and wherein the monitoring device data includes data identifying the location of individuals within a premises." Appellants agree with the Examiner that such a functionality is not disclosed by either reference. However, the Examiner asserts that such functionality is well known and expected. Appellants respectfully disagree. The Examiner's position is purely speculative and not founded in any particular cited figure or passage. Claim 28 adds significant functionalities to the present application. In particular, data identifying the location of individuals within a premises aids the present invention in its overall purpose of securing a

facility. The lack of such a functionality in the cited references only lends credence to appellants' position that the recitations of Claim 28 are not well known or expected.

In view of the above, and in addition to depending from an allowable independent claim, Claim 28 should be allowed.

Claim 29

Claim 29 recites "wherein the monitoring device data further identifies the identities of individuals within the premises." Appellants agree with the Examiner that such a functionality is not disclosed by either reference. However, the Examiner asserts that such functionality is well known and expected. Appellants respectfully disagree. The Examiner's position is purely speculative and not founded in any particular cited figure or passage. Claim 29 adds a significant functionality to the present application. In particular, identifying the identities of individuals within the premises aids the present invention in its overall purpose of securing a facility. The lack of such a functionality in the cited references only lends credence to appellants' position that the recitations of Claim 29 are not well known or expected.

In view of the above, and in addition to depending from an allowable independent claim, Claim 29 should be allowed.

Claim 30

Claim 30 recites "wherein generating an output corresponding to the processing of the monitoring device data includes generating an output dedicated to a particular individual identified within the premises." Appellants agree with the Examiner that such a functionality is not disclosed by either reference. However, the Examiner asserts that such functionality is well known and expected. Appellants respectfully disagree. The Examiner's position is purely speculative and not founded in any particular cited figure or passage. Claim 30 adds significant functionalities to the present application. In particular, generating an output dedicated to a

particular individual identified within the premises aids the present invention in its overall purpose of securing a facility. The lack of such a functionality in the cited references only lends credence to appellants' position that the recitations of Claim 30 are not well known or expected.

In view of the above, and in addition to depending from an allowable independent claim, Claim 30 should be allowed.

Independent Claim 34

With regard to Claim 34, appellants submit that neither Baxter nor Horon disclose or suggest each and every element of Claim 34 nor would it have been obvious to a person of ordinary skill in the art to implement a system as claimed in Claim 34 in view Baxter and Horon. Claim 34 recites:

> 34. A system for implementing an integrated information system, the system comprising:
>
> one or more monitoring devices corresponding to two or more geographically distinct sites organized according to geographic criteria and operable to continuously transmit monitoring device data;
>
> a central processing server, the central processing server operable to continuously obtain the monitoring device data from at least one monitoring device at each of the two or more geographically distinct sites;
>
> wherein the central processing server processes the monitoring device data according to one or more monitoring device rules corresponding to the one or more monitoring devices organized according to geographic criteria, wherein the central processing server generates an output corresponding to the processing, wherein the output reflects the results of processing the monitoring device data according to the rules;
>
> wherein the processing of monitoring device data performed by the central processing server includes determining whether the monitoring device data exceeds thresholds of security information indicative of whether an unauthorized access to a premises has occurred;
>
> wherein the processing of monitoring device data performed by the central processing server includes:
>
> characterizing the monitoring device data as asset data, resource data or event data;

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS PLLC
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100

obtaining asset rules if the monitoring device data is characterized as asset data that is from an identifiable object incapable of independent action;

obtaining resource rules if the monitoring device data is characterized as resource data from an object capable of independent action; and

obtaining device rules if the monitoring device data is characterized as event data from a device having a defined state; and

wherein the monitoring device rules identify a combination of thresholds for the monitoring device data that define a rule violation.

The cited references Baxter and Horon fail to disclose a system for implementing an integrated information system as recited in Claim 34. Baxter purportedly discloses an early warning detection and notification network for monitoring environmental conditions. Horon purportedly discloses a monitoring station that stores graphic information including site maps and floor plans to provide backgrounds, and device images positionable on the backgrounds to accurately depict device locations in the facility. Appellants note the failure of the Examiner to identify exactly where the elements of Claim 34 are taught within the cited references. To support a 35 U.S.C. § 103(a) rejection, the Supreme Court in KSR requires a clear articulation of the reasons why the subject matter of a claim would have been obvious. The Examiner has provided no such articulation, only offering that Claim 1 was rejected "for similar reasons as stated above."

Appellants submit that the 35 U.S.C. §103(a) rejection of Claim 34 is in error as not being based on a proper, *prima facie* case of obviousness and request that the Board overturn the rejection.

Claims 35-36, 38-47 depend either directly or indirectly from Claim 34 and are allowable for at least the same reasons as Claim 34 as well as for the additional subject matter they recite. For example, additional discussion of the patentability of the Claims 35,36, 38-41, and 44.

Claim 35

Claim 35 recites "further comprising at least one premises server in communication with at least one of the monitoring devices and with the central processing server, wherein the premises server is operable to obtain the monitoring device data from the monitoring device and to transmit the monitoring device data to the central processing server." The Examiner did not specify where such a recitation is disclosed within Baxter and Horon. Appellants have reviewed the cited references at length, and find nothing within either reference that teaches or suggests the subject matter claimed in Claim 35.

In view of the above, and in addition to depending from an allowable independent claim, Claim 35 should be allowed.

Claim 36

Claim 36 recites "wherein the at least one premises server includes two or more premises servers connected in parallel to each other." The Examiner did not specify where such a recitation is disclosed within Baxter and Horon. Appellants have reviewed the cited references at length, and find nothing within either reference that teaches or suggests the subject matter claimed in Claim 36.

In view of the above, and in addition to depending from an allowable independent claim, Claim 36 should be allowed.

Claim 38

Claim 38 recites "further comprising one or more rules databases for maintaining the monitoring device rules." The Examiner did not specify where such a recitation is disclosed within Baxter and Horon. Appellants have reviewed the cited references at length, and find nothing within either reference that teaches or suggests the subject matter claimed in Claim 38.

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS PLLC
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100

In view of the above, and in addition to depending from an allowable independent claim, Claim 38 should be allowed.

Claim 39

Claim 39 recites "wherein the one or more rules databases include an event rules database for maintaining monitoring device rules corresponding to event data." The Examiner did not specify where such a recitation is disclosed within Baxter and Horon. Appellants have reviewed the cited references at length, and find nothing within either reference that teaches or suggests the subject matter claimed in Claim 39.

In view of the above, and in addition to depending from an allowable independent claim, Claim 39 should be allowed.

Claim 40

Claim 40 recites "wherein the one or more rules databases include an asset rules database for maintaining monitoring device rules corresponding to asset data." The Examiner did not specify where such a recitation is disclosed within Baxter and Horon. Appellants have reviewed the cited references at length, and find nothing within either reference that teaches or suggests the subject matter claimed in Claim 40.

In view of the above, and in addition to depending from an allowable independent claim, Claim 40 should be allowed.

Claim 41

Claim 41 recites "wherein the one or more rules databases include a resource rules database for maintaining monitoring device rules corresponding to resource data." The Examiner did not specify where such a recitation is disclosed within Baxter and Horon. Appellants have reviewed the cited references at length, and find nothing within either reference that teaches or suggests the subject matter claimed in Claim 41.

In view of the above, and in addition to depending from an allowable independent claim, Claim 41 should be allowed.

Claim 44

Claim 44 recites "wherein the output devices include a speaker and microphone assembly." The Examiner did not specify where such a recitation is disclosed within Baxter and Horon. Appellants have reviewed the cited references at length, and find nothing within either reference that teaches or suggests the subject matter claimed in Claim 44.

In view of the above, and in addition to depending from an allowable independent claim, Claim 44 should be allowed.

Independent Claim 48

With regard to Claim 48, appellants submit that neither Baxter nor Horon disclose or suggest each and every element of Claim 48, nor would it have been obvious to a person of ordinary skill in the art to implement the system claimed in Claim 48 in view of Baxter and Horon. Claim 48 recites:

> 48. A system for implementing an integrated information system, the system comprising:
>
> one or more monitoring devices operable to continuously transmit monitoring device data from two or more geographically distinct sites organized according to geographic criteria; and
>
> central processing means for continuously obtaining the monitoring device data from the one or more monitoring devices, processing the monitoring device data according to one or more monitoring device rules corresponding to the one or more monitoring devices organized according to geographic criteria and generating outputs corresponding to the processing, wherein–the output reflects the results of processing the monitoring device data according to the rules;
>
> wherein the processing of monitoring device data performed by the processing means includes determining whether the monitoring device data exceeds thresholds of security information indicative of whether an unauthorized access to a premises has occurred;

EX2009 - Page 34 of 51
IPR2023-00419
Motorola Solutions, Inc. v. Applied Capital, Inc.

wherein the processing of monitoring device data performed by the central processing means includes:

characterizing the monitoring device data as asset data, resource data or event data;

obtaining asset rules if the monitoring device data is characterized as asset data that is from an identifiable object incapable of independent action;

obtaining resource rules if the monitoring device data is characterized as resource data from an object capable of independent action; and

obtaining device rules if the monitoring device data is characterized as event data from a device having a defined state; and

wherein the monitoring device rules identify a combination of thresholds for the monitoring device data that define a rule violation.

Appellants note the failure of the Examiner to identify exactly where the elements of Claim 48 are taught within the cited references Baxter and Horon. For at least the same reasons as previously discussed with respect to Claims 1 and 34, the cited references fail to disclose or suggest a system for implementing an integrated information system as recited in Claim 48. Furthermore, to support a 35 U.S.C. § 103(a) rejection, the Supreme Court in *KSR* required a clear articulation of the reasons why the subject matter of a claim would have been obvious. The Examiner has provided no such articulation.

Appellants submit that the 35 U.S.C. § 103(a) rejection of Claim 48 is in error as not being based on a proper, *prima facie* case of obviousness, and request that the Board overturn the rejection.

Claims 49-50 and 52-58 depend directly from Claim 48 and are allowable for at least the same reasons as Claim 48 as well as for the additional subject matter they recite. For example, additional discussion of the patentability of Claims 52-55 is provided as follows.

Claim 52

Claim 52 recites "further comprising means for maintaining the monitoring device rules." The Examiner did not specify where such a recitation is disclosed within Baxter and Horon.

Appellants have reviewed the cited references at length, and find nothing within either reference that teaches or suggests the subject matter claimed in Claim 52.

In view of the above, and in addition to depending from an allowable independent claim, Claim 52 should be allowed.

Claim 53

Claim 53 recites "wherein the means for maintaining the monitoring device rules include means for maintaining monitoring device rules corresponding to event data." The Examiner did not specify where such a recitation is disclosed within Baxter and Horon. Appellants have reviewed the cited references at length, and find nothing within either reference that teaches or suggests the subject matter claimed in Claim 53.

In view of the above, and in addition to depending from an allowable independent claim, Claim 53 should be allowed.

Claim 54

Claim 54 recites "wherein the means for maintaining the monitoring device rules include means for maintaining monitoring device rules corresponding to asset data." The Examiner did not specify where such a recitation is disclosed within Baxter and Horon. Appellants have reviewed the cited references at length, and find nothing within either reference that teaches or suggests the subject matter claimed in Claim 54.

In view of the above, and in addition to depending from an allowable independent claim, Claim 54 should be allowed.

Claim 55

Claim 55 recites "wherein the means for maintaining the monitoring device rules include means for maintaining monitoring device rules corresponding to resource data." The Examiner did not specify where such a recitation is disclosed within Baxter and Horon. Appellants have

reviewed the cited references at length, and find nothing within either reference that teaches or suggests the subject matter claimed in Claim 55.

In view of the above, and in addition to depending from an allowable independent claim, Claim 55 should be allowed.

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS PLLC
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100

VIII. CLAIMS APPENDIX

1. In an integrated information system including a central server in communication with two or more geographically distinct sites, a method for processing monitoring device data, the method comprising:

obtaining monitoring device data from the two or more geographically distinct sites, wherein the monitoring device data corresponds to two monitoring devices with at least one monitoring device at each geographically distinct site wherein the monitoring device data is obtained continuously;

obtaining one or more monitoring rules corresponding to the at least one monitoring device, wherein the one or more rules establish the thresholds of monitoring device data that define a rule violation and wherein obtaining one or more rules includes:

obtaining asset rules if the monitoring device data is characterized as asset data;

obtaining resource rules if the monitoring device data is characterized as resource data; and

obtaining device rules if the monitoring device data is characterized as event data;

processing the monitoring device data at the central server according to the monitoring rules to determine whether a rule violation occurred wherein a rule violation identifies a combination of thresholds for each of the two monitoring devices;

EX2009 - Page 38 of 51
IPR2023-00419
Motorola Solutions, Inc. v. Applied Capital, Inc.

wherein processing the monitoring device data according to the rules includes determining whether the monitoring device data exceeds thresholds of security information indicative of whether an unauthorized access to a premises has occurred; and

generating an output corresponding to the processing of the monitoring device data, wherein the output indicates whether a rule violation occurred;

characterizing the monitoring device data as asset data, resource data or event data;

wherein asset data includes data from an identifiable object that is not capable of independent action;

wherein resource data includes data from an object capable of independent action; and

wherein event data includes data from a device having a defined state.

2-3. (Canceled)

4. The method of Claim 1, wherein the monitoring device data is characterized as asset data and device data.

5. The method of Claim 1, wherein the monitoring device data is characterized as resource data and device data.

6. (Canceled)

7. The method of Claim 1, wherein the device rules establish a state threshold for a rule violation, and wherein processing the monitoring

device data according to the device rules includes determining whether the monitoring device data indicates a particular state.

8. The method of Claim 7, wherein the monitoring device data is motion detection data and wherein the device rule threshold is the detection of motion.

9. The method of Claim 1, wherein characterizing the monitoring device data comprises determining whether the monitoring device data includes data identifying a monitoring device generating the data.

10. The method of Claim 9, wherein characterizing the monitoring device data as asset data further includes comparing the data identifying the monitoring device generating the monitoring device data to a set of known assets.

11. The method of Claim 10, wherein the set of known assets are maintained in a database.

12. The method of Claim 9, wherein characterizing the monitoring device data as resource data further includes comparing the data identifying the monitoring device generating the monitoring device data to a set of known resources.

13. The method of Claim 12, wherein the set of known resources are maintained in a database.

14. The method of Claim 1, wherein generating an output corresponding to the processing of the monitoring device data includes generating a communication to one or more designated users, wherein

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS PLLC
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100

generating the communication includes identifying a hierarchy that prioritizes the communication to the one or more designated users.

15. The method of Claim 14, wherein generating an output to one or more designated users includes:

obtaining a schedule of preferred notification methods; and

selecting a notification method from the schedule of notification methods.

16. The method of Claim 15, wherein the schedule of preferred notification methods includes an indication of one or more preferred communication methods based on a time of day.

17. The method of Claim 15, wherein each designated user is associated with a schedule of preferred notification methods.

18. The method of Claim 14, wherein generating a communication to one or more designated users includes generating a wireless communication to a designated user.

19. The method of Claim 1, wherein generating an output corresponding to the processing of the monitoring device data includes initiating an action at a geographically distinct site where the monitoring data was obtained.

20. The method of Claim 19, wherein the action includes activating a physical device within a monitored premises.

21. The method of Claim 20, wherein the physical device generates a an output in a tangible medium.

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS PLLC
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100

22. The method of Claim 20, wherein the physical device is an audible alarm.

23. The method of Claim 20, wherein the physical device is a microphone and speaker assembly.

24. The method of Claim 1, wherein generating an output corresponding to the processing of the monitoring device data includes processing one or more additional monitoring device rules prior to generating an output.

25. The method of Claim 1, wherein the at least one monitoring device includes a network access monitor and wherein the monitoring device includes data identifying one or more users logged into a computer network.

26. The method of Claim 1, wherein the at least one monitoring device includes a movement sensor and wherein the monitoring device data includes data identifying whether an individual has passed through a monitored area.

27. The method of Claim 26, wherein the monitoring device data further includes data identifying a particular individual passing through the monitored data.

28. The method of Claim 1, wherein the at least one monitoring device includes a number of monitoring devices and wherein the monitoring device data includes data identifying the location of individuals within a premises.

29. The method of Claim 28, wherein the monitoring device data further identifies the identities of individuals within the premises.

30. The method of Claim 29, wherein generating an output corresponding to the processing of the monitoring device data includes generating an output dedicated to a particular individual identified within the premises.

31. The method of Claim 1, wherein obtaining monitoring device data from at least one monitoring device includes obtaining the monitoring device data from a distributed communication network.

32. A computer readable medium having computer-executable instructions for performing the method recited in Claim 1.

33. A computer system having a processor, a memory and an operating environment, the computer system operable to perform the method recited in Claim 1.

34. A system for implementing an integrated information system, the system comprising:

one or more monitoring devices corresponding to two or more geographically distinct sites organized according to geographic criteria and operable to continuously transmit monitoring device data;

a central processing server, the central processing server operable to continuously obtain the monitoring device data from at least one monitoring device at each of the two or more geographically distinct sites;

wherein the central processing server processes the monitoring device data according to one or more monitoring device rules

corresponding to the one or more monitoring devices organized according to geographic criteria, wherein the central processing server generates an output corresponding to the processing, wherein the output reflects the results of processing the monitoring device data according to the rules;

wherein the processing of monitoring device data performed by the central processing server includes determining whether the monitoring device data exceeds thresholds of security information indicative of whether an unauthorized access to a premises has occurred;

wherein the processing of monitoring device data performed by the central processing server includes:

characterizing the monitoring device data as asset data, resource data or event data;

obtaining asset rules if the monitoring device data is characterized as asset data that is from an identifiable object incapable of independent action;

obtaining resource rules if the monitoring device data is characterized as resource data from an object capable of independent action; and

obtaining device rules if the monitoring device data is characterized as event data from a device having a defined state; and

wherein the monitoring device rules identify a combination of thresholds for the monitoring device data that define a rule violation.

35. The system as recited in Claim 34 further comprising at least one premises server in communication with at least one of the

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS PLLC
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100

monitoring devices and with the central processing server, wherein the premises server is operable to obtain the monitoring device data from the monitoring device and to transmit the monitoring device data to the central processing server.

36. The system as recited in Claim 35, wherein the at least one premises server includes two or more premises servers connected in parallel to each other.

37. (Canceled)

38. The system as recited in Claim 34, further comprising one or more rules databases for maintaining the monitoring device rules.

39. The system as recited in Claim 38, wherein the one or more rules databases include an event rules database for maintaining monitoring device rules corresponding to event data.

40. The system as recited in Claim 38, wherein the one or more rules databases include an asset rules database for maintaining monitoring device rules corresponding to asset data.

41. The system as recited in Claim 38, wherein the one or more rules databases include a resource rules database for maintaining monitoring device rules corresponding to resource data.

42. The system as recited in Claim 34 further comprising one or more output devices in communication with the central processing server, wherein the output devices are operable to obtain an output from the central processing server.

43. The system as recited in Claim 42, wherein the output devices include an audible alarm.

44. The system as recited in Claim 42, wherein the output devices include a speaker and microphone assembly.

45. The system as recited in Claim 34, wherein one or more of the monitoring devices communicate with the central processing server via a data network.

46. The system as recited in Claim 45, wherein the data network is the Internet.

47. The system as recited in Claim 45, wherein the data network is a distributed data network.

48. A system for implementing an integrated information system, the system comprising:

one or more monitoring devices operable to continuously transmit monitoring device data from two or more geographically distinct sites organized according to geographic criteria; and

central processing means for continuously obtaining the monitoring device data from the one or more monitoring devices, processing the monitoring device data according to one or more monitoring device rules corresponding to the one or more monitoring devices organized according to geographic criteria and generating outputs corresponding to the processing, wherein–the output reflects the results of processing the monitoring device data according to the rules;

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS PLLC
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100

wherein the processing of monitoring device data performed by the processing means includes determining whether the monitoring device data exceeds thresholds of security information indicative of whether an unauthorized access to a premises has occurred;

wherein the processing of monitoring device data performed by the central processing means includes:

characterizing the monitoring device data as asset data, resource data or event data;

obtaining asset rules if the monitoring device data is characterized as asset data that is from an identifiable object incapable of independent action;

obtaining resource rules if the monitoring device data is characterized as resource data from an object capable of independent action; and

obtaining device rules if the monitoring device data is characterized as event data from a device having a defined state; and

wherein the monitoring device rules identify a combination of thresholds for the monitoring device data that define a rule violation.

49. The system as recited in Claim 48 further comprising data communication means in communication with at least one monitoring device and with the central processing means, wherein the data communication means obtains monitoring device data from the monitoring device and transmits the data to the central processing means.

50. The system as recited in Claim 49, wherein the communications means include parallel processing means obtaining and for data transmitting.

51. (Canceled)

52. The system as recited in Claim 48, further comprising means for maintaining the monitoring device rules.

53. The system as recited in Claim 52, wherein the means for maintaining the monitoring device rules include means for maintaining monitoring device rules corresponding to event data.

54. The system as recited in Claim 52, wherein the means for maintaining the monitoring device rules include means for maintaining monitoring device rules corresponding to asset data.

55. The system as recited in Claim 52, wherein the means for maintaining the monitoring device rules include means for maintaining monitoring device rules corresponding to resource data.

56. The system as recited in Claim 48 further comprising one or more output device means for obtaining outputs from the central processing means.

57. The system as recited in Claim 48, wherein one or more of the monitoring devices communicate with the central processing means via data network means.

58. The system as recited in Claim 57, wherein the data network means include a distributed data network means.

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS PLLC
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100

IX. EVIDENCE APPENDIX

None

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS PLLC
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100

X. RELATED PROCEEDINGS APPENDIX

None.

Respectfully submitted,

CHRISTENSEN O'CONNOR
JOHNSON KINDNESS[PLLC]



Clint J. Feekes
Registration No. 51,670
Direct Dial No. 206.695.1633

CJF/MLR:sbk/nfs

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS[PLLC]
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100

16340199.DOC