

DECLARATION OF EXPERT JAMES PARKER

\

U.S. Patent No. 7,583,191

Issue Date: September 1, 2009

Title: SECURITY SYSTEM AND METHOD FOR USE OF SAME

TABLE OF CONTENTS

I.	INTRODUCTION	1
II.	MY BACKGROUND AND QUALIFICATIONS	3
III.	RELEVANT LEGAL STANDARDS	7
IV.	OVERVIEW	10
V.	BACKGROUND	13
A.	SUMMARY OF THE '191 PATENT.....	13
B.	SUMMARY OF THE CHALLENGED CLAIMS	16
C.	PRIORITY DATE OF THE CHALLENGED CLAIMS.....	19
D.	CLAIM CONSTRUCTION	19
E.	LEVEL OF ORDINARY SKILL IN THE ART	20
F.	STATE OF THE ART.....	21
VI.	CHALLENGES	26
A.	IDENTIFICATION OF CHALLENGE.....	26
B.	PRIOR ART	26
1.	SCHRANZ (<i>EX-1004</i>).....	26
VII.	IDENTIFICATION OF HOW THE CHALLENGED CLAIMS ARE UNPATENTABLE.....	27
A.	GROUND 1: CLAIMS 21-47 ARE OBVIOUS OVER SCHRANZ	27
1.	THE SCHRANZ REFERENCE	27
2.	DETAILED APPLICATION OF SCHRANZ.....	30
VIII.	CONCLUSION.....	80
	CONCLUSION AND DECLARATION.....	81

APPENDIX A – MATERIALS RELIED UPON.....	83
---	----

APPENDIX B – <i>CURRICULUM VITAE</i>	84
--	----

I. INTRODUCTION

1. I am over the age of eighteen (18) and otherwise competent to make this Declaration.

2. I have been retained on behalf of Vivint LLC (“Petitioner”) as an independent technical expert. Although I am being compensated at my rate of \$525 per hour for the time I spend on this matter, no part of my compensation depends on the outcome of this proceeding, and I have no other interest in this proceeding. To the best of my knowledge, I have no financial interest in Vivint LLC.

3. This Declaration involves U.S. Patent No. 7,583,191 (the “’191 Patent”) (*EX-1001*), titled “SECURITY SYSTEM AND METHOD FOR USE OF SAME” and listing Duke W. Zinser as the inventor.

4. For the purposes of this declaration, as discussed later, I have been instructed to assume that the effective filing date of the claims of the ’191 Patent is no earlier than November 14, 2006, the filing date of U.S. Patent Application No. 11/559,808.

5. I understand that according to USPTO records, the ’191 Patent is currently assigned to Duke W. Zinser (“Zinser” or “Patent Owner”).

6. The ’191 Patent is directed to a doorbell monitoring system to allow remote monitoring and surveillance. I am familiar with the technology described in the ’191 Patent as of the earliest possible priority date of November 14, 2006.

Expert Declaration of James Parker

7. In preparing this Declaration, I have reviewed the '191 Patent (*EX-1001*), the file history of the '191 Patent (*EX-1002*), and each of the documents cited herein, and I have considered these documents in light of the general knowledge in the art as of November 14, 2006. For convenience, the materials I considered in forming my opinion are listed in Appendix A. In formulating my opinions, I have relied upon my experience in the relevant art. I have also considered the viewpoint of a person of ordinary skill in the art ("POSA") in the relevant field, as of November 14, 2006, who I described below (§V.E).

8. The opinions and comments formulated during this assessment are based on observations and information available at the time of the investigation. The findings presented herein are made to a reasonable degree of scientific certainty. I have made every effort to accurately and completely investigate all areas of concern identified during my investigation.

9. I have been asked to provide my technical expertise, analysis, insights, and opinions regarding the '191 Patent and relevant references that form the basis of the arguments set forth by Vivint, with respect to the validity of the '191 Patent. As I describe in detail below, I offer the following opinions in this Declaration:

- A POSA would have found Claims 21-47 of the '191 Patent obvious over Schranz.

II. MY BACKGROUND AND QUALIFICATIONS

10. My expertise qualifies me to do the type of analysis required in this case for the field of monitoring systems. Of particular relevance, I am an expert in Electronic Security Systems and Sensors with over 40 years of industry experience in Electronics R&D / New Product Development. I have contributed to the development of hundreds of products, including residential and commercial, burglar and fire alarm systems and their sensors. My expertise spans the entire lifecycle of these systems, from design and engineering to compliance with standards and regulations.

11. Throughout the remainder of this Declaration, I will refer to the field of monitoring systems as the “relevant field” or the “relevant art.” In formulating my opinions, I have relied upon my training, knowledge, and experience in the relevant art. A copy of my current curriculum vitae is provided in Appendix B or as *EX-1009*, and it provides a comprehensive description of my academic and employment history, including a list of relevant art patents and publications for at least the last 40 years.

12. I started in the relevant art as a student at the Radio College of Canada (now part of Yorkville University) where I earned a diploma, roughly equivalent to a U.S. Bachelor’s degree, in Electronic Engineering Technology in Toronto, Ontario, Canada in 1982. I am a named inventor on over 25 patents in electronic security

Expert Declaration of James Parker

systems, sensors, monitoring systems, fire alarm technology, and related technologies. A list of these patents is included in my curriculum vitae (Appendix B or EX-1009) while a summary with abstracts is available as EX-1010.

13. In 1983, I began my career in engineering with Thermetic Controls Limited as an Engineering Technologist which included the design and implementation of production test equipment for safety limit checks. After leaving Thermetic Controls Limited, I had the pleasure of joining Har-Tech Electronics Ltd. as a Technical Sales Representative serving the Greater Toronto Area by providing sales and technical support to customers and potential customers of electronic component manufacturers. Following my time at Har-Tech Electronics Ltd., I became the Vice President of Engineering at Swinemaster Inc. where I led a small research and development team in the development of an automated juvenile swine feeding machine.

14. In 1985, I became the head of Engineering at Tyco Security Products, formerly Digital Security Controls (DSC) Limited. DSC designed and supplied alarm system control panels and peripheral devices. Over the course of nearly 19 years, I played a central role in transforming DSC into one of the largest companies in its marketplace, with worldwide sales in over 120 countries. I was responsible for all of DSC's research and product development efforts. Tyco Security Products (TYCO) acquired DSC, and I was the Vice President of Engineering at TYCO until

Expert Declaration of James Parker

December 2003. As the head of a 200+ member engineering department, I was responsible for the research and product development efforts, including Six Sigma, ISO900X quality programs, microcontroller technology, KEYBUS and COMBUS protocols for interconnecting components, and Application Specific Integrated Circuits (ASICs) in relation to security and monitoring systems.

15. I developed the KEYBUS and COMBUS protocols for interconnecting components. These protocols have a proven track record and have been widely imitated and copied. I also developed DSC's wireless protocols for both 924 MHz DSSS (Direct Sequence Spread Spectrum) and 433 MHz tight narrow band.

16. I conceived and drove the development of over 12 mixed mode ASIC's (Application Specific Integrated Circuits). Mixed mode ASIC's combine analog and digital circuitry on a single chip. They offer superior capabilities and performance to "off the shelf" solutions while dramatically reducing cost and improving product reliability.

17. In addition to DSC's own engineering, I was also responsible for the engineering departments of the member companies of the DSC Group of Companies. At its pinnacle this group included Sur-Gard for Central Station Receivers, DeltaVision for CCTV equipment, Kantech for Access Control, Emerald Gateway for Automation, Secutron for Fire Alarm Systems in North America, Bentel for Fire

Expert Declaration of James Parker

and Security Systems in Europe, Safelink for Long Range RF and MCS Communications for Apartment Entry Systems.

18. While at DSC/Tyco, I was the principal architect and driving force behind most of DSC's major commercial product successes. These include the industry benchmark setting "Power" and "Maxsys" families, and the PC1550, which is one of the most prolific alarm control panels in the world with an installed base in the millions.

19. In 2004, I co-founded and became President of EE-Systems Group Inc. (EE-SGI) Canada (R&D) from 2004–2014, where I was responsible for new product and technology development. While at EE-SGI, I developed several new technologies such as ePIR for motion detection and eLEDing for high efficiency LED illumination. I also developed the eFAR100 False Alarm Reduction module using embedded Z8 MCU technology with firmware written in assembler (machine code), and a full scalable suite of technology for solar-powered, motion-controlled, LED illumination ranging from patio to parking lot sizes.

20. In 2011, I founded Parker Security Consulting, Inc. to provide technical consulting and expert witness services in electronics research and development, new product development, electronic alarm systems, and other areas. I am currently a consultant at Parker Security Consulting Inc. (PARSEC), where I draw on over 4 decades of industry experience to provide expert witness services in litigation matters

involving but not limited to fire and security alarm systems. My Curriculum Vitae, Appendix B and *EX-1009*, outlines my qualifications, experience, and contributions to the field in greater detail.

III. RELEVANT LEGAL STANDARDS

21. I am not a lawyer and do not provide any legal opinions in this Declaration. Although I am not a lawyer, I have been informed by counsel and understand that certain legal standards are to be applied by technical experts in forming opinions regarding the meaning and validity of patent claims. I have been asked to provide my opinions regarding whether the claims of the '191 Patent would have been obvious to a POSA at the time of the alleged invention, in light of the prior art.

22. I have been informed by counsel and understand that a patent claim is not patentable under 35 U.S.C. § 103 if the differences between the patent claim and the prior art are such that the claimed subject matter as a whole would have been obvious at the time the claimed invention was made to a POSA. Obviousness, as I have been informed by counsel and understand, is based on the scope and content of the prior art, the differences between the prior art and the claim, the level of ordinary skill in the art, and, to the extent that they exist, certain objective indicia of non-obviousness.

Expert Declaration of James Parker

23. I have been informed by counsel and understand that objective indicia can be important evidence regarding whether a patent is obvious or nonobvious, if it has an appropriate nexus to the claimed invention, i.e., is a result of the merits of a claimed invention (rather than the result of design needs or market-pressure advertising or similar activities). Such indicia include: commercial success of products covered by the patent claims; a long-felt need for the invention; failed attempts by others to make the invention; copying of the invention by others in the field; unexpected results achieved by the invention as compared to the closest prior art; praise of the invention by the infringer or others in the field; the taking of licenses under the patent by others; expressions of surprise by experts and those skilled in the art at the making of the invention; and the patentee proceeded contrary to the accepted wisdom of the prior art.

24. I have been informed by counsel and understand that whether there are any relevant differences between the prior art and the claimed invention is to be analyzed from the view of a POSA at the time of the invention. As such, my opinions below as to a POSA are as of the time of the invention, even if not expressly stated as such; for example, even if stated in the present tense. In this case, as I discuss in section V.C below, I have been instructed to assume that “the time of the invention” for the claims of the ’191 Patent is November 14, 2006.

Expert Declaration of James Parker

25. In analyzing the relevance of the differences between the claimed invention and the prior art, I have been informed by counsel and understand that I must consider the impact, if any, of such differences on the obviousness or non-obviousness of the invention as a whole, not merely some portion of it. The person of ordinary skill in the art faced with a problem is able to apply his or her experience and ability to solve the problem and also look to any available prior art to help solve the problem.

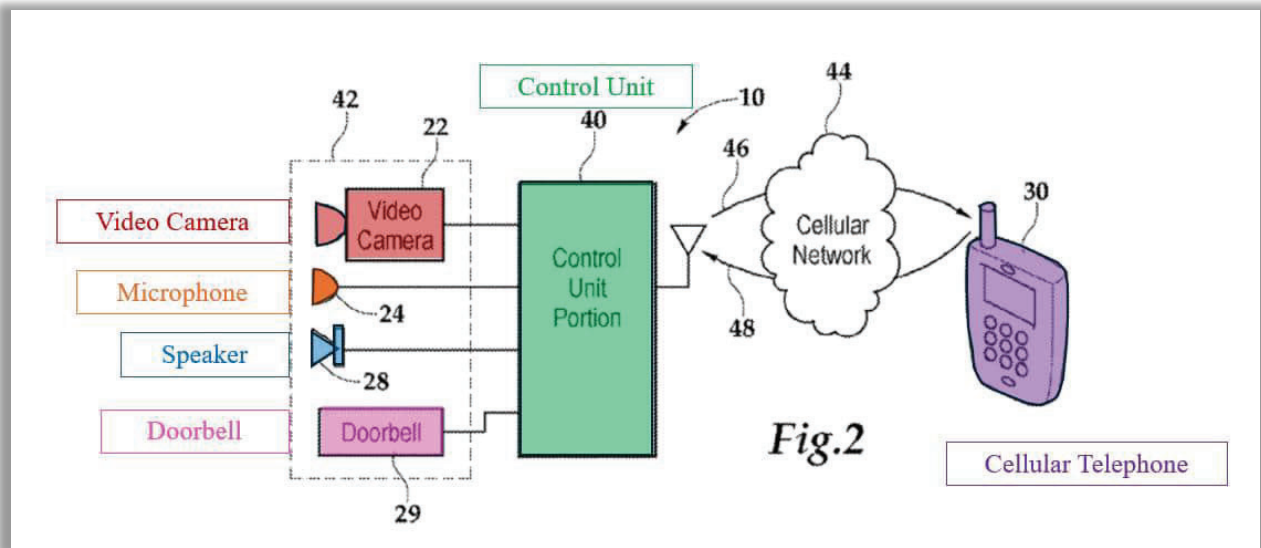
26. I have been informed by counsel and understand that a precise teaching in the prior art directed to the subject matter of the claimed invention is not needed. I have been informed by counsel and understand that one may take into account the inferences and creative steps that a POSA would have employed in reviewing the prior art at the time of the invention. For example, if the claimed invention combined elements known in the prior art and the combination yielded results that were predictable to a POSA at the time of the invention, then this evidence would make it more likely that the claim was obvious. On the other hand, if the combination of known elements yielded unexpected or unpredictable results, or if the prior art teaches away from combining the known elements, then this evidence would make it more likely that the claim that successfully combined those elements was not obvious.

Expert Declaration of James Parker

27. I have been informed by counsel and understand that there are recognized, exemplary, rationales for combining or modifying references to show obviousness of claimed subject matter. Some of the rationales include the following: combining prior art elements according to known methods to yield predictable results; simple substitution of one known element for another to yield predictable results; use of a known technique to improve a similar device (method or product) in the same way; applying a known technique to a known device (method or product) ready for improvement to yield predictable results; choosing from a finite number of identified, predictable solutions, with a reasonable expectation of success; known work in one field of endeavor may prompt variations of it for use in either the same field or a different one based on design incentives or other market forces if the variations are predictable to a POSA; and some teaching, suggestion, or motivation in the prior art that would have led a POSA to modify the prior art reference or to combine prior art teachings to arrive at the claimed invention.

IV. OVERVIEW

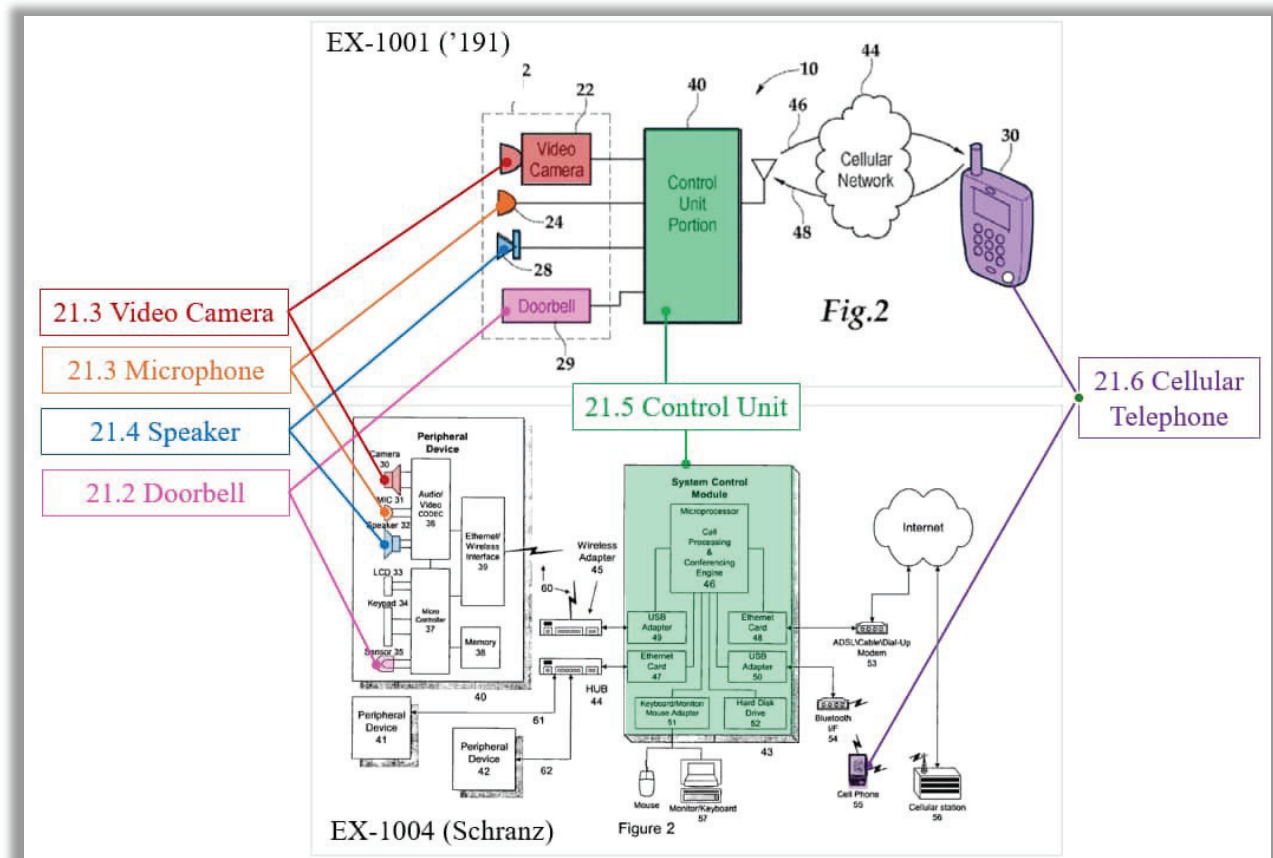
28. The '191 Patent is directed to a doorbell monitoring system to allow remote monitoring and surveillance. The architecture of the doorbell monitoring system is illustrated in Figure 2 of the '191 Patent and includes a control unit (green), in communication with video camera 22 (red), exterior microphone 24 (orange), exterior speaker 28 (blue) and doorbell 29 (pink).



EX-1001, Figure 2 (annotated to show limitations recited in independent Claim 21).

29. The control unit 40 interfaces with communication portion 42 and relays data and communications between the communication portion 42 and the cellular telephone 30 (purple) via a cellular network 44. In operation, when an individual approaches the doorway, an event is detected e.g., by ringing of the doorbell or the proximity detector. In turn, the video camera 22 and external microphone 24 capture visual and audio communications at the doorway 18 (not shown). The captured doorway visual and audio communications are transmitted to the cellular telephone 30 of the homeowner 16 (not shown) via the control unit 40 that is in communication with the video camera 22, external microphone 24 and exterior speaker 28 as well as the cellular network for communicating with the cellular telephone 30.

30. As I explain in section VII of my Declaration, Schranz discloses the same overall system architecture to provide doorbell monitoring services. The figure below illustrates a comparison of Figure 2 of the '191 Patent (top) with Figure 2 of Schranz (bottom) with common elements annotated with the limitations recited in independent Claim 21 of the '191 Patent:



EX-1001, Figure 2; EX-1004, Figure 2 (annotated).

31. Like the '191 Patent, Schranz discloses an architecture for a doorbell monitoring system that includes a control unit 43 (green), in communication with

video camera 30 (red), exterior microphone 31 (orange), exterior speaker 32 (blue) and doorbell 35 (pink).¹ The control unit 43 relays data and communications to the cellular telephone 55 (purple) via a cellular network. Like the '191 Patent, Schranz discloses that when an individual approaches the doorway, an event is detected, e.g., by ringing of the doorbell or activation of the motion sensor. In turn, the video camera 30 and external microphone 31 capture visual and audio communications at the doorway. The captured doorway visual and audio communications are transmitted to the cellular telephone 55 via a control unit 43 that is in communication with the video camera 30, external microphone 31, and exterior speaker 32 as well as a cellular network for communicating with the cellular telephone 55. The Challenged Claims of the '191 Patent recite well-known features associated with a doorbell monitoring system as disclosed by Schranz and are therefore unpatentable.

V. BACKGROUND

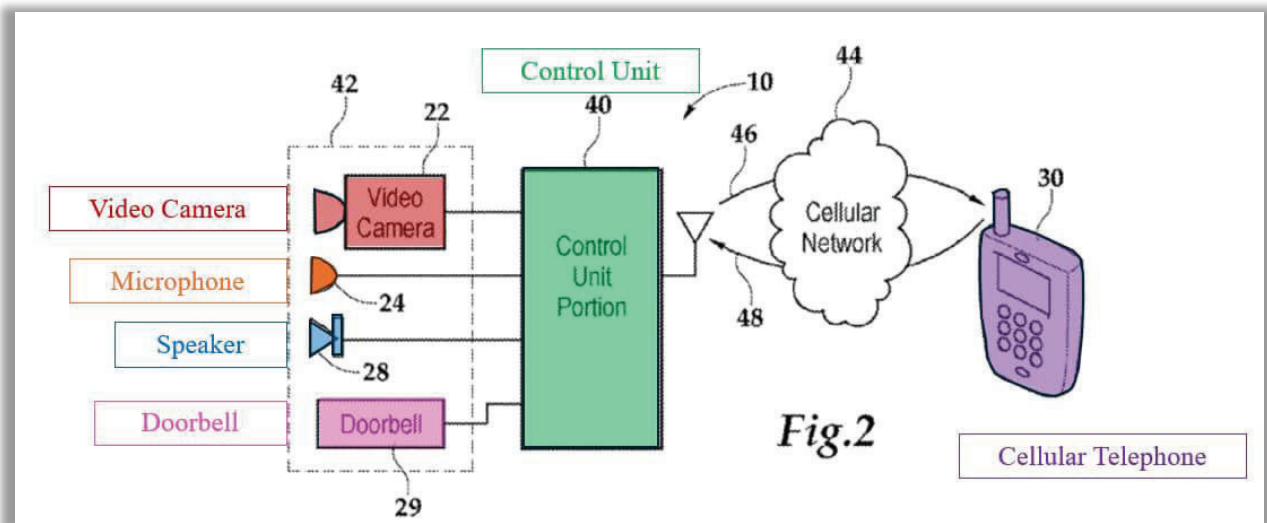
A. Summary of the '191 Patent

32. The '191 Patent is directed to a conventional security system that wirelessly streams audio and video from a property's entry point to a remote user's cellular telephone. *EX-1001*, Abstract. The '191 Patent explains that previous systems are merely "reactive" and typically only provide alarm monitors to

¹ Schranz discloses that sensor 35 may be a doorbell signal. *EX-1004*, ¶48.

predetermined third parties. *EX-1001*, 1:13-14, 1:23-26. The '191 Patent explains that there exists a need a for a “proactive” system that relays audio and visual information from the property to the remote user (*i.e.*, the property owner) during an alarm thereby deterring unwanted individuals. *EX-1001*, 1:31-44.

33. Figure 2 illustrates the doorbell monitoring security system and connection to the remote user’s cellular telephone.

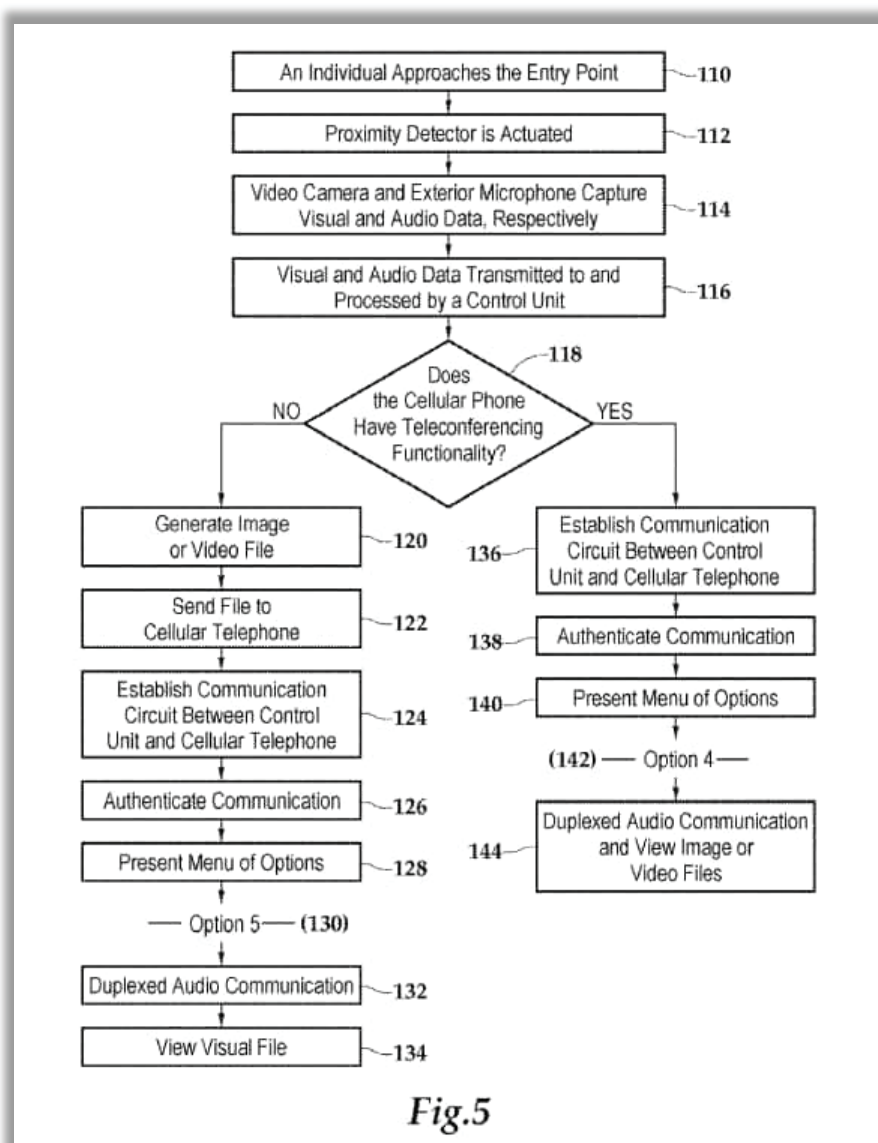


EX-1001, Figure 2.

34. As illustrated, the doorbell monitoring system utilizes a control unit 40 (green) to relay data from a communication portion 42 to the cellular network 44 and the remote user’s telephone 30 (purple). *EX-1001*, 3:10-13. The communication portion 42 includes a video camera 22 (red) and microphone 24 (orange) for capturing audio and visual information at the doorway. *EX-1001*, 2:36-37, 3:13-17. The communication portion 42 also includes doorbell 29 (pink) for detecting a triggering

event and speaker 28 (blue) to transmit audio from the remote user to the doorway. *EX-1001*, 2:38-47, 3:13-17.

35. The '191 Patent explains that the system operates as follows: (1) An individual approaches the doorway; (2) The proximity detector is activated; (3) Video camera 22 and microphone 24 capture the visual and audio data; (4) The control unit processes the received audio-visual data from the video camera and microphone; (5) The control unit notifies the remote user that a triggering event has occurred; (6) The control unit interfaces with the remote user's telephone allowing the remote user to receive additional information (*i.e.*, an image or a video file), and establish a real-time teleconferencing stream to the communication portion 42. *EX-1001*, Figure 5, 4:46-59, 6:13-67. The general operation of the system is illustrated by Figure 5 below. *EX-1001*, Figure 5.



EX-1001, Figure 5.

B. Summary of the Challenged Claims

36. The '191 Patent issued with twenty claims where Claims 1, 8, 14 and 19 being independent. I have been informed by counsel and I understand that the '191 patent was subject to a reexamination proceeding which resulted in a Reexamination Certificate that cancelled Claims 1, 8, 14 and 19, and found new Claims 21-47 patentable.

Expert Declaration of James Parker

37. Claims 21 and 34 are independent claims. Claim 21 is representative:

[21.0] A doorbell monitoring system comprising:

[21.1] a doorway having an environment;

[21.2] a doorbell located in an entry point, activation of the doorbell being a triggering event;

[21.3] a video camera and an external microphone disposed in the entry point, the video camera and the external microphone, responsive to the triggering event, for capturing visual and audio communications at the entry point and transmitting the captured visual and audio communications;

[21.4] an external speaker disposed in the entry point, the external speaker for rendering received audio communications;

[21.5] a control unit in communication with the video camera, the doorbell, and the external microphone, the control unit for communicating at least one portion of the visual and audio communications received from the video camera and the external microphone, and for communicating the received audio communications to the external speaker; and

[21.6] a cellular telephone disposed remotely to the doorway and the control unit, the cellular telephone for capturing cellular audio communications at the cellular telephone, transmitting the cellular audio communications to the

Expert Declaration of James Parker

control unit, and rendering the at least one portion of entry point visual and audio communications received from the control unit;

[21.7] wherein the doorbell, the video camera, the external microphone, the external speaker, and a proximity detector are part of a single communications unit;

[21.8] wherein the entry point visual and audio communications are wirelessly streamed to the control unit;

[21.9] wherein the control unit is configured to store the entry point visual and audio communications captured by the single communications unit in a data storage unit of the control unit wherein a control panel is configured to allow an individual to manage a security system;

[21.10] wherein an alarm system interface of the control panel is configured to interface with the security system;

[21.11] wherein the video camera is configured to collect the entry point visual communications captured by the single communications unit before the triggering event;

[21.12] wherein the video camera is configured to collect additional visual communications after the triggering event;

[21.13] wherein the doorbell monitoring system is configured to establish communication with the control unit upon activation of the doorbell;

[21.14] wherein at least a portion of an initial communication after the doorbell is activated is a notification sent to the cellular telephone; and

[21.15] wherein the doorbell monitoring system is configured to authenticate a user of the doorbell monitoring system.

C. Priority Date of the Challenged Claims

38. For the purposes of this Declaration, I have been instructed by counsel to assume that the effective filing date of the '191 Patent is November 14, 2006, the filing date of the application from which it issued. In this Declaration, when I use the shorthand "Priority Date" I am referring to November 14, 2006.

D. Claim Construction

39. I have been informed by counsel and I understand that in order to properly evaluate the Challenged Claims of the '191 Patent, the terms of the claims must first be interpreted. I have been informed by counsel and I understand that, for the purposes of this Declaration, the claims are to be construed under the so-called Phillips standard, under which each claim term in the Challenged Claims be given its plain and ordinary meaning in this proceeding as would be understood by a person of ordinary skill in the art ("POSA", defined below in Section V.E) as of the Priority Date (*see* Section V.C above) in light of the specification and prosecution history, unless the inventor has set forth a special meaning for the term. That is the meaning I have applied in my analysis.

40. I have been informed by counsel that no court or administrative board has construed any of the claims of the '191 Patent. If a board or court construes any term of the '191 Patent, I reserve the right to supplement my opinions in view of such construction. I have also been informed by counsel that the Board does not construe claims terms unless the terms are in controversy, and then only to the extent necessary to resolve the controversy.

E. Level of Ordinary Skill in the Art

41. I have been informed by counsel and I understand that a person of ordinary skill in the art ("POSA") is a hypothetical person who is presumed to be aware of all pertinent prior art, thinks along conventional wisdom in the art, and is a person of ordinary creativity. I have also been informed by counsel and understand that there are multiple factors relevant to determining the level of ordinary skill in the pertinent art, including (1) the levels of education and experience of persons working in the field at the time of the invention; (2) the sophistication of the technology; (3) the types of problems encountered in the field; and (4) the prior art solutions to those problems.

42. In my opinion, with respect to the '191 Patent, a POSA, as of its November 2006 Priority Date would have been someone knowledgeable and familiar with communication protocols used by components in a security system for transferring information between components. A POSA would have gained

knowledge of these concepts through a mixture of training and work experience, such as by having at least a bachelor's degree in electrical or electronic engineering, computer science, or a related field, and at least two to three years of training or additional work experience in the area of security system components, or a related field. Additional hands-on and design experience could compensate for less formal education, and vice versa.

43. The knowledge and skill of a POSA is further reflected in the prior art references themselves, as well as the State of the Art, which I discuss in section V.F below.

44. For purposes of this Declaration, in general, and unless otherwise noted, my statements and opinions, such as those regarding my experience and the understanding of a POSA generally (and specifically related to the references I consulted herein), reflect the knowledge that existed in the field as of the Priority Date of the '191 Patent. Unless otherwise stated, when I provide my understanding and analysis below, it is consistent with the level of a POSA as of the Priority Date of the '191 Patent.

F. State of the Art

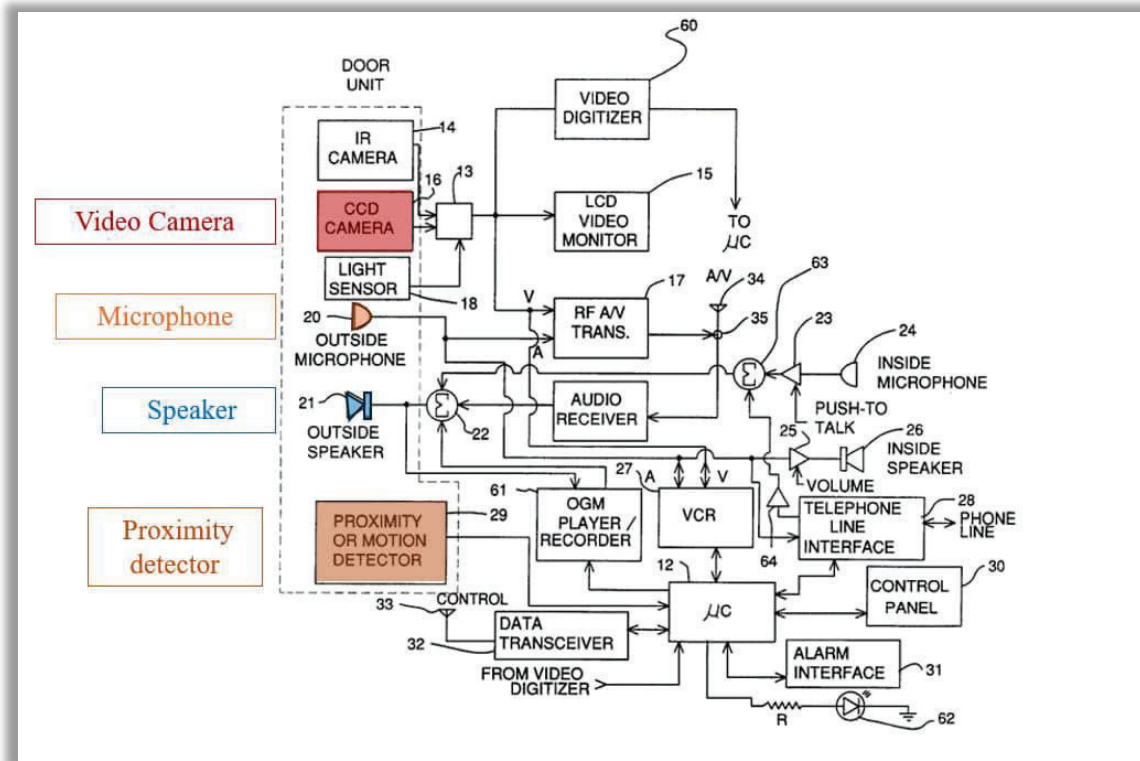
45. The following section describes the state of the art for monitoring systems as of the November 2006 Priority Date of the '191 Patent. This section, and the documentary evidence that I cite in this section, provide the factual support for

Expert Declaration of James Parker

the general description of the state of the art at the time of the invention, provide additional motivation to modify or combine the reference that I discuss in Section VII of my Declaration, and further demonstrates why doing so would involve a reasonable expectation of success. Accordingly, the Board should consider each of these references.

46. In my opinion, monitoring and security systems with cameras, microphones, speakers, proximity detectors, and control units was well-known in the art by November 2006.

47. Prior art security systems were generally used to monitor entrances to a building in order to prevent unauthorized access to the building. These systems used various sensors to detect unauthorized persons. One such system is shown below in Figure 1:



EX-1006, Figure 1.

48. The security system includes a door unit with several different types of sensors for generating signals, including a video camera 16 (red) for generating a video signal, an outside microphone 20 (orange) for generating an audio signal, an outside speaker 21 (blue) for playing an audio signal, and a proximity or motion detector 29 (brown) for detecting motion in the vicinity of the door. *EX-1006*, 4:10-54. A remote unit allows a person to remotely monitor the activity at the door, play video and audio captured at the door unit, and control the security system. *EX-1006*, 1:37-50. The remote unit also allows the remote user to communicate orally with a person at the door. *EX-1006*, 6:6-8.

Expert Declaration of James Parker

49. Another prior art security system, *EX-1007*, includes one or more cameras capable of capturing video and audio data, one or more audio devices capable of capturing and broadcasting audio data, and one or more intrusion devices capable of detecting any intrusion onto the premises, such as glass breakage sensors, motion detectors, contact switches, proximity or alignment sensors. One skilled in the art will appreciate that such system components are placed and installed about the premises to provide optimum surveillance and security capabilities while being inconspicuous or resistant to disablement. *EX-1007*, 3:56-4:8.

50. The security components communicate with an on-premises master terminal box, and the master terminal box communicates wirelessly with a remote command unit. The master terminal box is capable of two-way wireless audio and video communication with the command unit. The remote command unit includes an LCD screen, speaker, video camera, and microphone to allow two-way wireless audio and video communication between the user of the remote command unit and the security components connected to the master terminal box. *EX-1007*, 4:9-5:2.

51. Another prior art security system provided real-time monitoring with remote access through use of broadband features, including audio and video capabilities, web access and wireless capabilities. *EX-1008*, ¶30. The security system includes any type of sensor to detect alarm conditions including magnetic contact switches, audio sensors, infrared sensors, motion detectors, fire alarms, and

carbon monoxide sensors. *EX-1008*, ¶36. In addition, the security system includes one or more video cameras that operable to capture video of the monitored premises. *EX-1008*, ¶37.

52. The video cameras can include “smart” cameras to perform video capture, compression and storage and to communicate with the security system using a wireless network. *EX-1008*, ¶84. The smart camera may perform many functions including but not limited to analyzing data from the video camera to determine whether an alarm condition exists, accessing data stored in memory; generating alarm video to transmit to the security system in response to detection of an alarm condition; and communicating with the security system and a remote user. The video camera may capture and record video continuously in memory, and then based on predefined criteria, older video may be discarded. The remote user may adjust the predetermined criteria including adjusting the recording times, duration, and total length of recordings. *EX-1008*, ¶81.

53. In one prior art example, the video sent to the security system begins at least just prior to the occurrence of the alarm condition and may end after the conclusion of the alarm condition, which helps identify false alarms. *EX-1008*, ¶38. The remote user has the ability to control the functionality of the security system. Once authenticated, the remote user can control the functionality of the system including arming or disarming the security system; adjusting sensitivities of the

sensors; adjusting alarm condition detection sensitivity; remote surveillance; adjusting camera settings; and reviewing alarms and recordings. These functions may also include remote surveillance, referred to as “lifestyle video.” *EX-1008*, ¶43. The smart camera is capable of streaming live audio and video from the residence during alarm conditions, as well as for lifestyle viewing over the world wide web. *EX-1008*, ¶82.

VI. CHALLENGES

A. Identification of Challenge

54. Based on my understanding of the law of obviousness discussed in Section II above, Claims 21-47 of the '191 Patent are unpatentable as set forth in the grounds below.

Grounds	Claims	Basis	References
Ground 1	21-47	103	Schranz

B. Prior Art

1. Schranz (*EX-1004*)

55. I have been informed by counsel that U.S. Patent Publication 2004/0086093 (*EX-1004*) titled “VOIP SECURITY MONITORING & ALARM SYSTEM” which issued May 6, 2004, from U.S. Patent Application No. 10/694,678 filed on October 29, 2003, and claims priority to Provisional Application No.

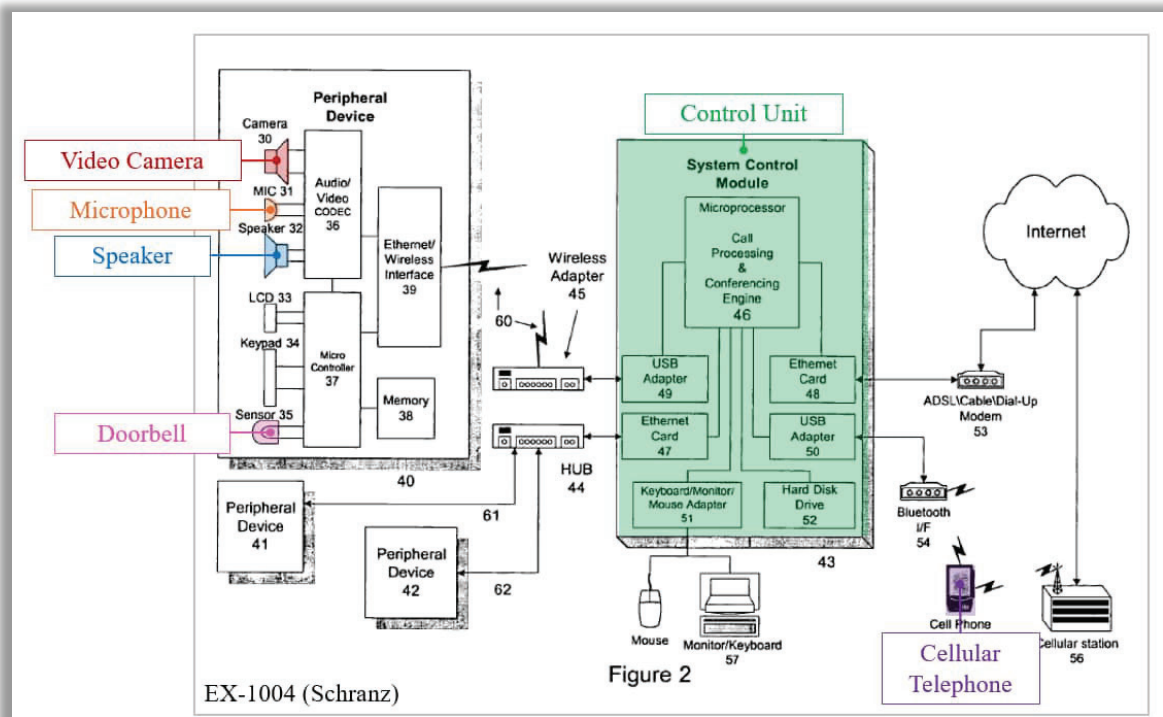
60/421,849 filed on October 29, 2002, qualifies as prior art under at least §102(a), (b) or (e).

VII. IDENTIFICATION OF HOW THE CHALLENGED CLAIMS ARE UNPATENTABLE

A. Ground 1: Claims 21-47 Are Obvious Over Schranz

1. The Schranz Reference

56. Schranz is directed to a residential, commercial or industrial security monitoring and alarm system. It includes a plurality of peripheral devices in communication with a system control module (SCM). Figure 2 illustrates that peripheral devices 40, 41, and 42 are situated throughout the user premises at strategic exterior or interior locations, such as doors, windows, hallways or rooms. These devices detect an event, called the detected agent, and signal the system control module (SCM) 43 via a wireline or wireless physical interface 60, 61 and 62, respectively. *EX-1004*, ¶47.



57. An Internet interface connects the SCM 43 to the Internet. Once notified of an alarm, the SCM 43 begins the process of establishing a VoIP call, defined as “Voice/Video over Internet Protocol” in Schranz (*EX-1004*, Abstract), with a remote user using VoIP call signaling protocols such as SIP or H.323. The remote user can be in the IP network, the PSTN or a cellular network. *EX-1004*, ¶47.

58. The peripheral devices include a camera 30 (red), microphone 31 (orange), speaker 32 (blue), and sensor 35 that could include a doorbell (pink). The peripheral devices will be located in various strategic locations including an intercom located in hallways and rooms, a doorbell-intercom located at the main entrance to the premises, and an environmentally hardened security surveillance unit located exterior to the building. *EX-1004*, ¶48.

59. Upon detection of an event the system establishes a Voice/Video over Internet Protocol (VoIP) call to a remote user or monitoring service. Schranz discloses that using VoIP technology leverages several inherent advantages related to IP packet networks. A VoIP call is one that uses a VoIP call signaling protocol to set up a call and a VoIP transport protocol to deliver the payload (audio and video information). Examples of VoIP call signaling protocols include, but are not limited to, the Session Initiation Protocol (SIP) from the Internet Engineering Task Force (IETF) and H.323 from the International Telecommunications Union (ITU). An example of a VoIP transport protocol includes, but is not limited to, the Real-Time Transport Protocol (RTP) from the IETF. *EX-1004*, ¶0001.

60. Schranz explains that the peripheral devices, including the camera 30 (red) and microphone 31 (orange), are typically placed in “a doorbell-intercom located at the main entrance to the premises.” *EX-1004*, ¶48. In armed mode, the peripheral devices, including camera 30 and microphone 31, monitor the environment and notify the SCM when someone is at the door or when motion takes place. *EX-1004*, ¶¶58-59, 61. The SCM then provides a notification to the remote user. *EX-1004*, ¶¶64; 61. The SCM routes the audio and video data from the peripheral device to the remote agent. *EX-1004*, ¶¶24, 63-64.

61. Schranz also discloses that a web server runs on the SCM and contains a user web application. The user can access this website remotely and securely

through monitor/keyboard 57 using any Internet browser that supports the https protocol. The website is a graphical monitor and control program. The user can visually see the current configuration and the status of all peripheral devices. Moreover, the user can change the configuration and initiate a VoIP call to any one of the peripheral devices and can control all aspects of the system. *EX-1004*, ¶50.

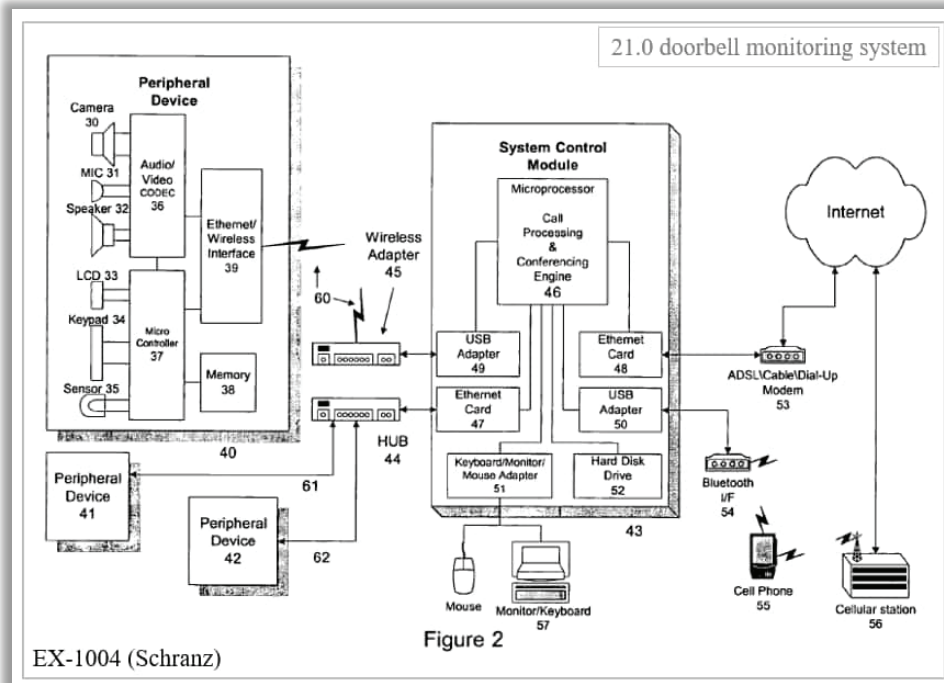
2. Detailed Application of Schranz

Claim 21

[21.0] A doorbell monitoring system comprising:

62. To the extent the preamble is limiting, Schranz discloses a VoIP security monitoring and alarm system in the form of a doorbell-intercom. *EX-1004*, Title, ¶48. The VoIP security monitoring and alarm system utilizes peripheral devices, including cameras, microphones, motion detectors, and doorbell signals, to detect an event and notify a remote user. *EX-1004*, Abstract, ¶48, *See also* ¶53 (“Peripheral devices with varying functionality can be chosen and installed simultaneously, such as intercoms, doorbell-intercoms or surveillance units.”). The VoIP security monitoring and alarm system can be located in hallways or “at the main

entrance to the premises.” *EX-1004*, ¶48. Therefore, Schranz discloses a *doorbell monitoring system* as shown below.



EX-1004, Figure 2 (Annotated).

[21.1] a doorway having an environment;

63. Schranz discloses this limitation. Schranz’s VoIP security monitoring and alarm system can be “situated throughout the user premises at strategic exterior or interior locations, such as doors, windows, hallways or rooms.” *EX-1004*, ¶47. The VoIP security system utilizes a number of peripheral devices such as “intercoms, doorbell-intercoms or surveillance units” that are mounted at strategic exterior locations to monitor “entrances to the building such as doors and windows.” *EX-1004*, ¶53. Further, Schranz discloses a system control module connected to the peripheral devices that can be “located anywhere in the home.” *EX-1004*, ¶53. A

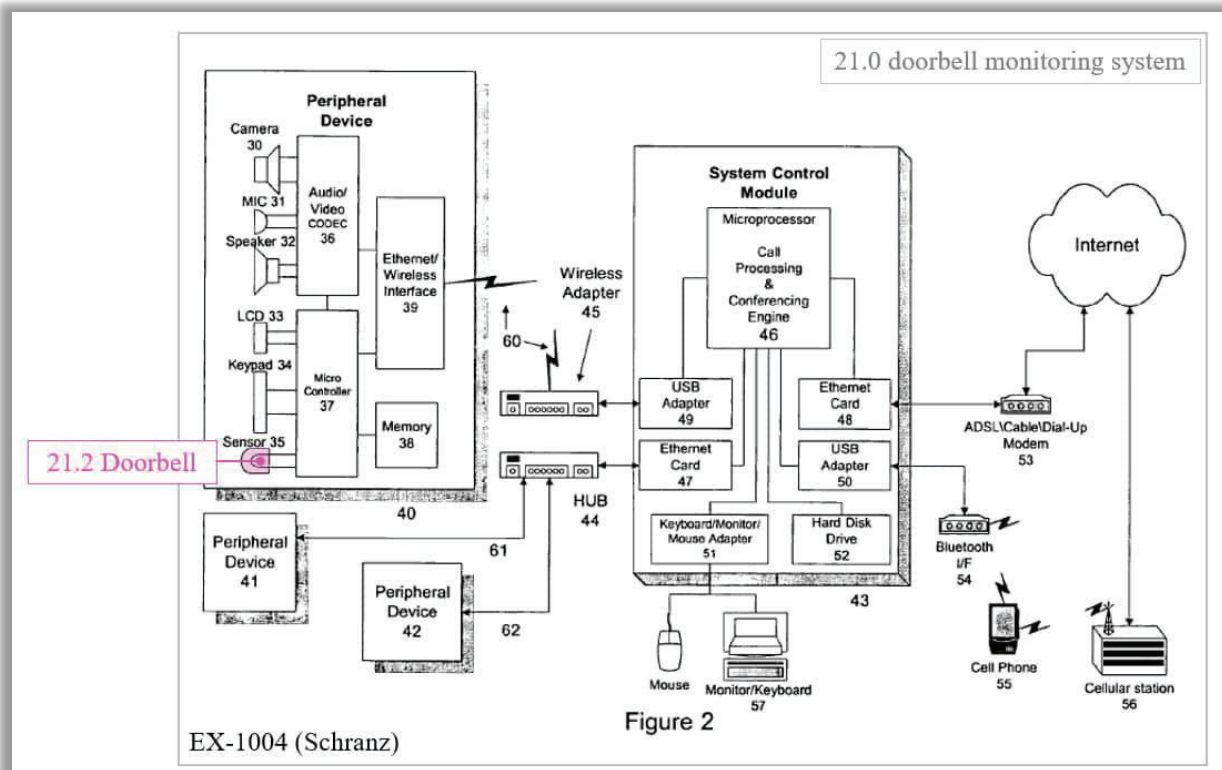
POSA understood that Schranz discloses that a doorway located at an entrance to a building is the recited *doorway having an environment*.

***[21.2] a doorbell located in an entry point,
activation of the doorbell being a triggering
event;***

64. Schranz discloses this limitation. Schranz's VoIP security monitoring and alarm system utilizes a number of peripheral devices such as "intercoms, doorbell-intercoms or surveillance units." *EX-1004*, ¶53. In particular and as shown below, one such device, peripheral device 40, includes sensor 35 (pink) which can be "a motion detector, infrared radiation sensor or ***doorbell signal***." *EX-1004*, ¶48 (emphasis added). Schranz further discloses that the doorbell is mounted at strategic exterior locations to monitor "entrances to the building such as doors and windows" [*a doorbell located in an entry point*]. *EX-1004*, ¶53. Schranz explains that the doorbell signal functions in two modes: normal mode and armed mode. *EX-1004*, ¶58. In normal mode, the doorbell, sensor 35, can simply be used to detect an event and notify that someone is at the door.

In the normal mode, the peripheral devices function as intercoms and doorbells. They can be used to page people in the house, place outgoing or answer incoming VoIP calls and notify that someone is at the door. They still notify the SCM when an event like motion, infrared radiation or vibration detection takes place.
EX-1004, ¶59.

65. In alarm mode, the doorbell, sensor 35, “functions as normal, but in addition to notifying people locally with a chime when pressed, it also places a call to a pre-configured VoIP address.” *EX-1004*, ¶60. In other words, the only difference between the normal and armed modes of Schranz’s system is that “[i]n Alarm Mode the SCM will generate an outbound call when a peripheral device notifies it of an event.” *EX-1004*, ¶61. Schranz discloses that the peripheral devices detect an event, called the detected agent, and signals the system control module (SCM) [*activation of the doorbell being a triggering event*]. *EX-1004*, ¶47. Therefore, a POSA understood that Schranz discloses that activation of a doorbell is an event that causes the triggering of actions [*a doorbell located in an entry point, activation of the doorbell being a triggering event*].



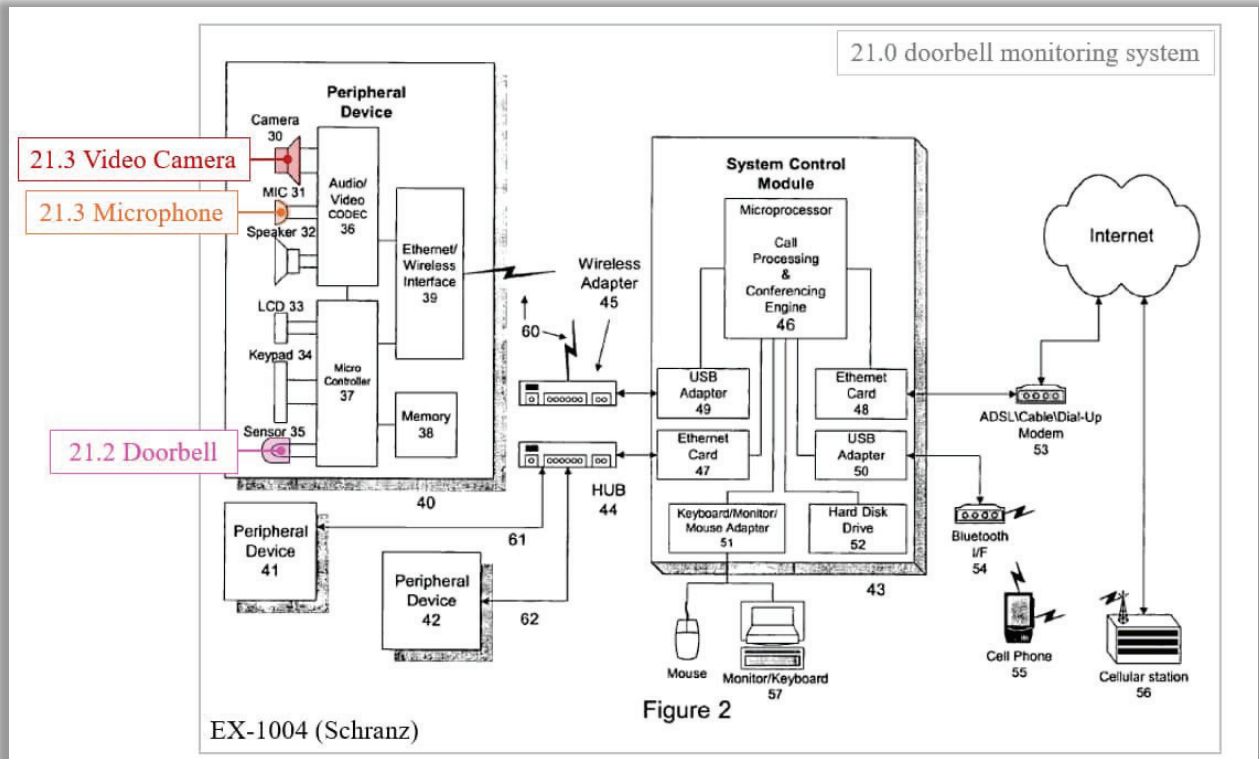
EX-1004, Figure 2 (Annotated).

[21.3] a video camera and an external microphone disposed in the entry point, the video camera and the external microphone, responsive to the triggering event, for capturing visual and audio communications at the entry point and transmitting the captured visual and audio communications;

66. Schranz discloses this limitation. Schranz discloses a VoIP security monitoring and alarm system with peripheral devices (*i.e.*, camera 30, microphone 31, speaker 32) situated at doors, windows, hallways or rooms [*a video camera and an external microphone disposed in the entry point*]. EX-1004, ¶47. The peripheral devices, including the doorbell, “detect an event” and notify the system control module. EX-1004, Abstract. The system control module then establishes a VoIP call with a remote user so that the remote user “will hear ambient audio and see video images from the peripheral device in the location of the alarm” [*for capturing visual and audio communications at the entry point and transmitting the captured visual and audio communications*]. EX-1004, Abstract, Claim 1.

67. Specifically with respect to Figure 2 below, Schranz discloses a VoIP security monitoring and alarm system utilizing peripheral device 40 which includes “*camera 30, microphone 31*, speaker 32, LCD 33, keypad 34, sensor 35, audio/video CODEC 36.” EX-1004, ¶48 (emphasis added). Schranz states that camera 30 (red) [*video camera*] may be a CCTV board camera that supports both video and audio

through CODEC 36. Schranz explains that CODEC 36 “digitizes the analog video signal into a standard digital format.” *EX-1004*, ¶48.



EX-1004, Figure 2 (Annotated).

68. Schranz further explains that the peripheral devices, including the camera 30 (red) [video camera] and microphone 31 (orange) [external microphone], are typically placed in “a doorbell-intercom located at the main entrance to the premises” [disposed in the entry point]. *EX-1004*, ¶48. Further Schranz states that, in armed mode, the peripheral devices, including the doorbell monitor the environment, and when someone rings the doorbell, in addition to notifying people locally with a chime when pressed, it also places a call to a pre-configured VoIP address via the SCM [responsive to the triggering event]. *EX-1004*, ¶¶60-61. The

SCM then provides a notification to the remote user. *EX-1004*, ¶¶64, 61. The SCM routes the audio and video data captured from the peripheral device to the remote agent. *EX-1004*, ¶¶24, 63-64. In other words, the microphone and camera of the peripheral device at the entry point send audio and video data to the SCM which routes the audio and video data to a remote user when a person rings the doorbell [capturing visual and audio communications at the entry point and transmitting the captured visual and audio communications].

69. Schranz's disclosure is consistent with the '191 Patent's disclosure that "a triggering event such as the ringing of a doorbell, initiates the contact of the control unit to the homeowner 16; however, the plurality of video cameras 22 collect video for the homeowner's review irrespective of the occurrence of the triggering event." *EX-1001*, 3:4-8, 4:46-51.

70. To the extent that Patent Owner asserts that Schranz does not expressly disclose capturing of the video and audio data responsive to the ringing of the doorbell, a POSA would be motivated to modify the teachings of Schranz to capture video and audio data responsive to the ringing of the doorbell and would have a reasonable expectation of success in doing so. As discussed in the State of the Art section, it was well-known and common at the time of the alleged invention to allow a user to adjust the system parameters, including sensor sensitivities, camera settings, and remote surveillance settings. *EX-1008*, ¶43. The purpose of this well-known

configurability was to allow for the user to adjust the amount of time to capture the video and audio data from before, during, and after triggering events (pressing the doorbell button).

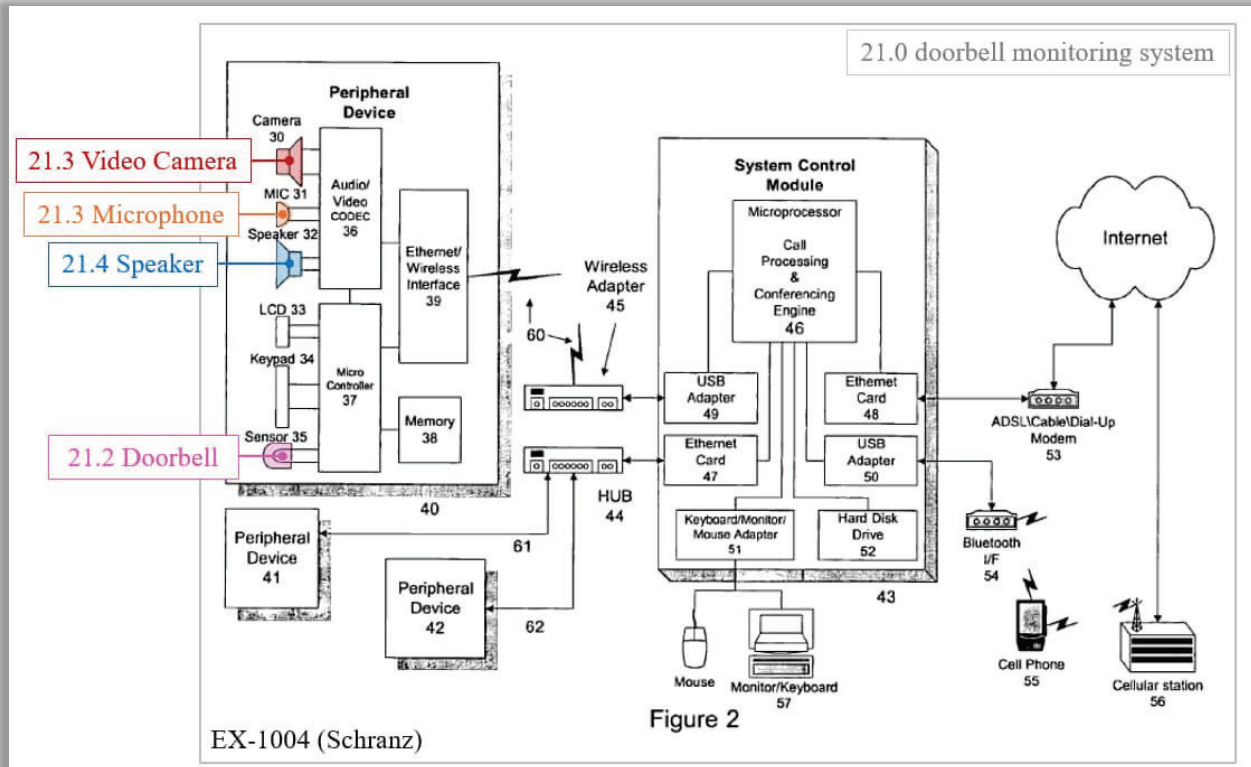
71. Schranz itself contemplates this type of user-driven configurability, and specifically discloses that the user sets up system control parameters. *EX-1004*, ¶¶56, 57. Accordingly, a POSA would have found it obvious to capture video and audio data responsive to the ringing of the doorbell, with the amount of time defined by the user's system control parameters. Such a modification would have amounted to nothing more than the application of a known technique, configurable capture timing, to improve a similar device in the same, predictable way.

[21.4] an external speaker disposed in the entry point, the external speaker for rendering received audio communications;

72. Schranz discloses this limitation. Specifically with respect to Figure 2 as shown below, Schranz's VoIP security monitoring and alarm system utilizes a peripheral device 40 which includes "a camera 30, microphone 31, **speaker 32**, LCD 33, keypad 34, sensor 35, audio/video CODEC 36." *EX-1004*, ¶48 (emphasis added). The speaker 32 (blue) in conjunction with CODEC 36 allows the remote user to play an announcement, prerecorded message, or to enable audio to be sent from the remote location to speaker 32 [*for rendering received audio communications*]. *EX-1004*, ¶33, 65. In particular, CODEC 36 decodes PCM samples from the system control

module 43 into an analog audio signal to be played by the speaker. *EX-1004*, ¶48.

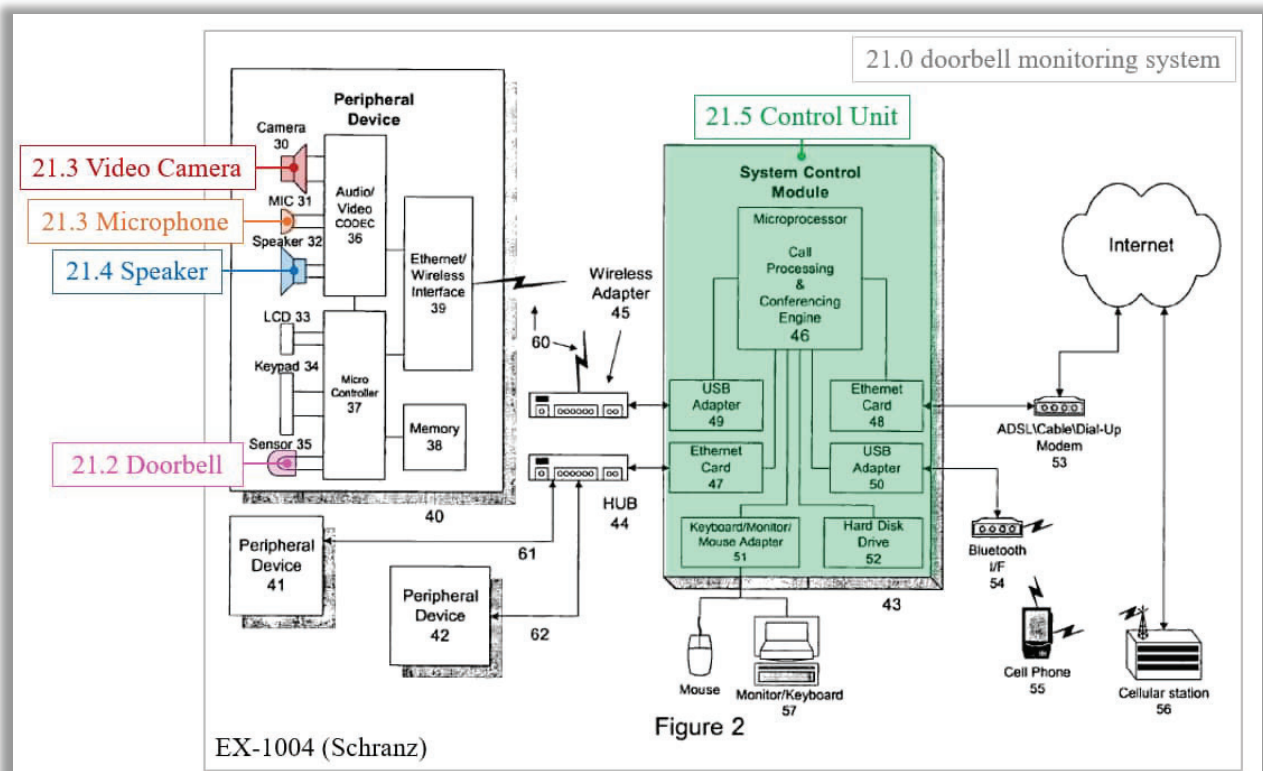
As explained above, Schranz’s peripheral devices, including speaker 32 (blue below), are typically placed in a “a doorbell-intercom located at the main entrance to the premises” [*disposed in the entry point*]. *EX-1004*, ¶48.



EX-1004, Figure 2 (Annotated).

[21.5] a control unit in communication with the video camera, the doorbell, and the external microphone, the control unit for communicating at least one portion of the visual and audio communications received from the video camera and the external microphone, and for communicating the received audio communications to the external speaker; and

73. Schranz discloses this limitation. As shown below in Figure 2, Schranz discloses a system control module 43 (green) [*control unit*] in communication with a set of peripheral devices, including camera 30 (red) [*video camera*], microphone 31 (orange) [*external microphone*], and speaker 32 (blue) [*external speaker*], via either ethernet or wireless connections. *EX-1004*, ¶48. Schranz explains that the system control module [*control unit*] is “any hardware platform that runs the Windows 98, 2000, ME, XP or Linux operating system.” *EX-1004*, ¶49.



EX-1004, Figure 2 (Annotated).

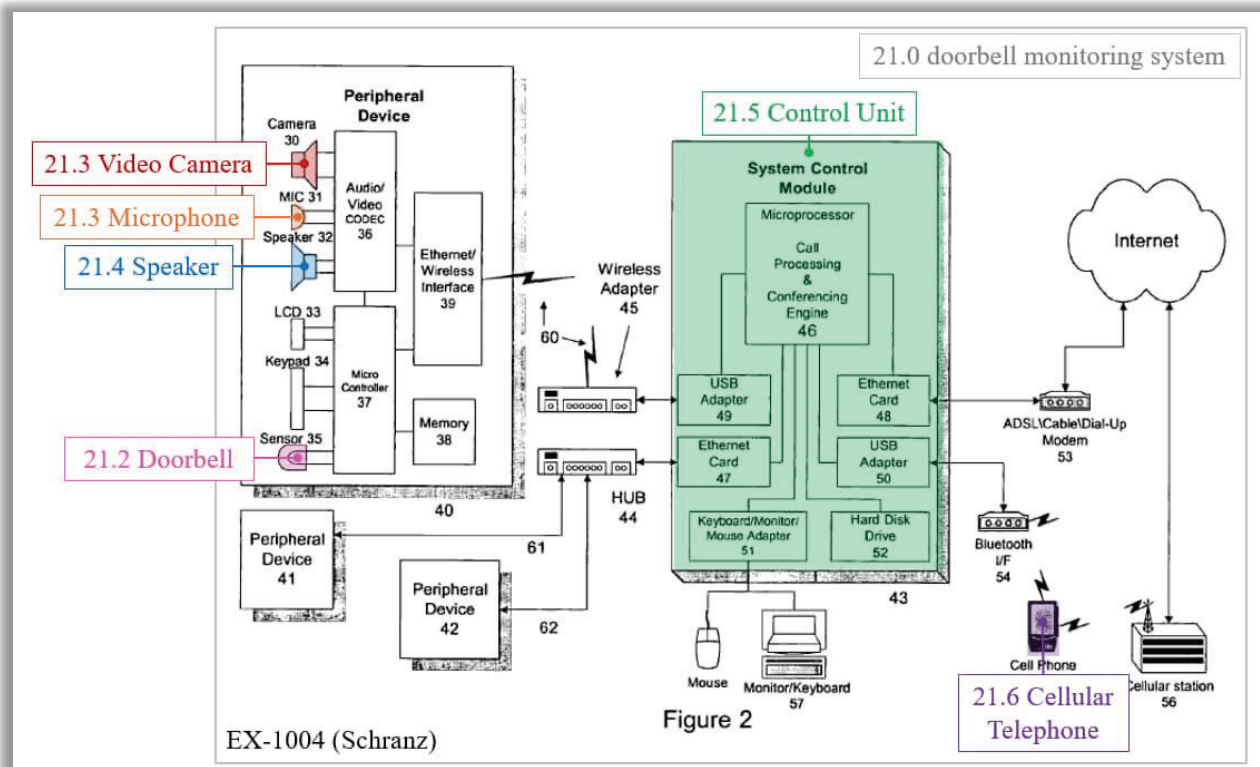
74. Further, Schranz explains that CODEC 36 “digitizes the analog video signal” from camera 30 and “codes the analog audio signal” from microphone 31 to provide the data to the system control module via wireless or wired channel. *EX-*

1004, ¶48. Upon event detection (*i.e.*, the ringing of the doorbell), the system control module then establishes a VoIP communication call to transmit voice and video information from the peripheral devices (*i.e.*, camera 30 and microphone 31) to the system control module and from the system control module to the remote user. *EX-1004*, Claim 1. Accordingly, Schranz system control module 43 is *for communicating at least one portion of the visual and audio communications received from the video camera and the external microphone.*

75. Finally, Schranz discloses that the remote user can enable audio to be sent from their location and device to the peripheral devices (*i.e.*, speaker 32). *EX-1004*, ¶65 (“The remote user can enable audio to be sent from his location to the peripheral device currently sourcing the ambient audio.”). In this case, the system control module establishes an audio call with the remote user and provides the data to CODEC 36 which “decodes PCM samples into an analog audio signal to the speaker.” *EX-1004*, ¶¶48, 63. Accordingly, Schranz system control module 43 is *for communicating the received audio communications to the external speaker.*

[21.6] a cellular telephone disposed remotely to the doorway and the control unit, the cellular telephone for capturing cellular audio communications at the cellular telephone, transmitting the cellular audio communications to the control unit, and rendering the at least one portion of entry point visual and audio communications received from the control unit;

76. Schranz discloses this limitation. Schranz's VoIP security monitoring and alarm system provides notification of an alarm event to a remote user via the remote user's "cell phone 150, a laptop computer 155, a VoIP phone 160..." *EX-1004*, ¶62. In reference to Figure 2, Schranz explains that the SCM is connected to the internet via Ethernet Card 48 and ADSL or cable modem 54. Further, Schranz explains that "the cellphone 55 communicates with a cellular station 56" to connect to the internet. *EX-1004*, ¶49. A POSA understood that the remote user's cell phone is disposed remotely to the doorway and control unit as shown below in Figure 2.



EX-1004, Figure 2 (Annotated).

77. Upon an alarm event, Schranz's system control module establishes a VoIP communication call to transmit voice and video information from the peripheral

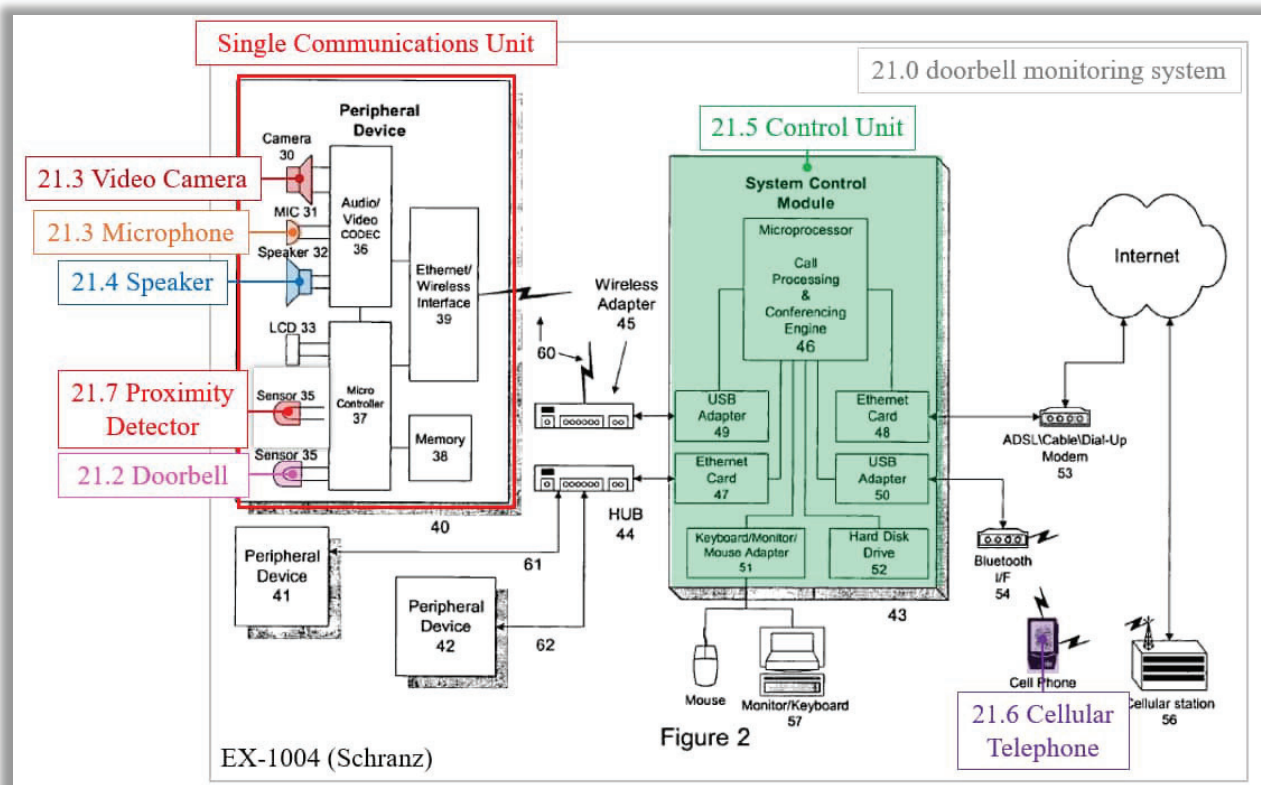
devices (i.e., camera 30 and microphone 31) to the system control module and from the system control module to the remote user. EX-1004, ¶24, Claim 1. The system control module “knows beforehand which device to contact (work phone, cell, laptop) and what method of message to send (text, voice, video, email).” EX-1004, ¶63 (emphasis added). In other words, the system control module may contact the remote user’s cell phone with an audio or video message from the alarm event thereby rendering the at least one portion of entry point visual and audio communications received from the control unit.

78. Once the audio call is established, the remote user can “enable audio to be sent from his location to the peripheral device currently sourcing the ambient audio.” EX-1004, ¶¶64-65. A POSA understood that remote user’s cellphone disclosed by Schranz is therefore for capturing cellular audio communications at the cellular telephone, transmitting the cellular audio communications to the control unit.

[21.7] wherein the doorbell, the video camera, the external microphone, the external speaker, and a proximity detector are part of a single communications unit;

79. Schranz discloses this limitation. As shown below in Figure 2, Schranz discloses a peripheral device 40 [*single communications unit*] including sensor 35 (pink) [*doorbell; proximity detector*], camera 30 (red) [*video camera*], microphone 31 (orange) [*external microphone*], and speaker 32 (blue) [*external speaker*]. EX-

1004, ¶48. Schranz discloses that sensor 35 “may be different types, such as a *motion detector*, infrared radiation sensor or *doorbell signal*.” EX-1004, ¶48 (emphasis added). A POSA would recognize that Schranz’s system could easily include both a motion detector (*proximity detector*) and a doorbell signal within peripheral device 40. Schranz therefore discloses a *doorbell*, *video camera*, *external microphone*, *external speaker*, and a *proximity detector*.



EX-1004, Figure 2 (Modified).

80. To the extent Patent Owner asserts that Schranz does not expressly describe a peripheral device with a doorbell and a proximity sensor, a POSA would be motivated by the teachings of Schranz to include both a doorbell and motion detector in a peripheral device at the entrance to a building in order to achieve the

express benefits of Schranz, which are to both monitor visitors and track intruders. EX-1004, ¶¶29-30, 58-60. First, as explained above, Schranz expressly teaches that its sensor 35 "may be different types," including both a "motion detector" and a "doorbell signal," thereby contemplating that peripheral devices may be configured with varying sensor functionality to suit particular security needs. EX-1004, ¶48. Second, Schranz discloses that the system is designed to be installed at the entrance of a building for the purpose of tracking intruders and monitoring visitors. EX-1004, ¶¶29-30, 58-60. A POSA reading Schranz would thus understand that combining both a doorbell and a motion detector within a single peripheral device 40 would directly advance these objectives: the doorbell enabling communication with expected visitors and the motion detector enabling detection of unexpected intruders. A POSA would recognize that this modification would provide complementary functionality that serves the purposes of Schranz's system and could be achieved with a reasonable expectation of success.

[21.8] wherein the entry point visual and audio communications are wirelessly streamed to the control unit;

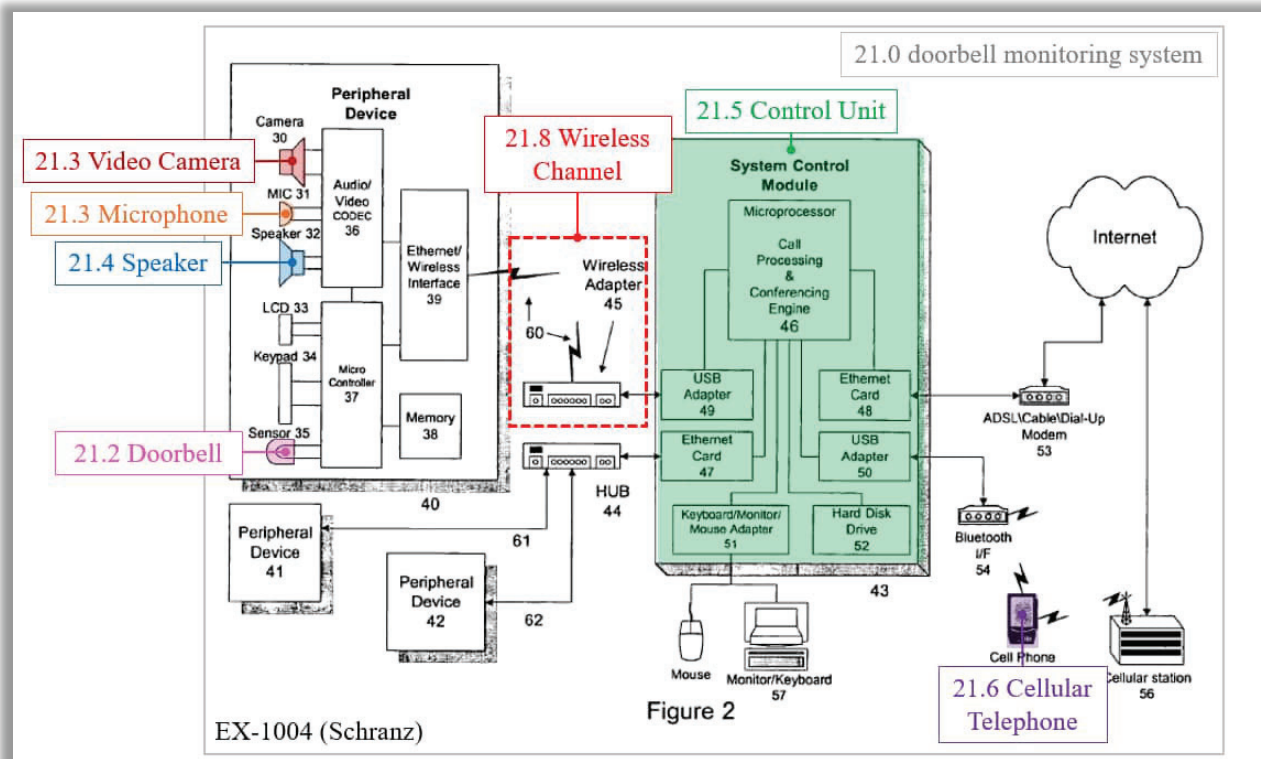
81. Schranz discloses this limitation. Schranz discloses peripheral devices 40 that include camera 30 (red) [*video camera*] and microphone 31 (orange) [*external microphone*]. EX-1004, ¶48. Camera 30 and microphone 31 transmit analog information to a CODEC 36 which, then, digitizes the information and provides

digital data to the system control module 43 (green) [*control unit*]. *EX-1004*, ¶48. Schranz states that the set of peripheral devices provide digital data to the system control module via a wired or wireless channel [*wirelessly streamed to the control unit*].

The peripheral device 40 connects to the SCM 43 via an Ethernet or wireless interface 39. The channel between the peripheral devices 40, 41 or 42 and the SCM 43 may be a wireless channel 60 or wireline channel 61 or 62.

EX-1004, ¶48.

82. As shown below in Figure 2, Schranz discloses wireless interface 39 connected to the peripheral device 40, a wireless channel 60, and a wireless transceiver at the system control module 43 to provide bidirectional communication between the peripheral device 40 and the system control module 50. *EX-1004*, ¶48. Therefore, Schranz's system discloses that *the entry point visual and audio communications are wirelessly streamed to the control unit*.

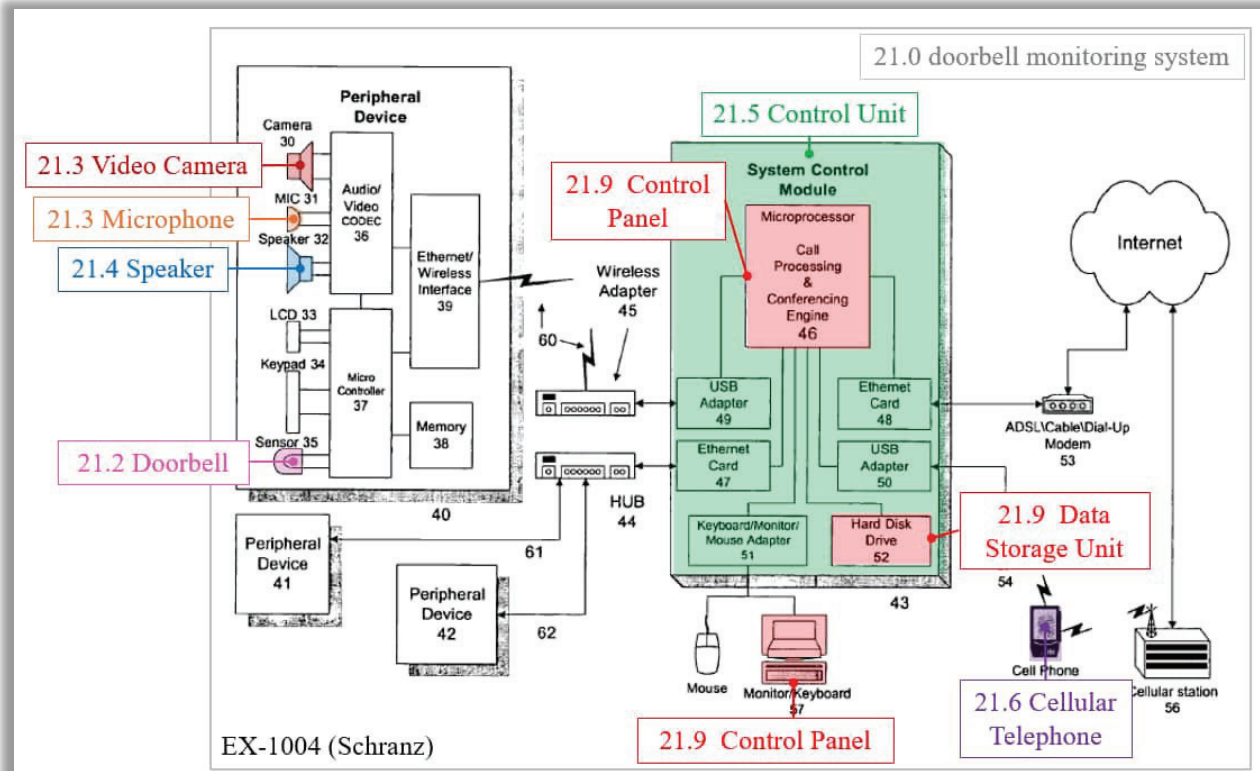


EX-1004, Figure 2 (Annotated).

[21.9] wherein the control unit is configured to store the entry point visual and audio communications captured by the single communications unit in a data storage unit of the control unit wherein a control panel is configured to allow an individual to manage a security system;

83. Schranz discloses this limitation. Schranz's system control module (green) [*control unit*] is "any hardware platform that runs the Windows 98, 2000, ME, XP or Linux operating system." EX-1004, ¶49. The system control module includes a hard disk drive 52 [*data storage unit*] "to record audio and video data from the peripheral devices during an alarm situation using standard formats." EX-1004,

¶49. Therefore, Schranz discloses a system where the control unit *is configured to store the entry point visual and audio communications captured by the single communications unit in a data storage unit of the control unit.*



EX-1004, Figure 2 (Annotated).

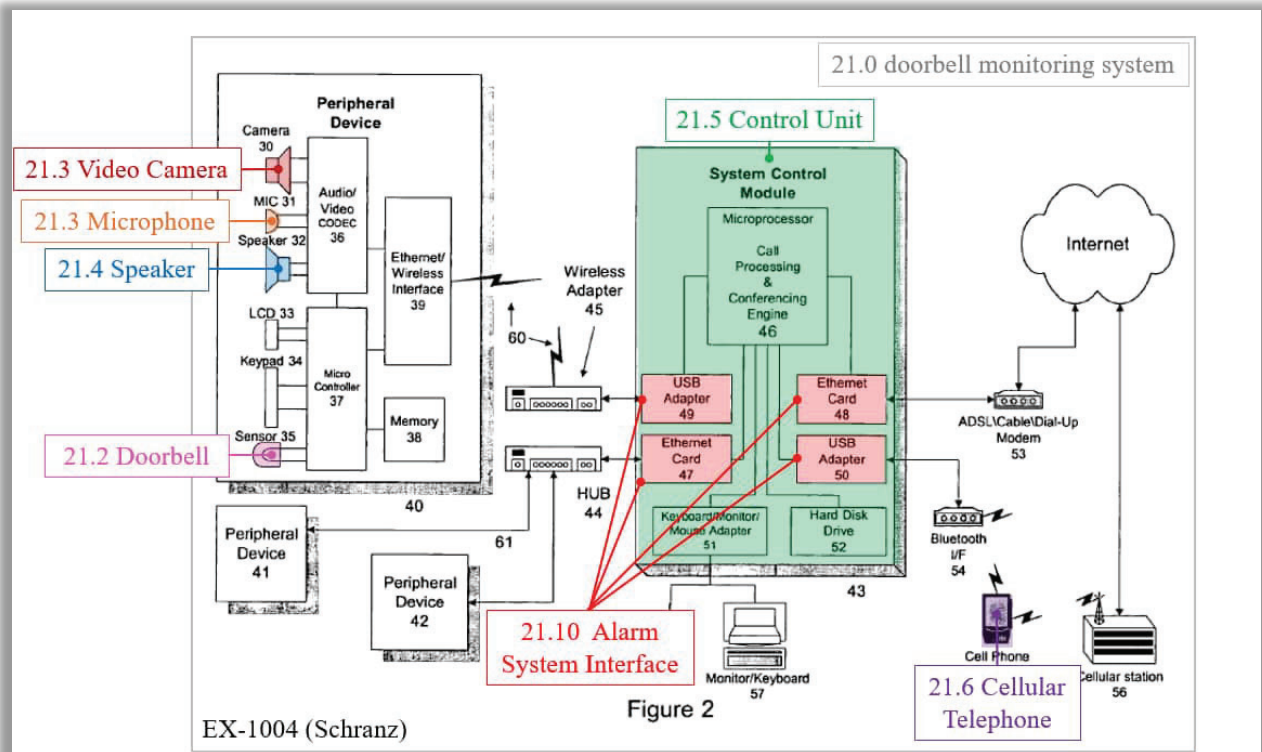
84. Further, Schranz’s system control module 43 [*control unit*] runs a user software application on the operating system which monitors and controls the peripheral devices, event detection, and VoIP call processing. EX-1004, ¶50. The user software application includes a web server and web application that the user can access remotely to “control all aspects of the system.” EX-1004, ¶50. Additionally, and as shown above, the system control module 43 includes a keyboard, mouse and monitor 57 “to set up the configurable parameters of the system.” EX-1004, ¶49, ¶56.

Schranz explains that keyboard and monitor 57 can be used to define “access codes, the VoIP addresses (URLs) to call during alarm, pre-recorded messages and zone definitions” for the VoIP security monitoring and alarm system. *EX-1004*, ¶56. The user software application, web server, web application, keyboard, and monitor are collectively a *control panel* that is *configured to allow an individual to manage a security system*.

[21.10] wherein an alarm system interface of the control panel is configured to interface with the security system;

85. Schranz discloses this limitation. As explained above with respect to limitation [21.9] which is incorporated herein, Schranz’s system control module 43 [*control unit*] runs a user software application with a web server, web application, keyboard and monitor [collectively the *control panel*]. *EX-1004*, ¶¶49-50. The system control module 43 includes “10/100BaseT Ethernet cards 47 & 48, two USB ports 49 & 50” [*alarm system interface*]. *EX-1004*, ¶49. As shown below, Ethernet card 47 and USB adapter 46 are connected to wireless channel 60 and wireline channel 62 which are in turn connected to peripheral devices 40, 41, and 42. Schranz explains that the ethernet card 47 and USB adapter 46 in the SCM allow the SCM to send control packets to and receive status packets from the peripheral devices. *EX-1004*, ¶48. Likewise, Schranz explains that Ethernet card 48 connects the SCM to modem 53 in order to provide a connection to the internet, and USB adaptor 50 may

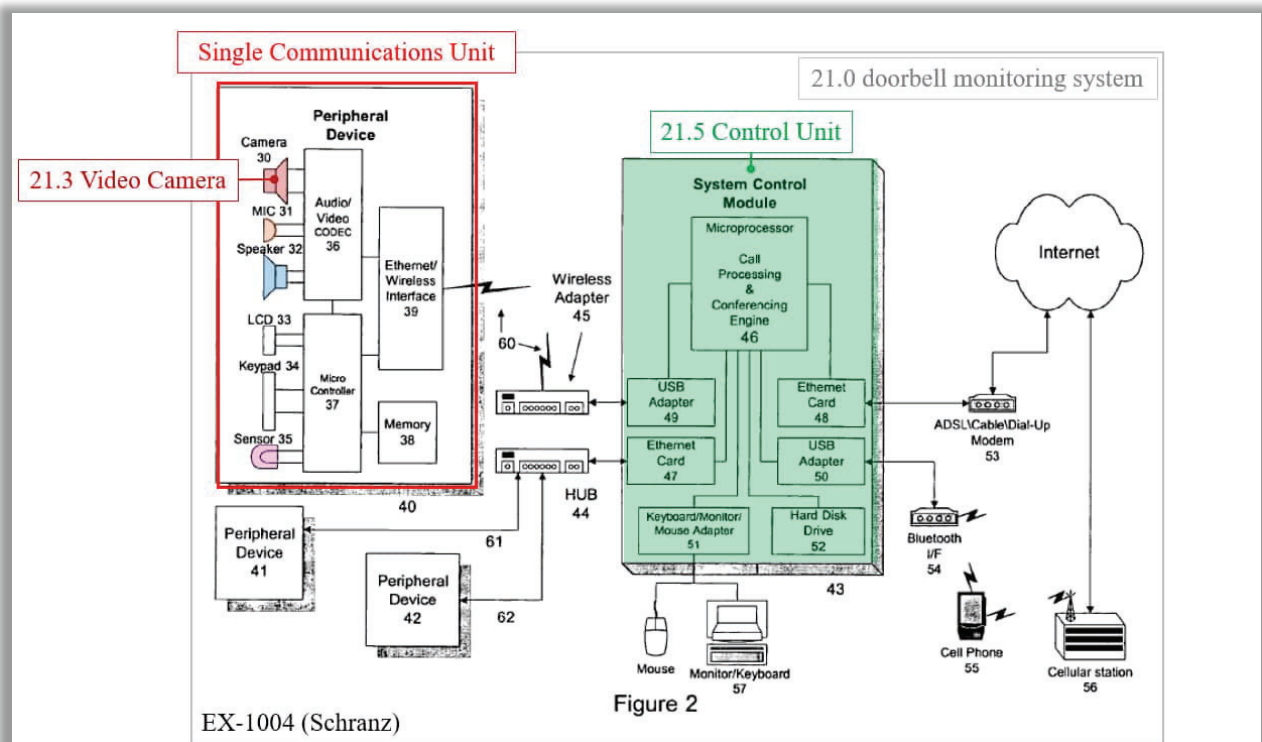
be used to connect to a Bluetooth enabled cell phone. *EX-1004*, ¶49. Schranz further discloses that the packets indicate an alarm detection that is then used by the SCM to locate and connect with the notified agent as quickly as possible using VoIP address resolution and VoIP presence protocols. *EX-1004*, ¶¶24, 25, 47. Therefore, ethernet card 47 and USB adapter 46 are that is configured to interface with the security system.



EX-1004, Figure 2 (Annotated).

[21.11] wherein the video camera is configured to collect the entry point visual communications captured by the single communications unit before the triggering event;

86. Schranz discloses this limitation. As shown below in Figure 2, Schranz discloses a peripheral device 40 [single communications unit] including a black and white or color “CCTV board camera,” camera 30 [video camera]. The peripheral device 40 [single communications unit] may be “located at the main entrance to the premises.” EX-1004, ¶47.



EX-1004, Figure 2 (Annotated).

87. A POSA understood that a CCTV is a “closed circuit” camera that typically records footage continuously, and in many cases records over previous footage periodically in a loop to save storage space. This was a known feature of security cameras as demonstrated in the State-of-the-Art section. See §IV.F. Specifically, it was well known to capture and record video continuously in memory,

and then based on predefined criteria, discard older video. EX-1008, ¶81. Thus, a POSA would have understood that Schranz's CCTV would include the well-known feature of capturing visual communications before the triggering event. Schranz's disclosure is consistent with the '191 Patent which itself lacks any detail regarding how its camera captures video before the triggering event, further demonstrating that this feature was well-known and would have been understood by a POSA without explicit instruction.

88. To the extent that Patent Owner argues that Schranz does not expressly disclose that its camera collects video before a triggering event, a POSA would be motivated to modify Schranz to incorporate such a feature and would have had a reasonable expectation of success in doing so. First, as discussed in the State-of-the-Art section, it was well-known and common at the time of the alleged invention to capture audio and video in a revolving buffer before saving to more permanent storage based on a triggering event. EX-1008, ¶81 ("video module 620 may buffer video from video cameras 112 in memory.") A revolving buffer was commonly implemented by allowing the user to define the amount of time to retain data from before and after the triggering event. EX-1007, ¶¶43, 81 ("Then, based on predefined criteria, older video that is not considered essential to any alarm signals may be discarded.") The purpose of this well-known technique was to allow for the observer

to see and capture data from before, during, and after triggering events (pressing of the doorbell button).

89. Schranz contemplates this type of user-driven configurability, and specifically discloses that the user sets up system control parameters. EX-1004, ¶¶56, 57. Accordingly, a POSA would have found it obvious to collect video and audio data before the ringing of the doorbell by continuously storing the captured audio and video in a buffer such that context proximate to the triggering event may be collected. Such a modification would have amounted to nothing more than the application of a known technique, revolving buffer storage triggered by a defined event, to improve a similar device in the same, predictable way.

90. Second, a POSA would be motivated to add such a feature because it provides the additional known benefit of helping identify false alarms as discussed in the State-of-the-Art section. EX-1008, ¶38. A POSA would have recognized that providing the ability to monitor surroundings even when a triggering event does not occur by using video surveillance was a common capability known as remote surveillance or “lifestyle video,” as discussed in the State of the Art. EX-1008, ¶¶43, 82. With lifestyle video, the observer can view the environment and manually verify triggering events thereby enhancing the accuracy of the security system. Thus, A POSA would have been motivated to include “lifestyle video” to limit the number of false alarms and enhance the accuracy of the security system. Moreover,

implementing this modification would have been straightforward because it could be accomplished using the existing equipment already disclosed in Schranz, and hardware storage could be easily expanded if archiving of the video were desired. A POSA would have had a reasonable expectation of success in making this combination given the well-known nature of continuous video recording in CCTV systems.

[21.12] wherein the video camera is configured to collect additional visual communications after the triggering event;

91. Schranz discloses this limitation. Schranz discloses once a peripheral device detects an event (*e.g.*, the ringing of the doorbell), it notifies the SCM, which then initiates a VoIP call to a remote agent using a pre-programmed VoIP uniform resource locator (URL). This VoIP call can reach a user in the IP network using an IP enabled communication device such as a VoIP phone or multimedia computer, or by going through a gateway it can terminate on a traditional POTS or cellular phone. The SCM then routes the audio and/or video data from the peripheral device to the remote agent as well as storing the data in real-time using standard audio and video formats.” *EX-1004*, ¶¶24, 32. Schranz further explains that the system provides real-time intruder tracking by monitoring the current location of the intruder using the advanced peripheral devices and motion sensors. The notified agent is kept up to date with the current location by periodic announcements from the SCM. *EX-1004*, ¶29.

A POSA understood that to track an intruder and update the remote users, the peripheral devices, including the camera would continue to capture video data after detecting an event [*configured to collect additional visual communications after the triggering event*].

[21.13] wherein the doorbell monitoring system is configured to establish communication with the control unit upon activation of the doorbell;

92. Schranz discloses this limitation. Schranz's VoIP security monitoring system utilizes peripheral devices including a "doorbell signal" to notify the system control module [*control unit*] upon event detection. *EX-1004*, ¶¶47, 48. Specifically, Schranz states that "once a peripheral device detects an event it notifies the SCM." *EX-1004*, ¶24. As explained above in [21.1] and [21.3] and incorporated herein, in both normal or armed mode, the peripheral devices monitor the environment and notify the SCM when an event takes place. *EX-1004*, ¶¶59-60. Therefore, Schranz's system *is configured to establish communication with the control unit upon activation of the doorbell*.

[21.14] wherein at least a portion of an initial communication after the doorbell is activated is a notification sent to the cellular telephone; and

93. Schranz discloses this limitation. Schranz states that during an alarm, such as when a doorbell signal is received, the system sends "some form of VoIP notification" to the remote user's "cell phone 150." *EX-1004*, ¶¶60-62. In addition,

Schranz discloses that the remote person can be notified of the event by the Instant Messaging feature of the Session Initiation Protocol [*wherein at least a portion of an initial communication after the doorbell is activated is a notification sent to the cellular telephone*]. EX-1004, Claim 6. Further, Schranz states that during an alarm “the SCM knows beforehand which device to contact (work phone, cell, laptop) and what method of message to send (text, voice, video, email).” EX-1004, ¶63. The system control module therefore provides *notification sent to the cellular telephone*.

[21.15] wherein the doorbell monitoring system is configured to authenticate a user of the doorbell monitoring system.

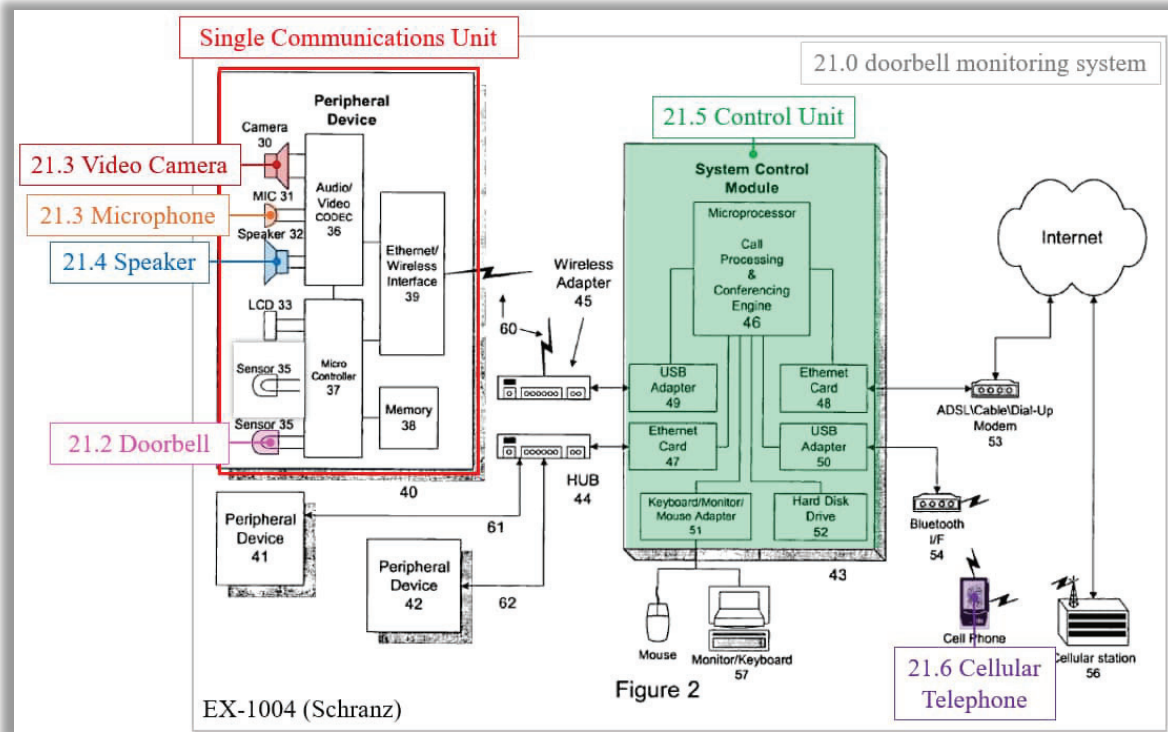
94. Schranz discloses this limitation. Schranz discloses that system configuration on initial setup requires the user to set “items such as *access codes*, the VoIP addresses (URLs) to call during alarm, pre-recorded messages and zone definitions.” EX-1004, ¶56. Likewise, Schranz discloses that, after system configuration, the user can access the “secure portal” or user web application to control all aspects of the system. EX-1004, ¶¶50, 56. A POSA understood that a “secure portal” and “access codes” are inherently *configured to authenticate a user of the doorbell monitoring system*.

Claim 22

[22] The doorbell monitoring system of claim 21, wherein the single communications unit is

configured to stream at least a portion of the captured visual and audio communications.

95. Schranz discloses this limitation. As shown below in Figure 2, Schranz discloses a peripheral device 40 [*single communications unit*] with a camera 30 (red) microphone 31 (orange) connected to system control module 43 (green). *EX-1004*, ¶48. Schranz explains that CODEC 36 “digitizes the analog video signal” from camera 30 and “codes the analog audio signal” from microphone 31 to provide the data to the system control module via wireless or wired channel. *EX-1004*, ¶48. The system control module “routes the audio and/or video data from the peripheral device to the remote agent.” *EX-1004*, ¶24. Furthermore, a POSA would understand that real-time delivery of video and audio requires streaming. Schranz further discloses use of the ‘Real-Time Transport Protocol (RTP),’ which a POSA would recognize as a protocol specifically designed for real-time transmission of audio and video streams over packet networks. *EX-1004*, Claim 4.



EX-1004, Figure 2 (Annotated)

Therefore, Schranz discloses *the single communications unit configured to stream at least a portion of the captured visual and audio communications.*

Claim 23

[23] The doorbell monitoring system of claim 21, wherein the single communications unit is configured to capture additional video from the video camera after the triggering event.

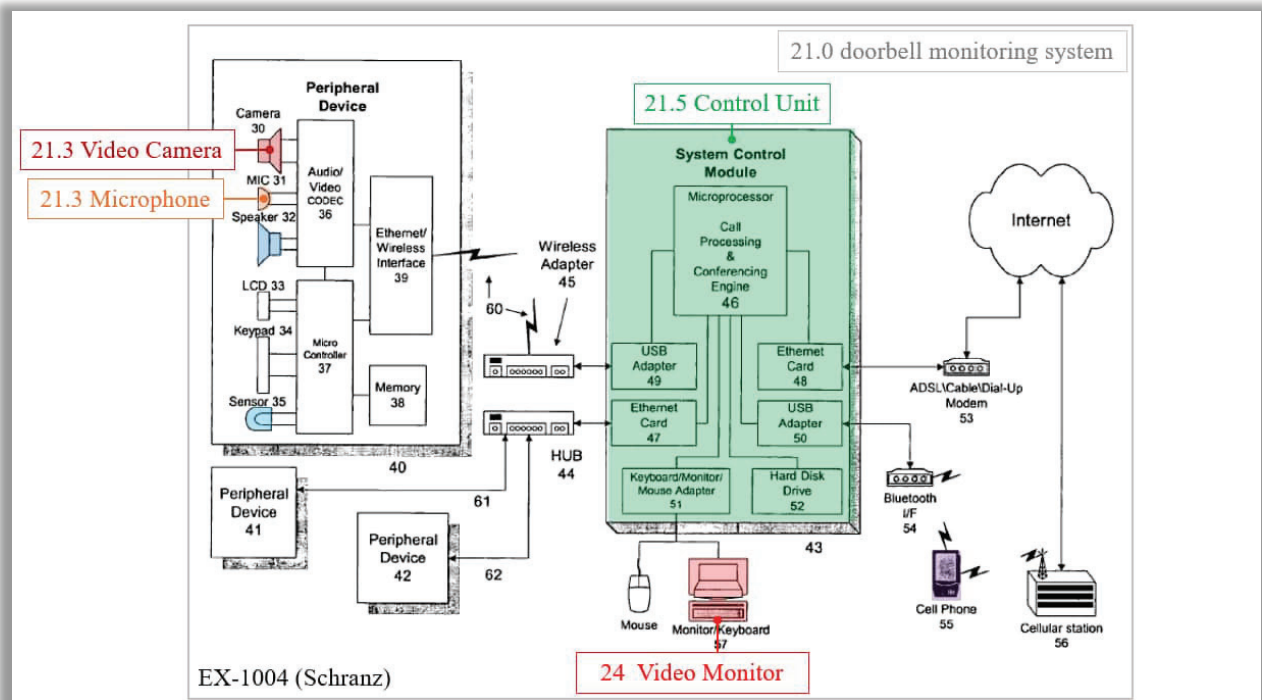
96. Schranz discloses this limitation for the same reasons as discussed with respect to limitation [21.12].

Claim 24

[24] The doorbell monitoring system of claim 21, wherein the control unit is configured to display the entry point visual and audio communications on the video monitor.

97. Schranz discloses this limitation. Schranz's discloses a system control module 43 (green) [*control unit*] that is "any hardware platform that runs the Windows 98, 2000, ME, XP or Linux operating system" and typically is an "off the shelf computer." *EX-1004*, ¶49. As shown below, the system control module 43 or off the shelf computer includes a keyboard, mouse and monitor 57 (red) [*video monitor*] "to set up the configurable parameters of the system." *EX-1004*, ¶¶49, 56. Further, the system control module runs a web server and website where "[t]he user can visually see the current configuration and the status of all peripheral devices." *EX-1004*, ¶50. As shown below, the system control module 43 is in communication with a set of peripheral devices, including camera 30 (red) [*video camera*] and microphone 31 (orange) [*external microphone*]. *EX-1004*, ¶48. The system control module 43 receives audio and video communication from camera 30 and microphone 31 via CODEC 36 which "digitizes the analog video signal into a standard digital format, codes the analog audio signal from the microphone into PCM samples." *EX-1004*, ¶48. Therefore, the user can see the audio and visual data from camera 30 and microphone 31 through the webserver and website on the system control module 43.

98. Schranz further explains that the user can access the website to see the audio and video data from “any Internet browser that supports the https protocol.” *EX-1004*, ¶50. As discussed above, the system control module 43 is typically an off the shelf computer and therefore has an internet browser that supports the https protocol. *EX-1004*, ¶49. A user can thereby access the website to see the audio and video data on the system control module 43 itself through a keyboard, mouse and monitor 57. Therefore, Schranz’s system control module 43 [*control unit*] is configured to display the entry point visual and audio communications on the video monitor.



EX-1004, Figure 2 (Annotated).

Claim 25

[25] The doorbell monitoring system of claim 24, wherein the control unit is configured to display the entry point visual and audio communications on the video monitor in substantially realtime.

99. Schranz discloses this limitation. As explained above with respect to Claim [24] and incorporated herein, Schranz systems operates as follows: (1) Camera 30 and microphone 31 capture audio and visual information from the entry point (*EX-1004*, ¶48); (2) CODEC 36 digitizes the audio and video data and transmits the digital data to the system control module via wireless channel 60 (*EX-1004*, ¶48); (3) The system control module 43 website or “graphical monitor and control program” displays the audio and video data to allow the user to “visually see the current configuration and the status of all peripheral devices” (*EX-1004*, ¶50). Furthermore, Schranz’s system allows the user to access the “graphical monitor and control program” through “any Internet browser” such as by using the system control module and monitor 57 [*video monitor*]. *EX-1004*, ¶48. Moreover, Schranz contemplates the bandwidth requirements of real-time bidirectional transmission of audio and video data and explains the “preferred method to connect [the SCM] to the Internet is by ADSL or Cable modem since their bandwidth capabilities are the best.” *EX-1004*, ¶49. Schranz explains that “Dial-Up modems may be used for audio only applications.” *EX-1004*, ¶49. A POSA understood that Schranz discloses communications protocols that allow for real-time bidirectional transmission of audio

and video data including Voice over Internet Protocol data information, used to deliver voice and/or video information between the peripheral devices, the computing platform including the video monitor and the remote person's device using Real-Time Transport Protocol (RTP) or Session Initiation Protocol (SIP) [*visual and audio communications on the video monitor in substantially realtime*]. EX-1004, Claims 2-4.

Claim 26

[26] The doorbell monitoring system of claim 21, wherein the control unit is configured to display the entry point visual and audio communications on the video monitor in substantially realtime; and wherein the doorbell monitoring system is configured to authenticate a user of the doorbell monitoring system.

100. Schranz discloses this limitation for the same reason as discussed with respect to limitations [25] and [21.15].

Claim 27

[27] The doorbell monitoring system of claim 21, wherein the control unit is configured to generate a file that includes at least a portion of the entry point visual and audio communications captured by the single communications unit.

101. Schranz discloses this limitation. Schranz's VoIP security monitoring and alarm system includes system control module 43 [*control unit*] with a hard disk drive 52 that is "used to record audio and video data from the peripheral devices

during an alarm situation using standard formats.” *EX-1004*, ¶49. A POSA would understand that digital video recording systems commonly store synchronized audio and video streams together as a multimedia recording, thereby generating a file containing both the captured visual and audio communications. The audio and video data are sourced from camera 30 and microphone 31 contained within peripheral device 40 [*single communications unit*]. *EX-1004*, ¶48. A POSA understood that the “standard formats” contemplated by Schranz include a file that contains a portion of the audio and video captured by the single communications unit. A POSA would have understood that, at the time of the invention, common standard multimedia file formats such as AVI or MPEG stored both audio and video data. Therefore, Schranz discloses a *control unit configured to generate a file that includes at least a portion of the entry point visual and audio communications captured by the single communications unit.*

Claim 28

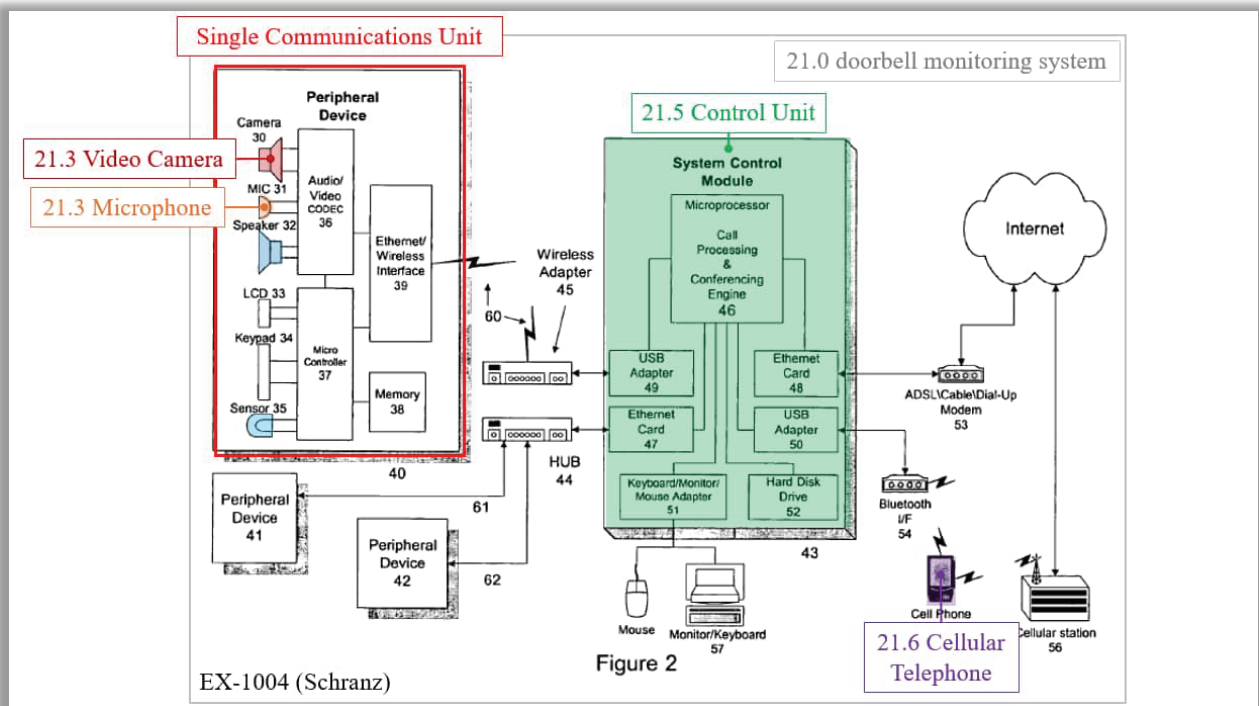
[28] The doorbell monitoring system of claim 21, wherein the cellular telephone comprises a user interface that allows user of the cellular telephone to take two or more actions after receiving at least a portion of the entry point visual and audio communications captured by the single communications unit.

102. Schranz discloses this limitation. Schranz’s VoIP security monitoring and alarm system utilizes peripheral devices to detect an event and a system control

module to establish a Voice/Video over IP (VoIP) call to a remote user via cellular networks. *EX-1004*, Abstract. The remote user will “will hear ambient audio and see video images from the peripheral device in the location of the alarm.” The remote user can then issue “DTMF commands to the SCM to control the audio, initiate conference calls and other functions” [*wherein the cellular telephone comprises a user interface that allows user of the cellular telephone to take two or more actions after receiving at least a portion of the entry point visual and audio communications captured by the single communications unit*]. *EX-1004*, Abstract.

103. Specifically with respect to Figure 2 (below), Schranz’s system includes camera 30 and microphone 31 disposed within peripheral device 41 [*single communications unit*] to capture audio and video data at “the main entrance to the premise.” *EX-1004*, ¶48. Once peripheral device 41 detects an event, the device notifies the system control module 43 which initiates a VoIP notification to a remote agent. *EX-1004*, ¶24, 60, 62. The VoIP notification may be sent to the remote user’s cell phone 150 [*cellular telephone*], laptop computer 155, or multimedia computer 170. *EX-1004*, ¶62. The remote user can then send “a text message commanding the SCM to make an **audio and video call** to the same device.” *EX-1004*, ¶63 (emphasis added). When the audio and video call is established, the remote user will hear the audio from microphone 31 and video from camera 30 at the location of the alarm. *EX-1004*, ¶¶64, 24, Abstract. The user can then “issue commands to the SCM” using

the cell phone's keypad [*user interface*] to issue DTMF commands. *EX-1004*, ¶¶64. The remote user can issue a variety of commands including “increase and decrease the volume of the audio path,” “play an announcement over the speaker,” and “initiate a conference call to a third-party.” *EX-1004*, ¶¶65-66. Therefore, Schranz discloses a cellular telephone with a user interface that allows user of the cellular telephone to take two or more actions after receiving at least a portion of the entry point visual and audio communications captured by the single communications unit.



EX-1004, Figure 2 (Annotated).

Claim 29

[29] The doorbell monitoring system of claim 28, wherein the two or more actions are at least one of (1) play a pre-recorded greeting, (2) request additional video and/or audio communications,

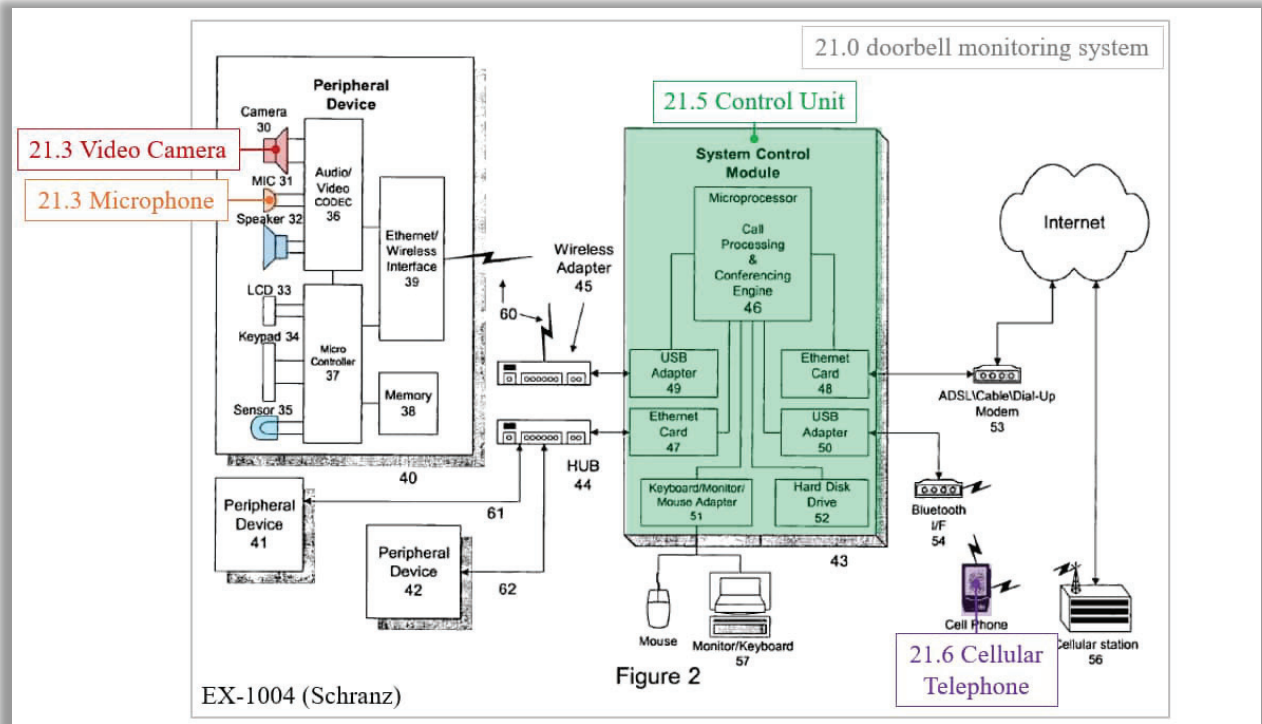
(3) institute two-way video communications between the user and the person at the entry point, (4) notify an alarm company, or (5) selection of no action.

104. Schranz discloses this limitation. As explained with respect to Claim [28], upon event detection, Schranz's system control module 43 establishes a VoIP audio and video call between the peripheral device (*i.e.*, peripheral device 40) and the remote user's cell phone (*i.e.*, cell phone 150). *EX-1004*, Abstract, ¶¶60, ¶62. During the call, the remote user can use the keypad on the cellphone to send DTMF tones which tell the system control module to perform a specific action. *EX-1004*, ¶64. Schranz explains that "[s]everal commands are available to the user, some of which are described." *EX-1004*, ¶64.

105. First, Schranz expressly discloses that the user "can direct the SCM to play an announcement over the speaker" [(1) *play a pre-recorded greeting*]. *EX-1004*, ¶65. Schranz explains that during initial system configuration the user can set-up configurable parameters including a "pre-recorded message." *EX-1004*, ¶56. A POSA understood that Schranz's system allows the announcement requested by the remote user to be one of the pre-recorded messages set-up during initial system configuration. Therefore, Schranz discloses that one of the actions requested by the remote user may be to (1) *play a pre-recorded greeting*.

Expert Declaration of James Parker

106. Second, Schranz expressly discloses that the user can “command a call transfer to a particular peripheral device” [(2) *request additional video and/or audio communications*]. *EX-1004*, ¶31. As shown in Figure 2, Schranz’s system control module 43 is connected to multiple peripheral devices including device 40, 41, and 42. In one instance, the user may be receiving audio and video information from peripheral device 40 over the VoIP call. The user may then request a transfer to peripheral device 41 to receive additional video and or audio communications from the scene. In another instance, when receiving audio and video information from peripheral device 40 over the VoIP call, Schranz discloses that the user can request additional information from the SCM “by querying the SCM using DTMF commands.” *EX-1004*, ¶29. Therefore, Schranz discloses that one of the actions requested by the remote user may be to (2) *request additional video and/or audio communications*.



EX-1004, Figure 2 (Annotated).

107. Third, Schranz discloses that once peripheral device 41 detects an event, the device notifies the system control module 43 which initiates a VoIP notification to a remote agent. EX-1004, ¶¶24, 60, 62. The VoIP notification may be sent to the remote user's cell phone 150 and the remote user can then send "a text message commanding the SCM to make an *audio and video call* to the same device." EX-1004, ¶¶62, 63 (emphasis added). When the audio and video call is established, the remote user will hear the audio from microphone 31 and video from camera 30 at the location of the event [(3) *institute two-way video communications between the user and the person at the entry point*]. EX-1004, ¶¶64, ¶24, Abstract. Further, Schranz discloses a VoIP communication call such that "voice and/or video

information is exchanged between the said peripheral device... and the remote person” [(3) *institute two-way video communications between the user and the person at the entry point*]. *EX-1004*, Claim 1.

108. Fourth, Schranz discloses that the remote user “can initiate a conference call to a third-party, such as his neighbour or the police.” *EX-1004*, ¶66. Schranz identification of “the police” as an exemplary third party demonstrates that the system was designed to facilitate emergency security communications in response to a detected event. A POSA would have understood that *an alarm company* is similarly a third-party resource for emergency security communications in response to a detected event. Indeed, contacting an alarm company in response to a security event was a well-known and routine practice in the home security field at the time of the alleged invention, and Schranz's open-ended reference to “a third-party” plainly encompasses such a contact. A POSA would have found it obvious to modify Schranz's system to include the ability to initiate a conference call to an alarm company, as doing so merely applies Schranz's own disclosed functionality, initiating a conference call with the police, to an additional, predictable recipient, *an alarm company*. Such a modification would have required no change to the underlying architecture of Schranz's system and would have yielded nothing more than the predictable result of expanding the set of third parties available for a conference call

to include an alarm company. Therefore, Schranz discloses that one of the actions requested by the remote user may be to *(4) notify an alarm company*.

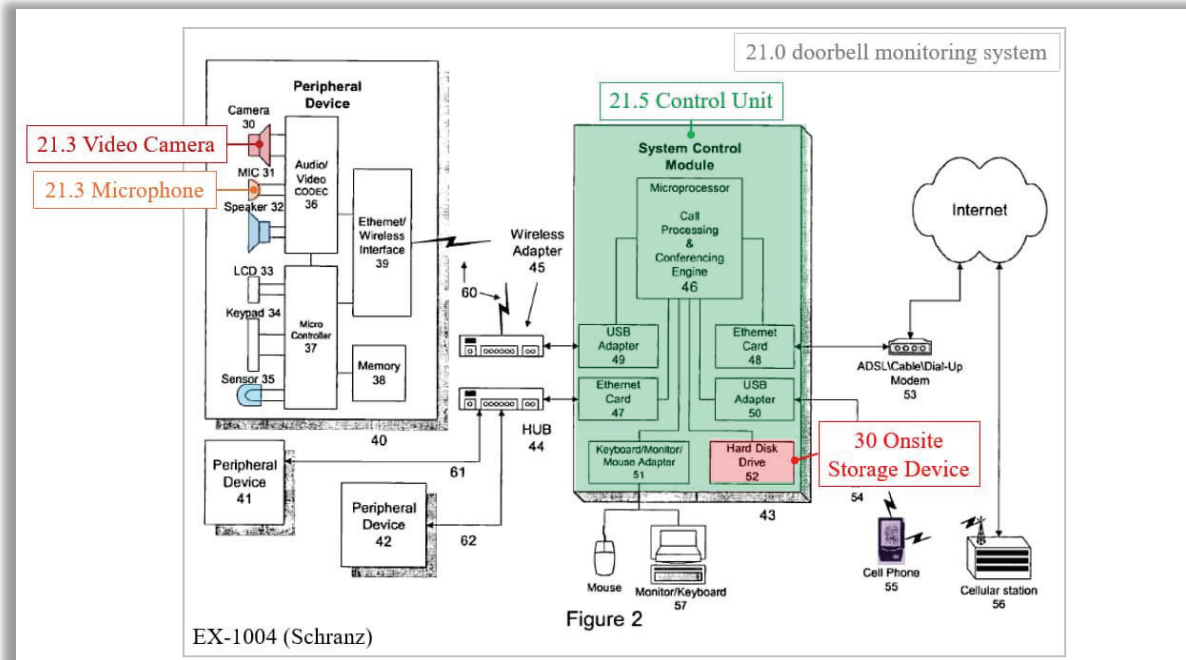
109. Finally, Schranz discloses the remote user may elect to send DTMF commands to the system control module, and includes the user electing not to send a DTMF a command [*(5) selection of no action*].

Claim 30

[30] The doorbell monitoring system of claim 21, wherein the control unit further communicates captured visual and audio communications to an onsite storage device and wherein the storage device stores the captured visual and audio communications.

110. Schranz discloses this limitation. Schranz system control module 43 [*control unit*] is “any hardware platform that runs the Windows 98, 2000, ME, XP or Linux operating system.” *EX-1004*, ¶49. As shown below, the system control module 43 (green) [*control unit*] is connected to hard disk drive 52 (red) [*onsite storage device*] which is designed “to record audio and video data from the peripheral devices during an alarm situation using standard formats” [*communicates captured visual and audio communications to an onsite storage device and wherein the storage device stores the captured visual and audio communications*]. *EX-1004*, ¶49. Therefore, Schranz system control module 43 [*control unit*] *communicates captured*

visual and audio communications to an onsite storage device and wherein the storage device stores the captured visual and audio communications.



EX-1004, Figure 2 (Annotated).

Claim 31

[31] The doorbell monitoring system of claim 30, wherein the stored video and audio communications are accessible by an additional device apart from the control unit.

111. Schranz discloses this limitation. As explained above with respect to Claim [30], Schranz system control module includes a hard disk drive 52 that “record[s] audio and video data from the peripheral devices during an alarm situation using standard formats.” *EX-1004*, ¶49. Additionally, Schranz system control module 43 runs a user software application with a web server and web application that the user can access remotely to “control all aspects of the system.” *EX-1004*,

¶50. Schranz explains that the user may access the “website remotely and securely using any Internet browser that supports the https protocol.” *EX-1004*, ¶50. A POSA understood that in order to control all aspects of the system, the user web application must allow the user to view and manage the audio and video data storage on hard drive 52. Moreover, as the user can access the website from any internet browser, a POSA understood the *stored video and audio communications* are accessible from any device with an internet browser and is therefore *accessible by an additional device apart from the control unit*.

Claim 32

[32] The system of claim 30, wherein the onsite storage device is configured to provide the additional device with access to the stored video and audio communications in substantially realtime.

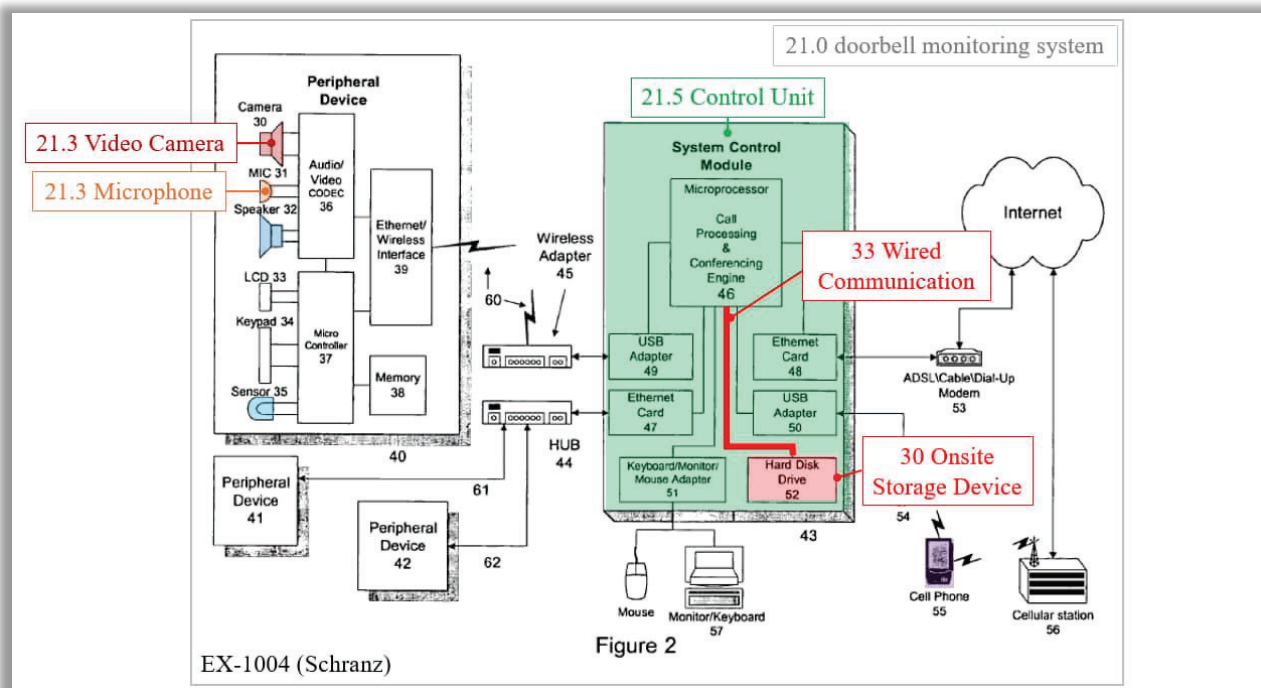
112. Schranz discloses this limitation. Schranz discloses that its onsite storage devices records video and audio communications in substantially real-time, e.g. “an audio and video recording mechanism that uses a hard disk drive to store the data in real-time using standard audio and video formats.” *EX-1004*, ¶32. Schranz’s further discloses that a user can remotely access the security system through a web portal to control all aspects of the system which a POSA understood would include access to the stored real-time audio and video data. *EX-1004*, ¶50, 56. Schranz explains that the user connects to the website via an internet browser that supports

the “https protocol,” and a POSA understood that the user is thereby provided access to the stored real-time audio and video data in *substantially realtime*. Therefore, Schranz’s user monitor and keyboard 57 with web interface or website provides access to the stored video and audio communications in *substantially realtime*.

Claim 33

[33] The system of claim 30, wherein the control unit communicates the captured visual and audio communications to the onsite storage device via wired communication.

113. Schranz discloses this limitation. As shown below in Figure 2, Schranz system control module 43 [control unit] provides audio and video data to hard drive 52 [onsite storage device] via wired communication.



EX-1004, Figure 2 (Annotated).

Claim 34

[34.0] A doorbell monitoring system comprising:

114. Schranz discloses this limitation for the same reasons as discussed with respect to limitation [21.0].

[34.1] a doorway having an environment;

115. Schranz discloses this limitation for the same reasons as discussed with respect to limitation [21.1].

[34.2] a doorbell located in an entry point, activation of the doorbell being a triggering event;

116. Schranz discloses this limitation for the same reasons as discussed with respect to limitation [21.2].

[34.3] a video camera and an external microphone disposed in the entry point, the video camera and the external microphone, responsive to the triggering event, for capturing visual and audio communications at the entry point and transmitting the captured visual and audio communications;

117. Schranz discloses this limitation for the same reasons as discussed with respect to limitation [21.3].

[34.4] an external speaker disposed in the entry point, the external speaker for rendering received audio communications;

118. Schranz discloses this limitation for the same reasons as discussed with respect to limitation [21.4].

[34.5] a control unit in communication with the video camera, the doorbell, and the external microphone, the control unit for communicating at least one portion of the visual and audio communications received from the video camera and external microphone, and for communicating the received audio communications to the external speaker;

119. Schranz discloses this limitation for the same reasons as discussed with respect to limitation [21.5].

[34.6] a cellular telephone disposed remotely to the doorway and the control unit, the cellular telephone for capturing cellular audio communications at the cellular telephone, transmitting the cellular audio communications to the control unit, and rendering the at least one portion of entry point visual and audio communications received from the control unit; and

120. Schranz discloses this limitation for the same reasons as discussed with respect to limitation [21.6].

[34.7] wherein the doorbell, the video camera, the external microphone, the external speaker, and a proximity detector are part of a single communications unit;

121. Schranz discloses this limitation for the same reasons as discussed with respect to limitation [21.7].

[34.8] wherein the single communications unit is configured to play a pre-recorded message to a visitor at the entry point and wirelessly streaming at least a portion of the captured visual and audio communications to the control unit;

122. Schranz discloses this limitation. Schranz's VoIP security monitoring and alarm system is designed to play a "pre-recorded audio playback at a peripheral device with an announcement stored on the SCM." EX-1004, ¶33. Schranz explains that the peripheral devices [single communication unit] are often located "at the main entrance to the premises" and typical examples of the pre-recorded message "include a doorbell chime, attack dogs barking or the speech of a person." EX-1004, ¶48, ¶33. Therefore, Schranz discloses a single communications unit configured to play a pre-recorded message to a visitor at the entry point. Moreover, for the same reasons as described with respect to limitation [21.8], Schranz's system discloses that the entry point visual and audio communications are wirelessly streamed to the control unit.

[34.9] wherein the video camera is configured to collect the entry point visual communications before the triggering event; and

123. Schranz discloses this limitation for the same reasons as discussed with respect to limitation [21.11].

[34.10] wherein the video camera is configured to collect additional visual communications after the triggering event.

124. Schranz discloses this limitation for the same reasons as discussed with respect to limitation [21.12].

Claim 35

[35] The doorbell monitoring system of claim 34, wherein the single communications unit is configured to stream at least a portion of the captured visual and audio communications.

125. Schranz discloses this limitation for the same reasons as discussed with respect to Claim [22].

Claim 36

[36] The doorbell monitoring system of claim 34, wherein the single communications unit is configured to capture additional video from the video camera after the triggering event.

126. Schranz discloses this limitation for the same reasons as discussed with respect to limitation [21.12].

Claim 37

[37] The doorbell monitoring system of claim 34, wherein the control unit is configured to display the entry point visual and audio communications on the video monitor.

127. Schranz discloses this limitation for the same reasons as discussed with respect to Claim [24].

Claim 38

[38] The doorbell monitoring system of claim 37, wherein the control unit is configured to display the entry point visual and audio communications on the video monitor in substantially realtime.

128. Schranz discloses this limitation for the same reasons as discussed with respect to Claim [25].

Claim 39

[39] The doorbell monitoring system of claim 34, wherein the control unit is configured to display the entry point visual and audio communications on the video monitor in substantially realtime; and wherein the doorbell monitoring system is configured to authenticate a user of the doorbell monitoring system.

129. Schranz discloses this limitation for the same reasons as discussed with respect to Claim [25] and limitation [21.15].

Claim 40

[40] The doorbell monitoring system of claim 34, wherein the control unit further comprises a data storage unit wherein the control unit is configured to store the entry point visual and audio communications in the data storage unit of the control unit.

130. Schranz discloses this limitation for the same reasons as discussed with respect to Claim [27].

Claim 41

[41] The doorbell monitoring system of claim 34, wherein the control unit is configured to generate a file that includes at least a portion of the entry point visual and audio communications captured by the single communications unit.

131. Schranz discloses this limitation for the same reasons as discussed with respect to Claim [27].

Claim 42

[42] The doorbell monitoring system of claim 34, wherein the cellular telephone comprises a user interface that allows user of the cellular telephone to take two or more actions after receiving at least a portion of the entry point visual and audio communications captured by the single communications unit.

132. Schranz discloses this limitation for the same reasons as discussed with respect to Claim [28].

Claim 43

[43] The doorbell monitoring system of claim 42, wherein the two or more actions are at least one of (1) play a pre-recorded greeting, (2) request additional video and/or audio communications, (3) institute two-way video communications between the user and the person at the entry

point, (4) notify an alarm company, or (5) selection of no action.

133. Schranz discloses this limitation for the same reasons as discussed with respect to Claim [29].

Claim 44

[44] The doorbell monitoring system of claim 34, wherein the control unit further communicates captured visual and audio communications to an onsite storage device and wherein the storage device stores the captured visual and audio communications.

134. Schranz discloses this limitation for the same reasons as discussed with respect to Claim [30].

Claim 45

[45] The doorbell monitoring system of claim 44, wherein the stored video and audio communications are accessible by an additional device apart from the control unit.

135. Schranz discloses this limitation for the same reasons as discussed with respect to Claim [31].

Claim 46

[46] The system of claim 44, wherein the onsite storage device is configured to provide the additional device with access to the stored video and audio communications in substantially realtime.

136. Schranz discloses this limitation for the same reasons as discussed with respect to Claim [32].

Claim 47

[47] The system of claim 45, wherein the control unit communicates the captured visual and audio communications to the onsite storage device via wired communication.

137. Schranz discloses this limitation for the same reasons as discussed with respect to Claim [33].

VIII. CONCLUSION

138. For all the reasons set forth within my Declaration, it is my opinion that Claims 21-47 of the '191 Patent are obvious over Schranz.

CONCLUSION AND DECLARATION

The findings and opinions set forth in this declaration are based on my research and analysis to date. I may continue my examinations in view of additional documents or other factual evidence over the course of this proceeding that may necessitate supplementing and/or refining my opinions. I reserve the right to add to, alter, or delete my opinions and my Declaration upon discovery of additional information. I reserve the right to make such changes as necessary.

In signing this declaration, I understand that the declaration may be filed as evidence in a contested case before the Patent Trial and Appeal Board of the United States Patent and Trademark Office. I acknowledge that I may be subject to cross-examination in the case and that cross-examination will take place within the United States. If cross-examination is required of me, I will appear for cross-examination within the United States during the time allotted for cross-examination.

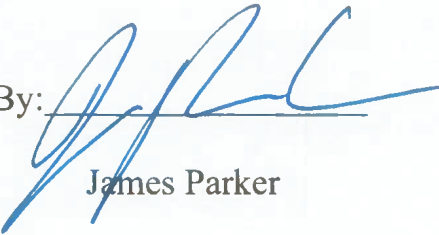
I declare that all statements made herein on my own knowledge are true, and that all statements made on information and belief are believed to be true, and that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or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

[SIGNATURE ON FOLLOWING PAGE]

Expert Declaration of James Parker

Dated: MARCH 16, 2026

By: _____



James Parker

APPENDIX A – MATERIALS RELIED UPON

<i>Exhibit #</i>	<i>Description</i>
1001	U.S. Patent No. 7,583,191 (“the ’191 Patent”)
1002	Prosecution History of the ’191 Patent (“File History”)
1003	<i>Intentionally Left Blank</i>
1004	U.S. Patent Publication 2004/0086093 (“Schranz”)
1005	Re-Exam Prosecution History of the ’191 Patent
1006	U.S. Pat. No. 6,429,893
1007	U.S. Pat. No. 6,778,084
1008	U.S. Patent Publication 2002/0147982
1009	<i>Curriculum Vitae</i> of James Parker
1010	James Parker Patent Summary

APPENDIX B – CURRICULUM VITAE

Electronics R&D - New Product Development

Electronic Security Systems and Sensors

40+ years of extensive electronic and security industry experience, spanning hands-on technical roles to senior executive leadership. Over 15 years as an Expert Witness and Technical Consultant.

Former Vice President of Engineering at Tyco Security Products / Digital Security Controls (DSC) – a premier global electronic security systems manufacturer with annual sales surpassing ~\$400 million. (DSC acquired by Tyco in 2001.)

Responsible for the research, development, and launch of hundreds of products, including Wired & Wireless Security Systems, Control Panels (Burglar / Fire / Access), Motion Detectors, Smoke Detectors, Intelligent Solar Powered LED Lighting Systems (patio to streetlight), Home Automation Controllers (smart home), and much more.

Comprehensive expertise in the entire product development lifecycle, from initial conception to mature production.

Named inventor on over 25 patents with thorough knowledge in patent identification, filing, and litigation process.

Seasoned in Civil, Criminal, & Patent Litigation, Arbitration, and Inter Partes Reviews (IPRs). Involved in **30+ cases**, marking significant experiences with at least **12 IPRs, 6 depositions, and 3 courtroom testimonies**; further contributed with multiple expert reports and declarations.

Previous Clients: (Partial List)
 2GIG Technologies | AIG Insurance Company | ADT | Alarm.com | AT&T Digital Life | Chubb Insurance | EarthCam Inc.
 Ecolink Intelligent Technology | ITX Security Co. | Lowe's Companies | MD Security Solutions | Nest Labs (Google)
 Protect America | SecureNet | Skybell | Slomin's Inc. | Telular | Wal-Mart Canada | Zmodo Technology | Zonoff
 Akerman | Ammons Law | Baker Botts | BoyneClarke | Bryan Cave Leighton Paisner | Cooley | Cravath Swaine & Moore
 Duane Morris | Fish & Richardson | Greenberg Traurig | Hennessy & Roach | Hinton Andrews Kurth | Kilpatrick Townsend
 King & Spalding | Morgan Lewis & Bockius | Perkins Coie | Pillsbury Winthrop Shaw Pittman | Weil | WeirFoulds

Areas of Expertise:

Burglar Alarm Security Systems	Electronic Security System and Sensor Design – Wired and Wireless	New Product Development (NPD)
Wired, Wireless and Hybrid Security Alarm Systems and Sensors	Electronic Circuit Design (Analog, Digital and RF)	Product Research & Development
Intrusion Detection Systems	Embedded Controllers (CPU/MCU) (Zilog Z8/eZ8, Microchip PIC, etc.)	Electronic Product Design
Premise Monitoring Systems	Software Coding (Assembler / C)	Engineering Management
Smoke and Fire Alarm Systems	Circuit Simulations and Analysis	Speed to Market
Integrated Security Systems	Narrowband RF wireless (433Mhz)	End to End Product Design & Manufacturing
CCTV / Video Surveillance and Monitoring, Video Alarm Verification	Spread Spectrum (902 to 928 Mhz)	Design for Manufacturability
Audio Listen In, Intercom, Paging with Security System	Battery Charging and Protection (CC/CV, LiFePO4, Li-Poly, etc.)	Design for Reliability
Access Control with Security	Low voltage (control) systems	Cost Reduction Programs
Home Automation with Security	Alarm System Monitoring & Communications to Central Station	R&D Budget Optimization
Occupancy Detection Systems	Alarm Signaling Technology, Cellular, Land Line, Long Range RF, TCP/IP	Compliance & Agency Approvals
Alarm Control Panels, Intrusion Control Panels, Alarm System Controllers, Burglar/Fire/Access Control Panels	Security Network Protocols (AML, Wireless, Keybus, Combus)	Environmental Immunity (ESD/EFT)
Keypads, Zone Expanders, Wireless Rx/Tx, Output Modules, Sensors, Digital Dialers / Communicators	Personal Emergency Response Systems (P.E.R.S.)	Radiated & Conducted Immunity
Motion Detectors, PIR (Passive IR) Fresnel Lens, Mirror Optic and Microwave Doppler (X/K Band)	Telephone, Thermostat, X-10 (PLC) Interactive Interface with Security	False Alarm Immunity
Smoke Detectors, Heat Detectors	SOHO PBX Telephone Systems with Touch Tone & voice interface	Plastic Enclosure (Tooling) Design for Production Injection Molding
Door and Window Sensors	Glassbreak Detectors, Vibration and Shock Sensors	Mixed Mode ASIC Development
Smart Home / Home Automation		Electronic (Smart) Thermostats
		Solar Cell Charging Circuitry (MPPT)
		Energy Management Systems
		LED Driver & Control Circuitry
		Solar Powered LED Lighting (Patio to Street Level)

Industry Work Experience

- **Electronics R&D – New Product Development**
- **Electronic Security Systems and Sensors**

Consultant at Parker Security Consulting Inc.

www.psecon.com

June 2011 to Present

I founded Parker Security Consulting Inc. in June 2011 to provide technical consulting and expert witness services in the areas of Electronic Security Systems and Sensors, Electronics R&D, and New Product Development. Drawing on my 40+ years of industry experience, I have handled over 30 separate cases, including more than 12 Inter Partes Reviews (IPRs), 6 depositions, and 3 courtroom testimonies. My responsibilities also encompass the authoring of numerous expert reports and declarations. For a detailed breakdown of my Expert Witness / Consultant Experience, please refer to page 6 of this document.

President at EE-Systems Group Inc. Canada (R&D)

www.eesgi.com

August 2004 - 2014

I co-founded EE Systems Group Inc. in both Canada (for R&D) and the United States (Operations), taking on full management and executive responsibility. My oversight extended to new product and business development, where I spearheaded the creation of multiple new technologies and intellectual property. This led to the development, filing, and/or granting of multiple patents in the United States, Canada, China, and internationally.

I also defined and negotiated major corporate contracts with several organizations, resulting in numerous new products being developed and introduced to production. Among the notable achievements was the development and licensing of EE-SGI's "ePIR" software to several multinational companies, including Zilog, now part of Littelfuse, Inc., for passive infrared motion detection (marketed under the name "ZMOTION"). The ePIR / ZMOTION solution provides for both intrusion and occupancy detection.

Additionally, I developed the eFAR100 False Alarm Reduction module using embedded Z8 MCU technology with firmware written in assembler (machine code), and a full scalable suite of technology for solar-powered, motion-controlled, LED illumination ranging from patio to parking lot / street sizes.

My leadership in R&D also led to the successful completion of multiple SR&ED (Scientific Research and Experimental Development) applications, resulting in significant government financial grants being awarded to EE-SGI for true R&D work.

Vice President of Engineering at Tyco Security Products

Head of Engineering at Digital Security Controls (DSC) Limited

(Note: DSC was acquired by Tyco Security Products in December 2001)

www.tycosecurityproducts.com | www.DSC.com

March 1985 - December 2003 (~19 years)

DSC began in 1979 as a basement operation supplying alarm control panels to the Canadian market. I joined DSC in March 1985, shortly after the company moved out of the founder's basement and into a small industrial unit, marking its sixth year of operation. Over the course of nearly 19 years, I played a central role in transforming DSC into one of the three largest companies in its marketplace, with worldwide sales in over 120 countries.

As the Head of a 200+ member engineering department, I was responsible for all of DSC's research and product development efforts. My leadership extended to cross-functional responsibilities in Marketing, New Business Development, and Manufacturing, as well as the development of policies, procedures, and practices. I also managed financial planning, budget generation, corporate patent administration, key vendor relationships, and major customer interactions.

In addition to DSC's own engineering, I was also responsible for the engineering departments of the member companies of the DSC Group of Companies. At its pinnacle this group included Sur-Gard for Central Station Receivers, DeltaVision for CCTV equipment, Kantech for Access Control, Emerald Gateway for Automation, Secutron

for Fire Alarm Systems in North America, Bentel for Fire and Security in Europe, Safelink for Long Range RF and MCS Communications for Apartment Entry Systems.

I was principally involved in several corporate initiatives such as Six Sigma, ISO900X quality programs, speed to market, ethics training, and major cost reductions. My efforts in driving the corporate speed to market initiative resulted in an average product development cycle reduction of nearly 50%, cutting development time in half.

My technical contributions to DSC were substantial. I brought microcontroller and other advanced technologies to the company, developed the KEYBUS and COMBUS protocols for interconnecting components, and conceived and drove the development of over twelve mixed-mode ASICs (Application Specific Integrated Circuits) with a perfect track record of commercial success. Furthermore, I designed and taught a 10 lesson in-house course on assembly language (machine code) programming.

I also played a crucial role in saving DSC from a 15% shortfall in annual production due to a clerical error, using my relationship with a supplier's senior management to resolve a critical component shortage.

Prior to DSC's sale to TYCO, I re-negotiated agreements with key suppliers, resulting in annualized savings of over ten million dollars. I also worked directly with one of Latin America's premier telephone operators to rapidly produce functional prototypes, demonstrating my ability to respond swiftly to client needs.

DSC's growth, fueled by an optimum combination of product feature set, cost, and quality, culminated in its acquisition by TYCO in December 2001 for approximately \$400 million dollars. My extraordinarily successful career at DSC is a testament to my technical expertise, leadership acumen, and unwavering commitment to innovation and excellence.

Vice President of Engineering at Swinemaster Inc.

June 1984 – March 1985

During my tenure at Swinemaster Inc., I led a small R&D team in the development and construction of several working prototypes for an automated juvenile swine feeding machine. This innovative project required a multipart component design, utilizing up to 10 Zilog Z8 Microcontroller Units (MCU's), with the software meticulously developed in assembly language (machine code).

My responsibilities extended beyond the technical aspects of the project, as I also implemented field trials to test the functionality and efficiency of the feeding machine. Through careful observation and analysis, we refined the design to enhance its performance and reliability.

The project culminated in moderate commercial success, reflecting the dedication, expertise, and innovation that characterized our approach. My leadership and hands-on involvement in both the hardware and software components of the automated juvenile swine feeding machine played a crucial role in bringing this unique solution to the market.

Technical Sales Representative at Har-Tech Electronics Ltd.

January 1984 – June 1984

In my role as a Technical Sales Representative at Har-Tech Electronics Ltd., I served the greater Toronto area (GTA), providing both sales and technical support to customers and potential customers of electronic component manufacturers, including Zilog.

One of my notable achievements during this period was introducing the Z8 MCU to Digital Security Controls (DSC). This introduction was not merely a routine sales effort; it marked the beginning of a significant relationship between DSC and Zilog. My ability to recognize the potential synergy between the products and the needs of DSC led to a successful collaboration that ultimately resulted in DSC becoming Zilog's largest customer in Canada several years later.

My experience at Har-Tech Electronics Ltd. showcases my ability to bridge the gap between technical expertise and sales acumen, understanding the intricate details of electronic components, and translating that knowledge into tangible business opportunities.

Engineering Technologist at Thermetic Controls Limited

January 1983 – December 1983

During my time at Thermetic Controls Limited, I played a pivotal role in enhancing the efficiency and quality of the company's production processes. My responsibilities were multifaceted and included the design and implementation of production test equipment specifically for baseboard heater safety limit switches.

One of my significant contributions was the design and construction of a working prototype of a digital setback thermostat. This innovative device controlled electric baseboard heaters by synchronized pulse width modulation (PWM) of 240 VAC mains, showcasing my ability to apply advanced technical concepts to practical applications.

Furthermore, I designed, built, and implemented Automated Test Equipment (ATE) for quality control checks on production baseboard heater safety limit switches. This automation not only streamlined the testing process but also saved considerable time and effort over the previous manual implementation.

Publications and other Documentation

The Greek Philosopher Plato and ... False Alarms

Published in the National Burglar and Fire Alarm Association (NBFAA) trade journal on June 6, 2005. Click [here](#) for a PDF copy from my archives.

Over 25 Patents

Named as an inventor on over 25 patents, reflecting a prolific and innovative career in electronic security systems, sensors, and related technologies. See next page for further details.

Proprietary Engineering and Product Specifications

Authored and contributed to a wide array of proprietary engineering documents and product specifications, reflecting my expertise in electronic security systems and related technologies.

Product Manuals and Guides

Made numerous contributions to product manuals and guides, providing clear and concise information to facilitate user understanding and enhance product usability.

Education

Yorkville University

Formerly **RCC Institute of Technology** ([RCC](#))

Toronto, Ontario, Canada

1980 – 1982

Electronic Engineering Technology

Earned a diploma in Electronic Engineering Technology, a qualification roughly equivalent to a U.S. bachelor's degree. This program provided a comprehensive foundation in electronic engineering principles, equipping me with the skills and knowledge to excel in the field.

Northern Secondary School

Toronto, Ontario, Canada

1975 – 1979

Engaged in Electronics as part of the Shop class curriculum, fostering an early interest in the field.

Actively participated in the Electronics Club, where I honed my skills as a hobbyist and project builder. This hands-on experience laid the groundwork for my future career in electronic engineering.

James Parker's Patents by Priority Date (Listed as an Inventor)

- **Wireless Alarm System (1993)** 
 - A security system having a two-way wireless keypad which operates in a particular manner for improved operation...
- **Method and Arrangement for Recognition of a Coded Transmitted Signal (1994)** 
 - The present invention is for fast, reliable recognition of coded signals where the signal includes a predetermined...
- **Security System with Two Signal Reporting (1997)** 
 - A security system having two distinct channels of communication and which uses a single communication device...
- **Home Automation and Security System Controller (1997)** 
 - The present invention, in one aspect, is directed to a security system which is capable of acting as an information...
- **Controllable Still Frame Video Transmission System (1997)** 
 - A video capture controller for selective capture of video images from a plurality of video cameras, the capture...
- **Programmable Temperature Sensor for Security System (1998)** 
 - The present invention in one aspect, provides for a programmable temperature sensor for a device as part of a...
- **Suspended Code for Alarm System (1998)** 
 - The system generates alarm suspension codes without direct interaction with the alarm panel. The alarm control...
- **Biometric Input Device for Security System (1998)** 
 - The present invention provides for a biometric input device for a security system. The biometric input device includes...
- **Dual Mode Panel (1999)** 
 - A dual mode alarm control panel includes a sensing arrangement for determining conditions of the environment in...
- **Alarm System Using Local Data Channel (1999)** 
 - An alarm system has an alarm unit in combination with a line seize module. The alarm unit includes a transmitter /...
- **Alarm System with Programmable Device Control (2000)** 
 - An alarm system providing programmable remote control of electrically controlled devices, such as lights, is provided...
- **Security Alarm Keypad with Message Alert (2000)** 
 - A security alarm system is adapted to retrieve e-mail status information and provide an alert signal for the user of the...
- **Remote Recovery Arrangement for Alarm System (2000)** 
 - A security alarm system cooperates with a remote monitoring station to improve the reliability of the alarm system...
- **Security Alarm Keypad with Message Alert (2000)** 
 - A security alarm system is adapted to retrieve e-mail status information and provide an alert signal for the user of the...
- **Remote Recovery Arrangement for Alarm System (2000)** 
 - A security alarm system cooperates with a remote monitoring station to improve the reliability of the alarm system...
- **Alarm System with Programmable Device Control (2000)** 
 - An alarm system providing programmable remote control of electrically controlled devices, such as lights, is provided...
- **Integrated Lightning Detector (2003)** 
 - An alarm panel of a security system is additionally provided with an interference circuit for evaluating the possible...
- **False Alarm Reduction Method and System (2005)** 
 - A digital verification control, which is incorporated with an alarm system, includes a first timer device for presetting a...
- **Security Device with Built-In Intercommunicated False Alarm Reduction Control (2005)** 
 - A security device includes a plurality of security detectors intercommunicating with each other. Each of the security...
- **Integrated Detecting Processor (2005)** 
 - An infrared sensor includes an infrared generator for generating infrared radiation within a detecting area, a pyro...
- **Energy Signal Detection Device Containing Integrated Detecting Processor (2005)** 
 - An energy signal detection device includes a pyroelectric sensor sensing an infrared radiation within a detecting area...
- **Process and System of Energy Signal Detection (2006)** 
 - A process and system of energy signal detection, which improves sensitivity, performance and reliability thereof and...
- **Process and System of Power Saving Lighting (2007)** 
 - A process and system of lighting with green energy source and intelligent power management, which saves energy...
- **Process and System of Energy Signal Detection (2008)** 
 - A process and system of energy signal detection, which improves sensitivity, performance and reliability thereof and...
- **Single MCU-Based Motion Detection, Local Alarm and Supervisory Arrangement for Alarm System (2008)** 
 - A device with single MCU-based motion detection, local alarm and supervisory arrangement for alarm system...

Click on the respective  icon above to open a corresponding PDF copy of the patent.

Expert Witness / Consultant Experience *(in reverse chronological order)*

Dartmouth Apartment Fire – Class Action Litigation

Retained: 11/05/2024. Completed: 12/13/2024

Retained by **Mr. David G. Coles, K.C., of BOYNECLARKE Lawyers LLP** as an expert witness for a class action litigation concerning a significant apartment building fire located at 81 Primrose Street, Dartmouth, Nova Scotia, that occurred on May 19th, 2018. Conducted a detailed technical investigation of the building's fire alarm system records, including comprehensive compliance assessments with NBC 2015 and CAN/ULC standards. Identified critical deficiencies in system maintenance, alarm audibility, regulatory adherence, and management practices. Authored extensive expert report highlighting systemic failures and providing conclusive technical insights and opinions.

Inter Partes Reviews (IPR) of U.S. Patent 10,692,340

Filing Date: 03/29/2023. Termination Date: Pending

Patent Trial & Appeal Board. IPR2023-00792.

Retained by **Greenberg Traurig LLP**, representing the patent owner **Ecolink Intelligent Technology, Inc.** (a subsidiary of Universal Electronics Inc.) in the above IPR proceedings. Reviewed the above patent as well as all relevant documentation. Prepared an expert declaration as part of the patent owners' response. Deposed by counsel for the patent challenger **Roku Inc.** Status pending (awaiting PTAB).

Civil Litigation - David Wilson vs. Lydia Security Monitoring, Inc., d/b/a COPS Monitoring.

Retained: 08/20/2023. Completed: 12/20/2023.

U.S. District Court, 238th Judicial District, Midland County, Texas.

Cause No. CV57412

I was retained by the **Ammons Law Firm LLP** representing the plaintiff **David Wilson** in this civil litigation matter. The defendant, **Lydia Security Monitoring, Inc.**, doing business as **COPS Monitoring** operated a large central station that erroneously dispatched the police to the home of David Wilson leading to the unfortunate death of a police officer. This led to David Wilson being arrested, charged with, tried, and ultimately found not guilty of murder. The above civil matter came as a result of this. I reviewed all relevant documentation and generated an expert report with my opinions and conclusions. I prepared for, and was deposed by, the defendant's attorneys. This matter settled out of court a few weeks before the scheduled trial start date.

Inter Partes Reviews (IPRs) of U.S. Patents 10,281,183 and 10,739,051

Filing Date: 03/06/2023. Termination Date: 07/25/2023

Patent Trial & Appeal Board. IPR2023-00685 and IPR2023-00691.

Retained by **Volpe and Koenig PC**, representing the petitioner **Testo Inc.** Assisted in the preparation of two (2) IPR petitions. Assisted in the search, vetting and prioritization of prior art (anticipatory) and obviousness references. Generated comprehensive expert declarations and was heavily involved in the preparation and review of the finalized IPR Petitions. The patent challenger prevailed in both IPR petitions with favorable rulings from the PTAB.

Capital Murder Trial 3 - The State of Texas vs. Antonio Armstrong Jr.

Retained: 10/17/2016. Completed: 08/02/2023.

178th District Court for Harris County (Houston), Texas 77002

Retained by **Collings & Associates AAL** on behalf of the **Armstrong** family for the third trial of Antonio Armstrong Jr. following mistrials in the first and second trials. Analyzed new records requested and provided after the previous trial ended that pertained to the functionality or lack thereof the entry and exit door sensors at the homicide location. Provided proof that these door sensors produced erroneous results. Attended trial via ZOOM to observe states expert's testimony. Provided cometary and analysis to defendant's attorneys regarding states expert's testimony.

Technical Consulting – EarthCam Inc.

Retained: 02/10/2022. Status: Active.

Retained by **EarthCam Inc.** to provide specialized technical consulting and product evaluation expertise supporting new product development and system enhancements. Responsibilities include detailed analysis and evaluation of electronic components and subsystems for suitability, reliability, and compliance with EarthCam's rigorous operational standards. Authored comprehensive technical reports, including an extensive performance evaluation of the DROK 090603 DC-DC buck converter module. Conducted thorough electrical testing, efficiency assessments, ripple analysis, and thermal performance evaluations, ultimately providing expert recommendations on component suitability for EarthCam's requirements.

Civil Litigation - Chubb Insurance Company of Canada vs. a.p.i. ALARM Inc.

Retained: 01/27/2022. Completed: 06/02/2022.

I was retained by the law firm of **WeirFoulds LLP** representing the **Chubb Insurance Company of Canada** (the Plaintiff). Reviewed all relevant case material. Provided direction and documentation to support and prepare plaintiffs counsel for deposing representatives of the defendant, A.P.I Alarm Inc. Provided subject matter information as required.

Civil Litigation - Jewelers Mutual Ins. Co. vs. Shiver Security Systems Inc. and Action Security.

Retained: 11/23/2021. Completed: 03/31/2022.

U.S. District Court for the Southern District of Indiana (New Albany Division).

Case 4:20-CV-217-TWP-DML

The Jewelers Mutual Insurance Company, as subrogee of Koerber's Fine Jewelry, Inc., launched a civil suit to recover damages paid to Koerber's Fine Jewelry. The co-defendants in this suit were **Shiver Security Systems Inc.** and Action Security, LLC. I was retained by **Brownyard Claims Management Inc.**, represented by **Hennessy & Roach, P.C.** responsible for the defense of the UL (Underwriters Laboratories) certified monitoring station **Shiver Security Systems** only. I was not involved in the defense of Action Security, the alarm installation and maintenance provider for the UL Certificated Mercantile Burglar Alarm system installed at the Koerber's Fine Jewelry premises. Reviewed and analyzed all relevant documents, including the plaintiff's expert report, deposition transcripts of all involved, police records, UL standards, UL records and certificates, equipment manuals, service agreements, operating procedures, audit trails, activity reports, and the like. Generated detailed expert report. Deposed by plaintiff's counsel (Cozen O'Connor LLP). The end result was a favorable outcome for Shiver Security Systems as they were dropped from the suit.

Inter Partes Review (IPR) of U.S. Patent 10,325,159

Filing Date: 10/18/2021. Termination Date: 05/30/2023.

Patent Trial & Appeal Board. IPR2022-00071

Retained by **Pillsbury Winthrop Shaw Pittman LLP**, representing the petitioner **ADT LLC**. Reviewed patent chain file histories and assisted in the search, vetting and prioritization of prior art (anticipatory) and obviousness references. Actively involved in the preparation of the Petition. Generated Expert Declaration to accompany the petition filing. Deposed by opposing counsel (Maschoff Brennan LLP). Successful outcome for the petitioner ADT LLC as the PTAB invalidated U.S. Patent 10,325,159 patent in May of 2023.

Civil Litigation Preparatory Investigation – Wal-Mart Canada Corp. vs. McDonald's Canada

Retained: 05/28/2021. Completed 04/21/2022.

I was retained by the law firm of **WeirFoulds LLP** representing **Wal-Mart Canada Corp.** and the **AIG Insurance Company of Canada**. I was asked to provide expert analysis and commentary pertaining to aspects of the operation, or lack thereof, of the security camera system installed in a specific McDonalds restaurant located within a Wal-Mart retail facility. The McDonalds restaurant had suffered a probable arson event causing significant damage to the adjacent Wal-Mart location. Reviewed and analyzed case material and other relevant documentation. Performed additional in-depth research. Generated detailed expert report providing my opinions and conclusions.

Patent Infringement - Alertus Technologies, LLC v. Desktop Alert Inc. et al

Filing Date: January 17, 2020. Termination Date: September 28, 2020.

U.S. District Court District of Maryland (Greenbelt). Case 8:20-cv-00154. Patent: US 7,889,092

Retained by **Norris McLaughlin & Marcus PA**, representing the defendant **Desktop Alert Inc.**

Reviewed the patent in suit (US 7,889,092) as well as other relevant case material. Searched for and provided potential prior art (anticipatory) references. Case settled before trial.

Capital Murder Trial 2 - The State of Texas vs. Antonio Armstrong Jr.

Retained: 10/17/2016. Declared a Mistrial: 10/26/2022.

178th District Court for Harris County (Houston), Texas 77002

Retained by **Collings & Associates AAL**, on behalf of the **Armstrong** (defendant's) family for the second trial of Antonio Armstrong Jr. following a mistrial in the first trial. Analysed new records asked for and provided after first trial ended (in a mistrial) that pertained to the functionality or lack thereof the motion detectors at the homicide location. Provided proof that these motion detectors produced erroneous results. Attended trial in person to observe states alarm system expert's testimony. Prepared defendant's attorneys for (a very successful) cross examination of the state's alarm system expert. As with the first trial, this trial also ended with a hung jury and was declared a mistrial.

Patent Infringement - Portus Singapore Pte Ltd. et al v. AT&T Digital Life, Inc.

Filing Date: February 6, 2019. Termination Date: March 30, 2020

U.S. District Court for the Eastern District of TEXAS (Marshall). Case 2:19-cv-00044.

Retained by **Kilpatrick Townsend & Stockton, LLP**, representing the defendant **AT&T Digital Life**.

Reviewed patents in suit as well as numerous references. Reviewed and assisted in generation of multiple claim charts. Helped with claim language. Identified indefinite terms. Case settled before trial.

Patent Infringement - Axxess International, Inc. v. Genetec (USA) Inc.

Filing Date: August 20, 2018. Termination Date: July 27, 2020.

U.S. District Court for the District of Delaware (Wilmington). Case 1:18-cv-01276.

Retained by **Perkins Coie LLP**, representing the defendant **Genetec (USA) Inc.** Review and discussion of patent in suit via teleconference. Researched and searched for prior art candidates. Generated claim charts and related documentation. Case settled before trial.

Patent Infringement - Karamelion LLC v. AT&T Digital Life, Inc.

Filing Date: August 1, 2018. Termination Date: September 5, 2019.

U.S. District Court for the Eastern District of TEXAS (Marshall). Case 2:18-cv-00331.

Retained by **McKool Smith PC**, representing the defendant **AT&T Digital Life**. Reviewed patents in detail. Analyzed claim language and documented results. Case settled before trial.

Patent Infringement - Alarm.com Incorporated et al v Protect America, Inc.

Filing Date: June 22, 2018. Termination Date: December 18, 2019.

U.S. District Court for the Western District of Texas (Austin). Case 1:18-cv-00521.

Retained by **Honigman LLP**, representing the defendant **Protect America**. Reviewed multiple patents and file histories. Reviewed initial complaint and infringement contentions. Analysed material and provided opinion. Case settled before trial.

Patent Infringement - Iron Gate Security, Inc. v. Slomin's, Inc.

Filing Date: April 9, 2018. Termination Date: January 21, 2020.

U.S. District Court for the Eastern District of New York (Central Islip). Case 2:18-cv-02106.

Retained by **King & Spalding LLP**, representing the defendant **Slomin's, Inc.** Reviewed patent in suit. Qualified and/or searched for and prioritized prior art and/or obviousness material. Reviewed claim terms and identified incomplete and/or indefinite terms. Documented results. Case settled before trial.

International Arbitration Tribunal - Avigilon Technologies Corp. v. ITX Security Co., Ltd. et al.

Date Filed: 08/16/2017. Completed: 03/15/2018.

American Arbitration Association International Centre for Dispute Resolution. Case 01-17-0004-5750

Retained by the **Devlin Law Firm LLC**, representing the Korean based **ITX Security Company**.

Researched and reviewed numerous archival documents. Reviewed ITX's products in detail including schematics, source code, manuals, and other documentation. Prepared detailed report. Prepared for, attended, and testified (with cross) at a three-day hearing held before the International Arbitration Tribunal of the American Arbitration Association in Dallas Texas.

Patent Infringement - Wireless Monitoring Systems LLC v. AT&T Digital Life, Inc. et al

Date Filed: 6/14/2017. Terminated: 12/01/2017.

U.S. District Court for the Eastern District of Texas (Marshall). Case 2:17-cv-00501.

Retained by **Baker Botts LLP**, representing the defendant **AT&T Digital Life**. Reviewed both patents in detail as well as other relevant case material. Searched for and provided multiple prior art candidates. Reviewed potential for Inter Partes Reviews (IPR) . Provided additional technical support. Case settled before trial.

Inter Partes Review (IPR) of U.S. Patent 9,516,284

Date Retained: 04/05/2017. Completed 09/26/2017.

Patent Trial & Appeal Board. PTAB-IPR2017 (not filed – see below)

Retained by **Stratum Law LLC**, and then **Bryan Cave Leighton Paisner LLP** representing the petitioner **Skybell Technologies Incorporated**. Assisted in the search, vetting and prioritization of prior art and obviousness references. Prepared multiple claim charts. Provided definitions of key claim terms with supporting documentation. Generated draft declaration and claim charts. Inter Partes Review (IPR) petition not filed as related litigation matter settled out of court.

Patent Infringement - Eyetalk365, LLC v. Zmodo Technology Corporation, Ltd.

Date Filed: 11/14/2016. Terminated: 10/18/2017.

U.S. District Court for the Western District of North Carolina (Charlotte). Case 3:16-cv-789.

Retained by **Akerman LLP**, representing the defendant **Zmodo Technology Corporation**. Reviewed Zmodo's preliminary claim construction and invalidity contentions. Reviewed plaintiff's preliminary infringement contentions. Researched material as required. Produced declaration regarding the construction of several key claim terms. Case terminated before trial.

Capital Murder Trial 1 - The State of Texas vs. Antonio Armstrong Jr.

Retained: 10/17/2016. Declared a Mistrial: 4/26/2019.

178th District Court for Harris County (Houston), Texas 77002

Retained by **Collings & Associates AAL**, on behalf of the **Armstrong** (defendant's) family. Inspected the homicide location and the security system equipment located therein. Reviewed all pertinent records and documentation. Generated expert opinion. Testified in front of the judge and jury. Cross examined at length by Assistant District Attorney. Trial ended with a hung jury and was declared a mistrial.

Inter Partes Review (IPR) of U.S. Patent 8,473,619, U.S. Patent 8,478,844, and U.S. Patent 8,073,931

Date Filed: 9/30/2016. Terminated: 05/22/2017.

Patent Trial & Appeal Board. PTAB-IPR2016-01919, PTAB-IPR2016-01920, PTAB-IPR2016-01911, PTAB-IPR2016-01916 and PTAB-IPR2016-01909 (Total of Five (5) IPR petitions involving Three (3) patents).

Retained by **Cooley LLP**, representing the petitioner **SecureNet Technologies** to assist in the preparation of 5 IPR petitions covering 3 patents. Assisted in the search, vetting and prioritization of prior art and obviousness references. Generated comprehensive expert declarations for each petition and was heavily involved in the preparation and review of the finalized IPR Petitions.

Inter Partes Review (IPR) of U.S. Patent 7,864,983

Date Filed: 12/4/2015. Terminated: 06/06/2017.

Patent Trial & Appeal Board. PTAB-IPR2016-00285

Retained by **Freitas & Weinberg LLP**, representing the patent owner, **MD Security Solutions**. Reviewed and analyzed relevant material. Provided declaration regarding key technical points. Reviewed and critiqued patent owner's response to the PTAB. Deposed by attorneys for the petitioner, RPX Corporation. Received positive feedback from Freitas & Weinberg post deposition.

Patent Infringement - ICN Acquisitions LLC v. Zonoff, Inc.

Date Filed: 11/30/2015. Terminated: 11/6/2017.

U.S. District Court for the District of Delaware (Wilmington). Case 1:15-cv-01109.

Retained by **Morgan Lewis & Bockius LLP**, representing the defendant **Zonoff Inc**. Expediently researched prior art as per (then urgent) request. Reviewed specific claims of '736 and '385 patents in light of identified prior art. Provided opinion with supporting documentation. Advised on subject material and helped clarify technical matters. Case terminated before trial.

Patent Infringement - Iron Gate Security, Inc. v. Lowe's Companies, Inc.

Date Filed: 11/09/2015. Terminated: 11/1/2016.

U.S. District Court for the Southern District of New York (Foley Square). Case 1:15-cv-08814.

Retained by **Hunton & Williams** (now **Hunton Andrews Kurth**) **LLP**, representing the defendant Lowe's. Searched for, identified, and prioritized prior art and/or obviousness references on a claim-by-claim basis to determine optimum combination for the generation of an IPR (Inter Partes Review) petition. Prepared expert declaration. Reviewed and assisted with the preparation of the completed IPR Petition. The IPR Petition was not filed as the matter settled out of court.

Patent Infringement - Script Security Solutions, LLC v. AT&T Digital Life, Inc. et al

Date Filed: 3/13/2015. Terminated: 2/19/2016.

U.S. District Court for the Eastern District of TEXAS (Marshall). Case 2:15-cv-00370.

Retained by **Duane Morris LLP**, representing the defendant **AT&T Digital Life**. Reviewed case material. Provided multiple prior art candidates. Generated supporting (invalidity) claim charts. Case settled before trial.

Wrongful Death Civil Suit - C. Lewis-Harris et al v. Interstate Realty et al

Date Filed: 12/31/2014. Terminated: 08/26/2016.

U.S. Circuit Court for Jackson County, MO (Independence). Case 1416-cv-29921.

Retained by **Langdon and Emison AAL**, representing the Plaintiff (**C. Lewis-Harris & S. Payne**) in a Wrongful Death suit. Reviewed all case material. Performed in-depth onsite inspection and testing of the suspect equipment. Completed detailed analysis of equipment and relevant documentation. Formulated theory of failure mechanisms. Deposed by defendants' attorneys. Matter settled out of court with favorable settlement for plaintiff.

Patent Infringement - Secured Structures, LLC v. Alarm Security Group, LLC

Date Filed: 12/12/2014. Terminated: 9/26/2016.

U.S. District Court for the Eastern District of TEXAS (Tyler). Case 6:14-cv-00930.

Retained by the **Tadlock Law Firm**, representing the plaintiff **Secured Structures LLC**. Reviewed and analyzed relevant material as required. Assisted with claim construction matters. Prepared expert declaration. Provided technical expertise and support. Case settled before trial.

Patent Infringement - iControl Networks, Inc. v. Zonoff, Inc.

Date Filed: 9/16/2014. Terminated: 11/6/2017.

U.S. District Court for the District of Delaware (Wilmington). Case 1-14-cv-01199.

Retained by **Morgan Lewis & Bockius LLP**, representing the defendant **Zonoff Inc.** Reviewed the 6 patents in suit, interrogatories, responses, email correspondence, infringement charts, and other case related material. Specifically researched and dug up material on a pre-existing two-way RF (Radio Frequency) wireless system (prior art candidate). Discussed possible IPR strategy. Generated multiple claim charts in support of potential Inter Partes Reviews (IPRs). Assisted in claim language interpretation. Case terminated before trial.

Civil Litigation - Product Liability (Class Action) –**Controllable On-Site Protection Security Systems Inc v. Telular Corp.**

Date Filed: 08/20/2014. Terminated: 03/12/2018.

U.S. District Court for the Little Rock Division (Arkansas Eastern District). Case 4:14-cv-00487.

Retained by **Mitchell Williams PLLC**, representing the defendant **Telular Corporation** in a class action product liability suit. Reviewed the Telular product hardware and software as required. Interviewed Telular engineers and service technicians. Generated preliminary opinion regarding the Telular products in question. Case settled out of court.

Patent Infringement - Alarm.com Incorporated v. Telular Corporation

Date Filed: 05/20/2013. Terminated: 1/9/2014.

U.S. District Court for the District of Delaware (Wilmington). Case 1:13-cv-00890.

Retained by **Cravath, Swaine & Moore LLP**, representing the plaintiff **Alarm.com Inc.** Reviewed case material. Provided initial support; then this matter was put on hold pending the outcome of the following related matter.

Patent Infringement - iControl Networks, Inc. v. Alarm.com Incorporated et al

Date Filed: 05/20/2013. Terminated: 1/9/2014.

U.S. District Court for the Eastern District of Virginia - (Alexandria). Case 1:13-cv-00834.

Retained by **Cravath, Swaine & Moore LLP**, representing the defendant (and plaintiff) **Alarm.com Inc.** in this claim / counterclaim case (11 patents in suit). Prepared extensive expert report and related documents. Assisted in rebuttals of other sides expert reports. Performed both infringement and invalidity analysis. Provided multiple prior art candidates. Case timeframe highly accelerated. Trained extensively for deposition. Matter settled out of court.

Patent Infringement - Honeywell International, Inc. v. Nest Labs, Inc. (*Google) et al

Date Filed: 02/06/2012. Terminated: 5/6/2016.

U.S. District Court for the District of Minnesota (DMN). Case 0:12-cv-00299.

Retained by **Fish & Richardson PC**, representing the defendant ***Nest Labs**. Asked to analyze electronic schematics and determine the precise functionality of several key components. Performed comparative analyses. Generated an initial Expert Declaration in 2012 and then a follow up Expert Declaration in 2015. Case settled out of court. *Note: Google acquired Nest Labs during this litigation matter.

Patent Infringement - Honeywell International, Inc. v. 2GIG Technologies, Inc. et al

Date Filed: 11/24/2009. Terminated: 04/07/2011.

U.S. District Court for the Eastern District of New York (Central Islip). Case 2-09-cv-05156.

Retained by **Weil, Gotshal & Manges LLP**, representing the defendant **2GIG Technologies**. Provided expert reports, rebuttals, and support, including prior art candidates and other material as required. Case settled before trial.

*** End of File ***