

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

MICROSOFT CORPORATION

Petitioner,

v.

SOFTEX, LLC

Patent Owner.

Case No. IPR2023-01185

Patent No. 8,506,649

PETITION FOR *INTER PARTES* REVIEW
UNDER 35 U.S.C. §§ 311-319 AND 37 C.F.R. § 42.1 *et seq.*

TABLE OF CONTENTS

I.	MANDATORY NOTICES	vii
A.	Real Party-In-Interest – § 42.8(b)(1).....	vii
B.	Related Matters – § 42.8(b)(2)	viii
1.	United States Patent & Trademark Office	viii
2.	District Court Matters	viii
C.	Counsel and Service Information – § 42.8(b)(3) and (b)(4)	ix
II.	INTRODUCTION	1
III.	CERTIFICATION OF STANDING	2
IV.	UNPATENTABILITY GROUNDS.....	2
V.	THE '649 PATENT.....	2
A.	Overview of the '649 Patent.....	2
1.	Registering Device with Security Service	3
2.	Periodically Checking Device Status.....	4
3.	Security Notifications and Associated Responses	4
4.	Protecting the Security Application from Modification	5
B.	Challenged Claims	6
C.	Level of Ordinary Skill in the Art.....	7
D.	Prosecution History	7
VI.	CLAIM INTERPRETATION	9
VII.	GROUNDS FOR UNPATENTABILITY	9
A.	Ground 1A: Claims 1-5, 7-13, 15-21, and 23-25: Anticipated and/or Obvious Over Andrews.....	9
1.	Andrews (EX1005)	9
a.	Registering Device with Security Service	11
b.	Periodically Checking Device Status	12
c.	Security Notifications and Associated Responses.....	13
2.	Independent Claims	14
a.	Preambles.....	14

b.	Structural Limitations	15
c.	Security Application Limitations	16
d.	Registration Limitations	17
e.	Sending Identifying Information Limitations.....	21
f.	Periodic Communication Limitations.....	24
g.	Security Notification Limitations	27
h.	Device Disabling Limitations.....	28
i.	Copying User Data Limitations.....	31
j.	Deleting User Data Limitation	34
k.	Restoring User Data Limitation.....	36
l.	Memory Area Limitations	39
3.	Claims 2, 10, and 18	43
4.	Claims 7, 15, and 23	44
5.	Claims 8, 16, and 24	44
6.	Claims 3-5, 11-13, and 19-21	44
B.	Ground 1B: Claims 1-5, 7-13, 15-21, and 23-25 Obvious over Andrews and Bonnett.....	48
1.	Bonnett.....	48
a.	Bonnett Overview	48
b.	Bonnett is Prior Art as of its Provisional.....	50
2.	Reasons to Combine Andrews and Bonnett	52
3.	Claim Analysis.....	58
a.	Independent Claims	58
b.	Dependent Claims.....	60
(1)	Claims 2, 10, and 18.....	60
(2)	Claims 3-5, 11-13, and 19-21.....	60
(3)	Claims 7, 15, and 23.....	60
(4)	Claims 8, 16, and 24.....	60
C.	Ground 1C: Claims 1-5, 7-13, 15-21, and 23-25 Obvious over Andrews and Cotichini.....	61

1.	Cotichini (EX1007).....	61
2.	Reasons to Combine Andrews with Cotichini.....	66
3.	Claim Analysis.....	69
a.	Independent Claims	69
a.	Dependent Claims.....	74
(1)	Claims 2, 10, and 18.....	74
(2)	Claims 3-5, 11-13, and 19-21.....	74
(3)	Claims 7, 15, and 23.....	75
(4)	Claims 8, 16, and 24.....	75
D.	Ground 1D: Claims 6, 8, 14-16, and 22-25 Obvious over Andrews and Hayward	75
1.	Hayward (EX1008).....	75
2.	Andrews-Cotichini-Hayward Combination.....	77
3.	Independent Claim 25.....	79
a.	Deleting User Data Limitations.....	79
b.	Restoring User Data Limitations	80
4.	Claims 6, 14, and 22	80
5.	Claims 7, 15, and 23	82
6.	Claims 8, 16, and 24	82
VIII.	NO BASIS FOR DISCRETIONARY DENIAL	83
A.	35 U.S.C. § 325(d).....	83
B.	35 U.S.C. § 314(a).....	84
IX.	CONCLUSION.....	86
X.	CLAIM LISTING.....	89

TABLE OF AUTHORITIES

Cases	Page(s)
<i>AC Techs., S.A. v. Amazon.com, Inc.</i> , 912 F.3d 1358 (Fed. Cir. 2019)	43
<i>Becton, Dickinson & Co. v. B. Braun Melsungen AG</i> , IPR2017-01586, Paper 8 (P.T.A.B. Dec. 15, 2017)	83
<i>Commscope Techs. LLC v. Dali Wireless, Inc.</i> , IPR2022-01242, Paper 23 (P.T.A.B. Feb. 27, 2023).....	86
<i>Dynamic Drinkware, LLC v. Nat’l Graphics, Inc.</i> , 800 F.3d 1375 (Fed. Cir. 2015)	50
<i>KSR Int’l v. Teleflex</i> , 550 U.S. 398 (2007).....	48, 78
<i>Thryv, Inc. v. Click-to-Call Techs., LP</i> , 140 S.Ct. 1367 (2020).....	84
<i>Vivid Techs. v. Am. Sci. & Eng’g</i> , 200 F3d 795 (Fed. Cir. 1999)	9
 Statutes, Rules & Regulations	
37 C.F.R. § 42.100(b)	9

APPENDIX LISTING OF EXHIBITS

Exhibit	Description
1001	U.S. Patent No. 8,506,649 (“’649 patent”)
1002	Prosecution History of U.S. Patent No. 8,506,649
1003	Declaration of John Black, PhD
1004	CV of John Black, PhD
1005	WIPO Pub. No. WO2001084455 (“Andrews”)
1006	U.S. Patent Pub. No. 2003/0051090 (“Bonnett”)
1007	WIPO Pub. No. 1998/043151 (“Cotichini”)
1008	UK Pat. App. No. GB2369205A (“Hayward”)
1009	U.S. Pat. App. 60/322,252 (“Bonnett Provisional”)
1010	Kingpin and Mudge, <i>Security Analysis of the Palm Operating System and its Weaknesses Against Malicious Code Threats</i> , Proceedings of the 10 th USENIX Security Symposium (August 13-17, 2001)
1011	U.S. Pat. No. 5,764,892
1012	U.S. Patent Pub. No. 2003/0126462
1013	U.S. Patent Pub. No. 2004/0110488
1014	U.S. Pat. No. 5,987,609
1015	Microsoft Computer Dictionary, Microsoft Press (2002 5 th ed.) (excerpts)
1016	Newton’s Telecom Dictionary, CMP Books (2003 19 th ed.) (excerpts)
1017	Webster’s New World Computer Dictionary, Houghton Mifflin (2003 10 th ed.) (excerpts)
1018	WIPO Pub. No. 1996/36194
1019	UK Pat. App. No. GB2349044A
1020	<i>Softex LLC v. Absolute Software Corp.</i> , <i>Softex LLC v. Dell Technologies Inc.</i> , <i>Softex LLC v. HP Inc.</i> , Joint Rule 26(f) Report and Discovery Plan
1021	Fact Sheet for Senior Judge David Alan Ezra

1022	<i>Digital cellular telecommunications system (Phase 2+); Mobile Stations (MS features)</i> (GSM 02.07), Version 5.1.0, July 1996
1023	<i>Digital cellular telecommunications system (Phase 2+); International Mobile station Equipment Identities (IMEI)</i> (GSM 02.16), Version 5.2.0, August 2000
1024	<i>Digital cellular telecommunications system (Phase 2+); Numbering, addressing and identification</i> (GSM 03.03), Version 5.0.0, March 1996
1025	United States District Courts – National Judicial Caseload Profile
1026	Andrei Khurshudov, <i>The Essential Guide to Computer Data Storage From Floppy to DVD</i> , Prentice Hall (2001) (excerpts)

I. MANDATORY NOTICES

A. Real Party-In-Interest – § 42.8(b)(1)

Petitioner Microsoft Corporation (“Petitioner”) is the real party-in-interest.

Out of an abundance of caution and without conceding that they are real parties-in-interest, Petitioner discloses that Dell Inc.; Dell Technologies Inc.; HP Inc.; Lenovo (Shanghai) Electronics Technology Co. Ltd.; Lenovo Group, Ltd.; Lenovo Beijing, Ltd.; Lenovo PC HK Limited; and Lenovo (United States), Inc. have been named as defendants in co-pending litigations filed in or after December 2022 (listed below) based, in part, on alleged activities relating to products incorporating Microsoft software. Whether such third parties are real parties-in-interest should not be resolved in this proceeding because it has no impact on this proceeding, including because even a determination that these parties are real parties-in-interest would not result in the application of any estoppel or time-bar under 35 U.S.C. § 315. *Unified Patents, LLC v. MemoryWeb, LLC*, Decision Granting Director Review Vacating-in-part the Final Written Decision and Vacating Board Order, IPR2021-01413, Paper 76, 5 (PTAB May 22, 2023) (citing *SharkNinja Operating LLC v. iRobot Corp.*, IPR2020-00734, Paper 11, 18 (PTAB Oct. 6, 2020) (precedential)).

B. Related Matters – § 42.8(b)(2)

1. United States Patent & Trademark Office

U.S. Patent No. 8,506,649 (“the ’649 patent”) claims the benefit of provisional application No. 60/497,182. The ’649 patent is a divisional of application number 10/925,161.

2. District Court Matters

The ’649 patent is at issue in the following pending cases:

- *Softex LLC v. Lenovo (Shanghai) Elecs. Tech. Co. Ltd., et al.*, Case No. 5:23-cv-00090 (E.D.N.C.)
- *Softex LLC v. Absolute Software Corp. et al.*, Case No. 1:22-01308 (W.D. Tex.)
- *Softex LLC v. Dell Tech. Inc. et al.*, Case No. 1:22-01309 (W.D. Tex.)
- *Softex LLC v. HP Inc. et al.*, Case No. 1:22-01311 (W.D. Tex.)

C. Counsel and Service Information – § 42.8(b)(3) and (b)(4)

Lead Counsel	Carrie A. Beyer, Reg. No. 59,195 FAEGRE DRINKER BIDDLE & REATH LLP 320 S. Canal St., Suite 3300 Chicago, IL 60606	
Backup Counsel	Kirstin Stoll-DeBell, Reg. No. 43,164 Zachary D. Kachmer, Reg. No. 75,414 FAEGRE DRINKER BIDDLE & REATH LLP 1144 15th Street, Suite 3400 Denver, Colorado 80202	
Service Information	<u>E-Mail:</u>	carrie.beyer@faegredrinker.com kirstin.stolldeb主@faegredrinker.com zach.kachmer@faegredrinker.com
	<u>Post & Hand-Delivery:</u>	FAEGRE DRINKER BIDDLE & REATH LLP 320 S. Canal St., Suite 3300 Chicago, IL 60606
	<u>Telephone:</u>	(312) 569-1000
	<u>Facsimile:</u>	(312) 569-3000

Powers of attorney are submitted with this petition. Counsel for Petitioner consents to service of all documents via electronic mail.

Petitioner requests *inter partes* review of claims 1-25 of the '649 patent.

II. INTRODUCTION

Microsoft Corporation (“Petitioner”) petitions for *inter partes* review of claims 1-25 of U.S. Patent 8,506,649 (“the '649 patent,” EX1001).” The '649 patent concerns a “system and method for securing and tracking an electronic device.” EX1001, Abstract. The device includes a security application that “periodically check[s] with [a] server computer system to see if the electronic device is reported stolen.” EX1001, 26:15-17. “[I]f the device is reported stolen, the ESTSM server may inform the ESTSM device...to take the appropriate action based on the service options selected by the user (e.g. disabling the electronic device...and more).” EX1001, 2:2-8. The security application is installed “to make sure that someone cannot bypass or circumvent the ESTSM application.” EX1001, 18:13-24, 18:62-65.

Security systems of this type were well-known before the '649 patent. Petitioner, supported by the declaration of Dr. John Black, demonstrates that the challenged claims are unpatentable.

Ground 1A demonstrates that Claims 1-5, 7-13, 15-21, and 23-25 are anticipated and/or rendered obvious by Andrews.

Ground 1B demonstrates that Claims 1-5, 7-13, 15-21, and 23-25 are obvious over Andrews and Bonnett.

Ground 1C demonstrates that Claims 1-5, 7-13, 15-21, and 23-25 are obvious over Andrews and Cotichini.

Ground 1D demonstrates that Claims 6, 8, 14-16, and 22-25 are obvious over Andrews, Cotichini, and Hayward.

III. CERTIFICATION OF STANDING

The '649 patent is available for IPR, and Petitioner is not barred or estopped from requesting IPR.

IV. UNPATENTABILITY GROUNDS

Petitioner requests cancellation of claims 1-25 as follows:

Ground	Reference(s)	Claim(s)	Basis
1A	Andrews	1-5, 7-13, 15-21, and 23-25	102/103
1B	Andrews-Bonnett	1-5, 7-13, 15-21, and 23-25	103
1C	Andrews-Cotichini	1-5, 7-13, 15-21, and 23-25	103
1D	Andrews-Cotichini-Hayward	6, 8, 14-16, and 22-25	103

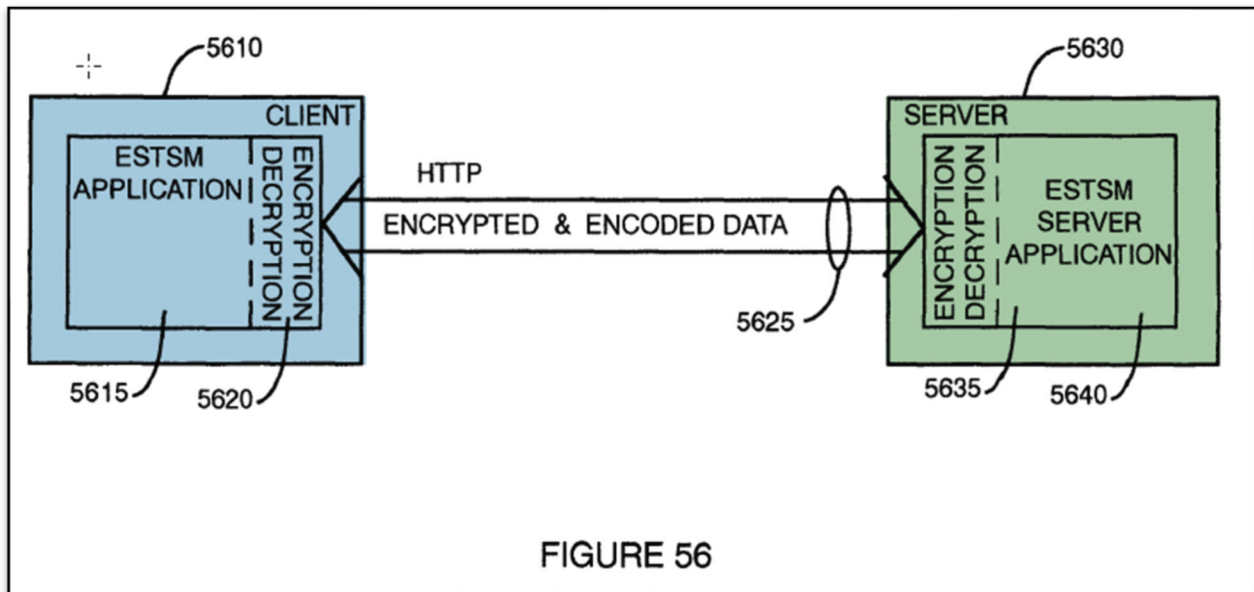
V. THE '649 PATENT¹

A. Overview of the '649 Patent

The '649 patent concerns an “electronic device security and tracking system and method (ESTSM).” EX1001, 1:37-40; EX1003, ¶74. The ESTSM generally includes an **ESTSM client device** (e.g., computer/PDA) that communicates via a network with one or more **ESTSM server(s)** (as shown in Fig. 56 below). 1:41-

¹ Unless otherwise noted, Section V's citations are to EX1001.

2:15; EX1003, ¶75; *see also* 1:30-32, 10:45-53, 17:49-55, 19:18-26, 19:30-35, 20:1-7, 20:21-31, 23:29-33.



In operation, the ESTSM device and server communicate to perform the following tasks to secure a client device, EX1003, ¶76:

1. Registering Device with Security Service

“If the electronic device is not registered for ESTSM services, then upon first time power-on and connection to the ESTSM server..., the user is prompted to register for different ESTSM services.” 1:48-52; EX1003, ¶77-79, 85-87. During registration, “[a] user creates an account..., specifies what ESTSM services he wishes to purchase,” 7:18-22, 8:7-56, such as having “the electronic device disabled when it is stolen,” 8:24-25.

2. Periodically Checking Device Status

After registration, the ESTSM device “periodically check[s]” with the ESTSM server over the Internet to determine whether the device has been reported stolen. 26:11-17; *see also* 7:31-33, 26:11-17, 26:57-61, 60:60-63; EX1003, ¶80-82. The ESTSM application sends a query to the ESTSM server that identifies the device by its “device system information” and, in response, receives the device status. 26:39-53. The application “wait[s] an interval and again contact[s] the ESTSM server.” 26:61-63.

3. Security Notifications and Associated Responses

“[T]he user can report the device as stolen” through the ESTSM system. 7:24-27; *see also* 7:33-39, 17:55-61, 26:63-67, 7:25-27, 10:10-14, 10:29-32, 13:10-12, 15:61-63; EX1003, ¶80. For example, “the user may click on the button labeled ‘Report Stolen’” at the ESTSM server. 10:27-37, 2:31-37, 10:33-37. In response, the ESTSM server may send messages with commands (“Cmd”) to be performed by the ESTSM device. Fig. 71; EX1003, ¶88-97.

For example, “[t]he ESTSM server may send a ‘DISABLE’ command.” 34:18-22. If such a command is sent, “the mobile device is disabled.” 34:15-18. Once the device is put in the DISABLED state, “[t]he system is now in the locked state and can not be used.” 13:35-39; *see also* 15:35-38, 26:67-27:6, 33:35-40, 33:47-50.

“If the Cmd is ‘BACKUP’..., the ESTSM server requests that the data on the mobile device be copied to the ESTSM server.” 34:22-28; *see also* 33:28-34, 34:57-60, 35:16-22. For example, “if during ESTSM registration the user had selected recovery of contacts and calendar data, these items will be backed-up.” 34:28-30.

The Cmd may be “ERASE HARDDISK” if “the user selected ‘Data Destroy Services’ option when registering.” 14:21-23. In this state, “the Application component on the electronic device erases the hard disk drive.” 16:2-5.

“If the Cmd is ‘RESTORE’..., the ESTSM server starts to restore the data 7199 backed up from the mobile device back to the original mobile device that may have been recovered or a new mobile device.” 34:37-46; *see also* 35:27-34, 35:34-39.

4. Protecting the Security Application from Modification

The ESTSM electronic device includes both processing components and various types of memory, such as a volatile memory that runs programs and a non-volatile memory such as Read-Only Memory (ROM) or flash memory. 19:8-18, 20:27-41, 20:55-64, 22:9-18; EX1003, ¶99.

The ’649 patent discloses aspects of the ESTSM meant to protect the ESTSM from user modification. EX1003, ¶99-100. For example, the ESTSM may protect itself by storing portions of the application in a “system area” that “is not

changeable by the user of the electronic device.” 3:44-49. In some instances, the system area is “flash memory” that “contain[s] ESTSM application programs,” is “non-viewable,” and is “implemented in non-volatile memory.” 19:8-18; *see also* 20:14-22. Additionally, ESTSM components may reside in a “hidden partition on the hard disk drive” or in a “Host Protected Area...that is not accessible by the operating system.” 2:48-53; *see also*, 31:29-43. The ESTSM may also utilize a “secure nonvolatile area that stores critical information present after electronic device power-off,” 2:61-66, including a “small piece of code...in the system BIOS ROM image,” 17:62-64. *See also* 18:3-12. The ’649 patent explains that these techniques “ensure[] that a thief cannot bypass or circumvent the ESTSM application from running.” 2:66-3:5.

B. Challenged Claims

Challenged system claims 1-25 are reproduced in the Claim Listing. *Infra* §X. Independent claims 1 and 17 each recite an apparatus storing software instructions that cause a security application to perform operations including (1) registering with a security service on a server; (2) periodically communicating with and sending device information to the server; and (3) receiving a security

notification and performing responsive actions. Independent claims 9 and 25 each recite a method comprising similar operations. EX1003, ¶109-111.

The dependent claims further specify common types of conventional implementation choices for a security service. For instance, the dependent claims recite scenarios in which the lost/stolen notification received by the device does not include a third-party certification (claims 2, 10, 18), the lost/stolen notification is an SMS message (claims 6, 14, 22), and the identifying information includes one or more standard device identifiers (claims 3-5, 11-13, 19-21).

C. Level of Ordinary Skill in the Art

A POSITA would have had a bachelor's degree in computer science, computer engineering, electrical engineering, or the equivalent and at least two years of experience in the relevant field, *e.g.*, electronic communications and/or computer security systems. EX1003, ¶29-73.

D. Prosecution History

The as-filed application included 52 claims. EX1002, 61-68. After a rejection, those 52 claims were canceled and replaced with 27 new claims. EX1002, 326-336.

Prior to allowance, the applicant faced several rejections under §§102 and 103. EX1003, ¶101-108. Of relevance to the grounds herein, the examiner rejected then-pending independent Claim 53 (which ultimately became issued Claim 1) as

anticipated by Komsí (2004/0110488, EX1013). EX1002, 70. In response, the applicant amended Claim 53, to recite, *inter alia*, “*wherein the non-volatile memory comprises...a system area that cannot be modified by the user*” and “*wherein the security application resides at least partially in the system area...and...receives the theft report from at least one of the servers via the system area.*” EX1002, 487-488. The applicant argued that these limitations were not disclosed by Komsí because Komsí “does not mention anything remotely pertaining to a system area that cannot be modified by a user.” EX1002, 498.

In the following office action, the examiner rejected the claims over Komsí in view of Hasebe (5,987,609, EX1014). EX1002, 508-518. The examiner stated, “analogous art Hasebe teaches...a security program storage area of the ROM,” explaining that “[s]ince [Hasebe’s] program is set up on the ROM, it cannot be altered or erased by a person using the information device.” EX1002, 513.

The applicant responded by amending Claim 53 to recite “*causing the mobile electronic device to periodically communicate with the security service*” and argued that Hasebe did not disclose such periodic communications. EX1002, 536-537, 546-550. The applicant did not dispute the examiner’s assertion that Hasebe’s ROM disclosed the claimed non-changeable system area or that it would have been obvious to combine Komsí’s lost-device system with Hasebe’s program in ROM. EX1002, 546-550.

The applicant received a notice of allowance only after Claim 53 was amended to recite “*automatically causing at least some user data to be copied from the mobile electronic device to at least one of the servers.*” EX1002, 597-606, 622-629.

VI. CLAIM INTERPRETATION

Claim limitations are construed according to their ordinary meaning in light of the specification and prosecution history. 37 C.F.R. §42.100(b). Because the prior art plainly discloses the claim limitations, no express constructions are necessary. *Vivid Techs. v. Am. Sci. & Eng’g*, 200 F3d 795, 803 (Fed. Cir. 1999); EX1003, ¶113.

VII. GROUNDS FOR UNPATENTABILITY

A. Ground 1A: Claims 1-5, 7-13, 15-21, and 23-25: Anticipated and/or Obvious Over Andrews²

1. Andrews (EX1005)

Andrews, published on November 8, 2001, is prior art under at least §102(b). EX1003, ¶116.

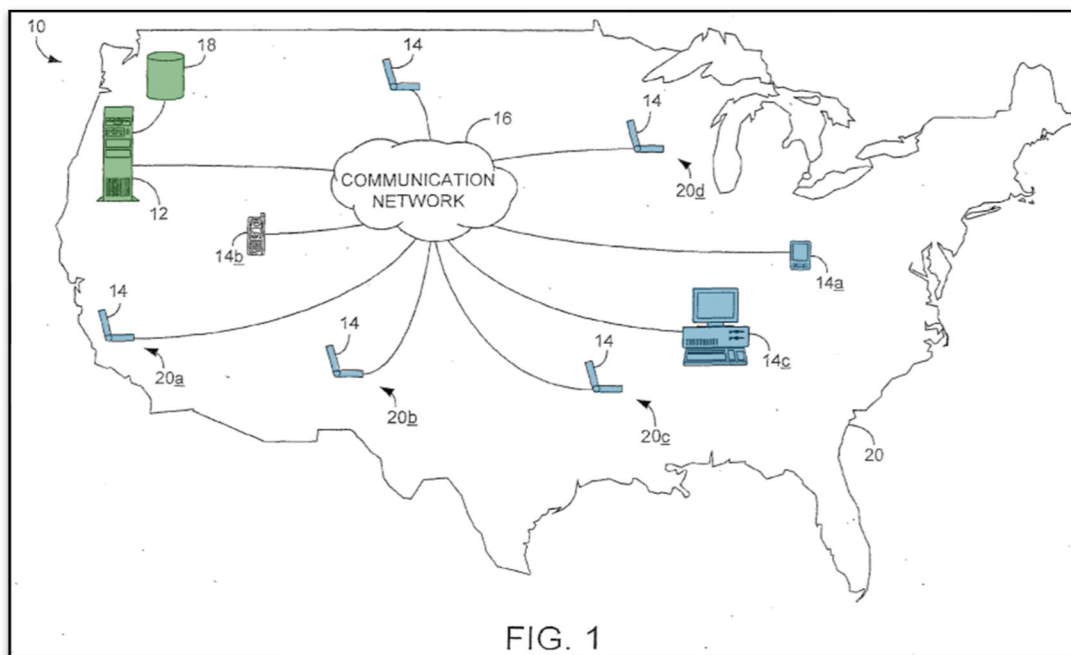
Like the ’649 patent, Andrews discloses security software for portable electronic devices, which are “particularly susceptible to loss and theft,” 1:13-14, and which store data that is “of a sensitive nature,” such that “public

² Unless otherwise noted, Section VII.A’s citations are to EX1005.

disclosure...may have detrimental consequences.” 1:17-19; EX1003, ¶117-121.

Like the '649 patent, Andrews's system causes “a responsive action to be taken in the event that a portable computing device becomes missing.” Abstract.

Like the '649 patent, Andrews discloses a “**host computer 12** and...**client computing devices**,” 8:4-8, linked by “communication network 16,” 13:3-19, as depicted below.



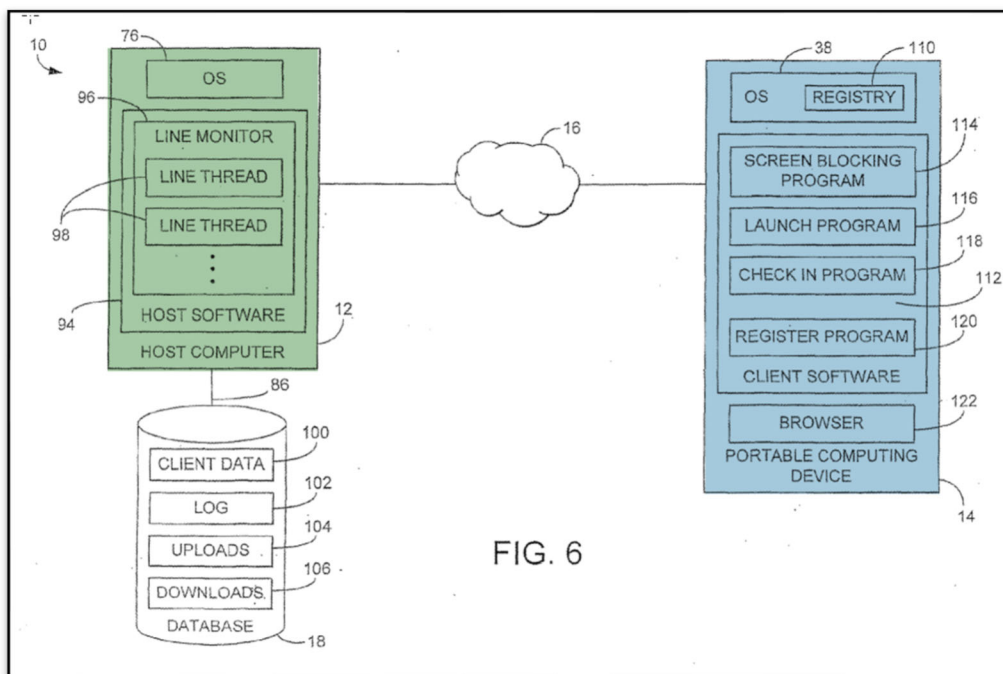


FIG. 6

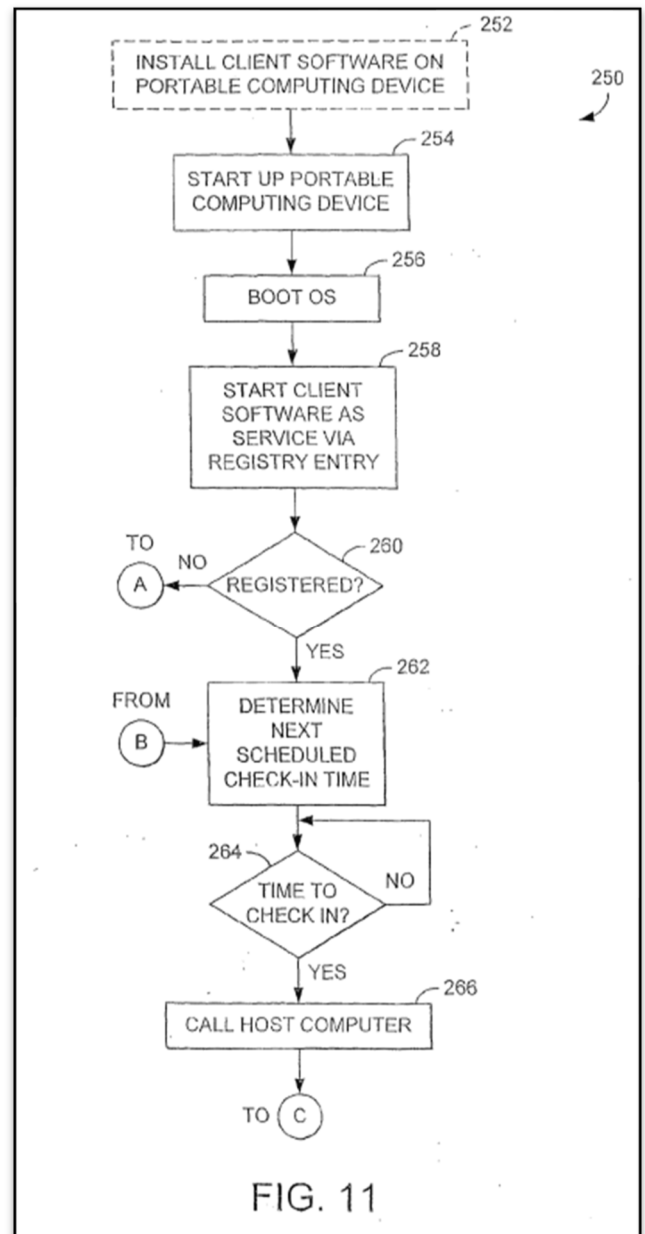
Andrews's client computing device can be a "portable computing device 14 such as a laptop computer[,],...personal data assistant (PDA) 14a, cellular phone 14b, or virtually any other portable computing device." 8:18-9:7. The device contains conventional components, such as a processor and memory. 10:3-11.

a. Registering Device with Security Service

Like the '649 patent, Andrews teaches that the security program on the portable device is registered with a server (i.e., the host computer 12). EX1003, ¶121-125. The client device runs "client programs" or "client software." 15:8-14. Client software may be a "security product," which "has features such as...retrieving and deleting data, tracking the location of the portable computing device, and locking up the portable computing device." 34:10-13. The software

may be run as a “service of the operating system” or “may be in firmware 25 or ROM BIOS 34 routines executed on start-up.” 32:9-14.

Andrews’s Figure 11 depicts the high-level operation of the client software. EX1003, ¶123-126. At step 252, the software is installed. 31:21-32:2. At 260, it is determined whether the client software is registered. 32:15-16. If not, a “registration program” “receive[s] user information” and sends it to “host computer” for storage. 16:9-11, 33:21-34:6. The software determines hardware and software configuration and sends it to host computer. 24:16-21, 35:15-20, 16:11-14.



b. Periodically Checking Device Status

Like the '649 patent, Andrews teaches that once the device is registered, Andrews’s security software runs a “check-in program,” “that periodically causes the portable computing device to contact the host computer according to the

contact schedule.” 29:7-9, 30:8-21; 33:2-6; EX1003, ¶127-131. In response, the client software receives a “reported status 148 of portable computing device.” 19:6-13. “The reported status may be virtually any status,” such as “NORMAL, MISSING, LOST, STOLEN, [etc.]” 19:14-16.

c. Security Notifications and Associated Responses

Like the '649 patent, the portable device can be reported as missing, lost, or stolen. 27:16-21; EX1003, ¶127-128. The report may be made “via a telephone call, email, online form, or virtually any other suitable communications method.” 19:6-13, 27:16-21, 37:6-13.

The host computer sends the reported status to the portable computing device, along with a “responsive action,” which “may be virtually any action,” such as “retrieving data..., deleting data..., [or] restricting access...” 28:17-22, 30:13. The host computer 12 “instruct[s] portable computing device 14 to take responsive action.” 30:13; EX1003, ¶129-131.

For example, a “LOCK-UP DEVICE” action will “instruct portable computing device 14 to restrict user access to portable computing device,” such as by “locking up the GUI” and/or “restricting the user’s access privileges” using a “screen-blocking program.” 22:21-23; 45:6-46:3.

The action “RETRIEVE FILE” will “instruct portable computing device 14 to transfer a file...to host computer....” 21:16-23, 34:10-13.

A “DELETE FILE” action will “instruct portable computing device 14 to delete a file....” 22:10-12, 40:14-19.

The “DOWNLOAD FILE” action “causes host computer 12 to download a file to portable computing device.” 23:7-10, 42:15-20.

2. Independent Claims

a. Preambles

[1P]	<i>A mobile electronic device, comprising:</i>
[9P]	<i>A method for providing security for a mobile electronic device, the method comprising:</i>
[17P]	<i>An article of manufacture comprising:</i>
[25P]	<i>A method for providing security for a mobile electronic device, the method comprising:</i>

To the extent they are limiting, Andrews discloses the preambles. Andrews discloses a “portable computing device,” which is a *mobile electronic device*. 8:4-9, 8:18-9:7. EX1003, ¶133-134. The computing device “includes a...memory 24 [and] a mass storage device 26,” each of which stores computer-readable instructions and which—independently or with the computing device—constitutes an *article of manufacture*. 10:3-14, EX1003, ¶216-217.

Andrews discloses “a method of communicating between a portable computing device and a host computer,” which is a *method for providing security*

for the mobile device. 3:2-5; see also 1:7-8, 1:13-14 (identifying loss/theft of portable electronic devices as problem to be addressed); EX1003, ¶197-198.

b. Structural Limitations

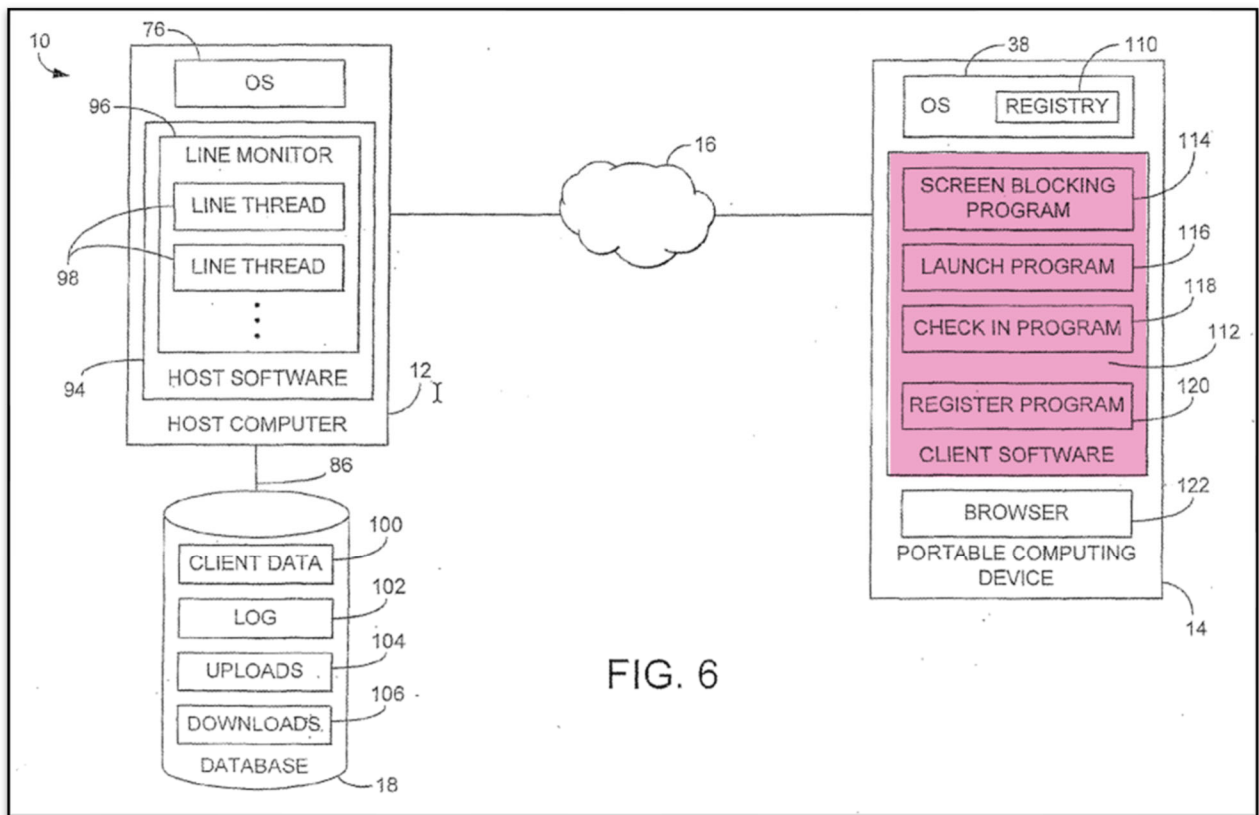
[1A]	<i>a processor;</i>
[1B]	<i>one or more non-transitory machine-readable storage media responsive to the processor...wherein the one or more non-transitory machine-readable storage media comprises non-volatile memory;</i>
[9A]	<i>wherein the mobile electronic device comprises non-volatile memory;</i>
[17A]	<i>a non-transitory machine-readable storage medium; and . . . non-volatile memory in the mobile phone</i>
[25A]	<i>wherein the mobile electronic device comprises non-volatile memory;</i>

Andrews discloses these Structural Limitations. EX1003, ¶135-138, 199-200, 218-219, 239-240. Andrews’s “portable computing device 14 typically includes a central processing unit 22.” 10:3-4. Thus, Andrews discloses the *processor* of claim 1. EX1003, ¶136. The portable computing device further includes “memory 24 [and] a mass storage device 26.” 10:3-14. As Andrews explains, “[m]ass storage device 26 may also be flash memory,” 10:6-8, while “[m]emory 24 typically includes...read only memory (ROM) 32.” 10:9-11. A POSITA would have understood flash memory and ROM to each be examples of *non-transitory machine-readable storage media* comprising *non-volatile memory*. EX1003, ¶137-138.

c. Security Application Limitations

[1C]	<i>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>
[17B]	<i>a security application encoded as instructions in the non-transitory machine-readable storage medium, wherein the security application, when executed by a mobile electronic device, enables the mobile electronic device to perform operations comprising:</i>

Andrews discloses the Security Application Limitations. EX1003, ¶139-142, 220-221. Andrews’s portable computing device includes “**client software 112**” as depicted below:



Client software includes “client programs,” which can be “implemented in software, but also may be implemented in firmware 25 and/or hardware, such as in the BIOS 34 of ROM 32.” 15:8-14. Client software can be a “security product,” 18:10-13, which can “has features such as determining if a portable computing device is missing and retrieving and deleting data..., and locking up the portable computing device.” 34:10-13; EX1003, ¶140-141.

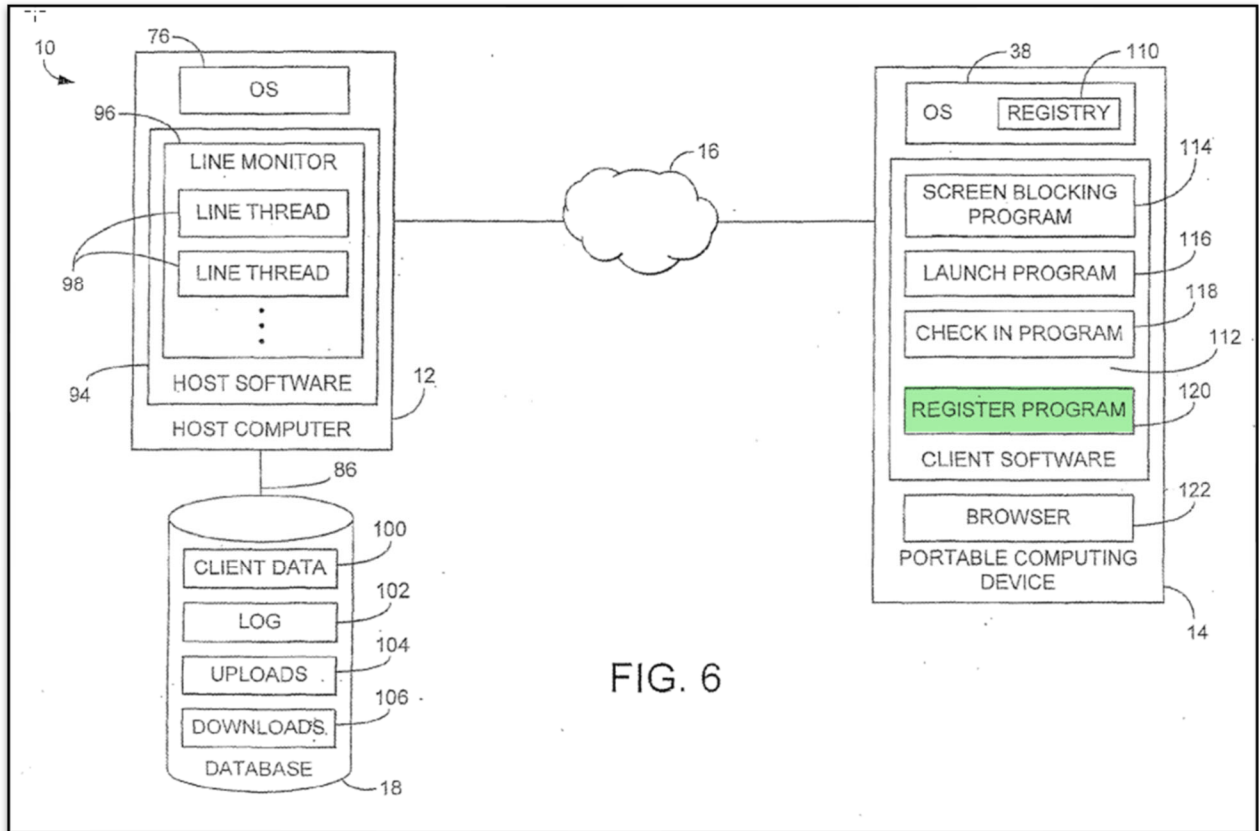
A POSITA would have understood Andrews’s client software to be a *security application in at least one of the non-transitory machine-readable storage media*, as claimed. EX1003, ¶142.

d. Registration Limitations

[1D]	<i>enabling 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>
[9B]/[17C]/[25B]	<i>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> <i>in response to the request from the owner, registering the mobile electronic device with the security service;</i>

Andrews discloses the Registration Limitations. EX1003, ¶143-151, 201-202, 222-223, 241-242. The “client software 112” *enables an owner of the device to request to register the device* with a remote host computer (i.e., a server on which a *security service at least partially resides*). EX1003, ¶149-150.

The client software “includes a **registration program 120**,” as depicted below. 16:9-11.



The registration program registers client software with host computer and includes a product identifier identifying the software as, *e.g.*, a security product. 18:5-13; *see also* 33:21-35:14; EX1003, ¶144-148. A “security product has features such as determining if a portable computing device is missing and retrieving and deleting data,...and locking up the portable computing device.” 34:10-13. The registration program is “configured to receive user information,”

which “is entered by the user...on a registration menu,” 16:9-11, and is “sent to host computer 12 for storage in database 18,” 19:1-5, 16:11-14, 39:2-4.

Annotated Figure 12 below depicts the operation of **receiving registration information** and **sending the registration information** to host computer for **storage in the host database**.

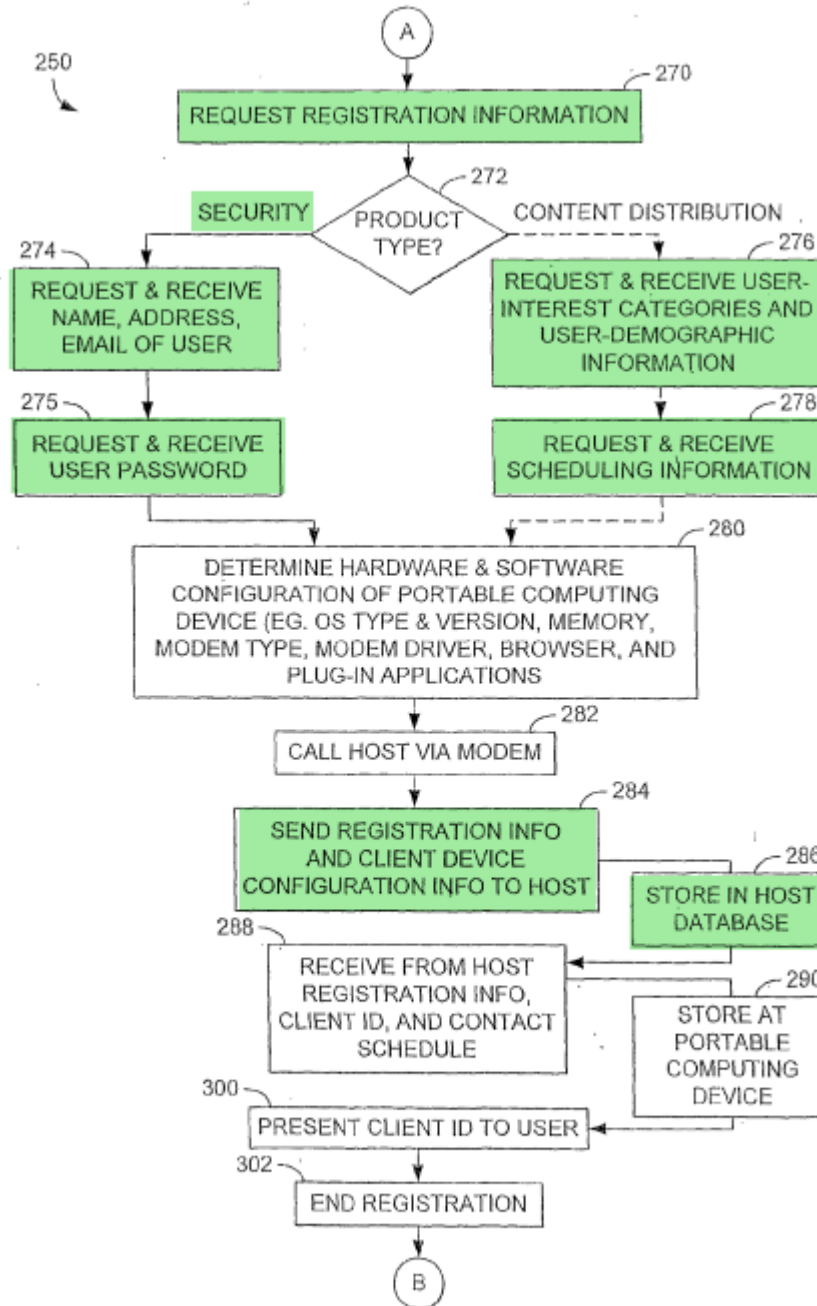


FIG. 12

A POSITA would have understood the submission of user information via registration program and the resulting enrollment in host computer's security service to constitute *"receiving a request to register"* and *"enabling an owner to register"*

the mobile electronic device and that the enrollment of the device occurs “*in response to*” the submission of user information via the registration program, as claimed. EX1003, ¶149.

Host computer 12 “includes a central processing unit 60 [and] memory 62,” 12:11-15, and is “linked to database 18,” 12:19-20. In operation, the host computer (with its associated database) stores “host software” that receives reports that a device has been stolen and, in response, transmits to the client device a device status, a responsive action, and/or a screen-blocking program. *See, e.g.*, 27:14-21, 19:6-13, 37:6-13 (receiving report of lost/stolen device), 28:17-22 (sending responsive actions), 22:21-23:4 (triggering screen-blocking program). A POSITA would therefore understand the host computer and associated database constitute the claimed *one or more servers* on which a *security service at least partially resides*. EX1003, ¶150-151.

e. Sending Identifying Information Limitations

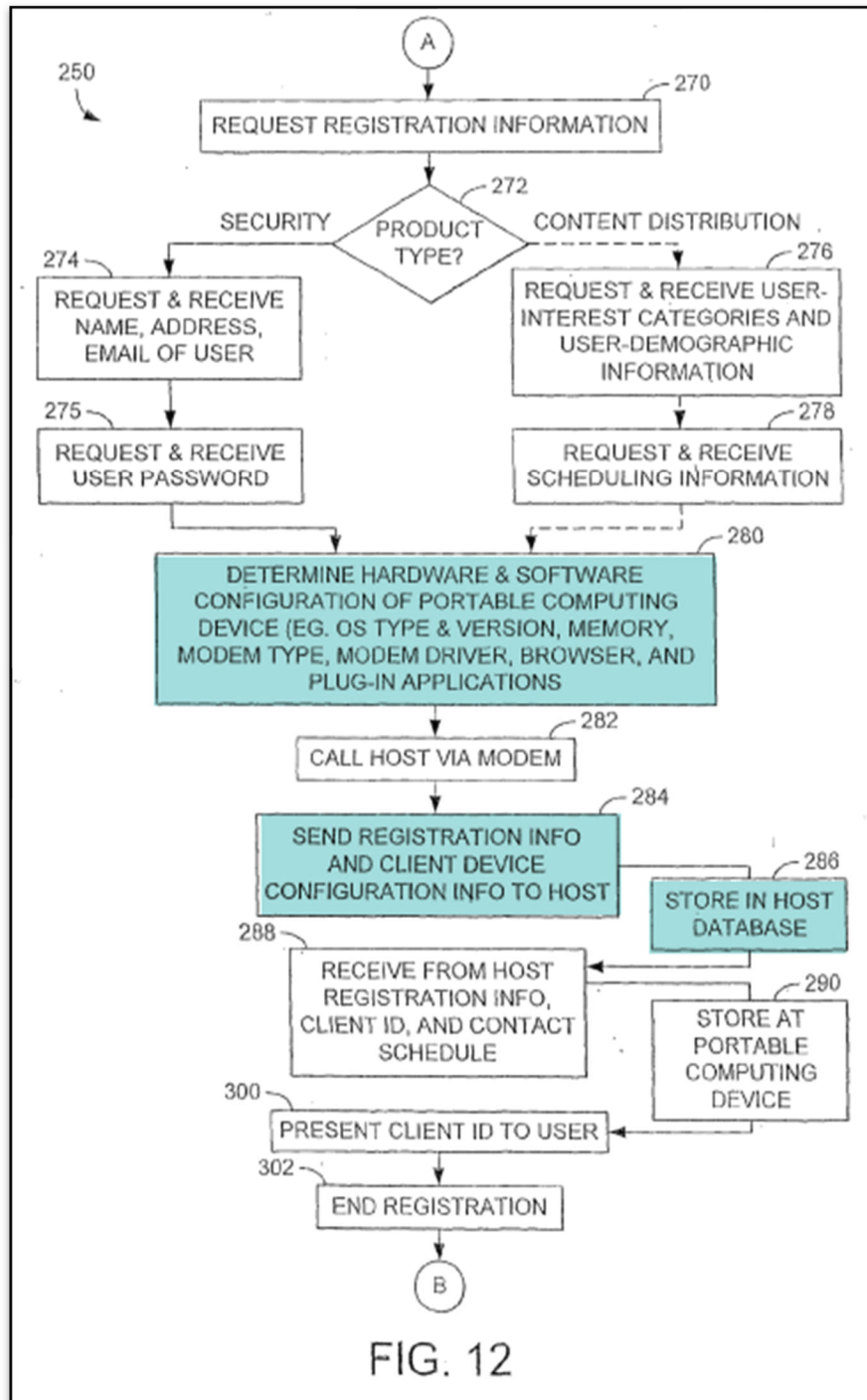
[1E]	<i>causing the mobile electronic device to automatically send identifying information for the mobile electronic device to the security service;</i>
[9C]/[17D]/[25C]	<i>automatically sending identifying information for the mobile electronic device from the mobile electronic device to the security service;</i>

Andrews discloses the Sending Identifying Information Limitations.

EX1003, ¶152-156, 203-204, 224-225, 243-244. Andrews’s portable computing

device sends “hardware and software configuration” to the host computer. 16:11-14. The hardware and software configuration is *identifying information for the portable computing device*, such as “a modem driver type[,]...a browser type, operating system type, available memory, available plug-in applications, and other parameters” of the device. 24:16-19; *see also* 35:15-20; EX1003, ¶153. The portable computer automatically sends this information to the host computer by “calling host computer 12 via the modem” and “sending...the hardware and software configuration.” 35:21-36:6; EX1003, ¶154-155.

These operations of **detecting the hardware/software configuration** and **sending the configuration** for **storage on the host computer database** are highlighted in annotated Figure 12 below:



A POSITA would have understood Andrews to disclose *automatically sending* this information from the portable computing device to the host computer, as claimed, because the client software determines and sends the information

without being instructed by a user to do so. EX1003, ¶154-155; 24:16-21. Andrews also discloses sending a “product identifier,” which a POSITA would have also understood to constitute *identifying information for the mobile electronic device* that the device *automatically sends to the security service* as claimed. 18:3-13, 34:2-13, 33:23-34:6; EX1003, ¶156.

f. Periodic Communication Limitations

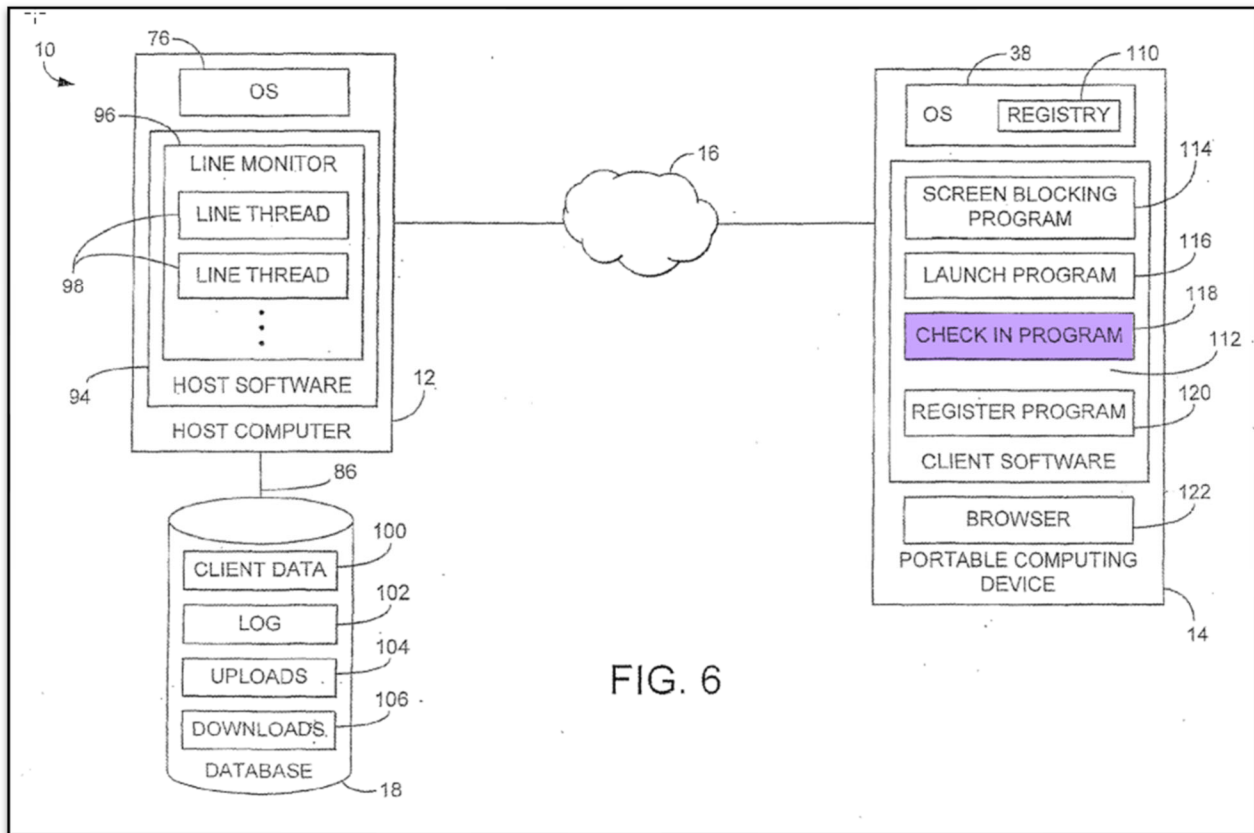
[1F]	<i>after the owner has registered the mobile electronic device with the security service, causing the mobile electronic device to periodically communicate with the security service, when the mobile electronic device is in a state other than a state in which the mobile electronic device is powered off;</i>
[9D]/[17E]	<i>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>

Andrews discloses the Periodic Communication Limitations. EX1003, ¶157-167, 207-208, 228-229, 245-246. Following registration, the client software receives “contact schedule information” from the host computer. 36:7-9.

Thereafter, “client software 112 is configured to **periodically**³ check in with host computer.” 15:19-16:8; *see also* 27:3-6 (check-in occurs “monthly, daily, hourly”), 16:15-17:4, 25:17-22, 26:1-12, 28:5-16, 19:3-9, 30:8-21, 31:10-16, 32:21-33:6,

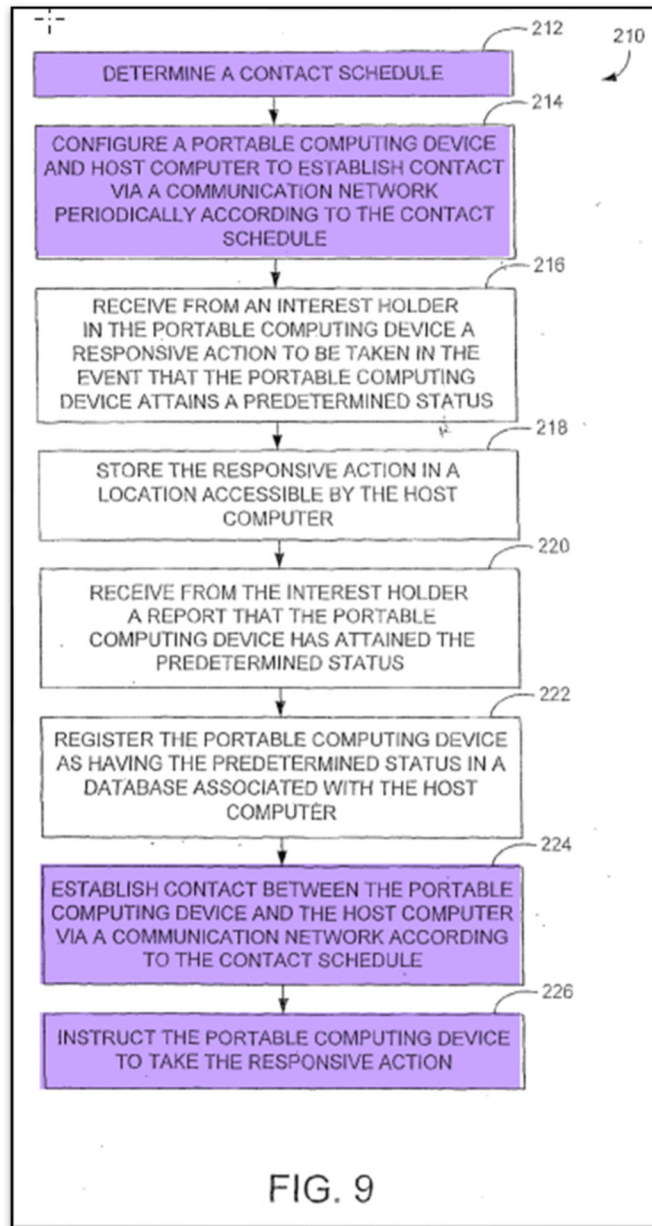
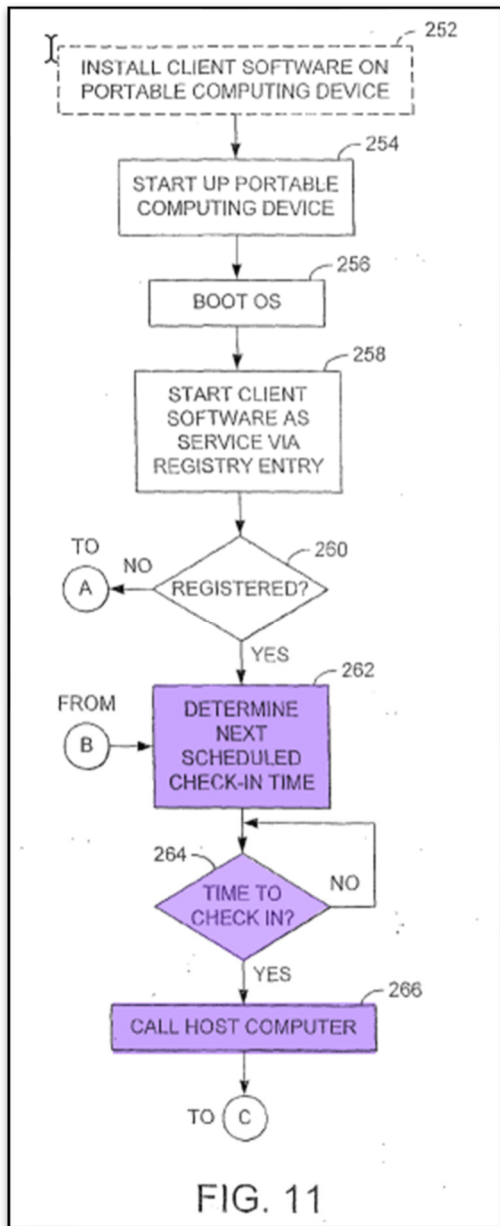
³ Unless otherwise indicated, emphasis by bold added.

30:8-21. More specifically, client software “includes a **check-in program 118**,” as depicted below. 16:15-17:4.



In response to the portable computing device checking in with the host computer, the host computer sends to the portable computing device a “reported status 148 of portable computing device.” 19:6-13.

These **operations** are depicted in annotated Figures 9 and 11 below:



A POSITA would have understood the portable computing device periodically contacting the host computer according to a periodic schedule and receiving, in response, a reported device status to constitute the claimed *periodically communicat[ing] with the security service*. EX1003, ¶158-165. The communication also occurs *after the owner has registered the mobile electronic*

device with the security service, as claimed, as shown in annotated Figure 11 above in which the **check-in operations** occur after the registration step 260. EX1003, ¶166. Moreover, the “check-in program” is “configured to launch upon start-up.” 16:15-17:4. Accordingly, a POSITA would have understood that the check-in program is running whenever the device is *in a state other than a state in which the mobile electronic device is powered off*. EX1003, ¶167.

g. Security Notification Limitations

[1G]	<i>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>
[9E]/[17F]/[25D]	<i>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>

Andrews discloses the Security Notification Limitations. EX1003, ¶168-171, 207-208, 228-229, 245-246. As discussed in connection with the Periodic Communication Limitations *supra* §VII.A.2.f, during operation the computing device receives a “reported [device] status” in response to periodically establishing communication with the host computer. This “reported [device] status” is “typically reported by an interest holder in portable computing device,...such as a

corporate or individual owner of the device.” 19:6-13. As Andrews explains, “the status of the device is LOST when the interest holder knows that the device is missing because it was lost,” 20:1-3; *see also* 21:3-11 (interest holder can select “lost action”). A POSITA would have understood the LOST status to be *a message indicating that the owner of the mobile electronic device has reported a loss*, as claimed. EX1003, ¶169-170.

Furthermore, the status may be accompanied by a message “instructing the portable computing device” to “take [a] responsive action,” which “may for example include...restricting access to portable computing device[.]” 28:17-22. A POSITA would have understood such a *message to indicat[e] that the owner of the mobile electronic device has...requested disabling of the mobile electronic device*, as claimed. EX1003, ¶171.

h. Device Disabling Limitations

[1H]/[9F]/[17G]/[25F]	<i>in response to [receiving]/[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>
-----------------------	--

Andrews discloses the Device Disabling Limitations. EX1003, ¶172-177, 209-210, 230-231, 247-248. A responsive action of “LOCK-UP DEVICE... will...instruct portable computing device 14 to restrict user access to portable

computing device.” 22:21-23:4; *see also* 30:12, 34:10-13 (“locking up” the device), 40:20-41:11 (using “lock-up programs to lock up portable computing device”), 45:6-46:3 (describing “method for restricting access” using “screen-blocking program”). Restricting user access may be “achieved by locking up the GUI 52,” and/or by “restricting the user’s access privileges.” 22:21-23:4. In an example embodiment, Andrews describes a “screen-blocking program [that] grabs the focus of the GUI 52...and prevents a user from interacting with the GUI to access the [device’s] files and folders.” 45:19-46:3. A POSITA would have understood the computing device’s restricting user access to constitute *disabling at least one user function of the mobile electronic device*. EX1003, ¶173-175.

Additionally, Andrews discloses that the client software *still allow[s] the mobile electronic device to communicate with the security service*, as claimed. EX1003, ¶176. For instance, as shown in Figs 14-15, communication between the device and the host computer occurs even after the locking of the device. EX1003, ¶176. At **step 376**, the computing device is locked up. Subsequently, at **steps 382, 388, 394, 400, 414, 418, 422**, the computing device communicates with the host computer.

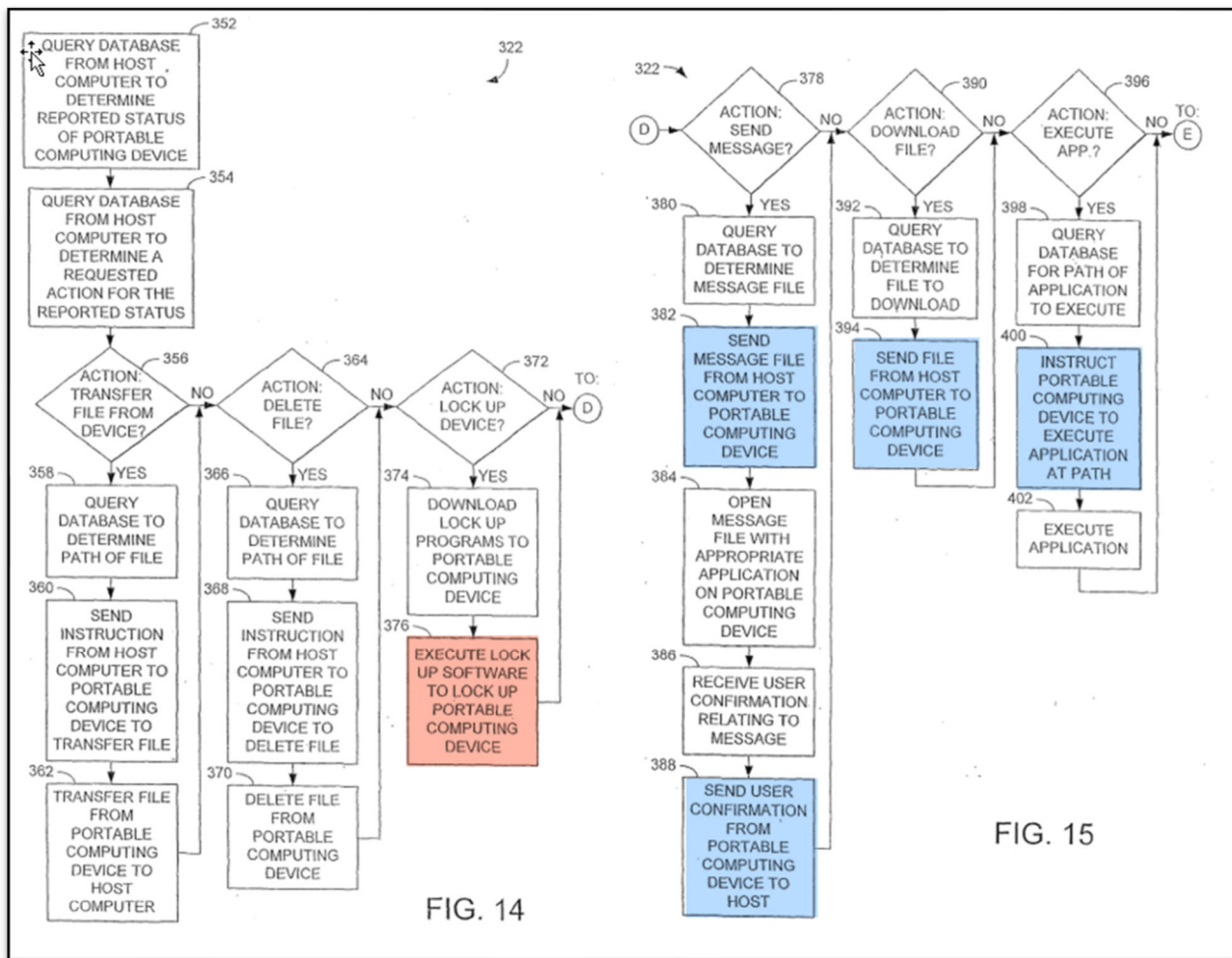
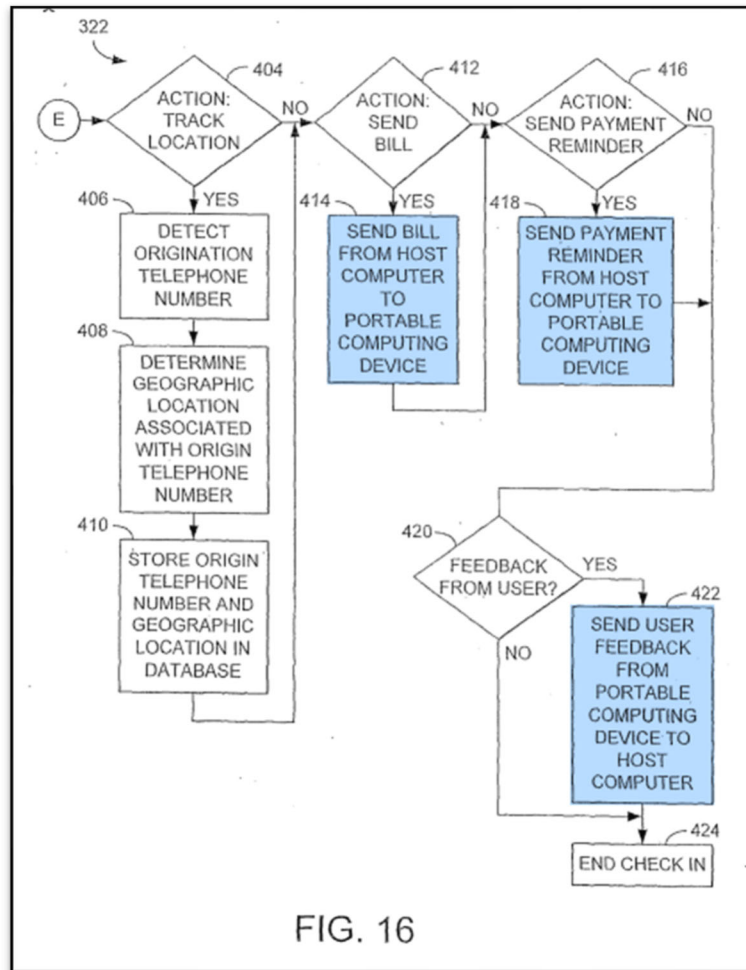


FIG. 15



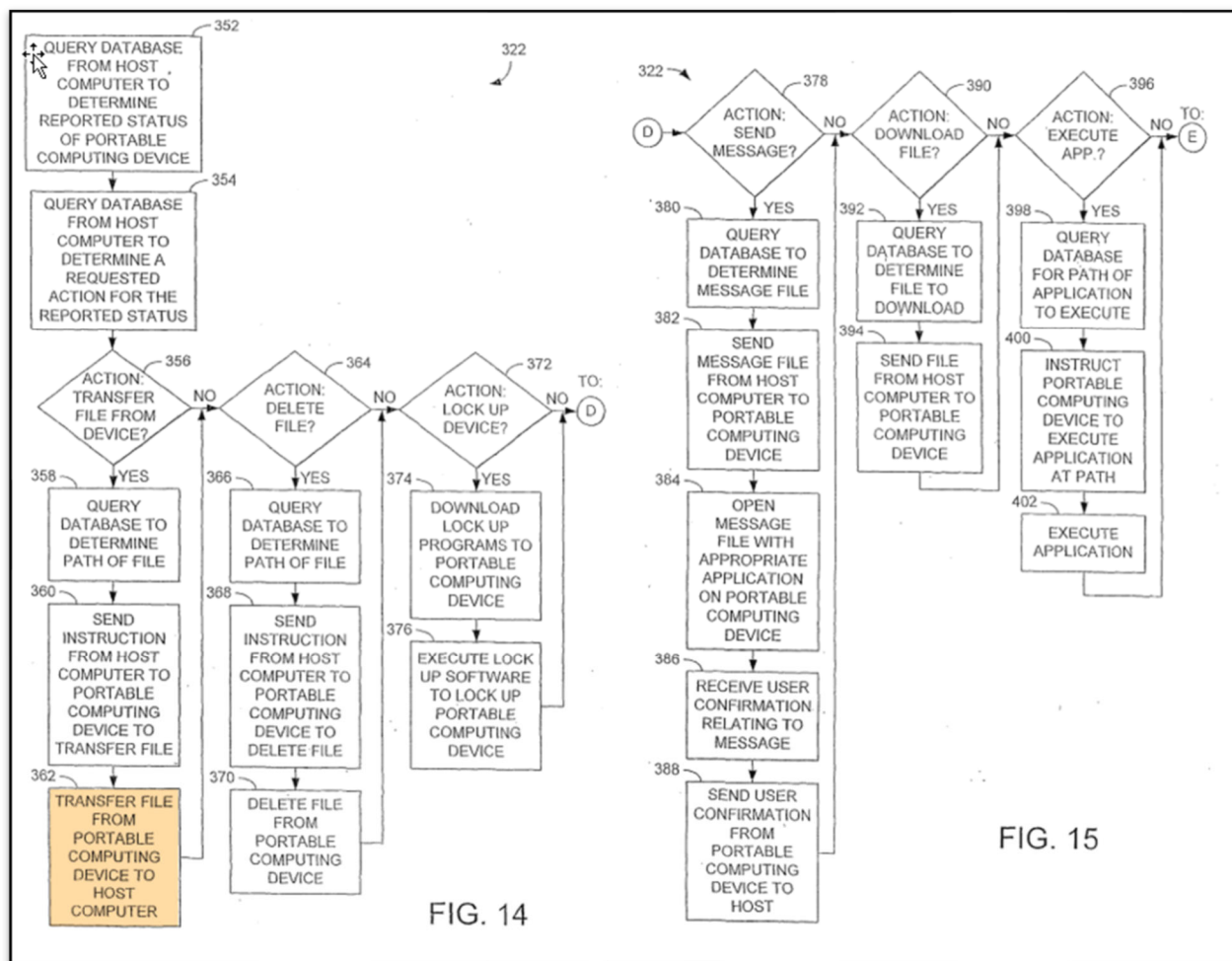
i. Copying User Data Limitations

[1I]/[9G]/[17H]/[25G]	<i>automatically causing at least some user data to be copied from the mobile electronic device to at least one of the servers;</i>
-----------------------	---

Andrews discloses the Copying User Data Limitations. EX1003, ¶178-185, 211-212, 232-233, 249-250. Andrews discloses that an owner of a “missing” device can use the security software installed on the device for “retrieving [] data.” 34:10-13. Thus, a responsive action of “RETRIEVE DATA... will cause host

computer 12 to instruct portable computing device 14 to transfer a file... to host computer 12 for storage as an upload 104 in database 18.” 21:16-23; *see also* 38:23-39:16 (describing “RETRIEVE DATA” operation mode), 40:5-13 (describing “RETRIEVE FILE” action). These files can include “data retrieved from a missing portable computing device” as well as “user feedback data” and “user messages,” each of which a POSITA would have understood to be *user data*. 14:18-21; EX1003, ¶181. A POSITA would have understood that to retrieve a file would constitute *causing at least some user data to be copied from the mobile electronic device to at least one of the servers*, as claimed. EX1003, ¶182-183.

Operation of the **RETRIEVE FILE** instruction is depicted in annotated Figure 14 below:



The RETRIEVE FILE command includes a “file-to-retrieve indicator,” which is a “path to a file or folder” specifying which file(s) should be transferred. 22:1-9; *see also* 40:5-13. In some cases, the device uses the file-to-retrieve indicator to “search for the file based on the partial or complete file name, and then transfer the file.” *Id.* Because the RETRIEVE FILE command causes a portable computing device to identify and transfer files without user intervention, a POSITA would have understood that the copying occurs *automatically*, as claimed. EX1003, ¶184-185.

j. Deleting User Data Limitation

[25H]	<i>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; and</i>
-------	--

Andrews discloses the Deleting User Data Limitation. EX1003, ¶251-256.

“[T]he action DELETE FILE will cause host computer 12 to instruct portable computing device 14 to delete a file on portable computing device 14.” 22:10-12.

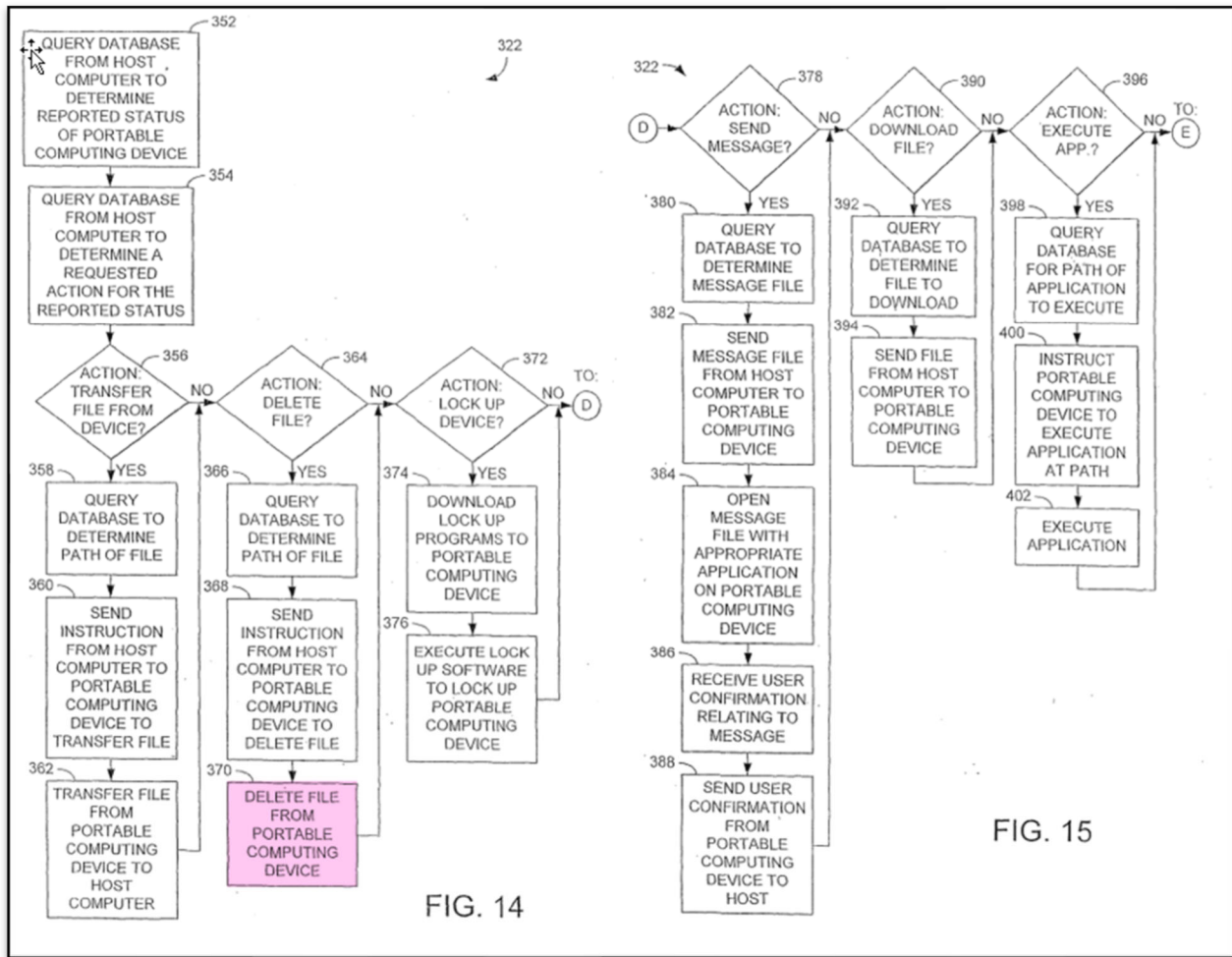
A file-to-delete indicator provides an “indicator or path 166 of a file to delete.”

40:14-19. The DELETE FILE command causes the device to “delet[e] the file

located at the path 166.” 40:14-19. A POSITA would therefore understand that the

DELETE FILE command *caus[es] files to be deleted from the mobile electronic device*, as claimed. EX1003, ¶252-254.

Operation of the **DELETE FILE** instruction is depicted in annotated Figure 14 below:



Moreover, a POSITA would have understood that the files being deleted from the portable computing device could include *at least some user data...from the mobile electronic device*, as claimed. EX1003, ¶255-256. Indeed, in the example embodiment depicted in cropped and annotated Figure 7 below, the **file-to-retrieve** indicator points to the same file as the **file-to-delete** indicator:

File to retrieve indicators	C:\files\importantfile.doc, c:\files\importantfolder\ "file.doc" 164a
File to delete indicators	c:\files\importantfile.doc, c:\files\importantfolder\ "sensitivefile.doc" 166a

k. Restoring User Data Limitation

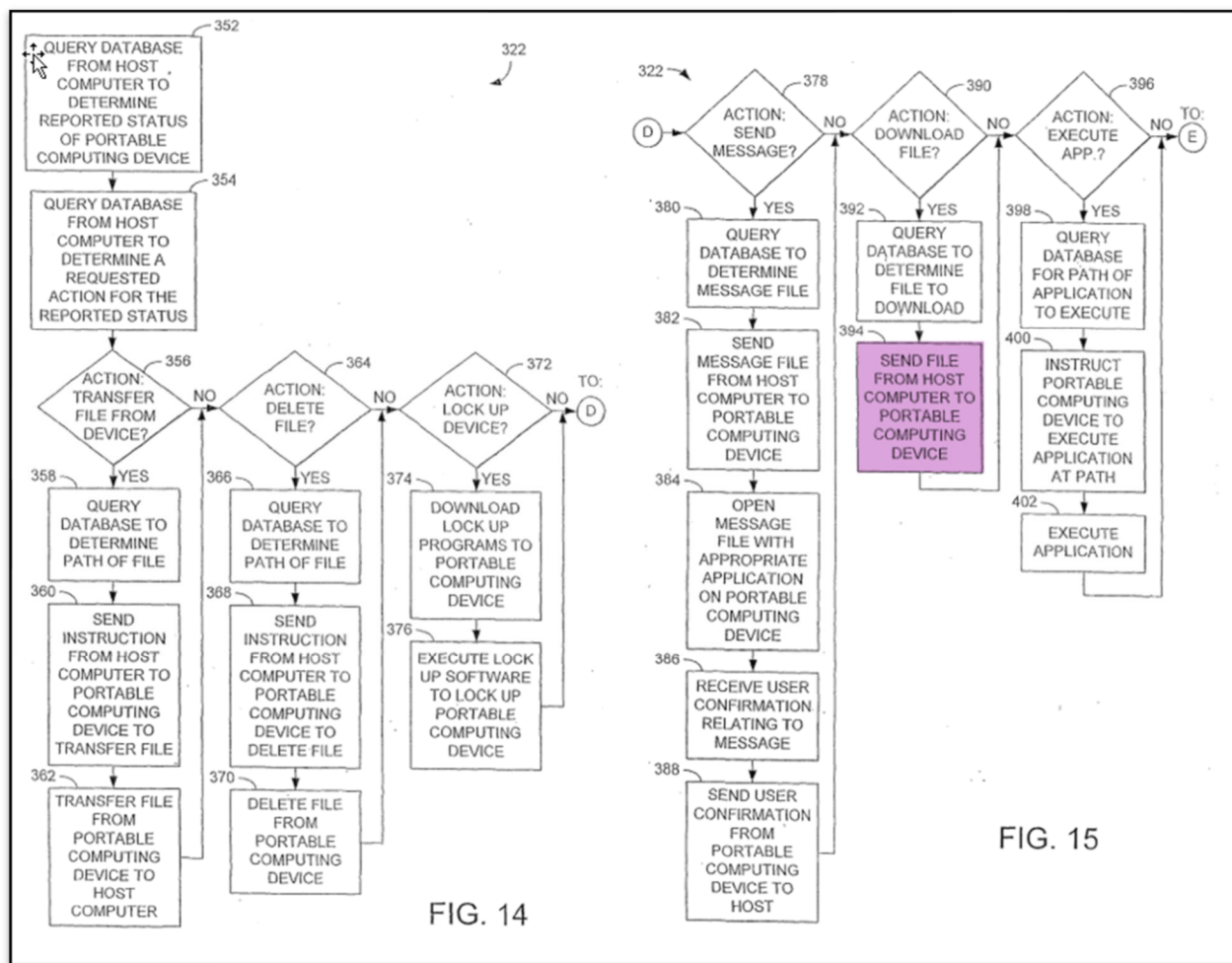
[25I]	<i>after the at least some of the user data has been deleted from the mobile electronic device, causing at least some of the user data to be copied from at least one of the servers to the mobile electronic device;</i>
-------	---

Andrews discloses the Restoring User Data Limitation. EX1003, ¶257-263.

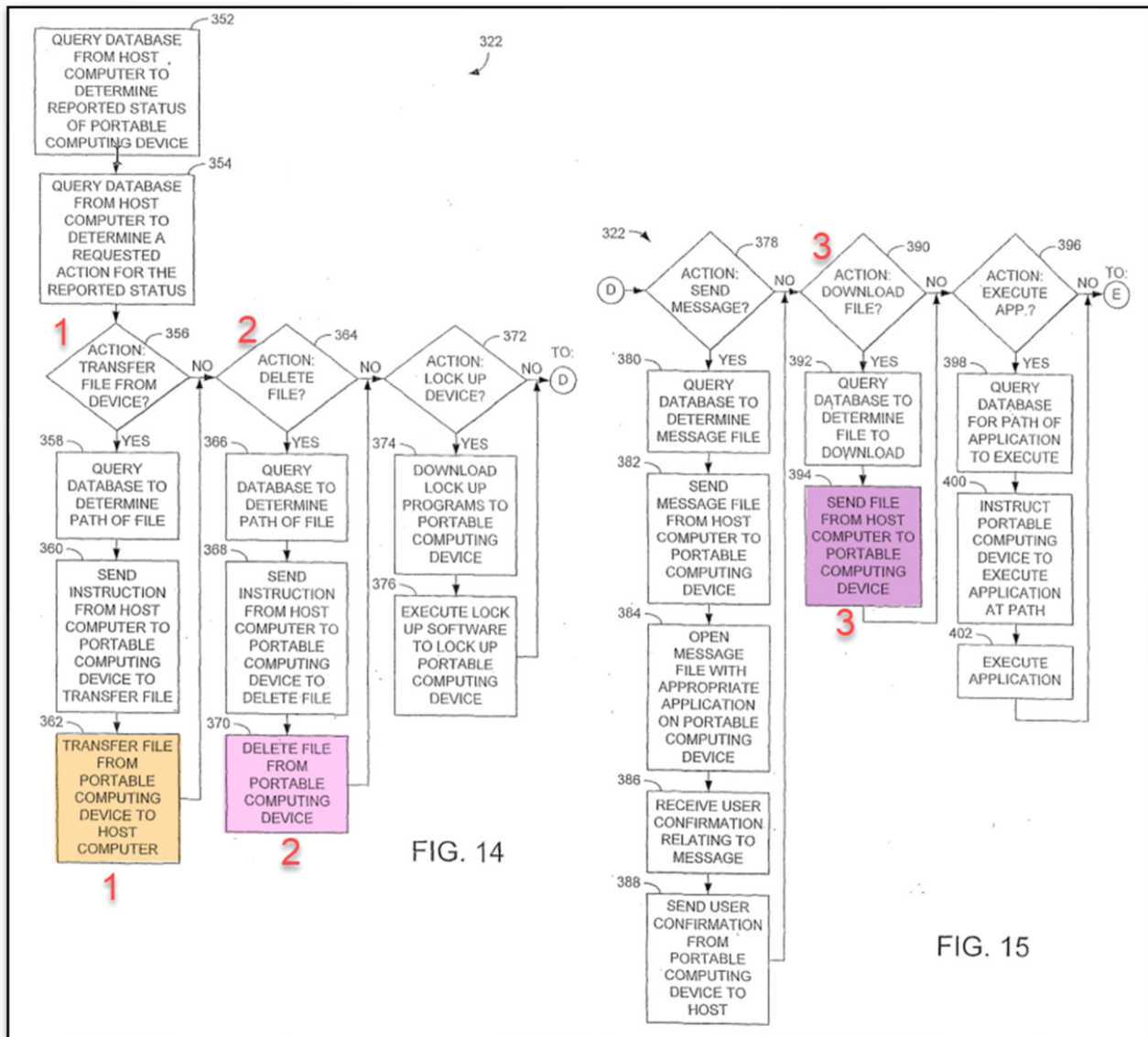
Andrews discloses a DOWNLOAD FILE operation, which “instruct[s] the portable computing device to download [an] appropriate file from host computer 12 to portable computing device 14 via communication network 16.” 42:15-20; *see also* 23:7-10. A POSITA would have understood downloading a file from host computer to portable computing device to constitute *causing a file to be copied from at least one of the servers to the mobile electronic device*, as claimed.

EX1003, ¶258-260.

Operation of the **DOWNLOAD FILE** instruction is depicted in annotated Figure 14 below:



Moreover, Andrews discloses that the responsive actions—such as RETRIEVE FILE, DELETE FILE, and DOWNLOAD FILE—can be “implemented singularly **or in combination**[.]” 21:14-15. Indeed, Figures 14 and 15 illustrate the operations performed when a portable computing device “determine[s] [its] reported status.” As shown in the annotated figures below, the portable computing device performs multiple responsive actions in combination, including (i) first, **RETRIEVE FILE**, (ii) second, **DELETE FILE**, and (iii) third, **DOWNLOAD FILE**. EX1003, ¶261-262.



Thus, a POSITA would have understood that the DOWNLOAD FILE operation occurs *after the at least some of the user data has been deleted from the mobile electronic device*. EX1003, ¶261-262.

Andrews further discloses that the “[d]ownloadable files 106 [] may include program data files” and “other file types.” 15:1-2. A POSITA would have understood that the DOWNLOAD FILE operation could be used to transfer any

type of file from the host computer to the portable computing device, including the *user data* previously copied and deleted from the portable computing device.

EX1003, ¶263. Indeed, a POSITA would have understood this to be one of the primary utilities of the functionality because it would allow a user to restore any files deleted from the portable electronic device while it was missing back to the device following its recovery. EX1003, ¶263. Thus, a POSITA would have understood Andrews to disclose *causing at least some of the user data user data to be copied from at least one of the servers to the mobile electronic device*, as claimed. EX1003, ¶263.

I. Memory Area Limitations

[1J]	<i>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> <i>wherein the security application utilizes code residing at least partially in the system area; and</i> <i>wherein the security application receives the notification from at least one of the servers via the system area.</i>
[9H]/[25J]	<i>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> <i>wherein the security application utilizes code residing at least partially in the system area; and</i> <i>wherein the operation of accepting the notification from the security service comprises receiving the notification from at least one of the</i>

	<i>servers via the system area.</i>
[17I]	<i>wherein the operation of accepting the notification from the security service comprises receiving the notification from at least one of the servers via a system area of non-volatile memory in the mobile phone; and</i> <i>wherein the system area is an area that cannot be modified by a user.</i>

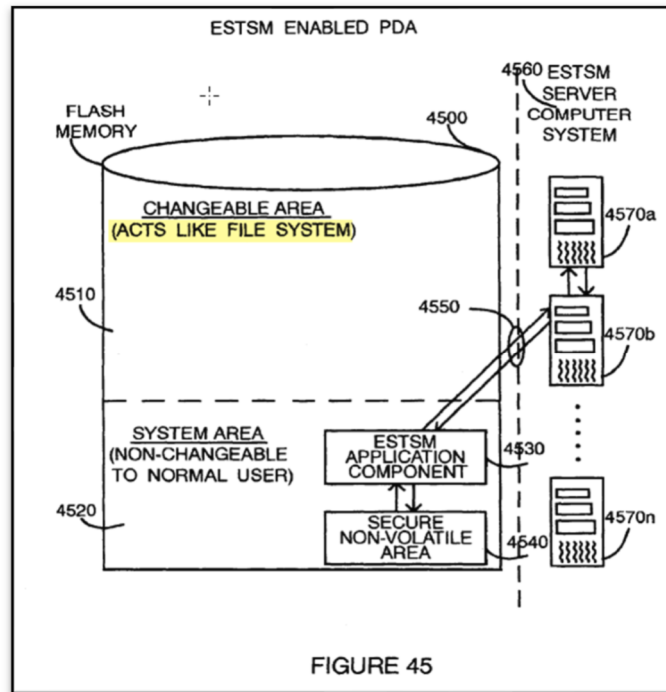
Andrews discloses the Memory Area Limitations. EX1003, ¶186-195, 213-214, 234-235, 264-265. As discussed *supra* §VII.A.1, VII.A.2.b, Andrews discloses that the portable computing device can include several different types of *memory*, including flash memory, firmware, and ROM, which a POSITA would have understood to be types of *non-volatile memory*. EX1003, ¶34-54 (explaining that flash and ROM are types of non-volatile memory).

Andrews further discloses that its client software can be implemented and installed in multiple ways. For instance, Andrews explains that the client software is “typically implemented in software, but also may be implemented in firmware 25 and/or hardware,” and can be stored in “ROM 32 on portable computing device 14,” 15:3-11, such that it is “executed on start-up of portable computing device 14.” 32:9-14.

A POSITA would have understood that ROM is *non-volatile memory* that *cannot be changed by a user*. EX1003, ¶188-190. Indeed, ROM is an acronym for **read-only** memory, which, as the name suggests, can be read—but not rewritten—

by a user. EX1003, ¶188-190. If the client software is stored in “ROM 32 on portable computing device 14,” as taught in Andrews, a POSITA would have understood the client software to be *utiliz[ing] code residing at least partially in [a] system area...that cannot be modified by the user*, as claimed. EX1003, ¶188-190, 35-50; EX1015 at 12; EX1016 at 5-6; EX1017 at 4.

Andrews also discloses the claimed *changeable area* of non-volatile memory. EX1003, ¶191-193. Andrews’s client device includes a “hard drive” that can be “flash memory,” which a POSITA would have understood to typically be a changeable memory used to store a user’s files/folders. 10:6-8; EX1003, ¶191-193 (explaining that flash memory is changeable and that a hard drive typically refers to the memory storing user files). This understanding of Andrews is consistent with Andrews’s DELETE FILE and RETRIEVE FILE operations, which use a “file-to-retrieve”/“file-to-delete” indicator to identify “a path to a file or folder” to be retrieved/deleted. 22:1-7. A POSITA would have understood these “files” and/or “folders” to conventionally be stored in file system, which would be a *changeable area* of memory that *can be modified by a user*. EX1003 ¶191-193 (citing “C” drive example). Indeed, the ’649 patent teaches that the *changeable area* “may include a file system,” EX1001, 20:14-17, and that the *changeable area* “acts like a file system,” as shown in Figure 45 below:



Moreover, Andrews's security application performs the security operations of Andrews's client software by, *inter alia*, receiving the reported device status from the host computer and performing operations in response to the received status, as described *supra* §VII.A.2.f, VII.A.2.g, VII.A.2.h. A POSITA would have understood that when performing these operations, the software is executed by a processor and, during execution, is given access to the reported device status sent from the host computer. EX1003, ¶194-195. Therefore, a POSITA would have understood Andrews to disclose that its client software *receives a notification from the security service from at least one of the servers via the system area*, as claimed. EX1003, ¶194-195.

Andrews discloses all limitations of the Independent Claims. EX1003, ¶115-265.

3. Claims 2, 10, and 18

[2]	<i>A mobile electronic device according to claim 1, wherein the notification includes no third-party certification.</i>
[10]	<i>A method according to claim 9, wherein the notification includes no third-party certification.</i>
[18]	<i>An article of manufacture according to claim 17, wherein the notification includes no third-party certification.</i>

Andrews discloses these limitations. EX1003, ¶266-268. Because these limitations recite what is not included in the claimed *notification*, they are negative limitations. Notably, “a reference need not state a feature’s absence in order to disclose a negative limitation.” *AC Techs., S.A. v. Amazon.com, Inc.*, 912 F.3d 1358, 1367 (Fed. Cir. 2019).

Andrews discloses a complete system and does not contain any indication that the reported status or associated responsive action sent from the host computer to the portable computing device is generated or provided by any third party. EX1003, ¶266-268. Rather, the reported status and responsive action are “typically reported by an interest holder in portable computing device,” such as a “corporate or individual owner” 19:8-13; 21:4-8. Accordingly, a POSITA would have understood that the message/command sent by the host computer to the portable

computing device *includes no third-party certification*, as claimed. EX1003, ¶266-268.

4. Claims 7, 15, and 23

[7]/[15]/[23]	<i>A [mobile electronic device]/[method]/[article of manufacture] according to claim [1]/[9]/[17], wherein...</i> <i>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>
---------------	---

Andrews discloses these limitations. See Deleting User Data Limitations, *supra* §VII.A.2.j; EX1003, ¶281.

5. Claims 8, 16, and 24

[8]/[16]/[24]	<i>A [mobile electronic device]/[method]/[article of manufacture] according to claim [7]/[15]/[23], wherein...</i> <i>after the at least some of the user data has been deleted from the mobile electronic device, causing at least some of the user data to be copied from at least one of the servers to the mobile electronic device.</i>
---------------	---

Andrews discloses these limitations. See Restoring User Data Limitations, *supra* § VII.A.2.k; EX1003, ¶282.

6. Claims 3-5, 11-13, and 19-21

[3]/[11]/[19]	<i>A [mobile electronic device]/[method]/[article of manufacture] according to claim [1]/[9]/[17], wherein...</i>
---------------	---

	<i>the operation of enabling the owner to register the mobile electronic device with the security service comprises providing the security service with at least three items from the group consisting of:</i> <i>a phone number for the mobile electronic device,</i> <i>a phone service provider for the mobile electronic device,</i> <i>an International Mobile Equipment Identifier (IMEI) number for the mobile electronic device, and</i> <i>a phone description for the mobile electronic device.</i>
[4]/[12]/[20]	<i>A [mobile electronic device]/[method]/[article of manufacture] according to claim [3]/[11]/[19], wherein...</i> <i>the identifying information automatically sent from the mobile electronic device to the security service comprises:</i> <i>a phone number for the mobile electronic device;</i> <i>an international mobile equipment identifier (IMEI) number for the mobile electronic device; and</i> <i>a model number for the mobile electronic device.</i>
[5]/[13]/[21]	<i>A [mobile electronic device]/[method]/[article of manufacture] according to claim [3]/[11]/[19], wherein...</i> <i>the identifying information automatically sent from the mobile electronic device to the security service comprises:</i> <i>a phone number for the mobile electronic device;</i> <i>an international mobile equipment identifier (IMEI) number for the mobile electronic device; and</i> <i>a model number for the mobile electronic device.</i>

Andrews discloses and/or renders obvious these limitations. EX1003, ¶269-280. As discussed *supra* §VII.A.2.e, Andrews’s client device sends identifying “hardware and software configuration” information to the host computer. Andrews

offers several examples of this type of information, such as “operating system type and version,” “modem type,” and “modem driver,” each of which describes the client device and would, therefore, qualify as a *phone description* in circumstances where the device is a cellular telephone. EX1005, 35:15-20. EX1003, ¶270.

Additionally, Andrews notes that beyond these expressly identified categories, the configuration information can include any “**other** hardware and software parameters.” EX1005, 35:15-20. Based on this teaching, a POSITA would have recognized that there are certain conventional types of information that might be sent to the host computer to identify the device. EX1003, ¶271-275. For a client device that is a “cellular telephone,” a POSITA would have understood that these hardware and software parameters would include *a phone number, a phone service provider, and an International Mobile Equipment Identifier (IMEI) number*. EX1003, ¶271-275. Indeed, Andrews teaches that the host computer stores a “cellular telephone number associated with a cellular modem of the portable computing device,” which the host computer can use to contact the client device. EX1005, 28:11-16. A POSITA would have understood that the host computer could receive this phone number by, *e.g.*, having it uploaded with the hardware and software configuration. EX1003, ¶272. Furthermore, a POSITA would have recognized an *IMEI* and *phone service provider* to be information that is typically used to identify a cellular telephone and that would be encompassed by

hardware/software parameters. EX1003, ¶¶272-273. For example, WIPO Pub. No. 96/36194 states that in a conventional “GSM system,” the “identity data” for a phone includes the “IMEI,” which is “automatically” transmitted to a server every time the device contacts the network. EX1018, 13:5-25; *see also* 3:25-4:3 (cellular networks check device IMEI to identify equipment and ensure that it is “not stolen”); EX1003, ¶¶273.

Moreover, Andrews discloses that the client device sends a “product identifier,” which is a “code assigned to the particular version of client software” on the device and which a POSITA would understand to be a *model number* assigned to the software on the device. EX1003, ¶¶280.

If Andrews is found not to disclose that its hardware/software configuration includes the claimed categories of identifying information, then a POSITA would have had reason to implement Andrews to include this conventional information. EX1003, ¶¶274-726. As discussed above, these categories of information are standard descriptors for any mobile phone operating on a mobile phone network, as evidenced by contemporaneous industry standards publications identifying these categories as such. EX1003, ¶¶275; EX1022 (disclosing IMEI and service provider); EX1023 (disclosing IMEI); EX1024 (disclosing phone number). Thus, to include a phone number, phone service provider, and IMEI in the uploaded hardware/software parameters would have been using a known technique

(uploading basic information about the device) to improve similar systems (mobile-device tracking system) in a predictable way (by providing information to identify devices on the network with more particularity). *KSR Int’l v. Teleflex*, 550 U.S. 398, 417 (2007); EX1003, ¶276.

B. Ground 1B: Claims 1-5, 7-13, 15-21, and 23-25 Obvious over Andrews and Bonnett⁴

1. Bonnett

a. Bonnett Overview

Bonnett published on March 13, 2003 from application 10/197,198, filed on July 17, 2002, and therefore is prior art under at least §102(e).

Bonnett teaches techniques for securely upgrading any program “capable of contributing to one or more functions of [a computing device]” while ensuring that the program is stored in the device’s memory so that it is inaccessible (and not changeable) to users. [0007]; EX1003, ¶283-289.

Various embodiments substantially restrict access to portions of a program stored in a memory accessible to an appliance. **Restricting access to programs and/or portions of a program can help prevent a user from deleting** or corrupting those portions of the program, which can lead to an improved reliability of the appliance. **In addition, restricting access to portions of the program can assist program**

⁴ Unless otherwise noted, Section VII.B’s citations are to EX1006.

designers in the protection of licensed code, firmware, and/or software.

[0011].

Bonnett's "appliance" is broadly defined as a "device or combination of devices" that are "capable of performing a desired...computing functionality" such as "a personal digital assistant (PDA), a cell phone, a digitized audio recorder/player, or any other digital or analog device." [0018]. A computer program is "stored on [a] memory device" of the appliance and "may include, for example, software, firmware, code, portions of code, data compilations, and/or a combination of these or any other type of information." [0019]. Bonnett specifically does **not** require that these "programs" be of any particular type/purpose, instead explaining that the programs can be any "program operable to carry out a desired functionality" by "contribut[ing] to one or more functions of appliance." [0018]-[0019]; EX1003, ¶284.

The "memory device" of the appliance includes "any...suitable volatile or nonvolatile storage." [0031]. The memory "includes at least an open partition of memory 126a and at least a hidden partition of memory 126b." [0032]. The hidden partition is "inaccessible through the external interface." [0010]. One or more of the above-described "programs" can be stored in the "hidden partition" area of the memory, which "prevent[s] a user from deleting or corrupting" the program and which "lead[s] to an improved reliability of appliance." [0032], [0037]; EX1003,

¶284-289. The open partition, on the other hand “store[s] those portions 225a of program 225 that are accessible to the user,” such as “media files, data files, and/or any other information desired by program designers to be made accessible to the user.” [0036].

b. Bonnett is Prior Art as of its Provisional

At a minimum, Bonnett is prior art under §102(e) as of the July 17, 2002 filing date of the non-provisional application. Additionally, Bonnett claims priority to provisional application 60/322,252 filed on September 10, 2001 (“Bonnett Provisional”, EX1009) and is also prior art under §102(e) as of that date. First, the Bonnett Provisional provides written description support for Bonnett’s Claim 1 as shown in the table below. EX1003, ¶290-296. Additionally, the subject matter recited in Bonnett’s Claim 1 encompasses the subject matter relied upon for prior art in the Ground 1B presented below. EX1003, ¶290-296. Therefore, the Bonnett Provisional satisfies the two-prong test of *Dynamic Drinkware, LLC v. Nat’l Graphics, Inc.*, 800 F.3d 1375, 1380 (Fed. Cir. 2015).

Bonnett Claim 1	Bonnett Provisional (EX1009)
1. An appliance, comprising:	“Programmable portable electronic devices or appliances , such as digitized audio recorder/players can require field upgrade of their operating software.” (p. 3)
a memory comprising at least a hidden portion of memory operable to store at	“This solution allows a single storage media that does not require removal from the appliance, thus reduces cost.” (5)

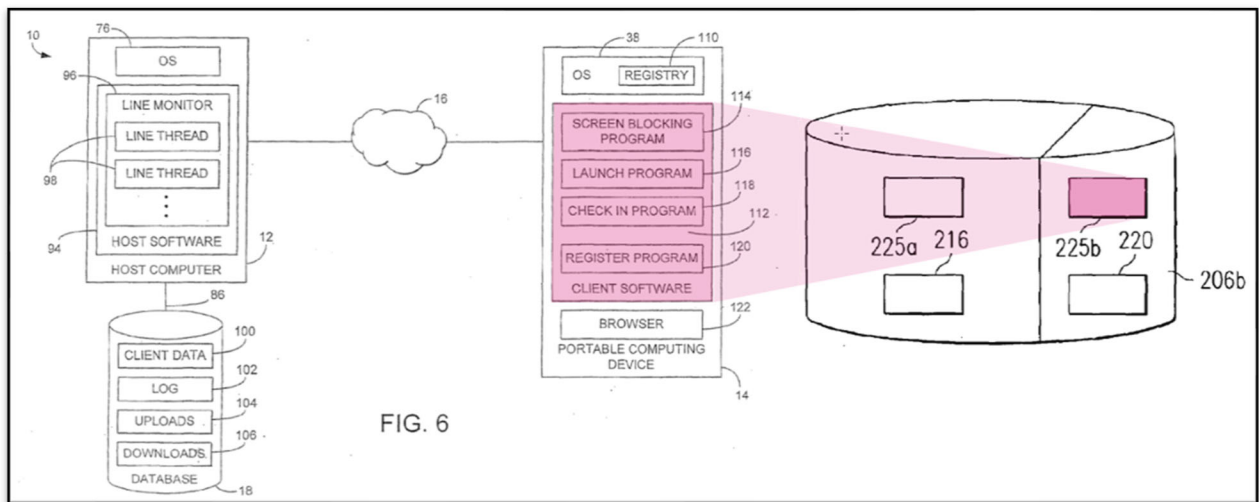
least a portion of a program capable of contributing to one or more functions of the appliance;	“This is facilitated by partitioning the single storage media into at least two sections. All but one of these sections are hidden from the host computer's operating system. The portable device moves this software from the partitions exposed to the host computer to a partition hidden from the host computer.” (4) “In order to solve this problem, we needed to limit access to the images. The images should only be accessible to the developing companies, and they should be hidden to all customers. Once this decision was reached we decided to create an upgrade utility that took our current NAND setup and integrated a second hidden partition to store these image files.” (11)
a controller operable to process at least a portion of the program stored on the hidden portion of memory; and	“The Internet Audio Applications team recently supported a DSP board design that incorporated a C54x based DSP, NAND flash memory, and USB capabilities.” (11) “The main workhorse of this system is the load image, which is stored in the DSP's RAM. This is the code that is initially boot-loaded from the NAND; it searches and finds the other images to load into the remaining DSP RAM.” (11)
an external interface operable to provide access to at least an open portion of the memory;	“An easy and convenient method to perform this upgrade is to connect the appliance to a host computer such that the device appears as a disk drive or Mass Storage Class device to that host computer's operating system.” (3)

	“The portable device moves this software from the partitions exposed to the host computer to a partition hidden from the host computer. Additionally, this solution incorporated a method for decrypting an encrypted file while moving the file from the exposed partition to the hidden partition.” (4)
wherein the hidden portion of memory is inaccessible through the external interface.	“All but one of these sections are hidden from the host computer's operating system.” (4) “Firmware security is also a major concern for firmware developers and device manufacturers: these developers want to prevent the firmware images from being viewed or manipulated in any form.” (11) “In order to solve this problem, we needed to limit access to the images. The images should only be accessible to the developing companies, and they should be hidden to all customers. Once this decision was reached we decided to create an upgrade utility that took our current NAND setup and integrated a second hidden partition to store these image files.” (11)

2. Reasons to Combine Andrews and Bonnett

A POSITA would have had multiple reasons to combine Andrews and Bonnett, which both relate to hardware and software solutions for improving security of computing systems and are, for at least that reason, analogous art. EX1003, ¶¶297-298. More specifically, a POSITA would have had reason to

combine Andrews and Bonnett by installing Andrews’s client software in a “hidden partition” of non-volatile memory, while maintaining an “open partition” to serve as a user-accessible file system. EX1003, ¶298. Andrews-Bonnett is illustrated in the annotated figure below, which shows Andrews’s client software being stored as Bonnett’s program 225b in hidden partition 206b:



First, Bonnett’s intended purpose is to use memory-management techniques to securely store **any type** of program. [0019]; EX1003, ¶299. Bonnett does so by storing the program in a “hidden” portion of memory that is not accessible to a user. EX1003, ¶299 Similarly, Andrews teaches a security program to help protect a device by initiating responsive actions when the device is lost or stolen. EX1005, 1:13-22; EX1003, ¶299. Based on these teachings, a POSITA would have been motivated to store Andrews’s security software using Bonnett’s hidden-partition memory-management techniques for their intended purpose of “prevent[ing] a user

from deleting or corrupting . . . the program” and “protect[ing] . . . software stored on memory [of the] device.” [0011], [0032], [0037]; EX1003, ¶299.

Bonnett provides a broad solution to prevent users from accessing computer programs. EX1003, ¶300-301. Thus, while Bonnett does not specifically suggest using it to protect a program from unauthorized access by a finder of a missing device, a POSITA would have recognized that protecting computer programs from unauthorized tampering would be a desirable outcome in a wide variety of situations, including in those situations most likely to arise for a program of the type disclosed in Andrews. EX1003, ¶300.

Indeed, Bonnett teaches that protecting a program from corruption “can lead to an improved reliability” of the device upon which it is installed. [0011], [0032], [0037]. A POSITA would have readily understood that reliability is critical for programs designed to allow a device owner to recover a lost/stolen device. EX1003, ¶301. A POSITA would have therefore recognized the benefits of using Bonnett’s techniques to “prevent[ing] a user from deleting or corrupting” such a security program, either inadvertently (e.g., in the case of a reckless device owner) or intentionally (e.g., in the case of an opportunistic thief). EX1003, ¶301.

Second, a POSITA would have been motivated to combine Andrews and Bonnett because utilizing Bonnett’s techniques to protect Andrews’s client software is consistent with (and furthers) Andrews’s teaching that it is desirable for

the client software to be implemented in a way that resists user tampering.

EX1003, ¶302.

When Andrews’s client software contacts the host computer, it does so “surreptitiously” and “silently, without interrupting any activity of the user.”

EX1005, 31:21-32:8. A POSITA would have understood this to suggest that the software should be designed to avoid detection by an unauthorized user who, upon detecting the software, may attempt to disable, disrupt, or delete it. EX1003, ¶303.

Additionally, Andrews describes a “screen-blocking program” that runs on the device when an owner has reported the device missing. Andrews teaches: “[i]f the user attempts to exit the screen-blocking program...the method includes restarting screen-blocking program.” EX1005, 46:11-16. Likewise, if the user attempts to “reboot” the device, the security software “cause[s] screen-blocking program 114 to execute, thereby again restricting user access.” EX1005, 46:17-22. A POSITA would have understood Andrews to be teaching that a user might attempt to bypass security mechanisms on the device (e.g., by exiting the screen-blocking program) and that it is advantageous to design a program resistant to such efforts (e.g., by automatically restarting the screen-blocking program). EX1003, ¶304. A POSITA would have recognized Bonnett as providing an additional means of resistance to such efforts by preventing attempts to disable, delete, or bypass the software. EX1003, ¶304.

Third, Andrews teaches that its security program can be stored in any number of different locations, such as “as a service of the [] operating system,” as “a ‘device’ of the operating system,” as “software,” as “firmware 25 and/or hardware, such as in...ROM 32.” EX1005, 15:3-18. The portable electronic device can also include various types of non-volatile memory, including “a hard drive,...flash memory,...firmware,” and “read only memory (ROM).” EX1005, 10:3-14. Likewise, Bonnett teaches that its appliance’s memory can be “any [] suitable volatile or nonvolatile storage.” [0031]. A POSITA would have understood the flexibility of both Andrews and Bonnett to provide compatibility of their disclosures, thus further motivating the combination. EX1003, ¶305.

Fourth, contemporaneous publications show that protecting a security program using software-based protections was both conventional and routine (as relevant to the preceding basis for combining) and independently demonstrate a motivation to combine Andrews and Bonnett. EX1003, ¶306-308.

For example, U.S. Patent No. 5,764,892 to Cain et al. (“Cain”) describes a “system for locating and monitoring electronic devices utilizing a security system that is secretly and transparently embedded within the software, firmware, or hardware of a computer.” EX1011, Abstract; *see also* 2:14-19. Cain’s system is meant for “smaller lost or stolen objects” to “facilitate the recovery of [a] stolen device.” EX1011, Abstract, 1:38-42; EX1003, ¶307. Similarly, US2003/0126462

to Howard et al. (“Howard”) describes a system for using “security program” to “prevent[] use of a wireless device” when the device has been stolen. EX1012, [0017]-[0018]. Howard recognized that users might attempt to disable or circumvent the security program and, therefore, disclosed techniques to “minimize[] the probability that the security protocols...will be circumvented by a malicious user.” EX1012, [0019]; *see also* [0030], EX1003, ¶308.

Fifth, a POSITA would have had a reasonable expectation of success in this combination, at least because it would have been routine and predictable to implement Andrews’s security software in Bonnett’s hidden partition. EX1003, ¶309. As discussed above, Andrews contemplates its client software being installed in a variety of formats (e.g., hardware, software, firmware) and in a variety of types of memory (e.g., ROM, flash, hard drive). EX1003, ¶309. Thus, to combine Andrews and Bonnett in the proposed manner would require only that a POSITA identify suitable non-volatile memory in the Andrews portable electronic device (e.g., memory 24 or mass storage 26) and then follow Bonnett’s teachings to (a) create a hidden partition in this memory and (b) program the Andrews client software in the hidden partition, both of which would have been routine. EX1003, ¶309.

3. Claim Analysis

As discussed *supra* §VII.A.2-6, Andrews discloses all limitations of Claims 1-5, 7-13, 15-21, and 23-25. Additionally, Andrews-Bonnett renders obvious each of these claims. EX1003, ¶310-403.

a. Independent Claims

Andrews-Bonnett discloses the Preambles and all other limitations of Claims 1-2, 7-10, 15-18, and 23-25 for the same reasons as discussed in connection with Ground 1A, *supra* §VII.A.2-6. EX1003, ¶310-403.

Additionally, Andrews-Bonnett discloses the Memory Area Limitations. EX1003, ¶328-333, 350-351, 370-371, 390-391. Andrews-Bonnett includes *non-volatile memory* (e.g., Bonnett’s memory 124, 212) that includes a *changeable area that can be modified by a user* (e.g., Bonnett’s open partition of memory 126a, 206a) and a *system area that cannot be modified by the user* (e.g., Bonnett’s hidden partition of memory 126b, 206b). Figs. 1-3, [0031]-[0033]. EX1003, ¶329.

Specifically, the memory 124 can be “any...nonvolatile storage” and is “operable to store one or more programs,” [0031], [0035]. The memory includes a “hidden partition” that stores, *e.g.*, “executable files, the operating portion of the program, operating system applications, [etc.]” that a “program designer desires to be made inaccessible to a user of appliance.” [0036]. Conversely, the open partition stores programs/files that “are accessible to the user.” [0036].

In Andrews-Bonnett, the *non-volatile memory* stores Andrews’s client software 112, which is the claimed *security application* for the reasons discussed in connection with the Security Application Limitations in Ground 1A. EX1003, ¶330. Accordingly, Andrews-Bonnett’s client software is a *security application* that *utilizes code residing at least partially in the system area*. EX1003, ¶330.

Moreover, Bonnett-Andrews’s client software receives a “reported [device] status” from the remote host computer and performs operations based on the status, such as those discussed *supra* §§ VII.A.2.h (disabling device), VII.A.2.i (copying user data), VII.A.2.j (deleting user data). EX1005, 19:6-13; EX1003, ¶331-332. A POSITA would have understood that when performing these operations, the software is executed by a processor from the hidden partition and, during execution, is given access to the reported device status sent from the host computer. EX1003, ¶332. Therefore, a POSITA would have understood Andrews-Bonnett to disclose that its client software *receives a notification from the security service from at least one of the servers via the system area*, as claimed. EX1003, ¶332-333.

Accordingly, Andrews-Bonnett discloses all limitations of Independent Claims 1, 9, 17, and 25. EX1003, ¶310-333, 350-351, 370-371, 390-391.

b. Dependent Claims

(1) Claims 2, 10, and 18

Andrews-Bonnett discloses and/or renders obvious these limitations for the same reasons as discussed above in connection with Ground 1A. *See supra*, §VII.A.3; EX1003, ¶392-393.

(2) Claims 3-5, 11-13, and 19-21

Andrews-Bonnett discloses and/or renders obvious these limitations for the same reasons as discussed above in connection with Ground 1A. *See supra*, §VII.A.6; EX1003, ¶394-399.

(3) Claims 7, 15, and 23

Andrews-Bonnett discloses these limitations for the same reasons as discussed above in connection with Ground 1A. *See supra*, §VII.A.4; EX1003, ¶400-401.

(4) Claims 8, 16, and 24

Andrews-Bonnett discloses these limitations for the same reasons as discussed above in connection with Ground 1A. *See supra*, §VII.A.5; EX1003, ¶402-403.

C. Ground 1C: Claims 1-5, 7-13, 15-21, and 23-25 Obvious over Andrews and Cotichini⁵

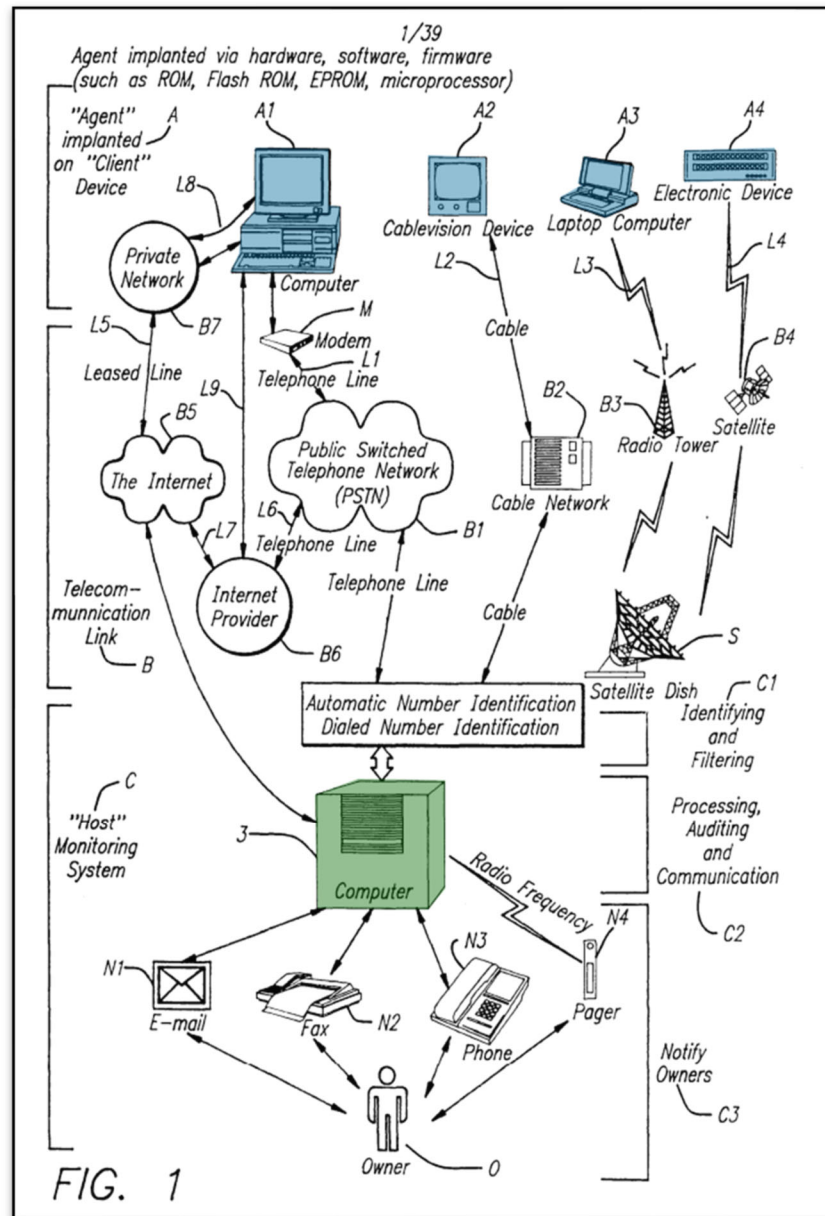
1. Cotichini (EX1007)

Cotichini published on October 1, 1998, from an application filed on March 24, 1998, and is prior art under at least §102(b).

Cotichini discloses “[a] system for locating and monitoring electronic devices utilizing a security system that is secretly and transparently embedded within the software, firmware, or hardware of a computer.” (57).

The structure of Cotichini’s system closely resembles the systems disclosed in the ’649 patent and Andrews. EX1003, ¶¶404-408. As depicted in Figure 1, below, Cotichini’s system includes a one or more “**client device[s]**” in communication with a “**host monitoring system C**” which controls the communications between the client device A and the host monitoring system C.” 12:3-11.

⁵ Unless otherwise noted, Section VII.C’s citations are to EX1007.



Like in the '649 patent and Andrews, Cotichini's client device communicates with the host monitoring system by periodically sending client-related information to the host computer. 22:6-11; EX1003, ¶408. The host computer uses this information to "determine whether the computer has been...reported lost or stolen," 55:17-21, and responds with an appropriate

message. If the computer has been reported stolen, the host computer takes steps to “facilitate the recovery of the missing equipment,” such as by alerting local authorities and/or by determining the location of the missing equipment. 28:28-29:5, 30:24-33, 23:20-24:8, 31:29-32:27.

Each client device is “implanted with” an “agent,” which “hides within the software/firmware/hardware of the electronic device” and performs the above-described security operations. 4:8-11; EX1003, ¶409-411. The agent operates “without interfering with the regular operation of the device,” 4:8-11, and is “designed to evade detection and resist attempts to disable it by an unauthorized user,” 4:21-23. By implementing the agent in this manner, Cotichini “overcomes disadvantages associated with the prior art by yielding a security device for small computers, cellular telephones and the like” that “is well cloaked and thus [] cannot be readily located or disabled even if the possibility of its existence is suspected.” 4:24-32; EX1003, ¶411.

Cotichini describes various embodiments for implementing its agent. EX1003, ¶412-417. The agent “may be implemented in the firmware or software” of the client device. 19:25-26. Alternatively, the agent “may be implemented in any component of” the device, “such as the DSP in a modem or the CPU in the computer.” 19:26-29. Or, the agent “may be implemented in the circuitry of any

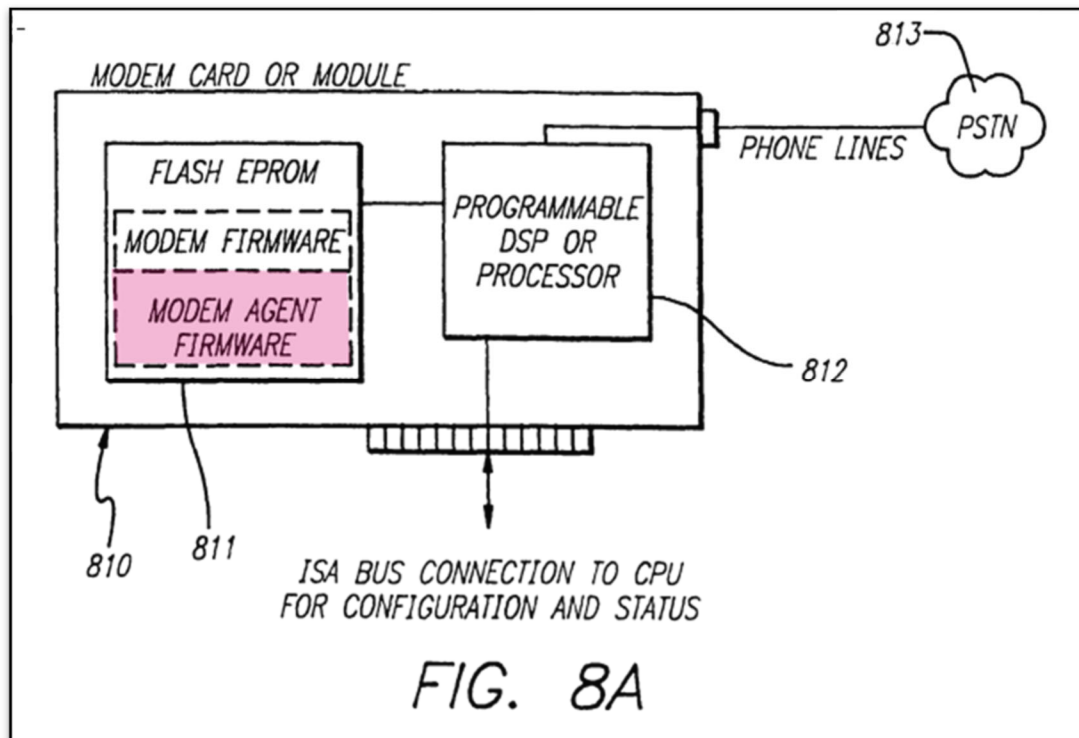
hardware device capable of establishing a communication link through sending and/or receiving packets of data.” 19:29-20:2.

In one example, the “agent security system [is] incorporated into the ROM of portable computers, cellular telephones or other such items when they are manufactured.” 57:7-14. In operation, the “Agent is loaded from the ROM after the CPU registers are saved.” 38:19-25.

In another example, the agent is installed in the “partition boot sector” of the client device. In operation, after the “computer 10 is powered on and the loading sequence begins,” the “partition boot sector is loaded” and “the agent is loaded with the operating system partition boot sector 94.” 37:4-13, 38:8-13.

In another example, the agent is a “Modem Agent” and is “imbedded [sic] into the modem Flash ROM (or EPROM 811) or DSP 812 of the computer modem, either on a plug-in card or built-in on the motherboard (810) of the computer[,]. . . by the manufacturer” 42:16-25. The modem agent operates “independent of the software running on the computer including the operating system,” 42:27-29, and “enables a monitored computer to communicate to the monitoring server even if a new disk drive is installed,” thus “provid[ing] a much more secure method of tracing . . . stolen computers,” 43:1-10. Even if a computer is “stripped for parts, the Modem Agent will still be able to be located.” 43:1-10.

The **Modem Agent** is depicted in example Figure 8A, which shows it “installed into the Flash ROM” of the modem. 42:17-21, 43:21-22. The modem is connected to a network (e.g., PSTN 813), allowing it to “communicate with the Host Monitoring System...at scheduled times.” 42:25-27.



Regardless of where or how the agent is installed on the client device, the system remains inaccessible to users as a result of “well-known deflection methods.” 24:9-10; EX1003, ¶417. Specifically, any “[a]ttempts to read or write to the location where the Agent has been installed are deflected in order to prevent discovery of the agent.” 24:10-12. And “[w]hen write attempts are made to the location where the Agent is installed, the client computer accepts the input data

and informs the user that the write has been successful,” but—crucially—“the data is not really stored, and thus the Agent is preserved.” 24:15-18.

2. Reasons to Combine Andrews with Cotichini

A POSITA would have had multiple reasons to combine Andrews and Cotichini, which both disclose systems for remotely tracking a portable electronic device and are, for at least that reason, analogous art. EX1003, ¶418. More specifically, a POSITA would have had reason to securely install Andrews’s security software in Andrews’s “portable computing device” to be hidden and unchangeable to a user, as taught by Cotichini’s installation of a security agent. *See* 4:8-11, 4:21-23, 24:9-21, 36:13-16, 58:22-23; EX1003, ¶419. Cotichini provides a POSITA a number of options for how to implement Andrews’s security software in this way, and a POSITA had reason to pursue this combination using any one of the disclosed techniques. EX1003, ¶419.

First, a POSITA would have been motivated to combine Andrews and Cotichini for many of the same reasons discussed above for Andrews-Bonnett. EX1003, ¶420-421, 297-309. In particular, Andrews’s teachings about the flexibility of how and where its client software can be installed and the routine nature of storing that software in any type of non-volatile memory apply to Andrews-Cotichini in the same way that they do to Andrews-Bonnett. EX1003, ¶420-421. Likewise, Andrews’s teachings about the desirability of designing a

program that can act surreptitiously and can resist circumvention motivate Andrews-Cotichini for the same reasons because, like Bonnett, Cotichini offers mechanisms to protect software from a user's attempts to disable, delete, or bypass the software. EX1003, ¶420-421. Indeed, Cotichini teaches discloses that its agent operates surreptitiously, further motivating the combination. 4:8-11, 4:21-22, 24:19-21 (agent operates “without interfering with the regular operation of the device” and is “designed to evade detection”); EX1003, ¶420-421.

Second, a POSITA would have recognized the benefits of using Cotichini's secretive installation and storage techniques to increase the chances that a finder or thief would not be able to delete Andrews's security software. EX1003, ¶422. As is the case for Andrews-Bonnett, contemporaneous publications like Cain and Howard describe systems for protecting a security program using software-based protections. EX1003, ¶422, 306-308.

Additionally, Cotichini itself discloses such a system and describes it as “**well-known.**” 24:9-10; EX1003, ¶423. Cotichini discloses “a security system that is secretly and transparently embedded within the software, firmware, or hardware of a computer.” Abstract; *see also* 1:22-25 (system designed to reduce “risk of theft), 2:19-23, 36:10-13 (“the software must remain undetectable once installed”).

Accordingly, a POSITA would have understood Cotichini to expressly motivate Andrews-Cotichini insofar as Cotichini expressly discloses the use of its

memory-protection techniques in a security system for portable electronic devices. EX1003, ¶423.

Third, a POSITA would have had a reasonable expectation of success in this combination, at least in part because Cotichini provides several different ways to install a hidden and unchangeable agent, thus providing a POSITA with the ability to pick the one(s) that would be most readily implemented in Andrews. EX1003, ¶424-427.

For instance, a POSITA could have implemented Andrews's security software as a "Modem Agent." EX1003, ¶425. Andrews's portable device is "configured to execute modem driver software which is used to configure and utilize modem 50" to "dial the host [computer]." EX1005, 11:10-15. Thus, a POSITA would have had an expectation of success installing Andrews's software as a Modem Agent on modem 50, where it would perform the same functions as described in both Andrews and Cotichini (e.g., contacting a host, sending identifying information, receiving notifications, etc.). EX1003, ¶425.

Similarly, a POSITA could have implemented Andrews's security software by "incorporat[ing]" it "into the ROM." EX1003, ¶426. As discussed in Ground 1A, Andrews discloses that its security software can be installed in the device ROM and loaded during start-up of the portable computing device. EX1005, 32:9-14. Cotichini likewise teaches that the software could be installed in ROM such

that the software can be “loaded from the ROM after the CPU registers are saved” and before the operating system is loaded. 38:19-25, Fig. 14C, 25:15-23; EX1003, ¶426.

Indeed, beyond these examples, every implementation described in Cotichini involves installing the security agent in a conventional computer component (e.g., a CPU, a hard drive, hardware, etc.), and Cotichini teaches that its system can be “added to existing computers without physical alteration.” 57:7-8; EX1003, ¶427. Thus, regardless of the specific Cotichini implementation chosen for the combination, a POSITA would have had an expectation of success. EX1003, ¶427.

3. Claim Analysis

a. Independent Claims

Andrews-Cotichini discloses the Preambles and all other limitations of Claims 1-2, 7-10, 15-18, and 23-25 for the same reasons as discussed in connection with Ground 1A, *supra* §VII.A.2-6.

Additionally, Andrews-Cotichini discloses the Memory Area Limitations. EX1003, ¶446-458, 475-476, 495-496, 515-516. In each of the above-described examples of Andrews-Cotichini combinations, Andrews’s security software is installed in non-volatile memory. EX1003, 447-449. For example if the software were implemented as a Modem Agent, the software would “embedded into the modem Flash ROM,” which a POSITA would have understood is a type of non-

volatile memory. 42:21-25; EX1003, ¶447. Similarly, if implemented as a ROM Agent, the software would be “incorporated into the ROM” of the device, which a POSITA would have understood to be non-volatile memory. 57:7-14; EX1003, ¶448.

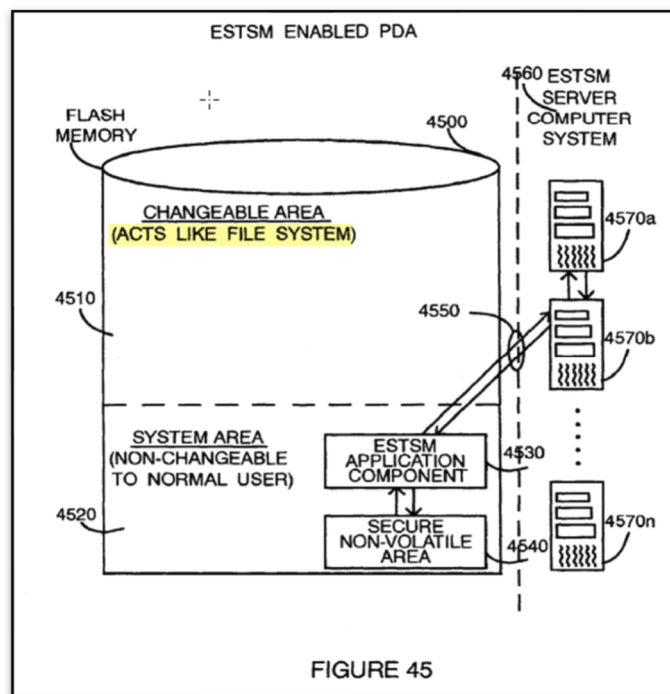
When installed as taught in Cotichini, Andrews’s software would be protected by “well-known deflection methods” such that any “[a]ttempts to read or write to the location where the Agent has been installed are deflected” and any attempted changes are “not really stored, and thus the Agent is preserved.” 24:9-18; EX1003, ¶450. Thus, the area of memory in which the security software is installed is a *system area* because it cannot be rewritten (i.e., *modified*) by a user. EX1003, ¶451.

Moreover, Andrews-Cotichini’s client software receives a “reported [device] status” from the remote host computer and performs operations based on the status, such as those discussed *supra* §§ VII.A.2.h (disabling device), VII.A.2.i (copying user data), VII.A.2.j (deleting user data). EX1005, 19:6-13; EX1003, ¶452. A POSITA would have understood that when performing these operations, the software is executed by a processor from an area of memory “protected by well-known deflection methods” and that the software, during execution, is given access to the reported device status sent from the host computer. EX1003, ¶452. Thus, a POSITA would have understood that Andrews-Cotichini’s client software would

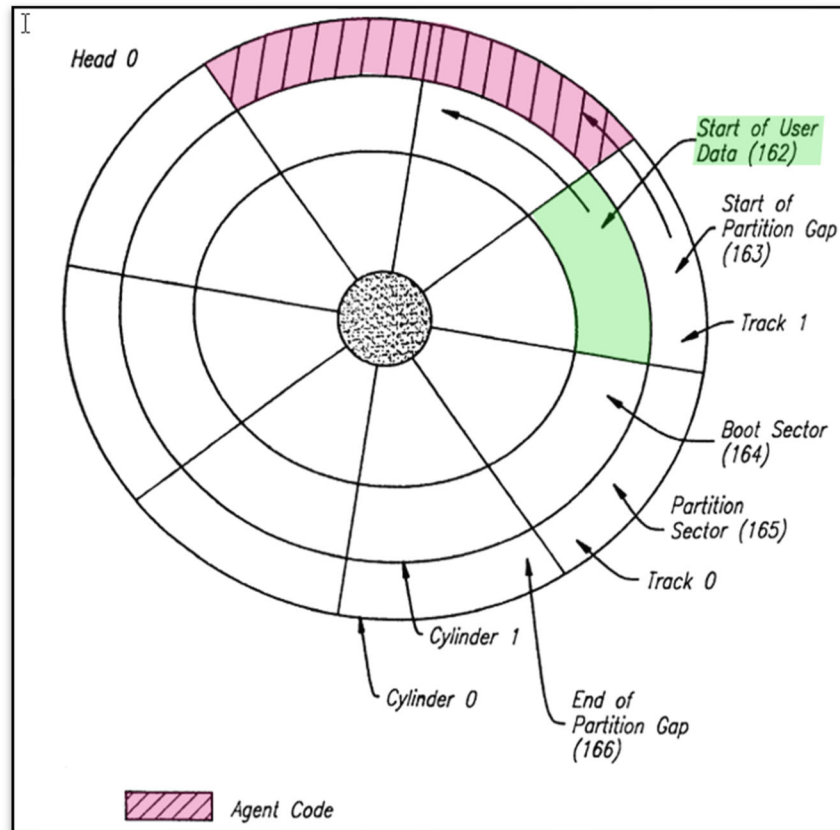
receive[] a notification from the security service from at least one of the servers via the system area, as claimed. EX1003, ¶452.

For example, if installed as a Modem Agent, Andrews-Cotichini's software would be installed in Andrews's modem 50 and would allow the modem to serve as the client device's "interface to the monitoring server" by "communicat[ing] with the host monitoring server directly," 45:10-11, 46:13-14; EX1003, ¶453. In this implementation of Andrews-Cotichini, the modem agent would therefore communicate with the host computer to receive *a notification from the security service...via the system area*. EX1003, ¶453.

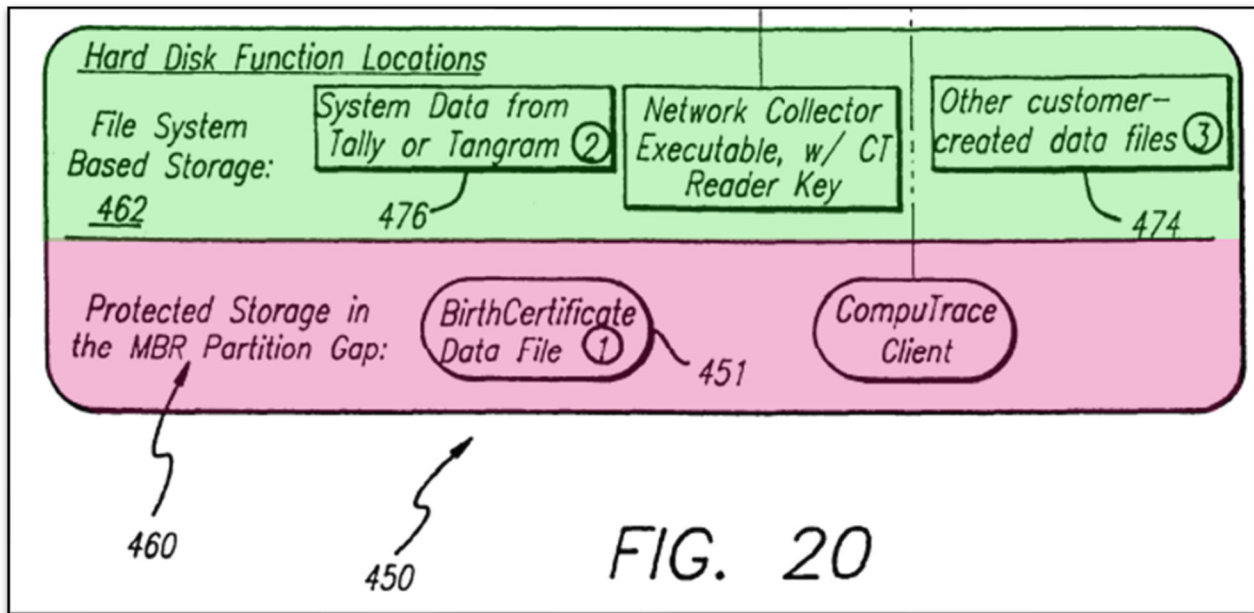
In Andrews-Cotichini, Andrews's client device would also maintain the *changeable area* of non-volatile memory in which the device maintains the "files" and/or "folders" that can be retrieved and deleted from the device by the host computer, as discussed above in connection with Ground 1A. EX1003, ¶454-458. For example, this *changeable area* might include the area of memory identified as "C:\files\importantfile.doc," which a POSITA would have understood to be an illustrative reference to the "C:" drive of a Windows operating system and which stores files that *can be modified by a user*, as claimed. EX1003, ¶454. Indeed, the '649 patent teaches that the *changeable area* "may include a file system," EX1001, 20:14-17, and that the *changeable area* "acts like a file system," as shown in Figure 45 below:



Retaining Andrews's changeable file system in Andrews-Cotichini is entirely consistent with Cotichini's teachings and, therefore, consistent with the proposed Andrews-Cotichini combination. EX1003, ¶455-458. For example, Cotichini's Figure 14H depicts a hard disk containing both protected **Agent Code** and **User Data**:



Likewise, Cotichini’s Figure 20 depicts a hard disk with both a **file system area** storing “customer-created files” as well as a “**protected storage**” in which the “CompuTrace Client” (or, agent) is stored:



Accordingly, Andrews-Cotichini discloses all limitations of Independent Claims 1, 9, 17, and 25. EX1003, ¶428-516.

a. Dependent Claims

(1) Claims 2, 10, and 18

Andrews-Cotichini discloses these limitations for the same reasons as discussed above in connection with Ground 1A. *See supra*, § VII.A.3; EX1003, ¶517-518.

(2) Claims 3-5, 11-13, and 19-21

Andrews-Cotichini discloses and/or renders obvious these limitations for the same reasons as discussed above in connection with Ground 1A. *See supra*, § VII.A.6; EX1003, ¶519-524.

(3) Claims 7, 15, and 23

Andrews-Cotichini discloses these limitations for the same reasons as discussed above in connection with Ground 1A. *See supra*, § VII.A.4; EX1003, ¶525-526.

(4) Claims 8, 16, and 24

Andrews-Cotichini discloses these limitations for the same reasons as discussed above in connection with Ground 1A. *See supra*, § VII.A.5; EX1003, ¶527-528.

D. Ground 1D: Claims 6, 8, 14-16, and 22-25 Obvious over Andrews and Hayward⁶

As discussed *supra* §VII.A.2-6, Claims 1-5, 7-13, 15-21, and 23-25 are disclosed by Andrews alone and rendered obvious by Andrews-Cotichini. Additionally, Claims 15-16 and 23-25 are disclosed by the combination of Andrews, Cotichini, and Hayward. EX1003, ¶539-542, 549-552.

Furthermore, Claims 6, 14, and 22 are disclosed by the combination of Andrews, Cotichini, and Hayward. EX1003, ¶543-548.

1. Hayward (EX1008)

Hayward published on May 22, 2002 from an application filed November 17, 2000 and is prior art under at least §102(b).

⁶ Unless otherwise noted, Section VII.D's citations are to EX1008.

Hayward discloses a “personal data device” storing “personal data” and “data protection software.” 1:23-2:4; EX1003, ¶529-533. The device may be a “mobile telephone” or “PDA.” The data device is in communication with a “database server,” which stores a “copy of the data stored in the data store 11 of the personal data device.” 20:28-21:2.

Using the data protection software, a user can “register the personal data device with the Internet database server.” 14:17-19; EX1003, ¶529-533. In some cases, a device may be “reported missing by contacting the database server via the Internet or telephone.” 21:27-28 In response, the database server “seeks to contact the missing device...in a manner undetectable to a user, for , by sending a SMS message.” 21:25-30. The database server also “compares the data stored in the personal data device with that stored for that device in the database and, if appropriate, updates the version stored in the database using the data stored in the personal data device.” 22:5-9. The server can also “signal[] the personal data device to delete...the data...held in the personal data device so that the data cannot be used by an unauthorized user.” 22:9-12.

Additionally, in some instances, the device is “further protected by automatic deletion of the data stored in the personal data device on failure successfully to log into the personal data device.” 23:17-19; EX1003, ¶529-533. In response to an unauthorized attempt to access the device, “the device deletes...all

the data...in the personal data device.” 23:23-25. However, “before deleting the data, the device contacts the database server 50 and uploads... any data...that is necessary to create a current backup.” 23:25-27. Thereafter, “[a]n authorized user may...reload the data from the backup into the personal data device.” 23:27-29.

2. Andrews-Cotichini-Hayward Combination

Like the '649 patent and Andrews, Hayward concerns techniques for protecting devices and their data and is, therefore, analogous art. EX1003, ¶534. A POSITA had reasons to use Hayward's data-protection techniques in the Andrews-Cotichini security system. EX1003, ¶534. Specifically, a POSITA had reason to implement Andrews-Cotichini's security system such that device owners could use the security service to automatically delete user data from that device and restore the user data to that device upon recovery. EX1003, ¶534.

First, both Andrews and Hayward are directed to systems for protecting personal data on mobile electronic devices. EX1003, ¶535. As Andrews explains, the “value of data stored on a lost or stolen portable computing device may eclipse the value of the device itself” and “may be of a sensitive nature.” EX1005, 1:17-19. Thus, the “recovery of the data” is a “high priorit[y].” EX1005, 1:20-22. To address this problem, Hayward discloses “data protection software” to, *e.g.*, prevent unauthorized access to data (10:25-11:5, 13:27-14:8), delete data that falls

into the wrong hands (23:17-20, 23:29-31, 15:12-17), and copy data to a database server to allow for data recovery (22:30-23:12, 23:25-29).

Although Andrews-Cotichini would have provided device owners the ability to protect their data as discussed in Ground 1C, Hayward's data protection software provides additional protection by automatically backing up and deleting data in response to unauthorized attempts to access the device, while also allowing the data to be restored to the device upon recovery. EX1003, ¶536.

Second, it would have been using known data-protection techniques to improve similar systems (for recovering and protecting portable devices) in the same way (automatically transmitting (and, thereafter deleting) data from a portable device). *KSR*, 550 U.S. at 417; EX1003, ¶537.

A POSITA would have had a reasonable expectation of success because Hayward discloses implementing its data-protection techniques in a system that is substantially similar to the one disclosed in Andrews. EX1003, ¶538. For instance, both systems include executing a computer program on a portable electronic device, such as a PDA. *Compare* EX1005, 8:18-9:7 *with* EX1008, 10:25-28, 15:28-31. In both systems, these devices communicate with a remote server system via a network. *Compare* EX1005, 15:19-16:8 *with* EX1008, 12:1-5. And in both systems, the devices send and receive user data to/from the remote server. *Compare* EX1005, 28:17-22 *with* EX1008, 14:9-33. It would have required only

ordinary skill for a POSITA to program Andrews's client software to execute the data-protection steps performed by Hayward's data protection software. EX1003, ¶538.

3. Independent Claim 25

Andrews-Cotichini-Hayward discloses the Preamble and all other limitations of Claim 25 for the same reasons as discussed in connection with Ground 1C, *supra* §VII.C.3. Additionally, Andrews-Cotichini-Hayward renders obvious this claim. EX1003, ¶534-542.

a. Deleting User Data Limitations

Andrews-Cotichini-Hayward discloses this limitation. EX1003, ¶539-540. In Andrews-Cotichini-Hayward, if the device detects an unauthorized attempt to access the device, "the device...uploads... any data to the database server that is necessary to create a current backup." 23:25-27, Fig. 11; EX1003, ¶540. After the data is backed up to the server, the server will "signal[] the personal data device to delete...the data...held in the personal data device so that the data cannot be used by an unauthorized user." 22:9-12. Additionally, "the device deletes...all the data...in the personal data device," but only after a "current backup" of the data is created on the server. 23:23-27.

b. Restoring User Data Limitations

Andrews-Cotichini-Hayward discloses this limitation. EX1003, ¶541-542. In Andrews-Cotichini-Hayward, after the data has been copied and deleted from the device, “[a]n authorized user may...subsequently reload the data from the backup into the personal data device.” 23:27-29; EX1003, ¶542.

4. Claims 6, 14, and 22

[6]	<i>A mobile electronic device according to claim 1, wherein: the system area comprises a short messaging service (SMS) component; the notification comprises a message in an SMS format; and the security application receives the notification from at least one of the servers via the SMS component.</i>
[14]	<i>A method according to claim 9, wherein: the system area comprises a short messaging service (SMS) component; the notification comprises a message in an SMS format; and the operation of accepting the notification from the security service comprises receiving the notification from at least one of the servers via the SMS component.</i>
[22]	<i>An article of manufacture according to claim 17, wherein: the notification comprises a message in an SMS format; and the operation of accepting the notification from the security service comprises receiving the notification from at least one of the servers via an SMS component residing in the system area of the non-volatile memory in the mobile electronic device.</i>

Andrews-Cotichini-Hayward discloses this limitation. EX1003, ¶543-548. In Andrews-Cotichini-Hayward, when a device is reported missing, the database

server “contact[s] the missing device...in a manner undetectable to a user, for example, by sending a SMS message.” 21:28-30.

A POSITA would have had reason to implement Hayward’s SMS communication technique in the Andrews-Cotichini-Hayward system. EX1003, ¶545-548.

First, as Hayward explains, using an SMS message allows the server to send a notification that is “undetectable to a user.” 21:28-30. This would be particularly beneficial in the circumstances in which the Andrews-Cotichini-Hayward system is intended to be used—that is, when an unauthorized user is in possession of a missing electronic device. EX1003, ¶546.

Second, a POSITA would have understood that using SMS was one of a finite number of known methods for sending data from a remote server to a portable client device, such as a PDA. EX1003, ¶547. Indeed, it was recognized in the prior art that “[t]he ideal means of push communication (i.e., communication which occurs without a request being issued by the recipient) in the GSM network is the short message facility (SMS).” EX1019, 8:27-29; EX1003, ¶547. The advantages of using SMS messages include, *inter alia*, “the provision of information from any database server on the Internet to a user’s PDA ‘on the fly’ ...and the sending of information to a PDA without a user request for that information[.]” EX1019, 7:7-16; EX1003, ¶547. Each of these advantages would

be beneficial in the Andrews-Cotichini-Hayward combined system in which the host computer would need to send commands to the portable electronic device to instruct the device to lock, delete data, backup data, etc. without a user request or intervention. EX1003, ¶547.

Moreover, Andrews-Cotichini-Hayward's *SMS component* would *resid[e]* in *the system area*. EX1003, ¶548. As discussed in connection with Ground 1C, *supra* §VII.C, Andrews-Cotichini includes Andrews's security software installed in a hidden and protected manner as taught in Cotichini. EX1003, ¶418-427. The Andrews-Cotichini software sends and receives messages from the security service via a modem, which may store the software in a *system area* as in Cotichini's "modem agent." EX1003, ¶418-427. To implement Hayward's SMS component in a *system area*, a POSITA would, therefore, simply configure the Andrews-Cotichini modem to communicate with the GSM network to send and receive SMS messages, which would have been a routine and conventional implementation of Hayward's SMS teachings in Andrews-Cotichini. EX1003, ¶548.

5. Claims 7, 15, and 23

See Deleting User Data Limitations, supra §VII.D.3.a; EX1003, ¶549-550.

6. Claims 8, 16, and 24

See Restoring User Data Limitations, supra § VII.D.3.b; EX1003, ¶551-552.

VIII. NO BASIS FOR DISCRETIONARY DENIAL

A. 35 U.S.C. § 325(d)

Discretionary denial under §325(d) is not appropriate. This is first proceeding before the Board challenging the patentability of the claims of the '649 patent. None of the prior art grounds in this Petition were considered or evaluated by the Patent Office. Indeed, Andrews and Hayward were not disclosed during prosecution and Bonnett and Cotichini were cited in an IDS, but not otherwise discussed during prosecution. *See Becton, Dickinson & Co. v. B. Braun Melsungen AG*, IPR2017-01586, Paper 8 at 17-18 (P.T.A.B. Dec. 15, 2017) (informative).

The specific arguments presented in this Petition were not before the Examiner during prosecution, nor did the Examiner have the benefit of the testimony of Petitioner's Expert, Dr. John Black, submitted herein. Thus, there is no overlap between arguments made during examination and the manner in which Petitioner relies on the prior art because there were no arguments made on the record related to Bonnett and Cotichini. Further, Petitioner presents combinations of Bonnett and Cotichini with Andrews, which was not disclosed to or known by the Examiner.

As shown herein, it is more likely than not that the Examiner erred by not relying on Bonnett and Cotichini during prosecution of the challenged claims. The Examiner's failure to assert a rejection based on Bonnett and Cotichini does not

refute the grounds for unpatentability set forth in this Petition as the arguments set forth in the Petition are not repeat of those that were made and vetted during prosecution, where Petitioner was not represented.

Further, this is not a case of serial petitions attempting to have multiple bites as the same apple. Taken as a whole, the facts of this case counsel that the Board institute Petitioner's IPR "to weed out bad patent claims efficiently." *Thryv, Inc. v. Click-to-Call Techs., LP*, 140 S.Ct. 1367, 1374 (2020). The *Becton* factors strongly favor institution.

B. 35 U.S.C. § 314(a)

The *Fintiv* factors weigh heavily against discretionary denial. It is highly unlikely that any of the parallel proceedings will proceed to trial before the projected final written decision date of January 2025 in this proceeding. Three of the parallel litigations – the litigations against HP, Dell, and Absolute – are currently pending before Senior Judge Ezra in the United States District Court for the Western District of Texas. The parties have submitted a disputed schedule with Softex and defendants each proposing that dispositive motion briefing completed in September 2024 and January 2025, respectively. EX1020. The court has not yet set the schedule, but it is Judge Ezra's practice not to set a trial date until dispositive motions have been resolved. EX1021 at 7. Further, the mean time to trial in the Western District is 28.2 months, which would mean the trial in those

cases would occur in April 2025, approximately four months after the projected final written decision date in this proceeding.⁷ EX1025 at 37. Similarly, the remaining litigation against Lenovo is pending in the United States District Court for the Eastern District of North Carolina and does not have a schedule entered, and the mean time to trial in that district is 32.7 months, which would mean the trial in that case would occur in August 2025, approximately seven months after the projected final written decision date in this proceeding. EX1025 at 21. Further, as of the date of filing of the Petition, the district courts have only ruled on motions to dismiss and transfer, and have not made any substantive rulings related to the '649 patent and likely will not do so prior to the January 2024 projected institution decision date.⁸ Finally, Microsoft is not a defendant in any of the parallel cases.

Additionally, as demonstrated above, this Petition presents compelling merits that the challenged claims are unpatentable. Microsoft has presented evidence plainly showing that one or more claims are unpatentable and it is highly

⁷ HP and Dell have filed motions to stay their cases due to the customer suit exception. If those are granted, then the trials in those cases will likely be later than April 2025.

⁸ The proposed scheduling in the Western District of Texas cases proposes the claim construction hearing occur in December 2023.

likely that Microsoft will prevail with at respect to at least one challenged claim.

See Commscope Techs. LLC v. Dali Wireless, Inc., IPR2022-01242, Paper 23

(P.T.A.B. Feb. 27, 2023) (precedential opinion).

Thus, the Board should not exercise its discretionary denial authority under *Fintiv* in the present proceeding because it is highly unlikely that any of the parallel proceedings will proceed to trial before the final written decision will issue, and the Petition presents compelling evidence of unpatentability.

IX. CONCLUSION

The Board should institute this IPR.

Respectfully submitted,

Dated July 11, 2023

/Carrie A. Beyer/
Carrie A. Beyer, Reg. No. 59,195
Kirstin Stoll-DeBell, Reg. No. 43,164
Zachary D. Kachmer, Reg. No. 75,414

Attorneys for Petitioner

CERTIFICATION UNDER 37 CFR §42.24

Under the provisions of 37 CFR §42.24(d), the undersigned hereby certifies that, in accordance with and reliance on the word count provided by the word-processing system used to prepare this Petition, the word count for the foregoing Petition for *Inter Partes* Review totals 13,983 words, which is less than the 14,000 allowed under 37 CFR §42.24. Pursuant to 37 C.F.R. §42.24(a), this word count is in compliance and excludes the table of contents, table of authorities, mandatory notices under §42.8, certificate of service, certificate of word count, appendix of exhibits, and any claim listing. This word count was prepared using Microsoft Word.

Dated July 11, 2023

/Carrie A. Beyer/

Carrie A. Beyer, Reg. No. 59,195

Kirstin Stoll-DeBell, Reg. No. 43,164

Zachary D. Kachmer, Reg. No. 75,414

Attorneys for Microsoft Corporation

CERTIFICATE OF SERVICE

Pursuant to 37 CFR §§42.6(e)(4)(i) et seq. and 42.105(b), the undersigned certifies that on July 11, 2023, a complete and entire copy of this Petition for *Inter Partes* Review and all supporting exhibits were provided, via Federal Express, to the Patent Owner by serving the correspondence address of record as follows:

**G+J Softex Temp
4301 W William Cannon Dr., Suite B150 PMB200
Austin, TX 78749-1487**

/Debbie Cairns/
Debbie Cairns, Paralegal

X. CLAIM LISTING

The following claim listing assigns element labels (*e.g.*, [1A], [1B], etc.) to certain claims for clarity.

Claim 1
[1] 1. A mobile electronic device, comprising:
[1A] a processor;
[1B] one or more non-transitory machine-readable storage media responsive to the processor...wherein the one or more non-transitory machine-readable storage media comprises non-volatile memory;
[1C] 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:
[1D] enabling 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;
[1E] causing the mobile electronic device to automatically send identifying information for the mobile electronic device to the security service;
[1F] 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 which the mobile electronic device is powered off;
[1G] 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;
[1H] 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
[1I] automatically causing at least some user data to be copied from the mobile electronic device to at least one of the servers;
[1J] 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; wherein the security application utilizes code residing at least partially in the system area; and

wherein the security application receives the notification from at least one of the servers via the system area.

Claim 2

2. A mobile electronic device according to claim 1, wherein the notification includes no third-party certification.

Claim 3

3. A mobile electronic device according to claim 1, wherein the operation of enabling the owner to register the mobile electronic device with the security service comprises providing the security service with at least three items from the group consisting of: a phone number for the mobile electronic device, a phone service provider for the mobile electronic device, an International Mobile Equipment Identifier (IMEI) number for the mobile electronic device, and a phone description for the mobile electronic device.

Claim 4

4. A mobile phen [sic] electronic device according to claim 3, wherein the identifying information automatically sent from the mobile electronic device to the security service comprises:

- a phone number for the mobile electronic device;
- an international mobile equipment identifier (IMEI) number for the mobile electronic device; and
- a model number for the mobile electronic device.

Claim 5

5. A mobile electronic device according to claim 3, wherein the identifying information automatically sent from the mobile electronic device to the security service comprises:

- a phone number for the mobile electronic device; and
- an international mobile equipment identifier (IMEI) number for the mobile electronic device.

Claim 6

6. A mobile electronic device according to claim 1, wherein:

- the system area comprises a short messaging service (SMS) component;
- the notification comprises a message in an SMS format; and
- the security application receives the notification from at least one of the servers via the SMS component.

Claim 7

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.
Claim 8
8. A mobile electronic device according to claim 7, wherein the operations the security application is operable to perform further comprise: after the at least some of the user data has been deleted from the mobile electronic device, causing at least some of the user data to be copied from at least one of the servers to the mobile electronic device.
Claim 9
[9P] 9. A method for providing security for a mobile electronic device, the method comprising:
[9A] wherein the mobile electronic device comprises non-volatile memory;
[9B] 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; in response to the request from the owner, registering the mobile electronic device with the security service;
[9C] automatically sending identifying information for the mobile electronic device from the mobile electronic device to the security service;
[9D] 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;
[9E] 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;
[9F] 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

[9G] automatically causing at least some user data to be copied from the mobile electronic device to at least one of the servers;

[9H] 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;

wherein the security application utilizes code residing at least partially in the system area; and

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.

Claim 10

10. A method according to claim 9, wherein the notification includes no third-party certification.

Claim 11

11. A method according to claim 9, wherein the operation of registering the mobile electronic device with the security service comprises:
providing the security service with at least three items from the group consisting of: a phone number for the mobile electronic device, a phone service provider for the mobile electronic device, an International Mobile Equipment Identifier (IMEI) number for the mobile electronic device, and a phone description for the mobile electronic device.

Claim 12

12. A method according to claim 11, wherein the identifying information automatically sent from the mobile electronic device to the security service comprises:
a phone number for the mobile electronic device; and
an international mobile equipment identifier (IMEI) number for the mobile electronic device.

Claim 13

13. A method according to claim 11, wherein the identifying information automatically sent from the mobile electronic device to the security service comprises:
a phone number for the mobile electronic device;
an international mobile equipment identifier (IMEI) number for the mobile electronic device; and
a model number for the mobile electronic device.

Claim 14

14. A method according to claim 9, wherein:

the system area comprises a short messaging service (SMS) component;
the notification comprises a message in an SMS format; and
the operation of accepting the notification from the security service
comprises receiving the notification from at least one of the servers via the
SMS component.

Claim 15

15. A method according to claim 9, further comprising:

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.

Claim 16

16. A method according to claim 15, further comprising:

after the at least some of the user data has been deleted from the mobile
electronic device, causing at least some of the user data to be copied from
at least one of the servers to the mobile electronic device.

Claim 17

[17P] 17. An article of manufacture comprising:

[17A] a non-transitory machine-readable storage medium; and . . .
non-volatile memory in the mobile phone

[17B] a security application encoded as instructions in the non-transitory
machine-readable storage medium, wherein the security application, when
executed by a mobile electronic device, enables the mobile electronic device to
perform operations comprising:

[17C] receiving, at the 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;

in response to the request from the owner, registering the mobile electronic
device with the security service;

[17D] automatically sending identifying information for the mobile electronic
device from the mobile electronic device to the security service;

[17E] 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;

[17F] 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;

[17G] 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

[17H] automatically causing at least some user data to be copied from the mobile electronic device to at least one of the servers;

[17I] wherein the operation of accepting the notification from the security service comprises receiving the notification from at least one of the servers via a system area of non-volatile memory in the mobile phone; and

wherein the system area is an area that cannot be modified by a user.

Claim 18

18. An article of manufacture according to claim 17, wherein the notification includes no third-party certification.

Claim 19

19. An article of manufacture according to claim 17, wherein the operation of registering the mobile electronic device with the security service comprises:

- providing the security service with at least three items from the group consisting of: a phone number for the mobile electronic device, a phone service provider for the mobile electronic device, an International Mobile Equipment Identifier (IMEI) number for the mobile electronic device, and a phone description for the mobile electronic device.

Claim 20

20. An article of manufacture according to claim 19, wherein the identifying information automatically sent from the mobile electronic device to the security service comprises:

- a phone number for the mobile electronic device; and
- an international mobile equipment identifier (IMEI) number for the mobile electronic device.

Claim 21

21. An article of manufacture according to claim 19, wherein the identifying information automatically sent from the mobile electronic device to the security service comprises:

- a phone number for the mobile electronic device;
- an international mobile equipment identifier (IMEI) number for the mobile electronic device; and
- a model number for the mobile electronic device.

Claim 22
22. An article of manufacture according to claim 17, wherein: the notification comprises a message in an SMS format; and the operation of accepting the notification from the security service comprises receiving the notification from at least one of the servers via an SMS component residing in the system area of the non-volatile memory in the mobile electronic device.
Claim 23
23. An article of manufacture according to claim 17, wherein the operations the security application, when executed by the mobile electronic device, enables the mobile electronic device 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.
Claim 24
24. An article of manufacture according to claim 23, wherein the operations the security application, when executed by the mobile electronic device, enables the mobile electronic device to perform further comprise: after the at least some of the user data has been deleted from the mobile electronic device, causing at least some of the user data to be copied from at least one of the servers to the mobile electronic device.
Claim 25
[25P] 25. A method for providing security for a mobile electronic device, the method comprising:
[25A] wherein the mobile electronic device comprises non-volatile memory;
[25B] 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;
in response to the request from the owner, registering the mobile electronic device with the security service;
[25C] automatically sending identifying information for the mobile electronic device from the mobile electronic device to the security service;
[25D] 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;

[25E] 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;

[25F] automatically causing at least some user data to be copied from the mobile electronic device to at least one of the servers;

[25G] 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; and

[25H] after the at least some of the user data has been deleted from the mobile electronic device, causing at least some of the user data to be copied from at least one of the servers to the mobile electronic device;

[25I] 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;

wherein the security application utilizes code residing at least partially in the system area; and

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.