

**UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE PATENT TRIAL AND APPEAL BOARD**

ROKU, INC.,
Petitioner,

v.

ECOLINK INTELLIGENT TECHNOLOGY, INC.,
Patent Owner.

Case IPR2023-00792
Patent No. 10,692,340

**DECLARATION OF JAMES PARKER
IN SUPPORT OF PATENT OWNER'S RESPONSE**

TABLE OF CONTENTS

I.	INTRODUCTION	1
A.	My Background, Qualifications, Publications, and Testimony	1
B.	Compensation.....	3
II.	SUMMARY OF MY OPINIONS	4
III.	LEGAL PRINCIPLES.....	4
A.	Legal Standard for Claim Construction	4
B.	Legal Standard for Obviousness	5
IV.	THE BASES FOR MY OPINIONS	7
V.	PERSON OF ORDINARY SKILL IN THE ART	7
VI.	THE BOARD’S INSTITUTION DECISION.....	9
VII.	OVERVIEW OF THE ‘340 PATENT AND THE CHALLENGED CLAIMS	10
VIII.	OVERVIEW OF THE ASSERTED PRIOR ART.....	16
A.	Lamb.....	17
B.	Williams	17
C.	Sharma.....	19
IX.	CLAIM CONSTRUCTION	21
A.	“[timed / first] alarm signal.”	21
1.	A “Status Signal” Is Not A “[timed / first] alarm signal.”.....	21
2.	Each Of A “Bypass Signal” And “A Signal That Causes An Alarm System To Be Disarmed” Is Not A “[timed / first] alarm signal.”	26
B.	“immediate alarm signal.”.....	30

X.	PETITIONER HAS FAILED TO MEET ITS BURDEN OF PROVING THAT THE CHALLENGED CLAIMS OF THE ‘340 PATENT ARE UNPATENTABLE.....	33
A.	Ground 1: Petitioner Has Failed To Show That Lamb In View Of Williams Renders Challenged Claims 1-2, 6, 11-12, And 16 Obvious.	33
1.	Petitioner Has Failed To Show That Lamb In View Of Williams Discloses, Teaches, Or Suggests Every Limitation Of Challenged Claims 1-2, 6, 11-12, And 16.	33
(a)	Petitioner Has Failed To Show That Lamb In View Of Williams Discloses Or Teaches “transmitting a timed alarm signal to a receiver associated with a security panel” (Claim 1), “processor-executable instructions that cause the barrier alarm device to: ... transmit, via the transmitter, the timed alarm signal to the receiver [associated with the security panel] only when it is determined that the human detection device indicates that the human being is inside the premises in proximity to the barrier” (Claim 1), And “transmitting by the barrier alarm device a timed alarm signal to the central security panel ... only when it is determined that the human detection device indicates that the human being is in inside the premises and in proximity to the barrier” (Claim 11) (Collectively, The “Timed Alarm Signal Limitations”).	33
(b)	Petitioner Has Failed To Show That Lamb Discloses “processor-executable instructions that causes the central security panel to: receive a first alarm signal from a barrier alarm device that monitors a barrier of a premises, the first alarm signal indicative of the barrier being opened” (Claim 6) And “receiving a first alarm signal from a barrier alarm device that monitors a barrier of a premises, the first alarm signal indicative of the barrier being opened” (Claim 16) (Collectively, The “First Alarm Signal Limitations”).	35
(c)	Petitioner Has Failed To Show That Lamb In View Of Williams Discloses Or Teaches “determine whether the	

	elapsed time has exceeded a predetermined time” And “generate a security response when it is determined that the elapsed time has exceeded the predetermined time.”	36
	(d) Petitioner Has Failed To Show That Lamb In View Of Williams Discloses “instructions that cause the barrier alarm device to transmit, via the transmitted, an immediate alarm signal” (Challenged Claim 2) And “transmitting by the barrier alarm device an immediate alarm signal” (Challenged Claim 12) (Collectively, The “Immediate Alarm Signal Limitations”).	39
2.	Petitioner And Mr. McNair Cannot Show That A POSITA Would Have Been Motivated To Modify Lamb In View Of Williams To Arrive At The Claimed Invention Of The ‘340 Patent.	40
3.	A POSITA Would Not Have Modified Lamb In View Of Williams As Petitioner And Mr. McNair Have Proposed.	47
	(a) The Sole Alleged Benefit Of Petitioner’s And Mr. McNair’s Proposed Modifications Is Outweighed By The Proposed Modifications’ Significant Drawbacks.....	47
	(b) Lamb And Williams Are Fundamentally Different.	54
	(c) Petitioner’s And Mr. McNair’s Proposed Modifications Would Change Lamb’s Basic Principle Of Operation. ..	57
	(d) Petitioner’s And Mr. McNair’s Proposed Modifications Would Frustrate Lamb’s Intended Purpose.....	59
B.	Ground 2: Petitioner Has Failed To Show That Sharma, Alone, Renders Challenged Claims 1 And 11 Obvious.....	60
XI.	CONCLUSIONS	62

I, James Parker, declare as follows:

I. INTRODUCTION

1. My name is James Parker. I have been retained by counsel for Patent Owner Ecolink Intelligent Technology, Inc. (“Patent Owner”) to provide my independent analysis regarding the patentability and validity of claims 1-2, 6, 11-12, and 16 (“Challenged Claims”) of U.S. Patent No. 10,692,340 (“the ‘340 patent”).

A. My Background, Qualifications, Publications, and Testimony

2. My background, qualifications, and educational and employment history are set forth in my curriculum vitae, which is attached hereto as **Exhibit 1**.

3. I earned a diploma in Electronic Engineering Technology from the Radio College of Canada, now RCC Institute of Technology, a Division of Yorkville University, in Toronto, Ontario, Canada in 1982.

4. I was an Engineering Technologist with Thermetic Controls Limited in 1983, a Technical Sales Representative at Har-Tech Electronics Ltd. in 1984, and Vice President of Engineering at Swinemaster Inc. from 1984 to 1985.

5. I was the Head of Engineering at Digital Security Controls (DSC) Limited starting in 1985. DSC designs and supplies alarm system control panels. 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. 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 December 2003.

6. I was the co-founder and President of EE-Systems Group Inc. (EE-SGI) Canada (R&D) from 2004–2014. I was responsible for new product development.

7. I am currently a consultant at Parker Security Consulting Inc. (PARSEC), which I founded to provide technical consulting and expert witness services in electronics research and development, new product development, electronic security systems, and other areas.

8. 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.

9. 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.

10. 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.

11. 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.

B. Compensation

12. My compensation in this case is \$325 per hour without regard to the outcome of this proceeding.

13. I am not, and never have been, an employee of Patent Owner. I am not receiving compensation for this declaration beyond my normal hourly fees based on my time actually spent analyzing and documenting my opinions herein on the '340 patent. My compensation is not related to the outcome of this proceeding, and I will not receive any additional compensation based on the outcome of any IPR or other proceeding involving the '340 patent.

II. SUMMARY OF MY OPINIONS

14. In summary, it is my opinion that each of the Challenged Claims of the ‘340 patent is patentable and valid. Petitioner and its expert, Mr. McNair, have failed to show that the Challenged Claims of the ‘340 patent are rendered obvious by the prior art under 35 U.S.C. § 103.

III. LEGAL PRINCIPLES

15. I will not offer opinions of the law, as I am not an attorney. However, patent counsel has informed me of several patent law principles, upon which I have relied to arrive at my conclusions.

A. Legal Standard for Claim Construction

16. It is my understanding that the purpose of the claim construction process is to determine the meaning of the terms in the Challenged Claims of the ‘340 patent to a person of ordinary skill in the art (“POSITA”) as of the time that the claimed invention was filed. I also understand that the words of the claims, the specification, and the prosecution history are to be primarily considered in order to construe the claims. These three sources are commonly referred to as “intrinsic evidence,” while everything else is referred to as “extrinsic evidence.”

17. It is my understanding that in an *Inter Partes* Review the words of a claim are generally given their ordinary and customary meaning to a POSITA as of the time that the patent application containing the claimed invention was filed.

18. It is my further understanding that the same words and phrases within a claim or claims are presumed to have the same meaning. It is also my understanding that different words and phrases within a claim or claims are presumed to have different meanings. Similarly, all words in a claim have meaning, and a word or phrase in a claim should not be interpreted so as to render other words or phrases in the claim superfluous.

19. It is also my understanding that a POSITA is deemed to read the claim term not only in the context of the particular claim in which the disputed term appears, but in the context of the entire patent, including the specification and the prosecution history.

B. Legal Standard for Obviousness

20. I understand that a patent claim may be unpatentable if the invention recited in the claim would have been obvious to a POSITA at the time the invention was made. In considering whether the Challenged Claims of the '340 patent are obvious, I have been asked to consider (a) the level of ordinary skill in the art at the time of the claimed invention, (b) the scope and content of the prior art, and (c) any differences between the prior art and the Challenged Claims of the '340 patent. I further understand that the patent owner may show "secondary factors" related to non-obviousness, including commercial success, long-felt but unresolved need, failure of others, copying, praise by others, and unexpected results.

21. I understand that a patent claim composed of several elements is not necessarily proved obvious merely by demonstrating that each of its elements was independently known in the prior art. I also understand that obviousness should not be analyzed using the benefit of hindsight. Instead, it must be analyzed from the standpoint of what was known and understood by a POSITA at the time of the claimed invention. I further understand that a party seeking to invalidate a patent claim as obvious must demonstrate that a POSITA would have had reason to combine the teachings of the prior art references to achieve the claimed invention, and that the POSITA would have had a reasonable expectation of success in doing so. I also understand that the party must persuasively explain how the references would be combined to arrive at the claimed invention. I understand that a proposed modification or combination is inappropriate for an obviousness inquiry when the modification or combination would change a prior art reference's basic principle of operation or would render the prior art reference inoperable for its intended purpose.

22. I understand that a reference qualifies as prior art for an obviousness determination only when it is analogous to the claimed invention. I understand that prior art is analogous if it is from the same field of endeavor or if it is reasonably pertinent to the particular problem the inventor is trying to solve.

IV. THE BASES FOR MY OPINIONS

23. I have reviewed the ‘340 patent, including the Challenged Claims and the prosecution history of the ‘340 patent. (EX1001 and EX1002).

24. I have also reviewed the Petition for *Inter Partes* Review filed by Petitioner Roku, Inc. (“Petitioner” or “Roku”), the attached Declaration of Bruce McNair (EX1003), the transcript of the deposition of Mr. McNair (EX2004), as well as the Exhibits attached to Roku’s Petition.

25. I have also reviewed the Board’s Institution Decision.

26. In forming my opinions, I have considered the materials listed above and any other documents cited in this declaration. I have also relied on my own education, knowledge, and experience in the relevant art.

27. I have also considered the understanding of a POSITA around the time of the invention of the Challenged Claims.

V. PERSON OF ORDINARY SKILL IN THE ART

28. I am informed that prior art and any opinions related to the prior art are to be analyzed from the perspective of a POSITA who would be involved in the same field as the ‘340 patent at the time of the invention of the Challenged Claims (*i.e.*, November 26, 2018).

29. All of the opinions that I express in this declaration have been made from the standpoint of a POSITA at the time of the invention of the Challenged Claims of the '340 patent.

30. I understand that Petitioner has proposed that a POSITA would have had a bachelor's degree in computer science, in electrical engineering, or a related field, and approximately two or more years of experience or equivalent study in sensor systems. (Petition at 12.)

31. I disagree with Petitioner's proposed definition of POSITA as it is inaccurate. The '340 patent states that the "present application relates to the field of home and business security." (EX1001, '340 patent, at 1:15-16; *see also* EX1003, McNair Declaration, ¶ 50 (Petitioner's expert stating that the field of endeavor of the '340 patent is "security and alarm systems").) Petitioner's definition of a POSITA, on the other hand, does not reference the appropriate field of art and encompasses individuals that have experience with: (i) only a single component of a security or alarm system; or (ii) sensor systems for any application. An individual with experience in sensor systems for speech recognition applications, for example, would not have been considered a POSITA with respect to the '340 patent. A sensor is merely one input or component of a security or alarm system.

32. It is my understanding that six factors may be considered when determining the level of ordinary skill in the art. The six factors are: (a) the education

level of the inventor; (b) the type of problems encountered in the art; (c) prior art solutions to those problems; (d) the rapidity with which innovations are made; (e) the sophistication of the technology; and (f) the education level of active workers in the field. I have used these factors in combination with the available information to determine the level of ordinary skill in the art.

33. I understand that a POSITA is presumed to possess the normal skills and technical knowledge of an individual focused on the particular problem that the claimed invention addresses. I further understand that a POSITA is presumed to have knowledge of all references that are sufficiently related to one another and to the pertinent art, and to have knowledge of arts pertinent to the particular problem that the claimed invention addresses.

34. I believe that a POSITA would have had at least a bachelor's or equivalent degree in electrical or electronic engineering or an equivalent field, and three or more years of commercial design and development experience in residential or business security and alarm systems.

35. As of the time of the invention of the Challenged Claims of the '340 patent, I qualified as a POSITA under both parties' definitions.

VI. THE BOARD'S INSTITUTION DECISION

36. I understand that the Board instituted review of the Challenged Claims of the '340 patent on two grounds: (1) alleged obviousness of claims 1-2, 6, 11-12,

and 16 over Lamb in view of Williams; and (2) alleged obviousness of claims 1 and 11 over Sharma alone.

VII. OVERVIEW OF THE ‘340 PATENT AND THE CHALLENGED CLAIMS

37. The ‘340 patent, entitled “Smart Barrier Alarm Device,” was issued on June 23, 2020 from U.S. Patent Application No. 16/200,172 (filed November 16, 2018). (EX1001, ‘340 patent, at [21], [22], [45], [54].)

38. The ‘340 patent and the Challenged Claims generally relate “to a barrier alarm device that helps reduce the occurrences of false alarms.” (*Id.* at 1:16-18.) According to the ‘340 patent, “[o]ne problem with [prior art] security systems is the relatively frequent occurrence of false alarms.” (*Id.* at 1:44-45.) “Often times, occupants forget that the security system is armed, and when they open a door or a window, a false alarm is triggered. These false alarms sometimes cause a response by police or fire personnel, wasting valuable public resources. ... Further, occupants are often startled if a local siren is triggered inside the home, because the siren is deliberately designed to be very loud.” (*Id.* at 1:49-57.) Thus, the ‘340 patent recognized the need for “a security system that allows occupants to open doors or windows while the security system is in an armed, ‘home’ mode of operation, without triggering an immediate, startling, audible alarm caused by a local siren.” (*Id.* at 1:58-62.)

39. The '340 patent created "a barrier alarm device" that comprises "a human detection device that detects the presence of a human being in proximity to the barrier alarm device, either inside or outside of monitored premises." (*Id.* at 4:7-10.) If a home's occupant "opens a monitored door or window while [the] security system is armed, an alarm will not immediately be triggered if the barrier alarm device senses the [occupant is] inside the structure in proximity to the barrier that was opened." (*Id.* at 4:11-16.) "Instead, a timed alarm signal is generated by the barrier alarm device and transmitted to a security panel which, in response, start[s] a countdown timer that allows a person to cancel a security response from occurring if a certain action is taken before the countdown timer expires." (*Id.* at 4:16-20.) "This new barrier alarm device operates on the principle that if a door or window is opened and a person is detected nearby the barrier alarm device on the inside of the premises, it is assumed that the person is authorized to be inside the premises, and a security response should not be immediately generated when the door or window is opened, allowing an authorized person time to cancel the security response." (*Id.* at 4:21-27.)

40. The '340 patent also created "a central security panel ... comprising a communication interface for receiving signals from a barrier alarm device..." (*Id.* at 2:22-24.) The central security panel "receive[s] a first alarm signal from [the] barrier alarm device ... indicative of [a] barrier being opened and that a human being

is inside the monitored premises and in proximity to the barrier...” (*Id.* at 2:28-32.)

In response to receiving the first alarm signal, the central security panel “begin[s] monitoring an elapsed time from when the first alarm signal was received...” (*Id.* at 2:33-34.) If the elapsed time exceeds a certain period of time, the central security panel “generate[s] a security response, and provide[s] the security response to a receiver via the communication interface.” (*Id.* at 2:34-39.)

41. Each of the Challenged Claims of the ‘340 patent is reproduced below:

1. A barrier alarm device, comprising:

a barrier status detection device for indicating that a barrier monitored by the barrier alarm device has been opened;

a human detection device for indicating that a human being is inside a premises in proximity to the barrier;

a transmitter for transmitting a timed alarm signal to a receiver associated with a security panel, the timed alarm signal for initiating a timer associated with the security panel;

a memory having processor-executable instructions stored thereon; and

a processor coupled to the barrier status detection device, the human detection device, the transmitter, and the memory, for executing the processor-executable instructions that cause the barrier alarm device to:

respond to the barrier status detection device indicating that the barrier has been opened by determining whether the human detection device indicates that the human being is inside the premises in proximity to the barrier; and

transmit, via the transmitter, the timed alarm signal to the receiver only when it is determined that the human detection device indicates that the human being is inside the premises in proximity to the barrier.

(*Id.* at claim 1.)

2. The barrier alarm of claim 1, wherein the processor-executable instructions further comprise instructions that cause the barrier alarm device to transmit, via the transmitter, an immediate alarm signal to the receiver for causing a security response to be initiated when it is determined that the human detection device does not indicate that the human being is inside the premises in proximity to the barrier.

(*Id.* at claim 2.)

6. A central security panel, comprising:

a communication interface for receiving signals from a barrier alarm device;

a memory for storing processor-executable instructions;
and

a processor coupled to the communication interface and the memory, for processing the processor-executable instructions that causes the central security panel to:

receive a first alarm signal from a barrier alarm device that monitors a barrier of a premises, the first alarm signal indicative of the barrier being opened;

respond to the first alarm signal by determining whether a human being has been indicated to be inside the premises and in proximity to the barrier;

begin a measuring of an elapsed time from when the first alarm signal was received when it is determined that the

human being has been indicated to be inside the premises in proximity to the barrier;

determine whether the elapsed time has exceeded a predetermined time;

generate a security response when it is determined that the elapsed time has exceeded the predetermined time; and

provide the generated security response to a receiver via the communication interface.

(*Id.* at claim 6.)

11. A method, comprising:

in response to a barrier status detection device associated with a barrier alarm device indicating that a barrier being monitored by the barrier alarm device has been opened, determining whether a human detection device associated with the barrier alarm device indicates that a human being is inside a premises monitored by a central security panel in proximity to the barrier; and

transmitting by the barrier alarm device a timed alarm signal to the central security panel for the purpose of initiating a timer associated with the central security panel only when it is determined that the human detection device indicates that the human being is in inside the premises and in proximity to the barrier.

(*Id.* at claim 11.)

12. The method of claim 11, further comprising transmitting by the barrier alarm device an immediate alarm signal to the central security panel for causing a security response to be initiated when it is determined that the human detection device does not indicate that the human being is in inside the premises and in proximity to the barrier.

(*Id.* at claim 12.)

16. A method performed by a central security panel, comprising:

receiving a first alarm signal from a barrier alarm device that monitors a barrier of a premises, the first alarm signal indicative of the barrier being opened;

responding to the first alarm signal by determining whether a human being has been indicated to be inside the premises in proximity to the barrier;

starting a countdown timer when it is determined that the human being has been indicated to be inside the premises in proximity to the barrier;

determining whether the countdown timer has expired;

in response to determining that the countdown timer has expired, generating a security response; and

providing the generated security response to a receiver via a communication interface.

(*Id.* at claim 16.)

42. Challenged Claims 1 and 11 of the '340 patent are directed to a barrier alarm device comprising a barrier status detection device and a human detection device. (*Id.* at claims 1 and 11.) When the barrier status detection device indicates that a barrier monitored by the barrier alarm device has been opened, the barrier alarm device responds by determining whether the human detection device indicates that a human being is inside the monitored premises in proximity to the barrier. (*Id.*) The barrier alarm device will transmit a timed alarm signal to a receiver associated

with a security panel only when it is determined that a human being is inside the premises in proximity to the barrier. (*Id.*)

43. Dependent Challenged Claims 2 and 12, which depend on Challenged Claims 1 and 11, respectively, specify that the barrier alarm device transmits an immediate alarm signal to the security panel when a barrier monitored by the barrier alarm device has been opened and a human has not been detected inside the premises in proximity to the barrier. (*Id.* at claims 2 and 12.)

44. Challenged Claims 6 and 16 of the ‘340 patent are directed to a central security panel comprising a communication interface for receiving signals from a barrier alarm device that monitors a barrier of the premises. (*Id.* at claims 6 and 16.) The central security panel receives a first alarm signal from the barrier alarm device indicating that a barrier of the premises has been opened, and responds to the first alarm signal by determining whether a human being has been indicated to be inside the premises in proximity to the barrier. (*Id.*) When a measured elapsed time exceeds a predetermined period of time (or, alternatively, when a countdown timer expires), the central security panel initiates a security response and provides the security response to a receiver via the communication interface. (*Id.*)

VIII. OVERVIEW OF THE ASSERTED PRIOR ART

45. I understand that Petitioner has asserted the following prior art references. These references are discussed in detail below:

Exhibit Number	Prior Art
1009	U.S. Patent App. Pub. No. 2016/0247370 (“Lamb”)
1010	U.S. Patent No. 6,057,764 (“Williams”)
1011	U.S. Patent No. 7,696,873 (“Sharma”)

A. Lamb

46. I have reviewed Lamb. Lamb is generally directed to a “barrier alarm device for reducing the number of false alarms that may occur in a home security system.” (EX1009, Lamb, at Abstract.) The “barrier alarm device, such as a door or window sensor, determines whether a barrier, such as a door or a window, has been opened, [and] determines whether a human being is in proximity to the door or window inside a monitored premises.” (*Id.*) If a door or window is opened and a person is detected near the barrier alarm device on the inside of the premises, the barrier alarm device assumes that the person is authorized to be inside the premises and either sends a bypass signal or does nothing. (*Id.*; *see also id.* at [0018].)

47. I understand that Petitioner does not contend that Lamb discloses or suggests “a timed alarm signal,” “measuring of an elapsed time from when [a] first alarm signal was received,” and “starting a countdown timer.” (Petition at 6.)

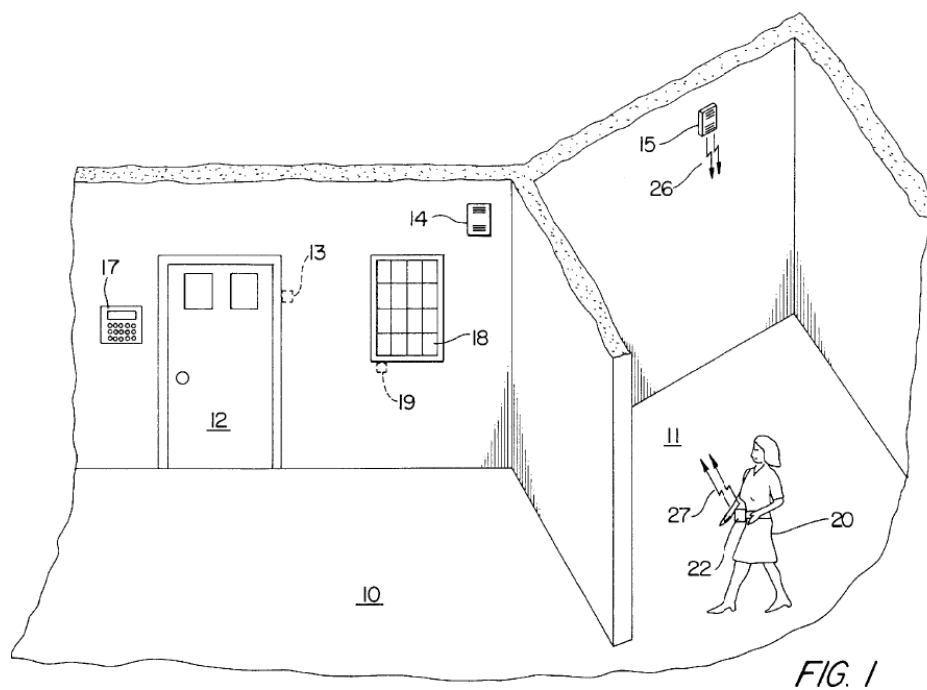
B. Williams

48. I have reviewed Williams. Williams is generally directed to “an alarm system [that] includes one or more motion detectors dispersed in diverse parts of a

secure space, each sensor having a receiver associated therewith.” (EX1010, Williams, at 1:54-57.) To “permit[] free utilization of the space by authorized persons and pets, while retaining security against intruders,” Williams devised a “portable device” to be worn by authorized users (including pets) “within the secure space when the alarm system is on.” (*Id.* at 1:44-53, 1:57-59, 2:25-38.) The “portable device” may be a badge, collar, bracelet, clip-on, etc. (*Id.* at 1:62-63, 2:25-34.)

49. According to Williams, “each activation of a motion detector causes a corresponding transceiver to inquire, by an electromagnetic transmission, whether or not there is an authorized user in the space.” (*Id.* at 1:64-67.) Assuming the motion detector is activated by an authorized person (or pet) carrying William’s “portable device,” the “portable device” responds to the electromagnetic inquiry by transmitting an “authorization code.” (*Id.* at 2:1-2, 2:25-31.) “[R]eceipt of an authorization code from one of the personal devices will negate treating the triggering of the motion detector as a violation of the secure space.” (*Id.* at 1:60-62.)

50. Figure 1 of Williams, which is reproduced below, illustrates “a pair of rooms in a house including an alarm system according to the present invention” (*id.* at 2:45-47):



(*Id.* at FIG. 1.)

51. As shown above, when motion detector 15 senses motion of person 20, “an interrogation by electromagnetic radiation or acoustic vibrations, as indicated by the arrows 26, will be received by the portable device 22.” (*Id.* at 3:9-13.) The portable device 22 “in turn will respond with electromagnetic radiation or acoustic vibrations in like kind with the transmission of the motion detector 15, the transmission from the device 22 including a code to authenticate the authority of the user to be within the secure space while the alarm is on.” (*Id.* at 3:13-18.)

C. Sharma

52. I have reviewed Sharma. Sharma is generally directed to a method and apparatus for automatically disarming a security system to prevent false alarms.

(EX1011, Sharma, at [54], 1:7-9.) Sharma's security system 100 includes door sensing units 104-108 configured to monitor doors 112-116, and window sensors 142 and 144 configured to monitor windows 156 and 158. (*Id.* at 3:1-20.) A first door sensing unit 104 has an RF transceiver 170, a door contact 172, a motion detector 174, a memory 173, and a processor 175. (*Id.* at 4:50-58.)

53. Sharma's security system 100 can be set to an "Armed Stay Mode" that protects the premises "from unwanted persons coming in from the outside while still allowing people to leave the facility without generating a false alarm." (*Id.* at 7:26-37.) In the "Armed Stay Mode," the motion detector 174 of the first door sensing unit 104 "monitors the area within the perimeter 140 proximate to the inside of the first door 112 for motion." (*Id.* at 7:47-49.) If the first door 112 is opened, the processor 175 of the first door sensing unit 104 "determines whether the motion detector 174 has detected motion within the perimeter 140." (*Id.* at 7:52-58.)

54. If motion is detected within the perimeter 140 when the first door 112 is opened, a "door open signal is not sent to the system control panel 102 and an alarm is not generated." (*Id.* at 8:1-5.) Instead, the system 100 "may enter a Timed Exit Mode for a predetermined amount of time" wherein the processor 175 of the first door sensing unit 104 "may ignore the door control signal and/or disable the door contact 172." (*Id.* at 8:10-15.) "The Timed Exit Mode allows people to leave

the house or facility without having to interact with the system 100.” (*Id.* at 8:19-21.)

55. Sharma’s Figure 5, which is reproduced below, is a flowchart illustrating the “Armed Stay Mode”:

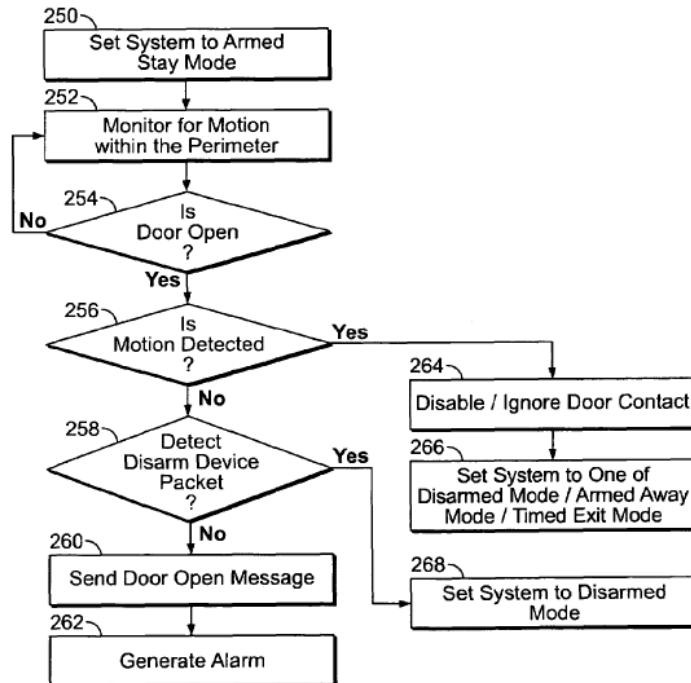


FIG. 5

(*Id.* at FIG. 5.)

IX. CLAIM CONSTRUCTION

A. “[timed / first] alarm signal.”

1. A “Status Signal” Is Not A “[timed / first] alarm signal.”

56. Each of the Challenged Claims of the ‘340 patent recites or requires an “alarm signal.” Challenged Claims 1 and 11 recite a “timed alarm signal,” and Challenged Claims 6 and 16 recite a “first alarm signal.” (EX1001, ‘340 patent, at

claims 1, 6, 11, 16.) I first address “time alarm signal” and “first alarm signal” and how those alarm signals differ from the signals that Petitioner and Mr. McNair contend meet them (*i.e.*, a status signal, bypass signal, and a signal that causes an alarm system to be disarmed).

57. I understand that Patent Owner asserts that a status signal is not a “[timed / first] alarm signal.” I agree with Patent Owner.

58. In the context of alarm and security systems, the plain and ordinary meaning of a status signal is a signal that indicates the state of a sensor (*e.g.*, motion detected). (*See, e.g.*, EX1001, ‘340 patent, at 8:60-64, 9:45-58.) I understand that Petitioner’s expert, Mr. McNair, agrees. (EX2004, McNair Transcript, at 106:2-18, 107:10-12.)

59. Consistent with the Challenged Claims, the specification, and the prosecution history of the ‘340 patent, a POSITA would not consider a status signal to be an alarm signal, and would not consider a status signal to be the “[timed / first] alarm signal.” A POSITA would understand that the “[timed / first] alarm signal” has a different meaning than a status signal.

60. First, the specification of the ‘340 patent supports that a POSITA would not consider a status signal to be the “[timed / first] alarm signal.” The specification distinguishes the “[timed / first] alarm signal” from a status signal. In one embodiment discussed in the ‘340 patent, the barrier alarm device “does not make

determinations as to when to transmit an alarm signal.” (EX1001, ‘340 patent, at 11:33-35.) Instead of transmitting an “alarm signal,” the barrier alarm device transmits to the security panel “a barrier status signal” and/or “a human status signal” when a change in the state of the barrier status detection device or the human detection device occurs, respectively. (*Id.* at 11:35-40.) The “barrier status signal” indicates whether the monitored barrier is open or closed, and the “human status signal” indicates whether a human is, or is not, detected in proximity to the monitored barrier. (*Id.* at 11:52-65; *see also id.* at 10:61-64.) The specification states that the security panel “receives these status signals and determines whether a local alarm condition exists and whether to transmit an alarm signal to one or more remote devices 406 of interested parties and/or to a remote monitoring station 124.” (*Id.* at 11:40-45; *see also id.* at 11:58-12:3.)

61. The specification of the ‘340 patent states that a “barrier alarm device” comprises a “barrier status detection device” and a “human detection device.” (EX1001, ‘340 patent, at FIGS. 5A and 10, 8:60-64, 9:45-10:21, 12:12-19, 12:64-67, 15:66-16:20, 16:54-63.) The specification further states that each of the “barrier status detection device” and “human detection device” send status signals (*i.e.*, signals indicating that a monitored barrier has been opened or that a human being is inside the premises in proximity to the barrier) to a processor in the “barrier alarm device.” (*Id.*) Depending on the status signals received from the “barrier status

detection device” and the “human detection device,” the “barrier alarm device” may respond by transmitting an “alarm signal” to a security panel. (*Id.*) The specification supports that a status signal is used by the “barrier alarm device” to determine whether to transmit an “alarm signal,” but a status signal is not an “alarm signal.” (*Id.*)

62. In another example discussed in the ‘340 patent, the specification states that rather than transmitting “an indication of an alarm condition being sensed” to the central security panel, the barrier alarm device instead transmits “raw data” to the central security panel from which the central security panel can determine “whether a local alarm condition has occurred” and generate one or more security responses. (EX1001, ‘340 patent, at 5:49-64.)

63. Second, the Challenged Claims support that a POSITA would not consider a status signal to be the “[timed / first] alarm signal.” The Challenged Claims distinguish the “[timed / first] alarm signal” from status signals. Challenged Claims 1 and 11 recite a “barrier alarm device” comprising a “barrier status detection device” and a “human detection device.” (EX1001, ‘340 patent, at claims 1, 11.) The “barrier status detection device” and the “human detection device” each send status signals (*i.e.*, signals indicating that a monitored barrier has been opened or that a human being is inside the premises in proximity to the barrier) to a processor in the “barrier alarm device.” (*Id.*) Depending on the status signals received from

the “barrier status detection device” and the “human detection device,” the “barrier alarm device” may respond by transmitting a “timed alarm signal” to a security panel. (*Id.*) The Challenged Claims also support that a status signal is used by the “barrier alarm device” to determine whether to transmit an “alarm signal,” but is not an “alarm signal.” (*Id.*)

64. Third, the prosecution history of the ‘340 patent supports that a POSITA would not consider a status signal to be the “[timed / first] alarm signal.” The prosecution history distinguishes the “[timed / first] alarm signal” from a status signal. U.S. Patent App. Pub. No. 2013/0257611 to Lamb et al. (“Lamb-611”), which is cited on the face of the ‘340 patent as prior art and was cited by the Examiner, distinguishes a “local alarm signal” from a “status message” or “raw data.” (EX2001, Lamb-611, at [0027], [0058], [0071]-[0072], [0102]-[0103], [0110].)

65. Lamb-611 discloses that, instead of transmitting a “local alarm signal,” the barrier alarm may alternatively transmit a “status message” or “raw data” to the central controller 116. (*Id.* at [0027], [0058], [0110].) The central controller 116 processes the “status message” or “raw data” to determine whether a local alarm condition exists. (*Id.*) Said differently, the central controller 116 uses the “status message” or the “raw data” to determine that a local alarm condition exists. (*Id.*) When a “local alarm signal” is sent, however, the central controller 116 need not

make this same determination because the “local alarm signal” itself indicates that a local alarm condition exists and instructs the central controller 116 to initiate a system alarm. (*Id.* at [0058], [0072], [0103], [0110].)

66. Fourth, the claims of U.S. Patent No. 9,940,797 (“the ‘797 patent”) and U.S. Patent No. 10,497,230 (“the ‘230 patent”), both of which are related to the ‘340 patent and are cited on the face of the ‘340 patent (*see* EX1001, ‘340 patent, at [60]), support that a POSITA would not consider a status signal to be a “[timed / first] alarm signal.”

67. The ‘797 patent claims an “alarm signal” and a “status signal” in different claims. (*Compare* EX1007, ‘797 patent, at claims 1-2, 4, 10-11, 13 *with id.* at claims 7, 16.) The ‘230 patent claims both an “alarm signal” and a “status signal” in the same claims. (*See* EX1005, ‘230 patent, at claims 8, 19; *see also id.* at claims 1-3, 5, 9, 12-14, 16.) The claims of the ‘797 and ‘230 patents confirm that a status signal and a “[timed / first] alarm signal” have different meanings.

2. Each Of A “Bypass Signal” And “A Signal That Causes An Alarm System To Be Disarmed” Is Not A “[timed / first] alarm signal.”

68. I understand that Patent Owner asserts that a bypass signal is not a “[timed / first] alarm signal.” I also understand that Patent Owner asserts that a signal that causes an alarm system to be disarmed is not a “[timed / first] alarm signal.” I agree with Patent Owner.

69. In the context of alarm and security systems, the plain and ordinary meaning of a bypass signal is an instruction to ignore future alarm signals or barrier status signals generated by a barrier alarm device. (*See, e.g.*, EX1001, ‘340 patent, at 8:20-25.)

70. I understand that Mr. McNair has provided a similar definition of the term “bypass signal.” (EX2004, McNair Transcript, at 116:12-17, 119:16-120:4, 127:15-17.)

71. In the context of alarm and security systems, the plain and ordinary meaning of “a signal that causes an alarm system to be disarmed” is exactly what the term describes.

72. I understand that Mr. McNair has provided a similar definition of the term “a signal that causes an alarm system to be disarmed.” (EX2004, McNair Transcript, at 127:18-128:1, 129:4-11.)

73. Consistent with the Challenged Claims, the specification, and the prosecution history of the ‘340 patent, a POSITA would not consider each of, a bypass signal, and a signal that causes an alarm system to be disarmed, to be the “[timed / first] alarm signal.” A POSITA would understand that the “[timed / first] alarm signal” has a different meaning than (i) a bypass signal; and (ii) a signal that causes an alarm system to be disarmed.

74. First, the specification of the ‘340 patent supports that a POSITA would not consider each of, a bypass signal, and a signal that causes an alarm system to be disarmed, to be the “[timed / first] alarm signal.” The specification of the ‘340 patent distinguishes the “[timed / first] alarm signal” from a signal that instructs to ignore an alarm signal or that disarms the alarm system. (EX1001, ‘340 patent, at 8:15-26, 10:53-61, 11:23-35, 12:58-63, 13:29-34, 13:45-61, FIGS. 5A-B.)

75. The specification of the ‘340 patent also teaches that the purpose of an “alarm signal” is to instruct the security panel to initiate a security response (*e.g.*, an audible alert). (EX1001, ‘340 patent, at Abstract, 2:28-39, 2:50-59, 4:10-20, 6:2-10, 16:64-17:4, 17:8-51, 21:13-35.) When a “timed alarm signal” is transmitted, a security response will be initiated if the alarm system is not disarmed within a predetermined time. (*Id.* at 17:8-34.) The specification of the ‘340 patent states that an “alarm signal” will not be sent when an authorized person opens a monitored barrier to prevent a false alarm from occurring. (*Id.* at 8:4-20, 10:53-59, 11:23-28, 12:58-63, 13:41-45.) The specification of the ‘340 patent supports that a signal that instructs to ignore an alarm signal or that disarms the alarm system is not the “[timed / first] alarm signal” because a signal that instructs to ignore an alarm signal or that disarms the alarm system does not instruct a security response to be initiated (and, in fact, prevents a security response from being initiated).

76. Second, the Challenged Claims support that a POSITA would not consider each of, a bypass signal, and a signal that causes an alarm system to be disarmed, to be the “[timed / first] alarm signal.” Challenged Claims 2, 6, 12, and 16 teach that the “alarm signal” instructs the security panel to initiate a security response. (EX1001, ‘340 patent, at claims 2 and 12 (“an immediate alarm signal ... for causing a security response to be initiated”); *id.* at claims 6 and 16 (“receiv[e/ing] a first alarm signal ... generat[e/ing] a security response”).) The Challenged Claims of the ‘340 patent support that a signal that instructs to ignore an alarm signal or that disarms the alarm system is not the “[timed / first] alarm signal” because a signal that that instructs to ignore an alarm signal or that disarms the alarm system does not instruct a security response to be initiated (and, in fact, prevents a security response from being initiated).

77. Third, the prosecution history of the ‘340 patent supports that a POSITA would not consider each of, a bypass signal, and a signal that causes an alarm system to be disarmed, to be the “[timed / first] alarm signal.” Lamb-611, which is cited on the face of the ‘340 patent as prior art cited by the Examiner, distinguishes transmitting a “local alarm signal” from placing the alarm system in a “bypass mode.” (EX2001, Lamb-611, at [0058]-[0059], [0064], [0072]-[0075], [0077], [0092], [0103]-[0105], [0107]-[0111].) When a “local alarm signal” is transmitted the system will, for example, sound an audible alarm. (*Id.*) When the

alarm system is placed in “bypass mode,” on the other hand, the alarm system will temporarily ignore local alarm signals. (*Id.*)

78. Fourth, the claims of the related ‘797 and ‘230 patents support that a POSITA would not consider each of a bypass signal and a signal that causes the alarm system to be disarmed to be the “[timed /first] alarm signal.” The ‘797 patent claims both an “alarm signal” and a “bypass signal” in the same claims. (EX1007, ‘797 patent, at claims 1, 10; *see also id.* at claims 2, 4, 11, 13.) Likewise, the ‘230 patent claims both an “alarm signal” and a “bypass signal” in the same claims. (EX1005, ‘230 patent, at claims 2, 13; *see also id.* at claims 1, 12.) The claims of the ‘797 and ‘230 patents further confirm that a bypass signal and a “[timed / first] alarm signal” have different meanings.

B. “immediate alarm signal.”

79. Challenged Claims 2 and 12 each recite transmitting “an immediate alarm signal.” (EX1001, ‘340 patent, at claims 2, 12.) In view of the specification and the Challenged Claims of the ‘340 patent, the plain and ordinary meaning of the term “immediate alarm signal” is an alarm signal that instructs the security panel to initiate a security response immediately. (*Id.* at 17:46-51 (“At block 1024, central security panel 116 receives the immediate alarm signal via receiver 906 from barrier alarm device 600 and, in response, immediately initiates one or more security responses, as described above, i.e., within 5 seconds, or some other short time period

on the order of seconds, of receipt of the immediate alarm signal.”); *see also id.* at 19:58-61, 26:65-27:2; *id.* at claims 1-2, 11-12 (distinguishing a “timed alarm signal,” which instructs the security panel to initiate a security response after a predetermined period of time, from an “immediate alarm signal,” which instructs the security panel to initiate a security response immediately).)

80. I understand that the Board preliminarily held that an “immediate alarm signal” could be an alarm signal that is transmitted immediately after the determinations that a barrier has been opened and that a person is not near the barrier. I disagree with the Board’s preliminary construction as it is inconsistent with the Challenged Claims and the specification of the ‘340 patent.

81. First, the Board’s preliminary construction of “immediate alarm signal” is inconsistent with the Challenged Claims. None of the Challenged Claims specify or require any particular amount of time to elapse between when the claimed determinations are made and when the “alarm signals” are transmitted. (EX1001, ‘340 patent, at claims 1-2, 6, 11-12, 16.) The Challenged Claims do not preclude the “timed alarm signal” or the “first alarm signal” from being transmitted immediately after the preceding determinations. (*Id.*) Practically speaking, it would make no sense to delay the transmission of the claimed “timed alarm signal” or the claimed “first alarm signal.”

82. The Challenged Claims also use the terms “timed alarm signal” and “immediate alarm signal” to distinguish how the security panel reacts to the received alarm signal, not to specify the amount of time that must elapse between when the claimed determinations are made and when the claimed alarm signals are transmitted. (EX1001, ‘340 patent, at claims 1-2, 11-12.)

83. Second, the Board’s preliminary construction of “immediate alarm signal” is inconsistent with the specification of the ‘340 patent. The specification of the ‘340 patent uses the terms “immediate” and “immediate alarm signal” to specify when a security response should be initiated (*i.e.*, immediately). (*See, e.g.*, EX1001, ‘340 patent, at FIG. 11B, 1:58-62, 4:21-33, 17:35-51, 18:47-51, 18:58-19:9, 19:55-61, 20:17-28, 20:61-21:4, 21:19-22, 24:41-44, 25:10-14, 25:39-41, 26:50-27:11.) On the other hand, the specification never states that an “immediate alarm signal” is an alarm signal that is transmitted immediately. (*Id.*) The specification also does not contain any disclosure regarding how much time elapses between when the determination(s) that a barrier has been opened and/or that a person is (or is not) near the barrier are made and when a “[timed / first / immediate] alarm signal” is transmitted. (*Id.*)

X. PETITIONER HAS FAILED TO MEET ITS BURDEN OF PROVING THAT THE CHALLENGED CLAIMS OF THE ‘340 PATENT ARE UNPATENTABLE

A. Ground 1: Petitioner Has Failed To Show That Lamb In View Of Williams Renders Challenged Claims 1-2, 6, 11-12, And 16 Obvious.

1. Petitioner Has Failed To Show That Lamb In View Of Williams Discloses, Teaches, Or Suggests Every Limitation Of Challenged Claims 1-2, 6, 11-12, And 16.

- (a) Petitioner Has Failed To Show That Lamb In View Of Williams Discloses Or Teaches “transmitting a timed alarm signal to a receiver associated with a security panel” (Claim 1), “processor-executable instructions that cause the barrier alarm device to: ... transmit, via the transmitter, the timed alarm signal to the receiver [associated with the security panel] only when it is determined that the human detection device indicates that the human being is inside the premises in proximity to the barrier” (Claim 1), And “transmitting by the barrier alarm device a timed alarm signal to the central security panel ... only when it is determined that the human detection device indicates that the human being is in inside the premises and in proximity to the barrier” (Claim 11) (Collectively, The “Timed Alarm Signal Limitations”).**

84. Challenged Claims 1 and 11 recite that the barrier alarm device transmits a “timed alarm signal” to a security panel. (EX1001, ‘340 patent, at claims 1, 11.) The barrier alarm device must transmit the “timed alarm signal” to a security panel only when it is determined that the human detection device indicates that the human being is inside the premises in proximity to the barrier. (*Id.*)

85. I understand that Petitioner and Mr. McNair do not assert that Lamb discloses or teaches a “timed alarm signal.” (Petition at 28; EX1003, McNair Declaration, ¶¶ 65, 69.) I also understand that Petitioner does not assert that Lamb discloses or teaches a “timed alarm signal.” (Petition at 6.) I further understand that Petitioner and Mr. McNair assert that “a POSITA would have been motivated to modify Lamb to transmit a timed alarm signal for initiating a timer when the barrier alarm device detects that the barrier has been opened and that a human is inside the premises, as taught by Williams.” (Petition at 28; *id.* at 41 (same); *see also id.* at 29 (“Williams discloses a transmitter for transmitting a timed alarm signal to a receiver associated with a security panel”); *id.* at 41 (“Williams discloses transmitting the timed alarm signal to the receiver”); EX1003, McNair Declaration, ¶¶ 52, 69.)

86. As discussed above, a status signal is not the “timed alarm signal.” Mr. McNair agrees that a status signal is not an “alarm signal.” (EX2004, McNair Transcript, at 110:19-111:13, 112:6-113:5, 126:1-6.) Petitioner and Mr. McNair have failed to show that the alleged “timed alarm signal” in Williams is anything more than a status signal. (*See, generally*, Petition at 28-34, 41-42; EX1003, McNair Declaration, ¶¶ 66, 69-71, 83, 85-86.)

87. Petitioner and Mr. McNair rely on Williams’ Figures 2 and 2A and their corresponding disclosures as teaching the claimed “timed alarm signal.” (Petition at 29-33; EX1003, McNair Declaration, ¶ 71.) Williams’ Figure 2 discloses a “test 34”

that “determines if the corresponding motion detector has detected motion.” (EX1010, Williams, at 3:56-58; *see also id.* at FIG. 2.) “[I]f motion has been detected, an affirmative result of test 34 will reach a step 38 to set the motion latch...” (*Id.* at 3:61-62.) “Then, a step 39 causes an inquiry signal to be transmitted” and “a step 41 initializes a timer.” (*Id.* at 3:64-4:3.)

88. In Williams, to the extent any signal is transmitted to the control panel in response test 34, this signal is nothing more than a signal indicating that motion has been detected (*i.e.*, a status signal). (EX1010, Williams, at FIG. 2, 3:56-62.) As shown in Williams’ Figure 2, test 34 simply asks whether motion has been detected. (*Id.* at FIG. 2.) If motion is detected, then a timer is initialized in step 41. (*Id.*)

(b) Petitioner Has Failed To Show That Lamb Discloses “processor-executable instructions that causes the central security panel to: receive a first alarm signal from a barrier alarm device that monitors a barrier of a premises, the first alarm signal indicative of the barrier being opened” (Claim 6) And “receiving a first alarm signal from a barrier alarm device that monitors a barrier of a premises, the first alarm signal indicative of the barrier being opened” (Claim 16) (Collectively, The “First Alarm Signal Limitations”).

89. Challenged Claims 6 and 16 recite that the claimed central security panel receives a “first alarm signal” from a barrier alarm device. (EX1001, ‘340 patent, at claims 6, 16.)

90. Petitioner and Mr. McNair assert that Lamb’s central security panel receives a “barrier status signal” from a barrier alarm device. (Petition at 47;

EX1003, McNair Declaration, ¶¶ 105-106.) Petitioner and Mr. McNair assert that Lamb’s “barrier status signal” is the “first alarm signal.” (Petition at 46-47; EX1003, McNair Declaration, ¶¶ 105-106.)

91. As discussed above, a status signal is not the “first alarm signal.” Mr. McNair agrees that a status signal is not an “alarm signal.” (EX2004, McNair Transcript, at 110:19-111:13, 112:6-113:5, 126:1-6.)

92. The claims, specification, and prosecution history of the ‘340 patent expressly distinguish a “barrier status signal” from an “alarm signal.” (*See, e.g.*, EX1001, ‘340 patent, at 11:33-12:3.) Similarly, Lamb distinguishes a “barrier status signal” from an “alarm signal.” (EX1009, Lamb, at [0043], claim 19.)

93. Because a “barrier status signal” is not the “first alarm signal,” Petitioner and Mr. McNair cannot show that Lamb discloses the claimed “first alarm signal” of Challenged Claims 6 and 16.

(c) Petitioner Has Failed To Show That Lamb In View Of Williams Discloses Or Teaches “determine whether the elapsed time has exceeded a predetermined time” And “generate a security response when it is determined that the elapsed time has exceeded the predetermined time.”

94. Challenged Claim 6 recites a central security panel that: (i) begins measuring an elapsed time from when a first alarm signal was received; (ii) determines whether the elapsed time has exceeded a predetermined time; and (iii)

generates a security response when it is determined that the elapsed time has exceeded the predetermined time. (EX1001, ‘340 patent, at claim 6.)

95. Petitioner and Mr. McNair do not assert that Lamb discloses or teaches a central security panel that begins measuring an elapsed time or determines whether an elapsed time has exceeded a predetermined time. (Petition at 6, 48-49; EX1003, McNair Declaration, ¶ 111.)

96. Petitioner and Mr. McNair assert that “Williams discloses that a countdown timer is initialized upon determination of a potential alarm ... and so discloses the control panel processor configured to begin measuring an elapsed time.” (Petition at 49; EX1003, McNair Declaration, ¶ 114.) Petitioner and Mr. McNair also assert that “Williams discloses that a ‘time-out of the timer’ or ‘timer timeout’ is determined.” (Petition at 51; EX1003, McNair Declaration, ¶ 119.) Petitioner and Mr. McNair propose combining Lamb with Williams’ “countdown timer” and assert that this proposed combination teaches the limitations of Challenged Claim 6. (Petition at 49-53; EX1003, McNair Declaration, ¶¶ 118, 121.)

97. Petitioner and Mr. McNair cannot show that Lamb in view of Williams discloses or teaches “determine whether the elapsed time has exceeded a predetermined time” and “generate a security response when it is determined that the elapsed time has exceeded the predetermined time” because Williams does not

disclose determining that an elapsed time has exceeded a predetermined time, as Challenged Claim 6 requires.

98. Williams discloses a countdown timer “to establish a period of time (perhaps a second or fraction thereof) within which an authorized response [to an inquiry signal] must be received.” (EX1010, Williams, at FIGS. 2-2A, 3:64-4:3.) “[I]f no response is received prior to time-out of the timer,” an alarm latch will be set. (*Id.* at 4:32-36; *see also id.* at 4:4-8, FIGS. 2-2A.)

99. Assuming Williams’ countdown timer measures an elapsed time, the measured elapsed time never exceeds the predetermined time. Rather, the measured elapsed time will always be less than or equal to the predetermined time.

100. In Williams, if the predetermined time is set to a second, Williams’ countdown timer, once initiated, begins counting down from one second. (EX1010, Williams, at 4:32-36; *see also id.* at 3:64-4:8, FIGS. 2-2A.) Williams’ countdown timer, like all countdown timers, stops measuring the elapsed time when the timer times-out (*i.e.*, reaches zero). (*Id.*) Countdown timers do not continue to measure elapsed time beyond the timer reaching zero, and I am unaware of any evidence that Williams’ countdown timer operates differently. The measured elapsed time in Williams’ countdown timer is at most equal to the predetermined time.

101. I also note that while Challenged Claim 6 recites “begin a measuring of an elapsed time” and “determin[ing] whether the elapsed time has exceeded a

predetermined time,” Challenged Claim 16 recites “starting a countdown timer” and “determining whether the countdown timer has expired.” (EX1001, ‘340 patent, at claims 6, 16.) The different claim language used in Challenged Claims 6 and 16 further supports that Williams does not determine whether an elapsed time has exceeded a predetermined time. At most, Williams determines whether its countdown timer has expired.

(d) Petitioner Has Failed To Show That Lamb In View Of Williams Discloses “instructions that cause the barrier alarm device to transmit, via the transmitted, an immediate alarm signal” (Challenged Claim 2) And “transmitting by the barrier alarm device an immediate alarm signal” (Challenged Claim 12) (Collectively, The “Immediate Alarm Signal Limitations”).

102. Challenged Claims 2 and 12 recite that the “barrier alarm device” must transmit an “immediate alarm signal” to the claimed “security panel.” (EX1001, ‘340 patent, at claims 2, 12.)

103. Petitioner and Mr. McNair assert that Lamb discloses a barrier alarm device that sends an “alarm signal” to a central security panel 116 when the barrier alarm device determines that a door is open and that a human is not inside the premises in proximity to the door. (Petition at 42-43; EX1003, McNair Declaration, ¶¶ 88-90.)

104. As discussed above, the claims and specification of the ‘340 patent support that an “immediate alarm signal” is an alarm signal that instructs a security

response to be initiated “immediately.” (*See, e.g.*, EX1001, ‘340 patent, at 17:46-51, 26:65-27:2.) Mr. McNair agrees that an “immediate alarm signal” is an alarm signal that instructs a security response to be initiated “immediately.” (EX2004, McNair Transcript, at 151:2-7; *id.* at 52:4-15, 130:6-18, 147:13-22.)

105. Petitioner and Mr. McNair fail to explain how Lamb’s “alarm signal” is an “immediate alarm signal” (*i.e.*, an alarm signal that instructs a security response to be initiated “immediately”). (Petition at 42-43; EX1003, McNair Declaration, ¶¶ 88-90.) Petitioner and Mr. McNair have failed to show that Lamb discloses the Immediate Alarm Signal Limitations.

2. Petitioner And Mr. McNair Cannot Show That A POSITA Would Have Been Motivated To Modify Lamb In View Of Williams To Arrive At The Claimed Invention Of The ‘340 Patent.

106. I understand that Petitioner and Mr. McNair have proposed modifying Lamb in view of Williams in three ways.

107. First, Petitioner and Mr. McNair have proposed modifying Lamb’s barrier alarm device to transmit a “timed alarm signal” to a security panel, as allegedly taught in Williams. (Petition at 17, 28, 41; EX1003, McNair Declaration, ¶¶ 52-54.)

108. Second, Petitioner and Mr. McNair have proposed modifying Lamb’s security panel to initialize a countdown timer, as allegedly taught in Williams. (Petition at 28, 49, 51-53; EX1003, McNair Declaration, ¶¶ 69-71, 113.)

109. Third, Petitioner and Mr. McNair have proposed modifying Lamb’s system to include Williams’ user-worn “personal device” that transmits an authorization code. (Petition at 17-18; *id.* at 19 (“A POSITA would have had a reasonable expectation of success modifying Lamb’s system to authenticate a potential alarm, via a timer and a device configured to transmit an authentication code, as taught by Williams.”); EX1003, McNair Declaration, ¶¶ 52-54.) I note that the Challenged Claims do not recite a “personal device” or anything similar to Williams’ “personal device.” (EX1001, ‘340 patent, at claims 1-2, 6, 11-12, and 16.)

110. Petitioner and Mr. McNair have identified only one reason why a POSITA would have modified Lamb in view of Williams. That reason is to “enhance security” by verifying that a potential alarm is indeed caused by an authorized person, and not an unauthorized person. (Petition at 17-18, 28, 41, 49 (citing EX1010, Williams, at 2:35-38); EX1003, McNair Declaration, ¶¶ 52-53.)

111. Petitioner and Mr. McNair cannot explain why a POSITA would have been motivated to modify Lamb in view of Williams in the specific manner of the claimed invention of the ‘340 patent for at least two reasons.

112. First, each of Challenged Claims 1-2 and 11-12 recites or requires (i) responding to a barrier status detection device indicating that a barrier has been opened by determining whether a human detection device indicates that a human

being is inside the premises in proximity to the barrier; and (ii) transmitting a timed alarm signal to a security panel only when it is determined that the human detection device indicates that the human being is inside the premises in proximity to the barrier. (EX1001, ‘340 patent, at claims 1-2, 11-12.) Challenged Claims 6 and 16 also recite a security panel that responds to a first alarm signal indicative of a barrier being opened by determining whether a human being has been indicated to be inside the premises in proximity to the barrier. (*Id.* at claims 6, 16.)

113. In *Lamb*, the purpose of the human detection device and the step of determining whether a human being is inside the premises in proximity to the barrier is to verify that an authorized person has opened the barrier. (EX1009, *Lamb*, at Abstract, FIG. 5, [0018], [0029]; *see also id.* at [0037], [0040]-[0043], [0050].) If a barrier is opened and a human is detected inside the premises in proximity to the barrier, *Lamb* assumes the person that opened the barrier is authorized to be inside the premises. (*Id.*)

114. In Petitioner’s and Mr. McNair’s proposed modifications to *Lamb*, however, Petitioner and Mr. McNair assert that a “device configured to transmit an authentication code” (*i.e.*, Williams’ “personal device”) is used to verify that an authorized person has opened a barrier. (EX1010, Williams, at 1:6-10, 1:54-62, 3:64-4:3; Petition at 18-19, 28, 41, 49; EX1003, McNair Declaration, ¶¶ 52-54.)

115. In Petitioner’s and Mr. McNair’s proposed modifications to Lamb, the “device configured to transmit an authentication code” (*i.e.*, Williams’ “personal device”) performs the exact same function as Lamb’s human detection device and Lamb’s step of determining whether a human being is inside the premises in proximity to the barrier: *i.e.*, verifying that an authorized person has opened a barrier. The only difference, according to Petitioner and Mr. McNair, is that the “device configured to transmit an authentication code” “actually verif[ies] authorization,” while Lamb is “simply making an assumption about the person” using the human detection device and the step of determining whether a human being is inside the premises in proximity to the barrier. (Petition at 18; EX1003, McNair Declaration, ¶ 53.)

116. In Petitioner’s and Mr. McNair’s proposed modifications to Lamb, Lamb’s human detection device and Lamb’s step of determining whether a human being is inside the premises in proximity to the barrier are rendered superfluous, redundant, and unnecessary, as the “device configured to transmit an authentication code” performs the same function of verifying that an authorized person has opened a barrier in an allegedly better way.

117. Even assuming a POSITA would have been motivated to modify Lamb in view of Williams in the first place, a POSITA would have eliminated Lamb’s superfluous, redundant, and unnecessary human detection device and step of

determining whether a human being is inside the premises in proximity to the barrier. By doing so, a POSITA would have significantly reduced the cost, complexity, and processing requirements of Lamb's modified system while providing practically the same functionality as Lamb's unmodified system. There is simply no reason why a POSITA would have retained Lamb's human detection device and Lamb's step of determining whether a human being is inside the premises in proximity to the barrier in Lamb's modified system.

118. Eliminating Lamb's superfluous human detection device and step of determining whether a human being is inside the premises, which is what a POSITA would have done if a POSITA were to modify Lamb in view of Williams as Petitioner and Mr. McNair propose, would not have resulted in the claimed invention of the '340 patent, as each of the Challenged Claims recites or requires a human detection device and/or determining whether a human is inside the premises in proximity to the barrier. (EX1001, '340 patent, at claims 1-2, 6, 11-12, 16.)

119. Second, each of Challenged Claims 1-2 and 11-12 recites or requires transmitting a "timed alarm signal" from a barrier alarm device to a security panel for the purpose of initiating a timer associated with the security panel. (EX1001, '340 patent, at claims 1-2, 11-12.) Challenged Claims 6 and 16 also recite a security panel that, in response to receiving a "first alarm signal" from a barrier alarm device,

“begin[s] a measuring of an elapsed time” or “start[s] a countdown timer,” respectively. (*Id.* at claims 6, 16.)

120. Petitioner’s and Mr. McNair’s sole proposed rationale for modifying Lamb (*i.e.*, to enhance security by verifying that a potential alarm was caused by an authorized person) is not logically connected to Petitioner’s and Mr. McNair’s proposed modifications to Lamb that are relevant to the Challenged Claims (*i.e.*, modifying Lamb’s barrier alarm device to transmit a “timed alarm signal” to a security panel and modifying Lamb’s security panel to initialize a timer).

121. Williams allegedly verifies that detected motion was caused by an authorized person using a user-worn “personal device 22” that transmits an authorization code. (EX1010, Williams, at 1:6-10, 1:54-2:38.) Williams does not use a timer to verify that a potential alarm was caused by an authorized person. (*Id.*) While Petitioner’s sole proposed rationale for modifying Lamb in view of Williams may be relevant to incorporating Williams’ user-worn “personal device,” such a device is not a claimed feature of the Challenged Claims. (*See generally* EX1001, ‘340 patent, at claims 1-2, 6, 11-12, and 16.)

122. Williams also discloses several alternatives to transmitting a signal from a motion detector to a security panel that causes a timer in the security panel to be initiated.

123. Williams discloses that each motion detector may itself interrogate the “personal device” and initiate its own timer whenever motion is detected. (EX1010, Williams, at FIG. 2, 1:54-67, 3:24-26, 3:67-4:3.)

124. Williams also discloses that, rather than transmitting a signal from a motion detector that causes a timer to be initiated, the “personal device” can instead transmit an authorization code periodically to bypass the motion detectors. (EX1010, Williams, at Abstract, 2:3-8, 2:25-34, 6:23-53, 7:59-63, 8:21-39.) In this embodiment, the transmission of an authorization code from the “personal device,” not a signal from a motion detector, causes a timer to be initiated. (*Id.*)

125. Petitioner and Mr. McNair do not explain why the goal of verifying that a potential alarm is caused by an authorized person, a goal that each of Williams’ embodiments accomplishes, would have led a POSITA to select the particular embodiment that Petitioner and Mr. McNair have applied to Lamb. Williams discloses that the embodiment where the “personal device” periodically transmits an authorization code is “much simpler” (EX1010, Williams, at 6:23-26, 7:64-65, 8:33-39), yet Petitioner and Mr. McNair completely ignore this embodiment.

3. A POSITA Would Not Have Modified Lamb In View Of Williams As Petitioner And Mr. McNair Have Proposed.

(a) The Sole Alleged Benefit Of Petitioner's And Mr. McNair's Proposed Modifications Is Outweighed By The Proposed Modifications' Significant Drawbacks.

126. A POSITA would not have modified Lamb in view of Williams as Petitioner and Mr. McNair have proposed because the sole alleged benefit of Petitioner's and Mr. McNair's proposed modifications to Lamb (*i.e.*, "enhanced security") is outweighed by the proposed modifications' significant drawbacks.

127. Petitioner and Mr. McNair have identified only one alleged benefit of their proposed modifications to Lamb (*i.e.*, "enhanced security" by only negating a potential alarm when an authorized person is detected). (Petition at 17-18; EX1003, McNair Declaration, ¶¶ 52-53.)

128. While Petitioner and Mr. McNair reproduce quotations from Williams to attempt to show that Williams provides "greater security" (Petition at 18 (citing EX1010, Williams, at 2:31-38, 5:63-66); EX1003, McNair Declaration, ¶ 53), Petitioner's and Mr. McNair's reliance on these quotations is misplaced.

129. Williams discloses that its system provides greater security than: (i) prior art systems that did not have a way to prevent false alarms in an armed stay mode (*i.e.*, where the system is armed while the premises are occupied), and (ii) prior art systems that used a "smart badge" that transmits ID numbers for tracking the whereabouts of personnel in a facility. (EX1010, Williams, at 1:13-53.) Lamb's

system does not fit into either of these categories because Lamb's system (i) does address preventing false alarms in an armed stay mode; and (ii) Lamb's system does not use a "smart badge." (EX1009, Lamb, at Abstract, [0002], [0005]-[0007].) Petitioner's and Mr. McNair's quotations from Williams do not demonstrate that their proposed modifications would "enhance security" in Lamb's system.

130. Petitioner and Mr. McNair also assert that Williams actually verifies that a potential alarm was triggered by an authorized person, while Lamb is "simply making an assumption about the person." (Petition at 18; EX1003, McNair Declaration, ¶ 53.) Petitioner and Mr. McNair are wrong. Williams is also making an assumption (*i.e.*, that a barrier was opened by an authorized person if Williams' "personal device" is present). (EX1010, Williams, at Abstract, 1:46-2:3, 2:25-38.)

131. Williams' assumption is not fool proof. If, for example, the user leaves his or her "personal device" in a room (or if a pet with the "personal device" is in or near the room) and an intruder opens a door or window to the room, Williams will incorrectly assume that the door or window was opened by an authorized person due to the presence of the "personal device" in (or near) the room.

132. Meanwhile, Lamb's assumption (*i.e.*, that if a barrier is opened and a person is detected inside the premises in proximity to the barrier it is assumed that the person is authorized to be inside the premises) is reasonable and makes sense. When an intruder attempts to enter a premises by opening a barrier, Lamb will

correctly generate an alarm because the intruder is not yet inside the premises. (EX1009, Lamb, at FIG. 5, [0021], [0029], [0037].)

133. Petitioner and Mr. McNair have failed to show that the proposed modifications to Lamb would provide any benefit. On the other hand, the proposed modifications to Lamb have numerous drawbacks, which I discuss in detail below.

134. One drawback of the proposed modifications is that the user must wear, or carry around with them, Williams' "personal device" when the user is inside the premises while the system is armed. Users would have found the need to carry around a "personal device" in their own home to be a major inconvenience, particular where the vast majority of security and alarm systems do not require the user to carry such a "personal device."

135. Another drawback is that if the user forgets or loses his or her "personal device," or if the "personal device" is broken or is not working properly, undesirable false alarms will result. Further exacerbating this issue is the fact that a user typically places his or her alarm system into the armed stay mode at night when he or she is tired or sleeping. A person is generally more forgetful when he or she is tired, which further increases the likelihood that the user will forget his or her "personal device" when he or she goes to open a door or window. Even if an instruction or warning to remember the "personal device" is included in the device instructions and/or on the

device itself, this will not (and cannot) prevent a user from forgetting or losing the “personal device.”

136. At the very least, a false alarm is an inconvenience. At worst, a false alarm could cause a real alarm to be incorrectly treated as a false alarm. (EX1010, Williams, at 1:29-35.) Even worse still, if a “personal device” is stolen, an intruder could enter a premises with no alarm being triggered at all.

137. Williams also does not take into account visitors and guests. To work properly, each visitor or guest would need to be provided with his or her own “personal device.” But visitors and guests, due to their lack of familiarity with the alarm system, are more likely to misplace or forget their “personal device.” The need for an increased number of “personal devices” in a household increases the likelihood that a “personal device” will be lost, stolen, or left somewhere it should not be (*e.g.*, in a monitored room).

138. Williams discloses that its “personal device” is: (i) an active device; or (ii) a passive RFID device. (EX1010, Williams, at 1:67-2:10, 6:18-22.) Each device type has its own technical and practical downsides.

139. An active device actively receives and sends signals (*e.g.*, radio frequency (“RF”) signals or acoustic signals). The process of actively receiving and sending signals consumes more power compared to passive devices, which do not require internal power sources for operation. The need for an internal power source

in an active device means that active devices are larger and heavier than passive devices, and thus even more of an inconvenience for the user to carry. The need for an internal power source also means that the “personal device” will not work (and a false alarm will be triggered) if the “personal device” runs out of battery power.

140. Implementing a system that relies on active communication for security purposes is also technologically complex. This complexity would translate into higher costs for development, production, and maintenance of the component devices, making such a system less practical, especially for widespread consumer applications. For example, the need for active transmission and reception by the “personal device” would lead to issues with signal interference and range limitations, both of which would negatively impact user convenience and system reliability.

141. An active “personal device” also must continuously be ready to receive an inquiry signal and to transmit an authorization code in response, which contributes to higher power consumption. The requirement that the active “personal device” function as both a transmitter and receiver impacts its battery life. Ensuring sufficient battery life in such a device would necessitate either larger, higher-capacity batteries, or more frequent re-charging or replacement of the batteries. Either case would affect user convenience and the practicality of the device and system.

142. A device with larger batteries must in turn be larger and heavier, which is very inconvenient and undesirable for a user to carry around. A device that requires frequent re-charging or replacement of the batteries places a greater burden on the user to prevent the device from running out of battery power, and thus increases the likelihood that the user will accidentally let the device die or will leave the device on the charging stand (both of which would lead to increased false alarms).

143. An active “personal device”-based system would also require a transceiver to be placed in every monitored room to transmit an inquiry signal and to receive a response from the “personal device” when a barrier is opened. (EX1010, Williams, at 3:24-29.) Transceivers are relatively expensive and have greater power requirements than a receiver (or transmitter) alone. The need for numerous transceivers in a premises, and to have each transceiver communicate with the central security panel, would increase the cost and complexity of the resulting system. Such a system would also require FCC approval.

144. The passive RFID version of Williams’ “personal device” is simply not feasible. Passive RFID technology inherently suffers from limited read ranges. Typically, passive RFID systems can be read from only a few centimeters or inches away from the reader. This limitation stems from the fact that passive RFID tags rely on the reader’s signal for power, which significantly restricts their operational

range. The limited range would be impractically short and would be a critical drawback in security applications where broader coverage is necessary to ensure seamless and convenient access control within larger spaces.

145. Notwithstanding the extremely limited range of passive RFID tags, a passive RFID-based security system would also require a higher density of readers, installed at numerous points within a premises (*i.e.*, at every barrier to be monitored). The overall system cost would increase due to the need for more RFID readers to be installed in a given area (as opposed to one transceiver per room in a system that uses active “personal devices”). This not only increases the initial setup cost but also the complexity and maintenance expenses over time.

146. The reliability of passive RFID systems can also be detrimentally affected by environmental factors and physical obstacles. Metals and liquids, for example, can interfere with RFID signals, leading to potential issues in detecting the “personal device” consistently. In a security context, where reliability is paramount, interference issues could result in unauthorized access or, conversely, prevent legitimate access due to failed detections. The inconsistency in performance as a result of certain environmental conditions poses a significant challenge.

147. In view of the numerous drawbacks to Petitioner’s and Mr. McNair’s proposed modifications to Lamb, and the fact that Petitioner and Mr. McNair have failed to show that the proposed modifications to Lamb would provide any benefit,

a POSITA would not have modified Lamb in view of Williams as Petitioner and Mr. McNair have proposed.

(b) Lamb And Williams Are Fundamentally Different.

148. A POSITA would not have modified Lamb in view of Williams as Petitioner and Mr. McNair have proposed because Lamb's and Williams' systems are fundamentally different.

149. First, Lamb's and Williams' systems operate in fundamentally different ways. Lamb discloses a barrier alarm device that receives and processes two device inputs (*i.e.*, inputs from a human detection device and a barrier status detection device) and responds in different ways depending on the two received inputs. (EX1009, Lamb, at FIG. 5, [0030], [0033]-[0035].) When the barrier alarm device receives and processes a signal indicating that a barrier (*e.g.*, a window) has been opened, the barrier alarm device will process a signal received from the human detection device to determine whether a human being is inside the premises in proximity to the barrier. (*Id.* at FIG. 5, [0037].) If a human being is determined to be inside the premises in proximity to the barrier, the barrier alarm device will either do nothing or will transmit a bypass signal to the security panel. (*Id.* at [0038], [0040].) If, however, a human being is not determined to be inside the premises in proximity to the barrier, the barrier alarm device will transmit an alarm signal to the security panel. (*Id.* at [0037], [0041].)

150. Williams, on the other hand, discloses an alarm system that comprises alarm switches (13, 19), motion detectors (14, 15), and a control panel (17). (EX1010, Williams, at FIG. 1, 2:66-3:6.) In Williams, each activation of an alarm switch or motion detector will cause an inquiry signal to be transmitted to determine if there is an authorized personal device in the space. (*Id.* at FIG. 2, 1:64-2:3, 3:9-24, 3:34-38, 3:60-67.) Unlike Lamb’s barrier alarm device, Williams’ alarm system does not receive and process two device inputs and respond in different ways depending on the two received device inputs. Rather, Williams’ alarm system responds to a single device input (*i.e.*, any activation of an alarm switch or motion detector) in the same way (*i.e.*, by transmitting an inquiry signal). (*Id.*)

151. Lamb also discloses a barrier alarm device that “operates on the principle that if a door or window is opened and a person is detected nearby the barrier alarm device on the inside of the premises, it is assumed that the person is authorized to be inside the premises, and an alarm signal should not be generated when the door or window is opened.” (EX1009, Lamb, at [0018]; *see also id.* at [0029].) In Lamb’s system, an authorized user does not need to do anything to prevent false alarms because the system will automatically refrain from sending an alarm signal (or will send a bypass signal) when a door or window is accidentally opened. (*Id.*)

152. In Williams’ system, on the other hand, a user must wear a “personal device 22” to prevent a false alarm from being triggered. (EX1010, Williams, at 1:54-2:10, 2:25-34.) If, for example, the user forgets to wear the “personal device 22” or the “personal device 22” runs out of battery power, then there is nothing to prevent a false alarm from being triggered. (*Id.*)

153. Second, Lamb’s and Williams’ systems operate under fundamentally different assumptions. Lamb discloses that its “barrier alarm device operates on the principle that if a door or window is opened and a person is detected nearby the barrier alarm device on the inside of the premises, it is assumed that the person is authorized to be inside the premises, and an alarm signal should not be generated when the door or window is opened.” (EX1009, Lamb, at [0018]; *see also id.* at [0029].)

154. Williams, on the other hand, discloses that any movement inside the premises is treated as a potential alarm. (EX1010, Williams, at 1:64-2:3, 3:9-38.) Lamb’s system thus operates under the assumption that motion detected inside a premises is indicative of a person authorized to be inside the premises, while Williams’ system operates under the assumption that any motion detected inside a premises is indicative of a person that is unauthorized to be inside the premises unless and until a “personal device 22” indicates otherwise. (EX1009, Lamb, at [0018], [0029]; EX1010, Williams, at 1:64-2:3, 3:9-38.)

155. Third, Lamb’s and Williams’ systems are intended to accomplish fundamentally different goals. Lamb expressly discloses that its goal is to provide “a barrier alarm device that helps reduce the occurrences of false alarms.” (EX1009, Lamb, at [0002].) Williams, on the other hand, discloses that its goal is to provide “significantly greater security.” (EX1010, Williams, at 1:46-53.)

156. Williams’ goal of providing “greater security” directly conflicts with Lamb’s goal of reducing false alarms. It was well known that attempts to “increase the security” of an alarm system, whether successful or not, typically resulted in an increased occurrence of false alarms.

157. Neither Petitioner nor Mr. McNair make any attempt to address (let alone rectify) Lamb’s and Williams’ fundamental differences. A POSITA would not have modified Lamb in view of Williams in view of the references’ significant, fundamental differences.

(c) Petitioner’s And Mr. McNair’s Proposed Modifications Would Change Lamb’s Basic Principle Of Operation.

158. A POSITA would not have modified Lamb in view of Williams as Petitioner and Mr. McNair have proposed because Petitioner’s and Mr. McNair’s proposed modifications to Lamb would change Lamb’s basic principle of operation.

159. Lamb discloses that its barrier alarm device “operates on the principle that if a door or window is opened and a person is detected nearby the barrier alarm

device on the inside of the premises, it is assumed that the person is authorized to be inside the premises, and an alarm signal should not be generated when the door or window is opened.” (EX1009, Lamb, at [0018]; *see also id.* at [0029].) That is, Lamb’s system assumes that motion detected inside a premises is indicative of a person authorized to be inside the premises. (*Id.*) A user of Lamb’s system does not need to do anything to prevent false alarms—the system will automatically refrain from sending an alarm signal (or will send a bypass signal) when a door or window is accidentally opened. (*Id.*)

160. Williams’ system, on the other hand, operates on the principle that any motion detected inside a premises is indicative of a person that is unauthorized to be inside the premises. (EX1010, Williams, at 1:64-2:3, 3:9-38.) Unlike Lamb’s system, a user of Williams’ system must wear a “personal device 22” to prevent a false alarm from being triggered. (*Id.* at 1:54-2:10, 2:25-34.) If Williams’ user forgets to wear the “personal device 22,” or if the “personal device 22” runs out of battery power, then there is nothing to prevent a false alarm from being triggered. (*Id.*)

161. Petitioner’s and Mr. McNair’s proposed modifications to Lamb, which incorporate Williams’ user-worn “personal device” that transmits an authorization code to negate potential alarms, would fundamentally alter Lamb’s basic principles of operation in two ways.

162. First, the proposed modifications would change Lamb from a system that operates on the principle that motion detected inside a premises is indicative of an authorized person to a system that operates on the principle that motion detected inside the premises is indicative of an unauthorized person. (EX1009, Lamb, at [0018], [0029]; EX1010, Williams, at 1:54-2:10, 2:25-34, 3:9-38.)

163. Second, the proposed modifications would change Lamb's system from one where the user does not need to do anything to prevent false alarms to one where the user must wear a "personal device" to prevent false alarms.

164. A POSITA would not have been motivated to modify Lamb in ways that would fundamentally alter its basic principles of operation, particularly in view of the numerous drawbacks of the proposed modifications discussed above.

(d) Petitioner's And Mr. McNair's Proposed Modifications Would Frustrate Lamb's Intended Purpose.

165. A POSITA would not have modified Lamb in view of Williams as Petitioner and Mr. McNair have proposed because Petitioner's and Mr. McNair's proposed modifications to Lamb would frustrate Lamb's intended purpose.

166. Lamb's intended purpose is to provide "a barrier alarm device that helps reduce the occurrences of false alarms." (EX1009, Lamb, at [0002].) In Lamb, the user does not need to do anything to prevent false alarms because Lamb's system

automatically refrains from sending an alarm signal (or will send a bypass signal) when a door or window is accidentally opened. (*Id.* at [0018], [0029].)

167. In the proposed modifications to Lamb the user must have in his or her possession Williams’ “personal device” to prevent false alarms. (Petition at 17-19; EX1010, Williams, at 1:54-2:10, 2:25-34.) A POSITA would have recognized that introducing Williams’ “personal device” into Lamb would increase the number of false alarms because a false alarm would occur, for example, every time the user forgets the “personal device,” or if the “personal device” runs out of battery power, breaks, or is lost/misplaced. Again, no such issues exist in Lamb’s (unmodified) system because the user of Lamb’s system does not need to do anything to prevent false alarms. The proposed modifications would thus frustrate Lamb’s intended purpose of reducing the occurrences of false alarms.

B. Ground 2: Petitioner Has Failed To Show That Sharma, Alone, Renders Challenged Claims 1 And 11 Obvious.

168. Challenged Claims 1 and 11 recite that the claimed barrier alarm device must transmit a “timed alarm signal” to a security panel. (EX1001, ‘340 patent, at claims 1, 11.)

169. Petitioner and Mr. McNair assert that Sharma discloses a barrier alarm device (*i.e.*, door sensing unit 104) that transmits signals to a system control panel 102 to enter a “Timed Exit Mode,” and that Sharma’s signal to enter the “Timed Exit

Mode” is the claimed “timed alarm signal.” (Petition at 67, 76; EX1003, McNair Declaration, ¶¶ 180-183.)

170. Petitioner and Mr. McNair cannot demonstrate that Sharma’s signal to enter the “Timed Exit Mode” is the claimed “timed alarm signal.”

171. Sharma’s “Timed Exit Mode” is a mode where Sharma’s door sensing unit 104 ignores door control signals and/or disables the door contact 172 so that occupants of a house or facility may leave within a predetermined amount of time without triggering an alarm. (EX1011, Sharma, at 8:6-21, FIG. 5; Petition at 67, 76.) Sharma’s “Timed Exit Mode” causes Sharma’s system to be disarmed or bypassed for a predetermined amount of time. (*Id.*)

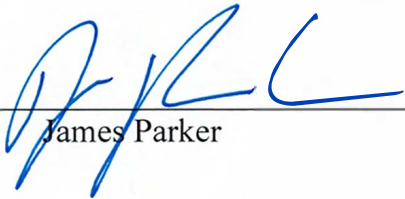
172. As discussed above, a bypass signal or a signal that causes an alarm system to be disarmed is not the claimed “timed alarm signal.” Sharma’s signal to enter the “Timed Exit Mode” (*i.e.*, the alleged “timed alarm signal”) cannot be the claimed “timed alarm signal” because it is a signal that causes Sharma’s system to be disarmed or bypassed and prevents an alarm from being triggered. (EX1011, Sharma, at 8:6-21.) A POSITA would not have considered Sharma’s “Timed Exit Mode” signal that causes Sharma’s system to be disarmed or bypassed to be a “timed alarm signal.”

XI. CONCLUSIONS

- The Challenged Claims of the '340 patent are valid, patentable, and not obvious.
- The Challenged Claims of the '340 patent were properly issued by the Patent and Trademark Office.

I have prepared this Declaration based upon my review of the materials referenced, and my own personal knowledge, education, skill and experience. I declare, under penalty of perjury under the laws of the United States of America, that the foregoing is true and correct.

Dated: February 6, 2024



James Parker

EXHIBIT 1

August 14th, 2023**James Parker**

416-302-7501



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

Over 35 years of deep industry experience, spanning hands-on technical roles to senior executive leadership.

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, Burglar / Fire / Access Control Panels, Motion Detectors, Smart Solar LED Lighting, among others.

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 the litigation process.

Seasoned in Civil, Criminal, & Patent Litigation, Arbitration, and Inter Partes Reviews (IPRs). Involved in **30+ cases**, marking significant experiences with **10 IPRs, 4 depositions, and 3 courtroom testimonies**; further contributed with multiple expert reports and declarations.

Previous Clients: 2GIG Technologies | AIG Insurance Company | ADT | Alarm.com | AT&T Digital Life | Chubb Insurance
(Partial List) ITX Security Co. | Lowe's Companies | MD Security Solutions | Nest Labs (Google) | Protect America
SecureNet | Skybell | Slomin's Inc. | Telular Corporation | Wal-Mart Canada | Zmodo Technology | Zonoff
Akerman | Baker Botts | Bryan Cave Leighton Paisner | Cooley | Cravath Swaine & Moore | Duane Morris
Fish & Richardson | Hennessy & Roach | Hunton 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	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 Ctrl Panels, Alarm System Controllers, Burglar/Fire/Access Control Panels	Security Network Protocols (AML, Wireless, Keybus, Combust)	Environmental Immunity (ESD/EFT)
Keypads, Zone Expanders, Wireless Rx/Tx, Output Modules, Sensors, Digital Dialers / Communicators	Personal Emergency Response System (P.E.R.S.)	Radiated & Conducted Immunity
Motion Detectors, PIR (Passive InfraRed) Fresnel & Mirror Optic, μ W Doppler (X/K Band Microwave)	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

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

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 35+ years of industry experience, I have handled over 30 separate cases, including more than 10 Inter Partes Reviews (IPRs), 4 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 5 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 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.

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.

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 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.

My work at Thermetic Controls Limited reflects my commitment to innovation, quality, and efficiency, as well as my ability to translate complex engineering concepts into tangible solutions that enhance production processes.

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)*

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** (defendant's) family for the third trial of Antonio Armstrong Jr. following mistrials in the first and second trials. Analysed new records asked for and provided after first and after second trial ended (both in mistrial) 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. Trial still in progress when this CV was released.

Technical Consulting – EarthCam Inc.

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

Retained by **EarthCam Inc.** to provide technical input on numerous occasions covering product design review, failure analysis, specification comparisons, and various other aspects of new product development.

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 council for deposing representatives of the defendant, A.P.I Alarm Inc. Provided subject matter information as required.

Civil Litigation - Jewelers Mutual Insurance Co. vs. Shiver Security Systems Inc. and Action Security, LLC.

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 council (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 council (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 of 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 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 analysed relevant material. Provided declaration regarding key technical points. Reviewed and critiqued patent owner's response to the PTAB. Deposed by attorneys for the petitioning party, 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 analysed 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 IPR(s). 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 result 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 ***

Summary of Patents – James Parker as a Named Inventor**1) Wireless Alarm System**

Priority Date

December 16, 1993

[US5625338A](#), CA2111929A1, CA2111929C, WO9516980A1, AU1104095A, EP0734560B1, EP0734560A1, DE69413848T2.

A security system having a two-way wireless keypad which operates in a particular manner for improved operation. The keypad processes information to effectively reduce communications between the control panel and the keypad. The keypad selectively activates and deactivates a transmitter and receiver arrangement for power conservation reasons. The system provides confirmation of communications between the keypad and the control panel to increase the reliability of the system.

2) Method and Arrangement for Recognition of a Coded Transmitted Signal

Priority Date

July 21, 1994

[US5517518A](#), CA2128587A1, AU2508195A, AU692260B2

The present invention is for fast, reliable recognition of coded signals where the signal includes a predetermined code sequence in a lead portion thereof. This has particular application in spread spectrum transmission and receptions. The code sequence is a long sequence of bits known to the receiver which breaks the long sequence into a series of bit segments which are more easily analysed. Each series of bits is analysed for a direct match and a decision whether a code segment has been received is based on the number of direct matches. For example, if there are 8-bit segments, each 16 bits in length, high reliability has been achieved if two direct matches are received within a time period corresponding to the transmission time of the code sequence. This system can also be used for assessing signal strength where many matches indicate good signal strength, approximately 50% indicates moderate signal strength, and less indicating poor signal strength.

3) Security System with Two Signal Reporting

Priority Date

April 22, 1997

[US5956388A](#), CA2203323A1, CA2203323C, WO9848564A1, AU7022598A

A security system having two distinct channels of communication and which uses a single communication device provides improved security. The system monitors a host of security alarm panels connected to a telephone system. A status signal is communicated between each control panel and a scanner placed at a switching station of the telephone system to confirm the integrity of the communication channel. An alarm event continues to be reported to a monitoring station using the telephone system in the normal manner.

4) Home Automation and Security System Controller

Priority Date

April 24, 1997

[CA2203591A1](#), WO9849663A1, EP0978111A1, EP0978111B1, AT209385T, PT978111E, DE69803282T2, DK0978111T3, ES2168748T3

The present invention, in one aspect, is directed to a security system which is capable of acting as an information display for display of user selected information not directly related to the security system. Such information may include weather information, news reports, sports information and financial information, the display of such information is preferably under user control and is selectable to be customized for each individual user. The security system includes an interface means for communicating with a data access provider for retrieval of the user selected information for display on the keypad controller. In another aspect, the present invention is directed to a controller for controlling the function of components of a security system. The controller has a graphical interface comprising a display screen capable of displaying a graphical representation of the security system and the components on the screen and graphical representation of the user selected information. The graphical display may include a touch screen such that the function of the components of the security system are controlled by touching a portion of the screen having the component or security system to be controlled displayed thereon.

5) Controllable Still Frame Video Transmission System

Priority Date	US6642954B1 , CA2301858C, CA2301858A1, WO9911069A1,
August 25, 1997	AU4006797A, EP1010328A1, EP1010328B1, AU749600B2, DE69713405T2
A video capture controller for selective capture of video images from a plurality of video cameras, the capture controller having multiple video signal inputs for receiving signals from video source devices, an arrangement for receiving input signals from a security system, a processor for processing the received input signals of such arrangement and comparing the received signals with a predetermined set of possible received signals and, based thereon, determining a particular video capture protocol from a set of video capture protocols associated with the set of possible received signals, and a controller associated with the multiple video signal inputs and the processor, the controller having a video output, the controller selectively connecting the multiple video inputs with the video output based on the particular protocol determined by the processor.	

6) Programmable Temperature Sensor for Security System

Priority Date	US6215405B1 , CA2235654C, CA2235654A1, WO9956261A1, AU3402099A,
April 23, 1998	EP1074009B1, EP1074009A1, AT214505T, DK1074009T3, DE69901027T2, ES2174598T3
The present invention in one aspect, provides for a programmable temperature sensor for a device as part of a security or alarm system. The programmable temperature sensor is capable of having multiple set points programmed, each set point individually programmable as to effect. In a preferred embodiment of the invention, there is provided a keypad controller having a programmable temperature sensor for use in an alarm system. The keypad controller includes an input for allowing a user to interface with the keypad controller and an alarm system to which the keypad controller is connected, an output display for providing one or more of visual and auditory feedback to a user on the status of the system, an interface for communicating with an alarm control panel of an alarm system, a processor for processing inputs from the input or an alarm control panel and causing the appropriate information to be provided to the output display, and a programmable temperature sensor for monitoring the temperature in the space in which the keypad controller is to be located, the temperature sensor being provided with at least one alarm set point programmable as to level.	

7) Suspended Code for Alarm System

Priority Date	US6078254A , CA2247600C, CA2247600A1
September 17, 1998	
The system generates alarm suspension codes without direct interaction with the alarm panel. The alarm control panel generates its own suspension codes for checking for proper validation when a suspension code is entered. The alarm panel generates suspension codes sequentially and will recognize any of several suspension codes that are current. The entry of a later suspension code cancels all earlier suspension codes.	

8) Biometric Input Device for Security System

Priority Date	CA2256809A1 , CA2256809C, WO0038118A1, AU1764500A
December 21, 1998	
The present invention provides for a biometric input device for a security system. The biometric input device includes a biometric sensor for sensing and input of biometric data, an image capture module for capturing and storage of the inputted biometric data from the biometric sensor, and an input/output module for passing the captured biometric data to a control panel and receiving data from the control panel. The invention also provides for a security system for controlling access to a premises. The security system includes a control panel for overall control of the security system, and one or more input devices for allowing users to interact with the security system., One or more of such input devices is a biometric input device capable of sensing biometric data from a user and capable of passing said sensed biometric data to the control panel for comparison against a database of biometric data of authorized users.	

9) Dual Mode Panel

Priority Date	US6380850B1 , CA2258817A1, CA2258817C, WO0041152A1,
January 5, 1999	AU1765100A, EP1149370B1, EP1149370A1

A dual mode alarm control panel includes a sensing arrangement for determining conditions of the environment in which the panel is installed. The results of the environmental assessment are used to determine an operating mode of the panel. In a first mode the panel is fully functional, and in a second mode the functions of the panel are restricted. This process assists in operating alarm control panels in an environment corresponding to the assumed design environment. In this way, non-compliance or operating alarm panels in unsuitable environments is reduced or avoided.

10) Alarm System Using Local Data Channel

Priority Date	US6252504B1 , US6895082B2, US2002029147A1, CA2260680A1,
February 2, 1999	CA2260680C

An alarm system has an alarm unit in combination with a line seize module. The alarm unit includes a transmitter/receiver, a control panel function, a keypad, an input/output port connected to a telephone line and an auto dialer for normally communicating with a remote monitoring station over the public switched telephone network. The line seize module includes an input communication port connected to the telephone line, a signal transmitter and receiver for communication over telephone wiring with the alarm unit, control logic, a line seize arrangement and an automatic dialer. Control logic processing signals are received by the input port. The line seize module, upon receiving an alarm signal from the alarm unit, reports the signal to a remote monitoring station using the automatic dialer and the public switched telephone network.

11) Alarm System with Programmable Device Control

Priority Date	CA2300465A1
March 10, 2000	

An alarm system providing programmable remote control of electrically controlled devices, such as lights, is provided. Geographic site and date information are provided to the alarm system. The parameters used to dictate the activation and deactivation of the controlled devices include the geographic site location and the sunrise and sunset times for the current date at that site. Accordingly, the activation and deactivation times of the controlled devices be programmed to automatically track the shifting sunset and sunrise times at the site.

12) Security Alarm Keypad with Message Alert

Priority Date	CA2300468C, CA2300468A1
March 10, 2000	

A security alarm system is adapted to retrieve e-mail status information and provide an alert signal for the user of the system that e-mail has been received and is awaiting retrieval. Preferably, the keypad of the security system includes a visual indicator which is activated when e-mail is received. The security alarm system uses the control panel and the auto dialer associated therewith, to contact the e-mail server and receive status information of one or more e-mail accounts. The control panel can contact the e-mail provider on a predetermined basis, or on a user scheduled basis. The accounting system's capability to initiate telephone communications and process signals from a remote computer is advantageously used for e-mail retrieval.

13) Remote Recovery Arrangement for Alarm System

Priority Date

March 10, 2000

[CA2300648A1](#)

A security alarm system cooperates with a remote monitoring station to improve the reliability of the alarm system. The alarm system includes a control panel which during communications with the remote monitoring station, receives information used for the operation of the system and preferably provides information for storage by the remote monitoring station which information is recovered by the control panel if necessary.

14) Security Alarm Keypad with Message Alert

Priority Date

May 15, 2000

[US6362747B1](#)

A security alarm system is adapted to retrieve e-mail status information and provide an alert signal for the user of the system that e-mail has been received and is awaiting retrieval. Preferably, the keypad of the security system includes a visual indicator which is activated when e-mail is received. The security alarm system uses the control panel and the auto dialer associated therewith, to contact the e-mail server and receive status information of one or more e-mail accounts. The control panel can contact the e-mail provider on a predetermined basis, or on a user scheduled basis. The accounting system's capability to initiate telephone communications and process signals from a remote computer is advantageously used for e-mail retrieval.

15) Remote Recovery Arrangement for Alarm System

Priority Date

May 15, 2000

[US6366211B1](#)

A security alarm system cooperates with a remote monitoring station to improve the reliability of the alarm system. The alarm system includes a control panel which during communications with the remote monitoring station, receives information used for the operation of the system and preferably provides information for storage by the remote monitoring station which information is recovered by the control panel if necessary.

16) Alarm System with Programmable Device Control

Priority Date

May 26, 2000

[US6310547B1](#)

An alarm system providing programmable remote control of electrically controlled devices, such as lights, is provided. Geographic site and date information is provided to the alarm system. The parameters used to dictate the activation and deactivation of the controlled devices include the geographic site location and the sunrise and sunset times for the current date at that site. Accordingly, the activation and deactivation times of the controlled devices be programmed to automatically track the shifting sunset and sunrise times at the site.

17) Integrated Lightning Detector

Priority Date

February 7, 2003

[US6960995B2](#), US2004257216A1, CA2418673C, CA2418673A1

An alarm panel of a security system is additionally provided with an interference circuit for evaluating the possible presence of a large electromagnetic interference signal such as lightning. The earth ground connection of the alarm panel to a power source is used to provide an input to the interference circuit. The earth ground connection receives large transient signals caused by such naturally occurring events. The alarm panel uses this additional information to modify the reporting of alarm conditions. This has particular application for addressing problems associated with motion detectors falsely triggering when a large electromagnetic signal is received. The solution of the alarm panel sensing this condition in contrast to each detector sensing this condition is more reliable, allows combining of detector information and is more cost effective.

18) False Alarm Reduction Method and System

Priority Date

February 16, 2005

US2006192666A1, [US7323978B2](#)

A digital verification control, which is incorporated with an alarm system, includes a first timer device for presetting a single zone verification time in the control panel and second timer device for presetting a multiple zone verification time in the control panel. The single zone verification time is a single detector time delay and arranged when one of the sensors detects at least two triggered signals in the respective detecting area within the single zone verification time, the local warning system is activated for producing a local warning signal. The multiple zone verification time, which is longer than the single zone verification time, is a multiple detector time delay and arranged when the two sensors detect two triggered signals in the detecting areas respectively within the multiple zone verification time, the local warning system is activated for producing the local warning signal.

19) Security Device with Built-In Intercommunicated False Alarm Reduction Control

Priority Date

May 6, 2005

US2006250231A1, [US7248155B2](#)

A security device includes a plurality of security detectors intercommunicating with each other. Each of the security detectors includes a first device for verifying a single zone verification time of the respective security detector and a second device for verifying a multiple zone verification time with another security detector corresponding to a distance between two security detectors at two different detecting areas. When one of the security detectors detects at least two triggered signals in the respective detecting area within the single zone verification time, the respective security detector activates the local warning system to produce a local warning signal. When two security detectors are intercommunicated with each other to detect two triggered signals in the detecting areas respectively within the multiple zone verification time, at least one of the security detectors activates the local warning system to produce the local warning signal.

20) Integrated Detecting Processor

Priority Date

November 18, 2005

[US2007114413A1](#)

An infrared sensor includes an infrared generator for generating infrared radiation within a detecting area, a pyroelectric sensor, a microprocessor, and an integrated detecting processor. The pyroelectric sensor is electrically communicated with the infrared generator, wherein the infrared radiation as an input signal is converted into a DC signal as an output signal having a real signal with low frequency and a noise signal mixed therewith. The microprocessor includes an A/D converter electrically connected with the pyroelectric sensor, wherein the microprocessor is arranged to receive the DC signal for data processing. The integrated detecting processor, which is electrically connected with the microprocessor, is adapted for stripping out the DC signal from the pyroelectric sensor to control a DC level of the DC signal, such that the real signal is allowed to be accurately processed in the microprocessor without data overflowing.

21) Energy Signal Detection Device Containing Integrated Detecting Processor

Priority Date

November 18, 2005

[US2007114414A1](#)

An energy signal detection device includes a pyroelectric sensor sensing an infrared radiation within a detecting area, a microprocessor, and an integrated detecting processor. The infrared radiation as an input signal is converted into a DC signal as an output signal having a real signal with low frequency and a noise signal mixed therewith. The microprocessor includes an ADC converter electrically connected with the pyroelectric sensor, wherein the microprocessor is arranged to receive the DC signal for data processing. The integrated detecting processor is adapted for stripping out the DC signal from the pyroelectric sensor to control a DC level of the DC signal, such that the real signal is allowed to be processed in the microprocessor without data overflowing.

22) Process and System of Energy Signal Detection

Priority Date

June 7, 2006

[US7546223B2](#), US2007288108A1, EP2035992A2, EP2035992A4, WO2008048365A3, WO2008048365A2, CN101573709A

A process and system of energy signal detection, which improves sensitivity, performance and reliability thereof and reduces false alarms by distinguishing between noise and real signals, includes the steps of receiving a plurality of data samples and generating a predetermined number of constructed sample windows of constructed samples in time, determining a control range for each of said constructed sample windows, determining whether there is an alarm pre-condition by comparing relationship between successive constructed sample windows, and generating an output signal when the alarm pre-condition is qualified.

23) Process and System of Power Saving Lighting

Priority Date

August 9, 2007

[US8194061B2](#), US2009039797A1

A process and system of lighting with green energy source and intelligent power management, which saves energy consuming and limits pollution. The system is using solar power, green battery, and LED which are clean, long life, save, and energy saving. A microcontroller coordinates devices and sensors to optimize the operation of the system to generate illumination. The process includes the steps of sensing the environment, selecting power source, determining the energy output, and driving the light device in order to most efficiently using energy and generate sufficient light for different purposes.

24) Process and System of Energy Signal Detection

Priority Date

April 11, 2008

[US20080218361](http://www.psecon.com), WO2009126300A2, WO2009126300A3,
EP2271967A4, EP2271967A2

A process and system of energy signal detection, which improves sensitivity, performance and reliability thereof and reduces false alarms by distinguishing between noise and real signals, includes the steps of receiving a plurality of data samples and generating a predetermined number of constructed sample windows of constructed samples in time, determining a control range for each of said constructed sample windows, determining whether there is an alarm pre-condition by comparing relationship between successive constructed sample windows, and generating an output signal when the alarm pre-condition is qualified, and detecting white light for preventing false alarm created by the white light.

25) Single MCU-Based Motion Detection, Local Alarm and Supervisory Arrangement for Alarm System

Priority Date

November 25, 2008

[US8410923B2](http://www.psecon.com), US2010219949A1

A device with single MCU-based motion detection, local alarm and supervisory arrangement for alarm system controlled by an alarm control panel (ACP) is disclosed. The device includes a sensor component to monitor environment, an output component to generate warning messages, a power supply component to provide power, and a microcontroller to communicate with sensor component, drive output component and monitor the status of ACP. The device can detect when intruders break in and make alarm warnings even when the ACP is destroyed. Plurality of devices and said ACP form a local warning matrix network (LWMN) to increase the detection area and scary effect to intruders. Each device of LWMN works independently when the ACP is destroyed.

End of File