

**Softex LLC v. Defendants, 1:22-cv-01308, 1:22-cv-01309, 1:22-cv-01311 (W.D. Tex.)
Defendants’ Initial Invalidity Contentions – Exhibit F-11**

Claim Chart Against U.S. Patent No. 8,506,649 (“’649 patent”)

Charted Reference: U.S. Patent No. 6,300,863 B1 to Cotichini et al. (“Cotichini”), entitled “Method and Apparatus to Monitor and Locate an Electronic Device using a Secured Intelligent Agent via a Global Network”

Cotichini, claiming priority to November 15, 1994, qualifies as prior art to the ’649 patent under at least 35 U.S.C. §§ 102(a) and/or (b).

As set forth in the chart below, all asserted claims of the ’649 patent are anticipated and/or obvious over Cotichini.¹

Except where specifically noted otherwise, this chart applies the apparent constructions of claim terms as used by Softex LLC (“Softex”) in its infringement contentions; such use, however, does not imply that Defendants adopt or agree with Softex’s constructions in any way.

To the extent the charted reference is held not to explicitly or inherently disclose any particular element below, such limitations were obvious for the reasons stated below and in Defendants’ Initial Invalidity Contentions, which are incorporated herein by reference.

Defendants are investigating this prior art and have not yet completed discovery from third parties who may have information concerning it. Defendants reserve the right to modify, amend, and/or supplement these contentions as information becomes available, and as discovery proceeds.

Evidence of Invalidity	
Claim Element	Claim 1
1.[pre] A mobile electronic device, comprising:	<i>To the extent that the preamble is limiting, it is disclosed or suggested by Cotichini. For example:</i> “This invention relates to a security apparatus and method for retrieving lost or stolen electronic devices such as portable computers, PCs (including stolen components such as CPU, hard drives, etc.), cablevision devices, personal digital assistants ”

¹ The excerpts cited herein are exemplary. For any claim limitation, Defendants may rely on excerpts cited for any other limitation and/or additional excerpts not set forth fully herein to the extent necessary to provide a more comprehensive explanation for a reference’s disclosure of a limitation. Where an excerpt refers to or discusses a figure or figure items, that figure and any additional descriptions of that figure should be understood to be incorporated by reference as if set forth fully therein.

**Softex LLC v. Defendants, 1:22-cv-01308, 1:22-cv-01309, 1:22-cv-01311 (W.D. Tex.)
Defendants' Initial Invalidity Contentions – Exhibit F-11**

Claim Element	Evidence of Invalidity
	(PDAs), cellular telephones, etc. This invention enables electronic devices to be surveyed or monitored by implanting thereon an intelligent agent with a pre-defined task set. This agent communicates with a preselected host monitoring system which is capable of multiple services including; tracing location, providing identifying indicia such as an electronic serial number (ESN), and electronically notifying the end user/owner of its location. The agent hides within the software/firmware/hardware of the electronic device, and operates without interfering with the regular operation of the device. According to one embodiment of the invention, the Agent is disposed on the ROM BIOS of the electronic device and the Agent takes control of the electronic device and its facilities during its boot-up. According to another embodiment of the invention, the Agent is disposed on the modem component of the electronic device and the Agent operates independently of the electronic device. Another embodiment of the Agent is on the processing unit (e.g., microprocessor) of the electronic device. Yet another embodiment of the Agent is a hardware implementation, such as hard-wired circuitry or a single integrated circuit. The Agent is further designed to evade detection and resist attempts to disable it by an unauthorized user. The invention overcomes disadvantages associated with the prior art by yielding a security device for small computers, cellular telephones and the like which can be programmed as firmware onto the non-volatile memory (such as ROM BIOS, ROM, Flash ROM, EPROM, EEPROM or the like) of such devices. Accordingly, no physical alteration is necessary or apparent to a thief. The existence of the security device is well cloaked and thus it cannot be readily located or disabled even if the possibility of its existence is suspected. Apparatuses and methods according to the invention can be very cost effective, requiring relatively inexpensive modifications to software or hardware and operation of relatively few monitoring devices.” (Cotichini, 2:27-67)² “Referring to FIG. 1, the preferred embodiment of the electronic article surveillance system is comprised of three main components: (1) client device A consisting of any

² Unless otherwise noted, all emphasis is added.

***Softex LLC v. Defendants*, 1:22-cv-01308, 1:22-cv-01309, 1:22-cv-01311 (W.D. Tex.)
Defendants’ Initial Invalidity Contentions – Exhibit F-11**

Claim Element	Evidence of Invalidity
	one of the electronic devices shown which have been implanted with the agent ; (2) A telecommunication link B such as a switched communications system, the Internet, radio tower, satellite and cable networks; and (3) The host monitoring system C which controls the communications between the client device A and the host monitoring system C.” (Cotichini, 6:22-30)

**Softex LLC v. Defendants, 1:22-cv-01308, 1:22-cv-01309, 1:22-cv-01311 (W.D. Tex.)
Defendants' Initial Invalidity Contentions – Exhibit F-11**

Claim Element	Evidence of Invalidity
	A1 to be monitored and through the use of (i) the public switched telephone network B1, (ii) the Internet B5, and (iii) local area networks B7, the CompuTrace server 3 maintains a database of records on computer A1's location and movements. Tracking information is collected during periodic telephone calls to the CompuTrace server 3; wherein server 3 identifies the unique agent A and obtains the phone number from which that call has been made. Once installed, the operation of the remote CompuTrace software is invisible to the user, and calls are made without the user's explicit awareness.” (Cotichini, 29:58-30:5) “The above description relates to the agent security system installed and operating in a conventional PC with an Intel 80X86 microprocessor or equivalent and with a conventional MS-DOS or PC-DOS operating system. It will be recognized that the system can be modified to fit other types of computers including, for example, those sold under the trademark Macintosh. The system can easily be modified to suit other types of operating systems or computers as they develop.” (Cotichini, 27:36-44) <i>See also</i> Ex. A Claim 1[a] for Cotichini. <i>To the extent that the preamble is not fully disclosed or suggested by Cotichini, the preamble would have been obvious to a person of ordinary skill in the art in combination with the general knowledge in the field, common sense, and/or with any of the references identified in the Initial Invalidity Contentions.</i>
1[a] a processor;	<i>This limitation is disclosed or suggested by Cotichini. For example:</i> “The above description relates to the agent security system installed and operating in a conventional PC with an Intel 80X86 microprocessor or equivalent and with a conventional MS-DOS or PC-DOS operating system. It will be recognized that the system can be modified to fit other types of computers including, for example, those

Softex LLC v. Defendants, 1:22-cv-01308, 1:22-cv-01309, 1:22-cv-01311 (W.D. Tex.)
Defendants’ Initial Invalidity Contentions – Exhibit F-11

Claim Element	Evidence of Invalidity
	sold under the trademark Macintosh. The system can easily be modified to suit other types of operating systems or computers as they develop.” (Cotichini, 27:36-44) “Referring now to FIG. 17A, each computer, peripheral and component such as computer 400, CPU 402, option card 404, printer 406, keyboard 408, mouse 410 modem 412, and software program 414, and agent 416 or other associated peripheral or component are assigned an identifying indicia, such as unique serial numbers 401, 403, 405, 407, 409, 411, 413, 415 and 417 respectively. The serial number of each component comes from the manufacturer or is embedded at the time of assembly or installation of the component, peripheral or software.” (Cotichini, 28:29-38)

**Softex LLC v. Defendants, 1:22-cv-01308, 1:22-cv-01309, 1:22-cv-01311 (W.D. Tex.)
Defendants' Initial Invalidity Contentions – Exhibit F-11**

Claim Element	Evidence of Invalidity
1[b] one or more non-transitory machine-readable storage media responsive to the processor; and	<i>This limitation is disclosed or suggested by Cotichini. For example:</i> “CPU Agent... The Agent may be implemented in a CPU using an existing technology in many current microprocessors which allows patching of the microcode. The microcode is the architectural layer of the CPU which translates an external macrocode algorithm stored in volatile or non-volatile memory into a microprocessor's internal execution codes. Referring to FIG. 13A, the microcode patch 90 is formatted and encrypted according to each specific chip manufacturer's specifications. It is uploaded from the BIOS 91 to a microcode patch area 93 and/or microcode storage 94 in the CPU 92, after reset, during the POST initialization of the computer. The microcode patch 90 can implement all the functions of the conventional algorithmic Agent. Referring also to FIG. 13B, the Agent may take a similar form as the BIOS Agent or the SPC of Segmented Agent described before. The SPC in the microcode patch initiates communication with the modem 95 asynchronously of the normal code stream (i.e., of the operating system or application program 96) via the logic unit and decoder 97 of the CPU 92.” (Cotichini, 24:44-63) “The security system may be recorded on the boot sector of a hard disk, on a hidden system file such as IO.SYS, MSDOS.SYS, IBMBIO.COM or IBMDOS.COM, or alternatively on the ROM BIOS of the computer, or a combination of both. The security system functions without interfering with the operating system or any running applications. The security system is loaded into memory whenever the electronic device is powered on or reset. It is loaded before the operating system. Alternatively, the security system may be recorded on the Flash ROM of the modem component of the electronic device. The security system functions independently of the main processor of the electronic device. Consequently, the security system as provided in either the ROM BIOS or the modem Flash ROM is operating system independent.” (Cotichini, 3:30-44) “FIGS. 3-1 and 3-2 is a flow chart of the agent work cycle. This work cycle describes the method by which the Agent is loaded when the client computer 10 is initially turned

**Softex LLC v. Defendants, 1:22-cv-01308, 1:22-cv-01309, 1:22-cv-01311 (W.D. Tex.)
Defendants' Initial Invalidity Contentions – Exhibit F-11**

Claim Element	Evidence of Invalidity
	on or reset, and the manner in which the operating system and the agent run concurrently. In this illustrative embodiment, the Agent is embedded in software. Once the client computer 10 is powered on 11, it performs a power on self-test (POST) 12. The POST tests the system hardware, initializes some of the devices for operation, and loads the master boot record (MBR) 13. Since the MBR was installed with an Agent subloader, the subloader is loaded into memory 14 and executed. The subloader's first task is to load the Agent into memory 15 (which is discussed in detail below in reference to FIG. 5.) Then the subloader loads the operating system (OS) into memory 16 and returns control to the operating system. Now both the operating system 17 and the Agent 18 are running simultaneously.” (Cotichini, 10:27-43) “Referring to FIG. 5, the Agent startup and loading sequence is described. The computer 10 is powered on and the loading sequence begins 700. As is well known in the art, the machine's start-up ROM procedure 701 in the computer 10 begins when the power is turned on. This process supervises the booting up and loading of the operating system of the computer. It performs the power-on self-test (POST) 702, in fact POST is carried out on every reset of the system, including the time when the power is first turned on. This test has two purposes: it performs a quick test 703 of the basic elements of the system; and it initializes the major hardware components for use. POST tests all of the ROMs on the system board by performing a checksum. This test adds together all of the bytes in the ROM module. As is does the addition, it discards any carry from the 8-bit result. If the final result is zero, the ROM passes the test. The initialization is done immediately after POST, it checks for new equipment and extensions to ROM 704. If it finds any 706, it momentarily turns control over to the ROM extensions so that they can initialize themselves. By design, the ROM Agent is a ROM extension, therefore its initialization routine will receive control 707 from the computer during the machine's start-up ROM procedure.” (Cotichini, 12:33-55) “Referring to FIG. 14A, the agent loading sequence is described for loading the agent on the operating system boot sector. The computer 10 is powered on and the loading

**Softex LLC v. Defendants, 1:22-cv-01308, 1:22-cv-01309, 1:22-cv-01311 (W.D. Tex.)
Defendants’ Initial Invalidity Contentions – Exhibit F-11**

Claim Element	Evidence of Invalidity
	sequence begins 64. As is well known in the art, the computer 10 performs an initial testing routine to assure that all components are working properly 65. Illustratively, the program incorporated is the IBM-PC compatible Power-On Self Test (POST) routine. The partition boot sector is loaded 66. Next the operating system boot sector with the installed agent is loaded 67. In an effort to maintain the transparency of the agent, the CPU registers (corresponding to the current state of the computer) are saved 68. Before the agent is installed there is a check for a Remote Procedure Load (RPL) signature 69. If the signature is present this indicates that the agent is already in memory and will not be loaded again. However, if there is no RPL signature then preparation is made to load the agent. First, space is reserved for the agent at the ceiling of conventional memory 70. Next, Interprocess Communication Interrupt (2Fh) is hooked 71, which enables communication with other programs. Interrupt Eah, which is the disc input/output handler, is hooked 72. The old timer interrupt is saved, and new hook timer interrupt is put into place 73. Now the CPU registers are restored 74 in order to maintain the transparency of the system. The original operating system boot sector is loaded 75. The original operating system had been moved to accommodate the agent installation. Finally, the operating system is loaded 76 and running 77 again.” (Cotichini, 18:34-61) “The RAM is used by the modem chip set as its main memory. The flash programmable EPROM is used to store the modem software. A/D and D/A converters with the POTS interface allow the chip set to send/receive signals over the analog PSTN phone lines.” (Cotichini, 21:58-62) <i>See also</i> Ex. C Claim 8[a] for Cotichini; <i>see also</i> Ex. E Claim 18[b] for Cotichini. <i>To the extent that this limitation is not fully disclosed or suggested by Cotichini, this limitation would have been obvious to a person of ordinary skill in the art in combination with the general knowledge in the field, common sense, and/or with any of the references identified in the Initial Invalidity Contentions.</i>

**Softex LLC v. Defendants, 1:22-cv-01308, 1:22-cv-01309, 1:22-cv-01311 (W.D. Tex.)
Defendants’ Initial Invalidity Contentions – Exhibit F-11**

Claim Element	Evidence of Invalidity
1[c] a security application in at least one of the non-transitory machine-readable storage media, wherein the security application is operable to perform operations comprising:	<i>This limitation is disclosed or suggested by Cotichini. For example:</i> “The Agent may be implemented in the firmware or software of any electronic device, such as a computer. Alternatively, the Agent may be implemented in any component of a computer, as with an electronic component such as the DSP in a modem or the CPU in the computer. Furthermore, the functionality of the Agent may be implemented in the circuitry of any hardware device capable of establishing a communication link through sending and/or receiving packets of data.” (Cotichini, 10:6-14) “The above description relates to the agent security system installed and operating in a conventional PC with an Intel 80X86 microprocessor or equivalent and with a conventional MS-DOS or PC-DOS operating system. It will be recognized that the system can be modified to fit other types of computers including, for example, those sold under the trademark Macintosh. The system can easily be modified to suit other types of operating systems or computers as they develop.” (Cotichini, 27:36-44) “FIGS. 3-1 and 3-2 is a flow chart of the agent work cycle. This work cycle describes the method by which the Agent is loaded when the client computer 10 is initially turned on or reset, and the manner in which the operating system and the agent run concurrently. In this illustrative embodiment, the Agent is embedded in software. Once the client computer 10 is powered on 11, it performs a power on self-test (POST) 12. The POST tests the system hardware, initializes some of the devices for operation, and loads the master boot record (MBR) 13. Since the MBR was installed with an Agent subloader, the subloader is loaded into memory 14 and executed. The subloader's first task is to load the Agent into memory 15 (which is discussed in detail below in reference to FIG. 5.) Then the subloader loads the operating system (OS) into memory 16 and returns control to the operating system. Now both the operating system 17 and the Agent 18 are running simultaneously.” (Cotichini, 10:27-43; <i>see also id.</i>, FIGS. 3-1 and 3-2, 12:33-64 (describing “Agent startup and loading sequence”)))

**Softex LLC v. Defendants, 1:22-cv-01308, 1:22-cv-01309, 1:22-cv-01311 (W.D. Tex.)
Defendants' Initial Invalidity Contentions – Exhibit F-11**

Claim Element	Evidence of Invalidity
	“BIOS Agent...] Turning to the operating system independent methods, referring to FIG. 6C, the Agent is implanted into the computer's BIOS 741 and runs directly from the BIOS 742. As more fully discussed below, variations of the BIOS Agent may include implanting the Agent in a DSP of a modem, a CPU of the electronic device, a hard wired circuitry or an integrated circuit in the electronic device.” (Cotichini, 19:54-60) “Segmented Agent... Referring to FIG. 7A, an alternate embodiment of the operating system independent BIOS Agent is described in which the Agent 751 is segmented into two components. The Secure Protocol Component (SPC) is implanted into the computer's BIOS 752. The SPC handles device tracking function only 753. Additional functions, such as asset and configuration management, are handled by a High Level Component (HLC) that resides on the computer's hard-disk 754 and run from the disk 755.” (Cotichini, 20:8-16) “Modem Agent... The Modem Agent enables a monitored computer to communicate to the monitoring server even if a new disk drive is installed. This provides a much more secure method of tracing the location of stolen computers where modifications are made to the computer. before they are used. In the case where computers are stripped for parts, the Modem Agent will still be able to be located. Integration of the Modem Agent onto the motherboard of the computer will not allow the Modem Agent to become separated from the motherboard, protecting the most important component of the computer.” (Cotichini, 21:8-32) “CPU Agent... The Agent may be implemented in a CPU using an existing technology in many current microprocessors which allows patching of the microcode. The microcode is the architectural layer of the CPU which translates an external macrocode algorithm stored in volatile or non-volatile memory into a microprocessor's internal

**Softex LLC v. Defendants, 1:22-cv-01308, 1:22-cv-01309, 1:22-cv-01311 (W.D. Tex.)
Defendants' Initial Invalidity Contentions – Exhibit F-11**

Claim Element	Evidence of Invalidity
	execution codes. Referring to FIG. 13A, the microcode patch 90 is formatted and encrypted according to each specific chip manufacturer's specifications. It is uploaded from the BIOS 91 to a microcode patch area 93 and/or microcode storage 94 in the CPU 92, after reset, during the POST initialization of the computer. The microcode patch 90 can implement all the functions of the conventional algorithmic Agent. Referring also to FIG. 13B, the Agent may take a similar form as the BIOS Agent or the SPC of Segmented Agent described before. The SPC in the microcode patch initiates communication with the modem 95 asynchronously of the normal code stream (i.e., of the operating system or application program 96) via the logic unit and decoder 97 of the CPU 92.” (Cotichini, 24:44-63) “Hardware Agent... The Agent may be implemented in hard wired circuitry or a single integrated circuit using existing technology which takes an engineer's logic specification and translates into the data which is used to program, build, or design the hardware device or circuit. The hardware device or circuit would then execute according to the engineer's logic specification and perform the functions of the Agent by establishing a communications link and sending and receiving data packets in order to establish both the identification and location of the electronic device within which the hardware device or circuit is included, thereby simulating the algorithmic function of the Agent.” (Cotichini, 25:6-18) <i>To the extent that this limitation is not fully disclosed or suggested by Cotichini, this limitation would have been obvious to a person of ordinary skill in the art in combination with the general knowledge in the field, common sense, and/or with any of the references identified in the Initial Invalidity Contentions.</i>
1[c][i] enabling an owner of the mobile electronic device to register the mobile electronic device with a	<i>This limitation is disclosed or suggested by Cotichini. For example:</i> “Agent 464 silently calls into monitoring center 472 on a periodic (programmable) basis. Call and other PC asset management activity is logged, and reported to

Softex LLC v. Defendants, 1:22-cv-01308, 1:22-cv-01309, 1:22-cv-01311 (W.D. Tex.)
Defendants’ Initial Invalidity Contentions – Exhibit F-11

Claim Element	Evidence of Invalidity
security service residing at least partially on one or more servers;	customers on-demand via the web-based Online Monitoring Service 468. The online monitoring service database 470 may include the following: Call-in phone number (retrieval option includes: name and address), Birth Certificate information such as file 451, Dynamic System information files such as file 476 (NetCensus, Asset Insight, etc.) Customer-created information files such as file 474” (Cotichini, 29:39-52) “We have identified four potential OEM configurations which embed the SPC. The SPC is disabled Provided for future use by the full CompuTrace driver suite. The SPC operates independently Provided for protecting the unit from the point of manufacture, through the channel, then disabled when identified as a legitimate sale. The SPC is bundled with the full CompuTrace driver suite. Provided as a value-added service for end-users direct from the point of manufacture. The SPC operates independently and is bundled with the full CompuTrace driver suite. A combination of channel protection and value-added protection for the end-user.” (Cotichini, 32:50-64)

Softex LLC v. Defendants, 1:22-cv-01308, 1:22-cv-01309, 1:22-cv-01311 (W.D. Tex.)
Defendants’ Initial Invalidity Contentions – Exhibit F-11

Claim Element	Evidence of Invalidity
	“Enable Monitoring... This command allows a configuration application to enable the monitoring service of the Modem Agent. This command is used to re-enable monitoring if the service has previously been disabled.” (Cotichini, 23:27-31) “Referring to FIG. 1, the preferred embodiment of the electronic article surveillance system is comprised of three main components: (1) client device A consisting of any one of the electronic devices shown which have been implanted with the agent; (2) A telecommunication link B such as a switched communications system, the Internet, radio tower, satellite and cable networks; and (3) The host monitoring system C which controls the communications between the client device A and the host monitoring system C.” (Cotichini, 6:22-30)

**Softex LLC v. Defendants, 1:22-cv-01308, 1:22-cv-01309, 1:22-cv-01311 (W.D. Tex.)
Defendants’ Initial Invalidity Contentions – Exhibit F-11**

Claim Element	Evidence of Invalidity
	A1 to be monitored and through the use of (i) the public switched telephone network B1, (ii) the Internet B5, and (iii) local area networks B7, the CompuTrace server 3 maintains a database of records on computer A1’s location and movements.” (Cotichini, 29:58-65) See also Cotichini, 14:48-51 (referring to a “host monitoring server”), FIG. 7B (illustrating a “server 762” and flow node “agent establishes communication link with remote server”), FIG. 23 (same)). <i>To the extent that this limitation is not fully disclosed or suggested by Cotichini, this limitation would have been obvious to a person of ordinary skill in the art in combination with the general knowledge in the field, common sense, and/or with any of the references identified in the Initial Invalidity Contentions.</i>
1[c][iii] causing the mobile electronic device to automatically send identifying information for the mobile electronic device to the security service;	<i>This limitation is disclosed or suggested by Cotichini. For example:</i> “Once a communication link has been established between the SPC and the Server 762, the Server asks the SPC to identify itself 763. The SPC responds with the ID of the device that is being tracked 764. The Server then sends a request to the SPC 765 asking that it perform one or more tasks at a specified future time (such as contacting the Server again). At the appropriate time, the SPC responds to any such request 766. All communications between the Agent and the Server will incorporate data encryption 767 to provide an additional layer of security and prevent the sophisticated and user from intercepting or transmitting messages in an attempt to interfere with device tracking. The Server will determine the location of the tracked device with whatever means are available through the particular communication service being utilized. For instance, if a link were established over standard phone lines, Caller ID/ANI could be used to fix the location, or if a link were establish over Internet, the ID address can be used to fix the location.” (Cotichini, 20:42-59)

**Softex LLC v. Defendants, 1:22-cv-01308, 1:22-cv-01309, 1:22-cv-01311 (W.D. Tex.)
Defendants' Initial Invalidity Contentions – Exhibit F-11**

Claim Element	Evidence of Invalidity
	“Referring now to FIG. 14F, a flow chart is provided which describes in detail the background process operations relating to the Internet application. The background process wakes up every four hours 200. It uses the current date and time together with the agent identification (serial number) to encode an Internet host name 205. This encoded host name is used in forming a DNS query 206 to be sent to the host Internet monitoring subsystem 9y. After sending this DNS query to the host Internet monitoring subsystem 9y through the Internet 207, the agent waits for a response 208. If an error is found 208a due to a missing DLL or poor TCP/IP configuration, or an error other than a timeout, then the agent will wait four hours and repeat the cycle 200. If no response is received after a predetermined time period has elapsed, the agent will sleep for one minute 209 and then send another DNS query 205. Upon receiving a valid response from the host Internet monitoring subsystem 9y, the Internet Protocol (IP) address is extracted 210. If this IP address equals "204.174.10.1" 211 then the background process sets the agent's mode to alert 212. If the IP address does not equal "204.174.10.1" 211, then the agent remains in active mode and does not attempt to send another DNS query to the host for four hours 200.” (Cotichini, 15:45-67) <i>See also Ex. E Claim 2[c] for Cotichini.</i> <i>To the extent that this limitation is not fully disclosed or suggested by Cotichini, this limitation would have been obvious to a person of ordinary skill in the art in combination with the general knowledge in the field, common sense, and/or with any of the references identified in the Initial Invalidity Contentions.</i>
1[c][iii] after the owner has registered the mobile electronic device with the security service, causing the mobile electronic device to periodically communicate with the security service, when the mobile electronic device is in a state other than a state in	<i>This limitation is disclosed or suggested by Cotichini. For example:</i> “Referring now to FIG. 14F, a flow chart is provided which describes in detail the background process operations relating to the Internet application. The background process wakes up every four hours 200. It uses the current date and time together with the agent identification (serial number) to encode an Internet host name 205. This encoded host name is used in forming a DNS query 206 to be sent to the host

**Softex LLC v. Defendants, 1:22-cv-01308, 1:22-cv-01309, 1:22-cv-01311 (W.D. Tex.)
Defendants' Initial Invalidity Contentions – Exhibit F-11**

Claim Element	Evidence of Invalidity
which the mobile electronic device is powered off;	Internet monitoring subsystem 9y. After sending this DNS query to the host Internet monitoring subsystem 9y through the Internet 207, the agent waits for a response 208. If an error is found 208a due to a missing DLL or poor TCP/IP configuration, or an error other than a timeout, then the agent will wait four hours and repeat the cycle 200. If no response is received after a predetermined time period has elapsed, the agent will sleep for one minute 209 and then send another DNS query 205. Upon receiving a valid response from the host Internet monitoring subsystem 9y, the Internet Protocol (IP) address is extracted 210. If this IP address equals "204.174.10.1" 211 then the background process sets the agent's mode to alert 212. If the IP address does not equal "204.174.10.1" 211, then the agent remains in active mode and does not attempt to send another DNS query to the host for four hours 200." (Cotichini, 15:45-67) <i>To the extent that this limitation is not fully disclosed or suggested by Cotichini, this limitation would have been obvious to a person of ordinary skill in the art in combination with the general knowledge in the field, common sense, and/or with any of the references identified in the Initial Invalidity Contentions.</i>
1[c][iv] after the owner has registered the mobile electronic device with the security service, accepting a notification at the mobile electronic device from the security service, wherein the notification comprises a message indicating that the owner of the mobile electronic device has reported a loss or requested disabling of the mobile electronic device;	<i>This limitation is disclosed or suggested by Cotichini. For example:</i> "There is provided according to another aspect of the invention a method for tracing lost or stolen electronic articles through a global network such as the Internet. The client computer sends DNS queries that contain encoded identification information to a remote station through the Internet. The remote station receives the queries and decodes the encoded identification information in order to determine if the client computer matches an entry on a list of reported lost or stolen computers. If so, the host sends a predefined response to the client computer indicating that it should initiate a traceroute to provide the host with the Internet communication links connecting the client computer to the host. Additionally, when the client computer receives this predefined response from the host it immediately attempts to contact the host via the telecommunications system." (Cotichini, 4:15-29)

Softex LLC v. Defendants, 1:22-cv-01308, 1:22-cv-01309, 1:22-cv-01311 (W.D. Tex.)
Defendants’ Initial Invalidity Contentions – Exhibit F-11

Claim Element	Evidence of Invalidity
	“After sending its DNS request, the Agent waits for a response. Upon receiving a valid response from the host 18e, the IP address is extracted from the response and compared against a reference IP address 18f. In this illustrative embodiment of the invention the reference IP address is "204.174.10.1". If the IP address equals "204.174.10.1" then the agent's mode is changed from "active" to "alert" on the Internet side 18g. The host will send this reference IP address only when it has determined that the Agent identification matches one of the entries on a list of reported lost or stolen computers stored at the host. If the IP address extracted from the host response does not equal "204.174.10.1" then the Agent remains in active mode and does not call the host for another four hours.” (Cotichini, 11:51-64) “Referring to FIG. 11B, the host processing, auditing and communication subsystem for the Internet application receives and transmits information to and from clients over the Internet. FIG. 11B is a flow diagram of the host communication program executed by host computer 3 in connection with the Internet application. After the host computer is powered on 36a, TCP/IP support is loaded and the computer waits for a DNS query from the client computer 36b. The host name is then extracted from the DNS query 36c. Next, the DNS request is decoded to determine the client computer identification 36d. A check is made to determine whether the computer has been stolen 36e. This is accomplished by comparing the identification number of the client computer with a list of reported lost or stolen computers which is stored by the host computer. If it has been stolen a suitable message 36f is returned to the client computer 10. In the preferred embodiment, the message is provided by setting the IP address of the next transmission to the client computer to "204.174.10.1" 36f. If the client computer is not stolen, an alternate message is returned 36g. In the preferred embodiment this is achieved by setting the IP address to "207.174.10.16" 36g. The host uses either of these two IP addresses to form a response to the DNS query received from the client computer 36h. The host then sends its response to the client computer 36i. The host also records the transaction on the hard disk. The host then prepares to repeat the entire cycle 36b.”

**Softex LLC v. Defendants, 1:22-cv-01308, 1:22-cv-01309, 1:22-cv-01311 (W.D. Tex.)
Defendants' Initial Invalidity Contentions – Exhibit F-11**

Claim Element	Evidence of Invalidity
	(Cotichini, 26:48-27:7) <i>To the extent that this limitation is not fully disclosed or suggested by Cotichini, this limitation would have been obvious to a person of ordinary skill in the art in combination with the general knowledge in the field, common sense, and/or with any of the references identified in the Initial Invalidity Contentions.</i>
1[c][v] in response to receiving the notification, automatically disabling at least one user function of the mobile electronic device while still allowing the mobile electronic device to communicate with the security service; and	<i>This limitation is disclosed or suggested by Cotichini. For example:</i> “Disable Monitoring... This command allows a configuration application to disable the monitoring service of the Modem Agent. This command is used when the owner of the monitored PC wishes to terminate the electronic device trace service. The command will turn off the Modem Agent functions and AT commands with the exception of the enable monitoring command.” (Cotichini, 23:32-39) <i>See also Ex. A Claim 12[h] for Cotichini; see also Ex. E Claim 4 for Cotichini.</i> <i>To the extent that this limitation is not fully disclosed or suggested by Cotichini, this limitation would have been obvious to a person of ordinary skill in the art in combination with the general knowledge in the field, common sense, and/or with any of the references identified in the Initial Invalidity Contentions.</i>
1[c][vi] automatically causing at least some user data to be copied from the mobile electronic device to at least one of the servers;	<i>This limitation is disclosed or suggested by Cotichini. For example:</i> “Agent 464 silently calls into monitoring center 472 on a periodic (programmable) basis. Call and other PC asset management activity is logged, and reported to customers on-demand via the web-based Online Monitoring Service 468. The online monitoring service database 470 may include the following: Call-in phone number (retrieval option includes: name and address), Birth Certificate information such as file 451,

**Softex LLC v. Defendants, 1:22-cv-01308, 1:22-cv-01309, 1:22-cv-01311 (W.D. Tex.)
Defendants' Initial Invalidity Contentions – Exhibit F-11**

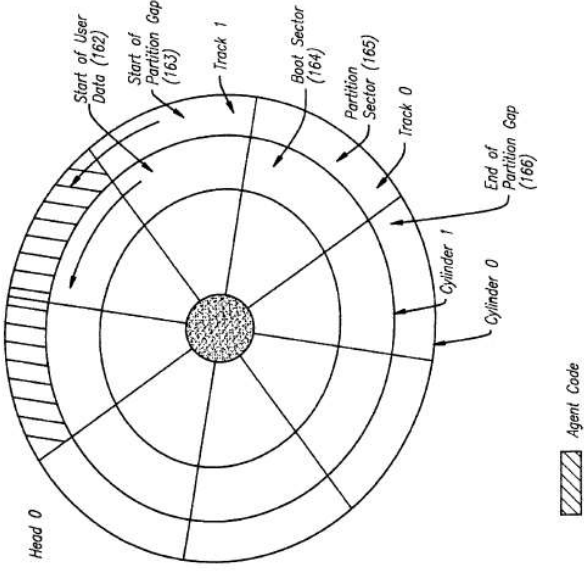
Claim Element	Evidence of Invalidity
	Dynamic System information files such as file 476 (NetCensus, Asset Insight, etc.) Customer-created information files such as file 474 The above data will be collected, aggregated per customer, and sent to a 3rd party data center on a regular basis. Stand-alone systems such as system 476 may be installed within the data center, or on-site at customer locations.” (Cotichini, 29:39-57) “If the DNS query fails, or the returned address is 204.174.10.1, or the traceroute fails the client attempts to establish a web session with the absolute web server. It first tries to establish the session directly, then it tries any available web proxy server. If it cannot establish a web session, it tries to establish an ftp session. The client first tries to establish the ftp session directly, then it tries any available ftp proxy server. Once a web session or ftp session has been successfully established, the sessions are used as secure, encrypted transport sessions. These sessions allow the secure transmission of dos commands and data files. The dos commands are executed on the client with the results returned and displayed on the server. This facility would allow an authorized user to search for files on the client, upload those files from the client to the server, and irreversibly erase the files from the client computer.” (Cotichini, 16:66-17:15) <i>To the extent that this limitation is not fully disclosed or suggested by Cotichini, this limitation would have been obvious to a person of ordinary skill in the art in combination with the general knowledge in the field, common sense, and/or with any of the references identified in the Initial Invalidity Contentions.</i>

Softex LLC v. Defendants, 1:22-cv-01308, 1:22-cv-01309, 1:22-cv-01311 (W.D. Tex.)
Defendants' Initial Invalidity Contentions – Exhibit F-11

Claim Element	Evidence of Invalidity
1[d] wherein the one or more non-transitory machine-readable storage media comprises non-volatile memory;	<i>This limitation is disclosed or suggested by Cotichini. For example:</i> “The invention overcomes disadvantages associated with the prior art by yielding a security device for small computers, cellular telephones and the like which can be programmed as firmware onto the non-volatile memory (such as ROM BIOS, ROM, Flash ROM, EPROM, EEPROM or the like) of such devices. Accordingly, no physical alteration is necessary or apparent to a thief. The existence of the security device is well cloaked and thus it cannot be readily located or disabled even if the possibility of its existence is suspected. Apparatuses and methods according to the invention can be very cost effective, requiring relatively inexpensive modifications to software or hardware and operation of relatively few monitoring devices.” (Cotichini, 2:55-67) “CPU Agent... The Agent may be implemented in a CPU using an existing technology in many current microprocessors which allows patching of the microcode. The microcode is the architectural layer of the CPU which translates an external macrocode algorithm stored in volatile or non-volatile memory into a microprocessor's internal execution codes. Referring to FIG. 13A, the microcode patch 90 is formatted and encrypted according to each specific chip manufacturer's specifications. It is uploaded from the BIOS 91 to a microcode patch area 93 and/or microcode storage 94 in the CPU 92, after reset, during the POST initialization of the computer. The microcode patch 90 can implement all the functions of the conventional algorithmic Agent. Referring also to FIG. 13B, the Agent may take a similar form as the BIOS Agent or the SPC of Segmented Agent described before. The SPC in the microcode patch initiates communication with the modem 95 asynchronously of the normal code stream (i.e., of the operating system or application program 96) via the logic unit and decoder 97 of the CPU 92.” (Cotichini, 24:44-63) “This invention also overcomes disadvantages associated with the prior art that may interfere with the operating system or running applications. This is accomplished by disposing the means for initiating communication with a host system in the firmware

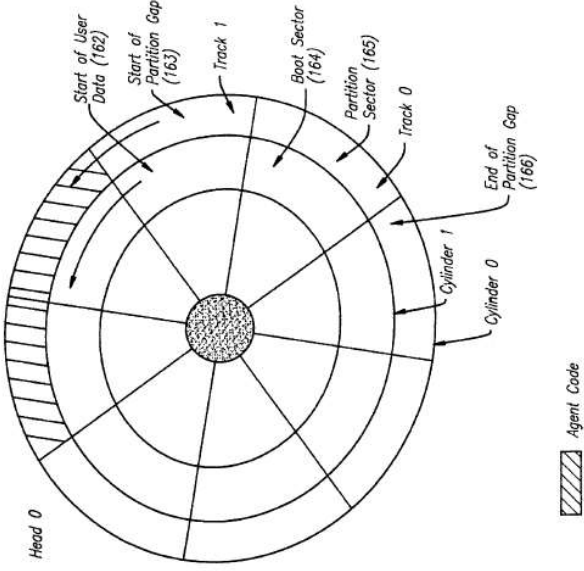
**Softex LLC v. Defendants, 1:22-cv-01308, 1:22-cv-01309, 1:22-cv-01311 (W.D. Tex.)
Defendants’ Initial Invalidity Contentions – Exhibit F-11**

Claim Element	Evidence of Invalidity
	such as on the ROM BIOS or the modem component of a client electronic device. This security system operates independently of the operating system running on the electronic device.” (Cotichini, 2:4-11) <i>See also</i> Ex. A Claim 1[d] for Cotichini. <i>To the extent that this limitation is not fully disclosed or suggested by Cotichini, this limitation would have been obvious to a person of ordinary skill in the art in combination with the general knowledge in the field, common sense, and/or with any of the references identified in the Initial Invalidity Contentions.</i>
1[e] wherein the non-volatile memory comprises a changeable area that can be modified by a user and a system area that cannot be modified by the user;	<i>This limitation is disclosed or suggested by Cotichini. For example:</i> “FIG. 14H is an isometric view, partly diagrammatic, of the physical structure of a computer disc.” (Cotichini, 5:50-51)

Claim Element	Evidence of Invalidity
1[f] wherein the security application utilizes code residing at least partially in the system area; and	 FIG. 14H (Cotichini, FIG. 14H) <i>To the extent that this limitation is not fully disclosed or suggested by Cotichini, this limitation would have been obvious to a person of ordinary skill in the art in combination with the general knowledge in the field, common sense, and/or with any of the references identified in the Initial Invalidity Contentions.</i> <i>This limitation is disclosed or suggested by Cotichini. For example:</i> “The Agent may be implemented in the firmware or software of any electronic device, such as a computer. Alternatively, the Agent may be implemented in any

**Softex LLC v. Defendants, 1:22-cv-01308, 1:22-cv-01309, 1:22-cv-01311 (W.D. Tex.)
Defendants' Initial Invalidity Contentions – Exhibit F-11**

Claim Element	Evidence of Invalidity
	component of a computer, as with an electronic component such as the DSP in a modem or the CPU in the computer. Furthermore, the functionality of the Agent may be implemented in the circuitry of any hardware device capable of establishing a communication link through sending and/or receiving packets of data.” (Cotichini, 10:6-14) “Four alternative ways of installing the agent security system during the disk boot are illustrated in FIGS. 14A-14D respectively. A conventional boot up method is described in detail in Appendix I. The system can also be installed with MS.SYS or IBMDOS.COM, but these are more difficult and less preferred than the three alternatives set out below. The loading program TENDER (further described in the Appendix) can be used to install the agent by one or more of these alternative installation methods. Thus, the agent may be installed in a variety of locations whereby second and third agents can provide back up support for the primary agent. The four locations where the agent can be installed on the client device are as follows: 1. The operating system boot sector--See FIG. 14A. 2. A hidden system file such as IO.SYS for MS-DOS or IBMBIO.COM for PC-DOS--See FIG. 14B. 3. The partition boot sector--See FIG. 14C. 4. The ROM BIOS--See FIG. 14D.” (Cotichini, 18:16-33)

Claim Element	Evidence of Invalidity
	 FIG. 14H (Cotichini, FIG. 14H) <i>To the extent that this limitation is not fully disclosed or suggested by Cotichini, this limitation would have been obvious to a person of ordinary skill in the art in combination with the general knowledge in the field, common sense, and/or with any of the references identified in the Initial Invalidity Contentions.</i>
1[g] wherein the security application receives the notification from at least one of the servers via the system area.	<i>To the extent that this limitation is not fully disclosed or suggested by Cotichini, this limitation would have been obvious to a person of ordinary skill in the art in combination with the general knowledge in the field, common sense, and/or with any of the references identified in the Initial Invalidity Contentions.</i>

**Softex LLC v. Defendants, 1:22-cv-01308, 1:22-cv-01309, 1:22-cv-01311 (W.D. Tex.)
Defendants’ Initial Invalidation Contentions – Exhibit F-11**

Claim Element	Evidence of Invalidity
Claim 2	
2. A mobile electronic device according to claim 1, wherein the notification includes no third-party certification.	<i>Because this claim recites a negative limitation, Cotichini need not affirmatively state that the notification includes no third-party certification. Rather, Cotichini discloses this limitation because its disclosures are complete and provide no indication that the disclosed “notification” (see cl. 1[c][iv] above) includes—or that there would be reason to include—a third-party certification.</i> <i>To the extent that this limitation is not fully disclosed or suggested by Cotichini, this limitation would have been obvious to a person of ordinary skill in the art in combination with the general knowledge in the field, common sense, and/or with any of the references identified in the Initial Invalidation Contentions.</i>
7. A mobile electronic device according to claim 1, wherein the operations the security application is operable to perform further comprise: after the at least some user data has been copied from the mobile electronic device to at least one of the servers, causing at least some of the user data to be deleted from the mobile electronic device.	<i>This limitation is disclosed or suggested by Cotichini. For example:</i> “Agent 464 silently calls into monitoring center 472 on a periodic (programmable) basis. Call and other PC asset management activity is logged, and reported to customers on-demand via the web-based Online Monitoring Service 468. The online monitoring service database 470 may include the following: Call-in phone number (retrieval option includes: name and address), Birth Certificate information such as file 451, Dynamic System information files such as file 476 (NetCensus, Asset Insight, etc.) Customer-created information files such as file 474 The above data will be collected, aggregated per customer, and sent to a 3rd party data center on a regular basis. Stand-alone systems such as system 476 may be installed within the data center, or on-site at customer locations.” (Cotichini, 29:39-57)

**Softex LLC v. Defendants, 1:22-cv-01308, 1:22-cv-01309, 1:22-cv-01311 (W.D. Tex.)
Defendants' Initial Invalidity Contentions – Exhibit F-11**

Claim Element	Evidence of Invalidity
	“If the DNS query fails, or the returned address is 204.174.10.1, or the traceroute fails the client attempts to establish a web session with the absolute web server. It first tries to establish the session directly, then it tries any available web proxy server. If it cannot establish a web session, it tries to establish an ftp session. The client first tries to establish the ftp session directly, then it tries any available ftp proxy server. Once a web session or ftp session has been successfully established, the sessions are used as secure, encrypted transport sessions. These sessions allow the secure transmission of dos commands and data files. The dos commands are executed on the client with the results returned and displayed on the server. This facility would allow an authorized user to search for files on the client, upload those files from the client to the server, and irreversibly erase the files from the client computer.” (Cotichini, 16:66-17:15) See also Ex. B Claim 1[a] for Cotichini. <i>To the extent that this limitation is not fully disclosed or suggested by Cotichini, this limitation would have been obvious to a person of ordinary skill in the art in combination with the general knowledge in the field, common sense, and/or with any of the references identified in the Initial Invalidity Contentions.</i>
9.[pre] A method for providing security for a mobile electronic device, the method comprising:	Claim 9 <i>To the extent that the preamble is limiting, it is disclosed or suggested by Cotichini. For example:</i> “This invention relates to a security apparatus and method for retrieving lost or stolen electronic devices such as portable computers, PCs (including stolen components such as CPU, hard drives, etc.), cablevision devices, personal digital assistants

Softex LLC v. Defendants, 1:22-cv-01308, 1:22-cv-01309, 1:22-cv-01311 (W.D. Tex.)
Defendants’ Initial Invalidity Contentions – Exhibit F-11

Claim Element	Evidence of Invalidity
	(PDAs), cellular telephones, etc. This invention enables electronic devices to be surveyed or monitored by implanting thereon an intelligent agent with a pre-defined task set. This agent communicates with a preselected host monitoring system which is capable of multiple services including; tracing location, providing identifying indicia such as an electronic serial number (ESN), and electronically notifying the end user/owner of its location. The agent hides within the software/firmware/hardware of the electronic device, and operates without interfering with the regular operation of the device. According to one embodiment of the invention, the Agent is disposed on the ROM BIOS of the electronic device and the Agent takes control of the electronic device and its facilities during its boot-up. According to another embodiment of the invention, the Agent is disposed on the modem component of the electronic device and the Agent operates independently of the electronic device. Another embodiment of the Agent is on the processing unit (e.g., microprocessor) of the electronic device. Yet another embodiment of the Agent is a hardware implementation, such as hard-wired circuitry or a single integrated circuit. The Agent is further designed to evade detection and resist attempts to disable it by an unauthorized user. The invention overcomes disadvantages associated with the prior art by yielding a security device for small computers, cellular telephones and the like which can be programmed as firmware onto the non-volatile memory (such as ROM BIOS, ROM, Flash ROM, EPROM, EEPROM or the like) of such devices. Accordingly, no physical alteration is necessary or apparent to a thief. The existence of the security device is well cloaked and thus it cannot be readily located or disabled even if the possibility of its existence is suspected. Apparatuses and methods according to the invention can be very cost effective, requiring relatively inexpensive modifications to software or hardware and operation of relatively few monitoring devices.” (Cotichini, 2:27-67) “Referring to FIG. 1, the preferred embodiment of the electronic article surveillance system is comprised of three main components: (1) client device A consisting of any one of the electronic devices shown which have been implanted with the agent; (2) A telecommunication link B such as a switched communications system, the Internet,

***Softex LLC v. Defendants*, 1:22-cv-01308, 1:22-cv-01309, 1:22-cv-01311 (W.D. Tex.)
Defendants’ Initial Invalidity Contentions – Exhibit F-11**

Claim Element	Evidence of Invalidity
	radio tower, satellite and cable networks; and (3) The host monitoring system C which controls the communications between the client device A and the host monitoring system C.” (Cotichini, 6:22-30)

Claim Element	Evidence of Invalidity
	The diagram illustrates the CompuTrace system architecture. At the top, an 'Agent' (A) is implanted on a 'Client' device (A1), which can be a Computer, Cablevision Device, Laptop Computer, or Electronic Device (A2-A4). These devices connect to a 'Private Network' (L5) via a 'Leased Line' (L9) or 'Cable' (L2). The Private Network connects to 'The Internet' (B5) via a 'Telecom--munication Link' (B). The Internet connects to an 'Internet Provider' (L7) via a 'Telephone Line' (L6). The Internet Provider connects to a 'Public Switched Telephone Network (PSTN)' (B1) via a 'Telephone Line' (B6). The PSTN connects to a 'Cable Network' (B2) via a 'Cable' (B1). The Cable Network connects to a 'Radio tower' (B3) via a 'Cable' (B2). The Radio tower connects to a 'Satellite' (B4) via a 'Radio tower' (B3). The Satellite connects to a 'Satellite Dish' (C1) via a 'Radio tower' (B3). The Satellite Dish connects to a 'Processing, Auditing and Communication' unit (C2) via a 'Radio tower' (B3). The Processing unit connects to a 'Host' Monitoring System (C) via a 'Radio tower' (B3). The Host Monitoring System connects to a 'Computer' (N1) via a 'Radio tower' (B3). The Computer connects to a 'Fox' (N2), a 'Pager' (N3), and a 'Phone' (N4) via a 'Radio tower' (B3). The Computer also connects to an 'Automatic Number Identification Dialed Number Identification' unit (N5) via a 'Radio tower' (B3). The Automatic unit connects to a 'Notify Owners' unit (C3) via a 'Radio tower' (B3). The Notify Owners unit connects to an 'Owner' (O) via a 'Radio tower' (B3). FIG. 1

**Softex LLC v. Defendants, 1:22-cv-01308, 1:22-cv-01309, 1:22-cv-01311 (W.D. Tex.)
Defendants' Initial Invalidity Contentions – Exhibit F-11**

Claim Element	Evidence of Invalidity
	A1 to be monitored and through the use of (i) the public switched telephone network B1, (ii) the Internet B5, and (iii) local area networks B7, the CompuTrace server 3 maintains a database of records on computer A1's location and movements. Tracking information is collected during periodic telephone calls to the CompuTrace server 3; wherein server 3 identifies the unique agent A and obtains the phone number from which that call has been made. Once installed, the operation of the remote CompuTrace software is invisible to the user, and calls are made without the user's explicit awareness.” (Cotichini, 29:58-30:5) “The above description relates to the agent security system installed and operating in a conventional PC with an Intel 80X86 microprocessor or equivalent and with a conventional MS-DOS or PC-DOS operating system. It will be recognized that the system can be modified to fit other types of computers including, for example, those sold under the trademark Macintosh. The system can easily be modified to suit other types of operating systems or computers as they develop.” (Cotichini, 27:36-44) <i>See also</i> Ex. B Claim 1[pre] for Cotichini. <i>To the extent that the preamble is not fully disclosed or suggested by Cotichini, the preamble would have been obvious to a person of ordinary skill in the art in combination with the general knowledge in the field, common sense, and/or with any of the references identified in the Initial Invalidity Contentions.</i>
9[a] receiving, at a mobile electronic device, a request from an owner of the mobile electronic device to register the mobile electronic device with a security service residing at least partially on one or more servers;	<i>This limitation is disclosed or suggested by Cotichini. For example:</i> <i>See claim 1[c][i].</i> <i>To the extent that this limitation is not fully disclosed or suggested by Cotichini, this limitation would have been obvious to a person of ordinary skill in the art in combination with the</i>

**Softex LLC v. Defendants, 1:22-cv-01308, 1:22-cv-01309, 1:22-cv-01311 (W.D. Tex.)
Defendants' Initial Invalidity Contentions – Exhibit F-11**

Claim Element	Evidence of Invalidity
9[b] in response to the request from that owner, registering the mobile electronic device with the security service;	<i>general knowledge in the field, common sense, and/or with any of the references identified in the Initial Invalidity Contentions.</i> <i>This limitation is disclosed or suggested by Cotichini. For example:</i> “Agent 464 silently calls into monitoring center 472 on a periodic (programmable) basis. Call and other PC asset management activity is logged, and reported to customers on-demand via the web-based Online Monitoring Service 468. The online monitoring service database 470 may include the following: Call-in phone number (retrieval option includes: name and address), Birth Certificate information such as file 451, Dynamic System information files such as file 476 (NetCensus, Asset Insight, etc.) Customer-created information files such as file 474” (Cotichini, 29:39-52) “We have identified four potential OEM configurations which embed the SPC. The SPC is disabled Provided for future use by the full CompuTrace driver suite. The SPC operates independently Provided for protecting the unit from the point of manufacture, through the channel, then disabled when identified as a legitimate sale. The SPC is bundled with the full CompuTrace driver suite. Provided as a value-added service for end-users direct from the point of manufacture.

**Softex LLC v. Defendants, 1:22-cv-01308, 1:22-cv-01309, 1:22-cv-01311 (W.D. Tex.)
Defendants’ Initial Invalidity Contentions – Exhibit F-11**

Claim Element	Evidence of Invalidity
	The SPC operates independently and is bundled with the full CompuTrace driver suite. A combination of channel protection and value-added protection for the end-user.” (Cotichini, 32:50-64) “Enable Monitoring... This command allows a configuration application to enable the monitoring service of the Modem Agent. This command is used to re-enable monitoring if the service has previously been disabled.” (Cotochini, 23:27-31) “Referring to FIG. 1, the preferred embodiment of the electronic article surveillance system is comprised of three main components: (1) client device A consisting of any one of the electronic devices shown which have been implanted with the agent; (2) A telecommunication link B such as a switched communications system, the Internet, radio tower, satellite and cable networks; and (3) The host monitoring system C which controls the communications between the client device A and the host monitoring system C.” (Cotichini, 6:22-30)

Claim Element	Evidence of Invalidity
	The diagram illustrates the CompuTrace system architecture. At the top, an 'Agent' is implanted on a 'Client Device' (A1), which can be a Computer, Cablevision Device, Laptop Computer, or Electronic Device (A2-A4). These devices connect to various networks: Private Network (L5), Leased Line (L9), The Internet (L7), Public Switched Telephone Network (PSTN) (L6), Cable Network (B1), and Satellite (B3, B4). The PSTN connects to a Telephone Line (B6) and an Internet Provider (B7). The Internet connects to an Internet Provider (B7). The Cable Network connects to a Cable (B2). The Satellite connects to a Radio tower (B3) and a Satellite Dish (C1). The central 'Computer' (3) is connected to a 'Host' Monitoring System (C) and an 'Automatic Number Identification Dialed Number Identification' (N1). The Computer also connects to a 'Pager' (N3), 'Phone' (N4), 'Fax' (N2), and 'E-mail' (N1). The Host Monitoring System connects to a 'Processing, Auditing and Communication' (C2) and 'Notify Owners' (C3). The diagram is labeled 'FIG. 1'. (Cotichini, FIG. 1) “CompuTrace is designed as a system to track the physical location of computers. The CompuTrace Agent such as agent A of FIG. 1 is installed on a remote computer.

**Softex LLC v. Defendants, 1:22-cv-01308, 1:22-cv-01309, 1:22-cv-01311 (W.D. Tex.)
Defendants’ Initial Invalidity Contentions – Exhibit F-11**

Claim Element	Evidence of Invalidity
	A1 to be monitored and through the use of (i) the public switched telephone network B1, (ii) the Internet B5, and (iii) local area networks B7, the CompuTrace server 3 maintains a database of records on computer A1’s location and movements.” (Cotichini, 29:58-65) See also Cotichini, 14:48-51 (referring to a “host monitoring server”), FIG. 7B (illustrating a “server 762” and flow node “agent establishes communication link with remote server”), FIG. 23 (same)). <i>To the extent that this limitation is not fully disclosed or suggested by Cotichini, this limitation would have been obvious to a person of ordinary skill in the art in combination with the general knowledge in the field, common sense, and/or with any of the references identified in the Initial Invalidity Contentions.</i>
9[c] automatically sending identifying information for the mobile electronic device from the mobile electronic device to the security service;	<i>This limitation is disclosed or suggested by Cotichini. For example:</i> See claim 1[c][ii]. <i>To the extent that this limitation is not fully disclosed or suggested by Cotichini, this limitation would have been obvious to a person of ordinary skill in the art in combination with the general knowledge in the field, common sense, and/or with any of the references identified in the Initial Invalidity Contentions.</i>
9[d] after the owner has registered the mobile electronic device with the security service, periodically communicating with the security service, when the mobile electronic device is in a state other than a state in which the mobile electronic device is powered off;	<i>This limitation is disclosed or suggested by Cotichini. For example:</i> See claim 1[c][iii]. <i>To the extent that this limitation is not fully disclosed or suggested by Cotichini, this limitation would have been obvious to a person of ordinary skill in the art in combination with the general knowledge in the field, common sense, and/or with any of the references identified in the Initial Invalidity Contentions.</i>

**Softex LLC v. Defendants, 1:22-cv-01308, 1:22-cv-01309, 1:22-cv-01311 (W.D. Tex.)
Defendants' Initial Invalidity Contentions – Exhibit F-11**

Claim Element	Evidence of Invalidity
9[e] after the owner has registered the mobile electronic device with the security service, accepting a notification from the security service, wherein the notification comprises a message indicating that the owner of the mobile electronic device has reported a loss or requested disabling of the mobile electronic device;	<i>This limitation is disclosed or suggested by Cotichini. For example:</i> See claim 1[c][iv]. <i>To the extent that this limitation is not fully disclosed or suggested by Cotichini, this limitation would have been obvious to a person of ordinary skill in the art in combination with the general knowledge in the field, common sense, and/or with any of the references identified in the Initial Invalidity Contentions.</i>
9[f] in response to accepting the notification, automatically disabling at least one user function of the mobile electronic device while still allowing the mobile electronic device to communicate with the security service; and	<i>This limitation is disclosed or suggested by Cotichini. For example:</i> See claim 1[c][v]. <i>To the extent that this limitation is not fully disclosed or suggested by Cotichini, this limitation would have been obvious to a person of ordinary skill in the art in combination with the general knowledge in the field, common sense, and/or with any of the references identified in the Initial Invalidity Contentions.</i>
9[g] automatically causing at least some user data to be copied from the mobile electronic device to at least one of the servers;	<i>This limitation is disclosed or suggested by Cotichini. For example:</i> See claim 1[c][vi]. <i>To the extent that this limitation is not fully disclosed or suggested by Cotichini, this limitation would have been obvious to a person of ordinary skill in the art in combination with the general knowledge in the field, common sense, and/or with any of the references identified in the Initial Invalidity Contentions.</i>
9[h] wherein the mobile electronic device comprises non-volatile memory;	<i>This limitation is disclosed or suggested by Cotichini. For example:</i> See claim 1[d].

Softex LLC v. Defendants, 1:22-cv-01308, 1:22-cv-01309, 1:22-cv-01311 (W.D. Tex.)
Defendants’ Initial Invalidity Contentions – Exhibit F-11

Claim Element	Evidence of Invalidity
9[i] wherein the non-volatile memory comprises a changeable area that can be modified by a user and system area that cannot be modified by the user;	<i>To the extent that this limitation is not fully disclosed or suggested by Cotichini, this limitation would have been obvious to a person of ordinary skill in the art in combination with the general knowledge in the field, common sense, and/or with any of the references identified in the Initial Invalidity Contentions.</i> <i>This limitation is disclosed or suggested by Cotichini. For example:</i> <i>See claim 1[e]</i> <i>To the extent that this limitation is not fully disclosed or suggested by Cotichini, this limitation would have been obvious to a person of ordinary skill in the art in combination with the general knowledge in the field, common sense, and/or with any of the references identified in the Initial Invalidity Contentions.</i>
9[j] wherein the security application utilizes code residing at least partially in the system area; and	<i>This limitation is disclosed or suggested by Cotichini. For example:</i> <i>See claim 1[f]</i> <i>To the extent that this limitation is not fully disclosed or suggested by Cotichini, this limitation would have been obvious to a person of ordinary skill in the art in combination with the general knowledge in the field, common sense, and/or with any of the references identified in the Initial Invalidity Contentions.</i>
9[k] wherein the operation of accepting the notification from the security service comprises receiving the notification from at least one of the servers via the system area.	<i>This limitation is disclosed or suggested by Cotichini. For example:</i> <i>See claim 1[g]</i> <i>To the extent that this limitation is not fully disclosed or suggested by Cotichini, this limitation would have been obvious to a person of ordinary skill in the art in combination with the general knowledge in the field, common sense, and/or with any of the references identified in the Initial Invalidity Contentions.</i>

**Softex LLC v. Defendants, 1:22-cv-01308, 1:22-cv-01309, 1:22-cv-01311 (W.D. Tex.)
Defendants' Initial Invalidity Contentions – Exhibit F-11**

Claim Element	Evidence of Invalidity
	Claim 10
10. A method according to claim 9, wherein the notification includes no third-party certification.	<i>This limitation is disclosed or suggested by Cotichini. For example:</i> See claim 2. <i>To the extent that this limitation is not fully disclosed or suggested by Cotichini, this limitation would have been obvious to a person of ordinary skill in the art in combination with the general knowledge in the field, common sense, and/or with any of the references identified in the Initial Invalidity Contentions.</i>
	Claim 15
15. A method according to claim 9, further comprise: after the at least some user data has been copied from the mobile electronic device to at least one of the servers, causing at least some of the user data to be deleted from the mobile electronic device.	<i>This limitation is disclosed or suggested by Cotichini. For example:</i> See claim 7. <i>To the extent that this limitation is not fully disclosed or suggested by Cotichini, this limitation would have been obvious to a person of ordinary skill in the art in combination with the general knowledge in the field, common sense, and/or with any of the references identified in the Initial Invalidity Contentions.</i>