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

_____

DECLARATION OF JOHN BLACK, PhD

TABLE OF CONTENTS

I. PERSONAL AND PROFESSIONAL BACKGROUND 1

II. MATERIALS REVIEWED AND CONSIDERED 5

III. MY UNDERSTANDING OF PATENT LAW 6

A. Anticipation 8

B. Obviousness 9

IV. PERSON OF ORDINARY SKILL IN THE ART ("POSITA") 11

A. Qualifications of a Person of Ordinary Skill in the Art 11

B. Knowledge of a Person of Ordinary Skill in the Art 13

1. ROM (Read-Only Memory) 14

2. Flash Memory 21

3. Other Kinds of Memory 22

4. Computer Types and Memories Used 26

5. Restricting Access to Memory 27

6. Disk Partitions 28

7. Controlled Software Environments 29

8. Software-Based Controls with Privileged Access Permissions 31

V. THE '649 PATENT 33

A. ESTSM Operation 34

1. Registration 35

2. Device-Server Communication 36

3. Security Notifications and Responses 38

a. Register 39

b. Disable 40

c. Backup 42

d. Delete 45

e. Restore 46

B. Memory Access Restrictions for Security Application 49

C. Prosecution History of the '649 Patent 52
D. The Challenged Claims 56
VI. CLAIM INTERPRETATION 58
VII. THE CHALLENGED CLAIMS ARE UNPATENTABLE IN LIGHT OF THE PRIOR ART IDENTIFIED IN THE PETITION 58
A. Ground 1A: Claims 1-5, 7-13, 15-21, and 23-25 are Anticipated by and/or Would Have Been Obvious Over Andrews 58
1. Overview of Ground 1 58
2. Andrews (EX1005): WIPO Pub. No. WO2001084455 59
3. Independent Claim 1 68
a. Preamble 1[pre] 69
b. Structural Limitations 1[A] and 1[B] 70
c. Security Application Limitation 1[C] 71
d. Registration Limitation 1[D] 73
e. Sending Identifying Information Limitation 1[E] 78
f. Periodic Communication Limitation 1[F] 81
g. Security Notification Limitation 1[G] 85
h. Device Disabling Limitation 1[H] 87
i. Copying User Data Limitation 1[I] 91
j. Memory Area Limitation 1[J] 95
4. Independent Claim 9 99
a. Preamble 9[pre] 100
b. Structural Limitation 9[A] 101
c. Registration Limitation 9[B] 101
d. Sending Identifying Information Limitation 9[C] 102
e. Periodic Communication Limitation 9[D] 102
f. Security Notification Limitation 9[E] 103
g. Device Disabling Limitation 9[F] 103
h. Copying User Data Limitation 9[G] 104

i. Memory Area Limitation 9[H] 104
5. Independent Claim 17 105
a. Preamble 17[pre] 106
b. Structural Limitation 17[A] 106
c. Security Application Limitation 17[B] 106
d. Registration Limitation 17[C] 107
e. Sending Identifying Information Limitation 17[D] 107
f. Periodic Communication Limitation 17[E] 108
g. Security Notification Limitation 17[F] 108
h. Device Disabling Limitation 17[G] 109
i. Copying User Data Limitation 17[H] 109
j. Memory Area Limitation 17[I] 110
6. Independent Claim 25 110
a. Preamble 25[pre] 111
b. Structural Limitation 25[A] 112
c. Registration Limitation 25[B] 112
d. Sending Identifying Information Limitation 25[C] 113
e. Security Notification Limitation 25[D] 113
f. Device Disabling Limitation 25[E] 113
g. Copying User Data Limitation 25[F] 114
h. Deleting User Data Limitation 25[G] 114
i. Restoring User Data Limitation 25[H] 117
j. Memory Area Limitation 25[I] 121
7. Dependent Claims 2, 10, 18 122
8. Dependent Claims 3, 11, 19 123
9. Dependent Claims 4, 12, 20 128
10. Dependent Claims 5, 13, 21 129
11. Dependent Claims 7, 15, 23 131
12. Dependent Claims 8, 16, 24 132

B. Ground 1B: 1-5, 7-13, 15-21, and 23-25 Obvious over Andrews and Bonnett 133
1. Bonnett (EX1006): U.S. Patent Pub. No. 2003/0051090 133
a. Overview of Disclosure 133
b. Bonnett Provisional 135
2. The Andrews-Bonnett Combination 139
3. Independent Claim 1 145
a. Preamble 1[pre] 145
b. Structural Limitations 1[A] and 1[B] 146
c. Security Application Limitation 1[C] 146
d. Registration Limitation 1[D] 147
e. Sending Identifying Information Limitation 1[E] 147
f. Periodic Communication Limitation 1[F] 148
g. Security Notification Limitation 1[G] 149
h. Device Disabling Limitation 1[H] 149
i. Copying User Data Limitation 1[I] 150
j. Memory Area Limitation 1[J] 150
4. Independent Claim 9 153
a. Preamble 9[pre] 153
b. Structural Limitation 9[A] 153
c. Registration Limitation 9[B] 154
d. Sending Identifying Information Limitation 9[C] 154
e. Periodic Communication Limitation 9[D] 155
f. Security Notification Limitation 9[E] 155
g. Device Disabling Limitation 9[F] 156
h. Copying User Data Limitation 9[G] 156
i. Memory Area Limitation 9[H] 157
5. Independent Claim 17 157
a. Preamble 17[pre] 157

b. Structural Limitation 17[A] 158
c. Security Application Limitation 17[B] 158
d. Registration Limitation 17[C] 159
e. Sending Identifying Information Limitation 17[D] 159
f. Periodic Communication Limitation 17[E] 160
g. Security Notification Limitation 17[F] 160
h. Device Disabling Limitation 17[G] 161
i. Copying User Data Limitation 17[H] 161
j. Memory Area Limitation 17[I] 162
6. Independent Claim 25 162
a. Preamble 25[pre] 162
b. Structural Limitation 25[A] 163
c. Registration Limitation 25[B] 163
d. Sending Identifying Information Limitation 25[C] 163
e. Security Notification Limitation 25[D] 164
f. Device Disabling Limitation 25[E] 164
g. Copying User Data Limitation 25[F] 165
h. Deleting User Data Limitation 25[G] 165
i. Restoring User Data Limitation 25[H] 165
j. Memory Area Limitation 25[I] 166
7. Dependent Claims 2, 10, 18 166
8. Dependent Claims 3, 11, 19 167
9. Dependent Claims 4, 12, 20 167
10. Dependent Claims 5, 16, 21 167
11. Dependent Claims 7, 15, 23 168
12. Dependent Claims 8, 16, 24 168
C. Ground 1C: Claims 1-5, 7-13, 15-21, and 23-25 Obvious over Andrews and Cotichini 168
1. Cotichini (EX1007): WIPO Pub. No. 1998/043151 168

2. The Andrews-Cotichini Combination....175
3. Independent Claim 1....179
a. Preamble 1[pre]....179
b. Structural Limitations 1[A] and 1[B]....179
c. Security Application Limitation 1[C]....180
d. Registration Limitation 1[D]....180
e. Sending Identifying Information Limitation 1[E]....181
f. Periodic Communication Limitation 1[F]....181
g. Security Notification Limitation 1[G]....182
h. Device Disabling Limitation 1[H]....182
i. Copying User Data Limitation 1[I]....183
j. Memory Area Limitation 1[J]....183
4. Independent Claim 9....189
a. Preamble 9[pre]....189
b. Structural Limitation 9[A]....189
c. Registration Limitation 9[B]....190
d. Sending Identifying Information Limitation 9[C]....190
e. Periodic Communication Limitation 9[D]....191
f. Security Notification Limitation 9[E]....191
g. Device Disabling Limitation 9[F]....192
h. Copying User Data Limitation 9[G]....192
i. Memory Area Limitation 9[H]....193
5. Independent Claim 17....193
a. Preamble 17[pre]....193
b. Structural Limitation 17[A]....194
c. Security Application Limitation 17[B]....194
d. Registration Limitation 17[C]....195
e. Sending Identifying Information Limitation 17[D]....195
f. Periodic Communication Limitation 17[E]....196

g. Security Notification Limitation 17[F] 196
h. Device Disabling Limitation 17[G] 197
i. Copying User Data Limitation 17[H] 197
j. Memory Area Limitation 17[I] 198
6. Independent Claim 25 198
a. Preamble 25[pre] 198
b. Structural Limitation 25[A] 199
c. Registration Limitation 25[B] 199
d. Sending Identifying Information Limitation 25[C] 199
e. Security Notification Limitation 25[D] 200
f. Device Disabling Limitation 25[E] 200
g. Copying User Data Limitation 25[F] 201
h. Deleting User Data Limitation 25[G] 201
i. Restoring User Data Limitation 25[H] 202
j. Memory Area Limitation 25[I] 202
7. Dependent Claims 2, 10, 18 203
8. Dependent Claims 3, 11, 19 203
9. Dependent Claims 4, 12, 20 204
10. Dependent Claims 5, 16, 21 204
11. Dependent Claims 7, 15, 23 204
12. Dependent Claims 8, 16, 24 205
D. Ground 1D: Claims 6, 8, 14-16, and 22-25 Obvious over Andrews, Cotichini, and Hayward 205
1. Hayward (EX1008): UK Pat. App. No. GB2369205A 205
2. The Andrews-Cotichini-Hayward Combination 208
3. Independent Claims 25 211
a. Deleting User Data Limitation 25[G] 211
b. Restoring User Data Limitation 25[H] 211
4. Dependent Claims 6, 14, 22 212

5. Dependent Claims 7, 15, 23 215
6. Dependent Claims 8, 16, 24 215
VIII. Claim Listing 218

I, John Black, declare:

1. I have been retained by Faegre Drinker Biddle & Reath, counsel for Petitioner Microsoft Corp., to assess claims 1-25 (the "challenged claims") of U.S. Patent No. 8,506,649 ("the '649 patent"). I am being compensated for my time at my standard rate of $625 per hour, plus actual expenses. My compensation is not dependent in any way upon the outcome of the *inter partes* review of the '649 patent.

I. PERSONAL AND PROFESSIONAL BACKGROUND

2. My complete qualifications and professional experience are described in my curriculum vitae, a copy of which is provided as Exhibit 1004. The following is a brief summary of my relevant qualifications and professional experience.

3. My qualifications can be found in my Curriculum Vitae (filed herewith as EX1004), which includes my detailed employment background, professional experience, and list of technical publications and patents.

4. I am an Associate Professor of Computer Science at the University of Colorado, Boulder. I received a B.S. in Mathematics and Computer Science from the California State University at Hayward (now "California State University, East Bay") in 1988. I received an M.S. in Computer Science in 1997, and a Ph.D. in Computer Science in 2000, both from the University of California at Davis.

5. I have taught more than 60 classes in computer science, on subjects including data structures, algorithms, networking, operating systems, software engineering, security, cryptography, discrete mathematics, and quantum computing. I have authored or coauthored more than 20 publications, primarily on issues relating to computer security. I have been involved with computers for over 40 years in both commercial and academic capacities.

6. My earliest interest was in networks and security. My first memories in this regard were around 1975 when a group of friends and I learned about the telephone network and its security. A few years later, personal computers became available and I spent most of my free time studying, programming, and modifying them. I worked extensively with various networking products throughout the 1980s, and developed an interest in cryptography soon thereafter. Although my undergraduate institution had no courses in cryptography or security in the 1980s, I decided to pursue self-study at the time, and opted to double major in Computer Science and Mathematics because cryptography is a blend of these two subject areas.

7. After earning my B.S. degree in 1988, I worked for six years at Ingres Corp as a software developer, writing and reviewing code written in C. My work primarily was directed at transaction logging, data type support, and security.

8. In 1995, I began my Ph.D. at UC Davis under cryptographer Phillip Rogaway. My area of focus was cryptography and security and my research involved encryption, authentication, hash functions, and network security.

9. After graduation I took a position as an Assistant Professor at the University of Nevada at Reno. In the Fall of 2001, I taught the networking class there, which included coverage of Ethernet, interior gateway protocols, exterior gateway protocols, ARP, DHCP/BOOTP, IP, UDP, TCP, HTTP, SMTP and other protocols. In 2001, a graduate student and I looked at the security of ARP and invented a new protocol "AuthARP" to add security to the protocol.

10. In 2002, I moved to the University of Colorado at Boulder where I am currently employed. In the Fall of 2002, I co-designed and co-taught a new course called "Foundations of Computer and Network Security," which included descriptions of security issues around both wired and wireless security challenges, mostly for public-facing network services including the world-wide web. I have taught this class seven more times since then, including modern topics such as wireless networking, the Internet of Things, and so forth.

11. In my career at the University of Colorado, I have published several more papers in the area of cryptography and network security. I have taught more than 30 courses in network security and cryptography, and have graduated several PhD students in these areas.

12. I also have worked for a consulting company at times, writing software on contract basis. Although most projects are covered by NDAs, many involved networks and/or aspects of computer security.

13. In 2011, I began technical consulting for a local company called Cardinal Peak, which focuses primarily on video encoding and delivery systems. My work for Cardinal Peak has largely been directed to video encoding, transcoding, compression, encryption, and DRM, but also has included networking projects and embedded device work. For example, I designed the security system for the Pro1 smart thermostat, implemented the DRM for the Yonder Music App, worked on 802.1X code for smart dog collars, and helped design the cryptography used in Fitbit devices for wireless transfer of a Fitbit watch to a phone or laptop.

14. In 2016, I took a two-and-a-half year leave of absence from the University of Colorado to start a company named "SecureSet" in Denver, Colorado. The objective of SecureSet is to take reasonably proficient technical people and turn them into computer and network security specialists via five months of intensive training. SecureSet was sold to WeWork in 2019 and continues to offer computer security classes today. In 2018 I returned to my position at the University where I remain employed to the present day.

II. MATERIALS REVIEWED AND CONSIDERED

15. My findings, as explained below, are based on my years of education, research, experience, and background in the field of computer science, as well as my investigation and study of relevant materials for this declaration. When developing the opinions set forth in this declaration, I assumed the perspective of a person having ordinary skill in the art, as set forth in Section IV below. In forming my opinions, I have studied and considered the materials identified in the list below.

Exhibit	Description
1001	U.S. Patent No. 8,506,649 ("'649 patent")
1002	Prosecution History of U.S. Patent No. 8,506,649
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, *Security Analysis of the Palm Operating System and its Weaknesses Against Malicious Code Threats*, Proceedings of the 10th 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 5th ed.) (excerpts)
1016	Newton's Telecom Dictionary, CMP Books (2003 19th ed.) (excerpts)
1017	Webster's New World Computer Dictionary, Houghton Mifflin (2003 10th ed.) (excerpts)
1018	WIPO Pub. No. 1996/36194
1019	UK Pat. App. No. GB2349044A
1020	*Softex LLC v. Absolute Software Corp.*, *Softex LLC v. Dell Technologies Inc.*, *Softex LLC v. HP Inc.*, Joint Rule 26(f) Report and Discovery Plan
1021	Fact Sheet for Senior Judge David Alan Ezra
1022	*Digital cellular telecommunications system (Phase 2+); Mobile Stations (MS features)* (GSM 02.07), Version 5.1.0, July 1996
1023	*Digital cellular telecommunications system (Phase 2+); International Mobile station Equipment Identities (IMEI)* (GSM 02.16), Version 5.2.0, August 2000
1024	*Digital cellular telecommunications system (Phase 2+); Numbering, addressing and identification* (GSM 03.03), Version 5.0.0, March 1996
1025	United States District Courts – National Judicial Caseload Profile
1026	Andrei Khurshudov, *The Essential Guide to Computer Data Storage From Floppy to DVD*, Prentice Hall (2001) (excerpts)

III. MY UNDERSTANDING OF PATENT LAW

16. In developing my opinions, I discussed various relevant legal principles with Petitioner's attorneys. Though I do not purport to have prior knowledge of such principles, I understood them when they were explained to me and have relied upon such legal principles, as explained to me, in the course of

forming the opinions set forth in this declaration. My understanding in this respect is as follows:

17. I understand that "*inter partes* review" (IPR) is a proceeding before the United States Patent & Trademark Office for evaluating the patentability of an issued patent's claims based on prior-art patents and printed publications.

18. I understand that, in this proceeding, Petitioner has the burden of proving that the challenged claims of the '649 patent are unpatentable by a preponderance of the evidence. I understand that "preponderance of the evidence" means that a fact or conclusion is more likely true than not true.

19. I understand that, in IPR proceedings, claim terms in a patent are given their ordinary and customary meaning as understood by a person of ordinary skill in the art ("POSITA") in the context of the entire patent and the prosecution history pertaining to the patent. If the specification provides a special definition for a claim term that differs from the meaning the term would otherwise possess, the specification's special definition controls. I have applied these standards in preparing the opinions in this declaration.

20. I understand that determining whether a particular patent or printed publication constitutes prior art to a challenged patent claim may require determining the effective filing date (also known as the priority date) to which the challenged claim is entitled. I understand that for a patent claim to be entitled to

the benefit of the filing date of an earlier application to which the patent claims priority, the earlier application must have described the claimed invention in sufficient detail to convey with reasonable clarity to the POSITA that the inventor had possession of the claimed invention as of the earlier application's filing date. I understand that a disclosure that merely renders the claimed invention obvious is not sufficient written description for the claim to be entitled to the benefit of the filing date of the application containing that disclosure.

21. I understand that for an invention claimed in a patent to be patentable, it must be, among other things, new (novel—*i.e.*, not anticipated) and not obvious from the prior art. My understanding of these two legal standards is set forth below.

A. Anticipation

22. I understand that, for a patent claim to be "anticipated" by the prior art (and therefore not novel), each and every limitation of the claim must be found, expressly or inherently, in a single prior-art reference. I understand that a claim limitation is disclosed for the purpose of anticipation if a POSITA would have understood the reference to disclose the limitation based on inferences that a POSITA would reasonably be expected to draw from the explicit teachings in the reference when read in light of the POSITA's knowledge and experience.

23. I understand that a claim limitation is inherent in a prior art reference if that limitation is necessarily present when practicing the teachings of the reference, regardless of whether a person of ordinary skill recognized the presence of that limitation in the prior art.

B. Obviousness

24. I understand that a patent claim may be unpatentable if it would have been obvious in view of a single prior-art reference or a combination of prior-art references.

25. I understand that a patent claim is obvious if the differences between the subject matter of the claim and the prior art are such that the subject matter as a whole would have been obvious to a person of ordinary skill in the relevant field at the time the invention was made. Specifically, I understand that the obviousness question involves a consideration of:

i. the scope and content of the prior art;

ii. the differences between the prior art and the claims at issue;

iii. the knowledge of a person of ordinary skill in the pertinent art; and

iv. if present, objective factors indicative of non-obviousness, sometimes referred to as "secondary considerations." To my knowledge, the Patent Owner has not asserted any such secondary considerations with respect to the '649 patent.

26. I understand that in order for a claimed invention to be considered obvious, a POSITA must have had a reason for combining teachings from multiple prior-art references (or for altering a single prior-art reference, in the case of obviousness in view of a single reference) in the fashion proposed.

27. I further understand that in determining whether a prior-art reference would have been combined with other prior art or with other information within the knowledge of a POSITA, the following are examples of approaches and rationales that may be considered:

v. combining prior-art elements according to known methods to yield predictable results;

vi. simple substitution of one known element for another to obtain predictable results;

vii. use of a known technique to improve similar devices in the same way;

viii. applying a known technique to a known device ready for improvement to yield predictable results;

ix. applying a technique or approach that would have been "obvious to try," *i.e.*, choosing from a finite number of identified, predictable solutions, with a reasonable expectation of success.

x. known work in one field of endeavor may prompt variations of it for use in either the same field or a different one based on design

incentives or other market forces if the variations would have been predictable to one of ordinary skill in the art;

xi. some teaching, suggestion, or motivation in the prior art that would have led one of ordinary skill to modify the prior-art reference or to combine prior-art reference teachings to arrive at the claimed invention. I understand that this teaching, suggestion or motivation may come from a prior-art reference or from the knowledge or common sense of one of ordinary skill in the art.

28. I understand that for a single reference or a combination of references to render the claimed invention obvious, a POSITA must have been able to arrive at the claimed invention by altering or combining the applied references.

IV. PERSON OF ORDINARY SKILL IN THE ART ("POSITA")

A. Qualifications of a Person of Ordinary Skill in the Art

29. I have been informed and understand that for purposes of assessing whether prior-art references disclose every element of a patent claim (thus "anticipating" the claim) and/or would have rendered the claim obvious, the patent and the prior-art references must be assessed from the perspective of a person having ordinary skill in the art ("POSITA") to which the patent is related, based on the understanding of that person at the time of the patent claim's priority date. I have been informed and understand that a POSITA is presumed to be aware of all

pertinent prior art and the conventional wisdom in the art, and is a person of ordinary creativity. I have applied this standard throughout my declaration.

30. The ’649 patent involves technology in the field of electronic communications and systems and electronic device security systems. I have been asked to provide my opinions as to the state of the art in this field by 2003. I use this timeframe because the face of the ’649 patent indicates an earliest claimed priority date of the August 23, 2003 filing date of a provisional application. ’649 patent (EX1001), (60). Whenever I offer an opinion in this declaration about the knowledge of a POSITA, the manner in which a POSITA would have understood the claims of the ’649 patent or its description, the manner in which a POSITA would have understood the prior art, or what a POSITA would have been led to do based on the prior art, I am referencing this 2003 timeframe, even if I do not say so specifically in each case.

31. I understand that the Patent Owner may attempt to prove that the alleged invention recited in the challenged claims was conceived at some time prior to the earliest claimed priority date on the face of the patent. At the time of this declaration, I am unaware of the Patent Owner having alleged any earlier conception date or produced any evidence to establish any earlier conception date.

32. In my opinion, a person having ordinary skill in the art (“POSITA”) at the time of the alleged invention of the challenged claims 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 . Significantly more practical experience could also qualify one not having the aforementioned education as a person of ordinary skill in the art while, conversely, a higher level of education could offset a lesser amount of experience.

33. By 2003, I held a Ph.D. in Computer Science, and I was therefore a person of at least ordinary skill in the art at the time of the priority date of the '649 Patent. When developing the opinions set forth in this declaration, I assumed the perspective of a person having ordinary skill in the art, as set forth above.

B. Knowledge of a Person of Ordinary Skill in the Art

34. Around 1978 I bought my first computer. It was a TRS-80 Model I, with 4KB RAM and 4KB ROM. It also had a cassette tape unit for persistent storage (which rarely worked, in my experience: I would save files three times hoping maybe one of them might be successfully retrieved). Later, in the early 1980s, IBM launched the Personal Computer or "PC" running Microsoft MS-DOS. The model I owned, the 5150, had 8KB of ROM (for the BIOS) and 16KB of RAM, as well as 5.25" floppy disks for persistent storage of user data. By the 1990s, the types of memory that could be found in desktop or smaller devices, such as laptops and PDAs, continued to expand. In this technology background section

I will review the various types of memory one could find in consumer grade computers, focusing on the state of the art around the year 2003.[1] I will also review some of the ways in which user access was limited or restricted to various parts of the memories contained in these devices.

1. ROM (Read-Only Memory)

35. One of the oldest and most basic types of memory is the "ROM" which stands for "Read-Only Memory." A ROM is a memory chip that is installed in a computing device, including desktops, laptops, palm-tops, etc., usually on the main board (or "motherboard") of the computer, and usually at the time of manufacture. EX1026, at 8.

36. A ROM is a memory. EX1026, at 20 (identifying types and characteristics of ROM). Therefore the CPU of a computer can "address" this memory as part of the "address space" of the computer system. In other words, if a CPU attempts to read address 123 from memory, it will place the address "123" on the "address bus" of the computer system[2] and indicate that a "read" operation is

[1] In this field, some people use "storage" to refer to non-volatile memory storing computer programs and "memory" to refer to working memory where programs are executed. *See, e.g.,* EX1026, at 15-17. Others use "memory" to refer to both of these categories of storing computer information. In this declaration, I take the latter approach and use "memory" generally to refer to both categories of information storage.

[2] One can think of an "address bus" as a collection of wires from the CPU to the memory system; each wire can be set to a 1 or a 0, depending on its voltage level.

desired. If address 123 is an address where the ROM resides, the ROM will read the contents according to address 123 and remit the resulting value back on the "data bus" so the CPU can collect that value and use it. If instead the CPU attempts to *write* to value 123, it won't work: a ROM is read-only and attempts to write to any address within its address space will fail.

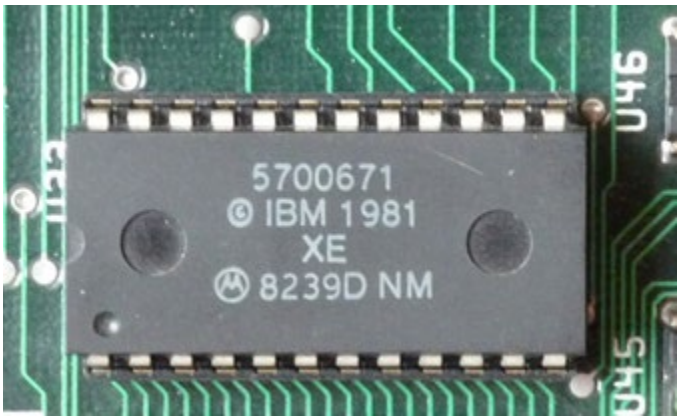
37. Technical dictionaries from 2002-2003 corroborate my opinions that ROM was non-volatile memory that could not be re-written. For example:

38. Newton's 2003 Telecom Dictionary defined ROM as "Computer memory which can only be read from. **New data cannot be entered** and the existing data is **non-volatile**. This means it stays there even when power is turned off. A ROM is a memory device which is programmed at the factory and whose contents thereafter **cannot be altered**. In contrast is the type of memory called RAM, whose contents can be altered." EX1016, at 5-6.

39. Microsoft's 2002 Computer Dictionary defined ROM as "Any semiconductor circuit serving as a memory that contains instructions or data that can be **read but not modified** (whether placed there by manufacturing or by a programming process, as in PROM and EPROM)." EX1015, at 12.

40. Webster's 2003 New World Computer Dictionary defined ROM as "The portion of a computer's primary storage that does not lose its contents when one switches off the power. ROM contains essential system programs that **neither**

the user nor the computer can erase. Because the computer's internal memory is blank at powerup, the computer can perform no functions unless given startup instructions. These instructions are stored in ROM. A growing trend is toward including substantial portions of the operating system on ROM chips instead of on disk." EX1017, at 4.



A ROM used in the 1981 IBM PC, depicted as installed in the motherboard[3]

41. In the original IBM PC, the maximum amount of RAM ("Random Access Memory", discussed below) at the time was 640KB. Therefore the ROM was mapped to the address space above the RAM in what was called "Upper Memory Area."

42. The primary purpose of the ROM in these early computer models was to hold the Basic Input-Output System or "BIOS." EX1026, at 11. The BIOS contained code that supported the Operating System's communication with various Input-Output facilities (or "I/O facilities") such as communication with the

[3] See https://www.minuszerodegrees.net/5150/bios/5150_bios_revisions.htm

keyboard or Direct Memory Access (DMA) controllers or interrupt processors. The BIOS also held the computer instructions that would be the first instructions run when the computer is turned on. EX1026, at 26. When a computer was first powered on (or first rebooted), the CPU would need to start somewhere to bring the computer into a normal functional state. This "somewhere" was a specific address within the ROM that contained the initial instructions. These instructions usually began with a Power-On Self Test (or "POST"), which ran various checks on the hardware before attempting to actually "boot" the system. For example, one of my early computers used to run a memory test on the RAM as part of the POST. Other tests might include testing peripherals or various components on the motherboard.

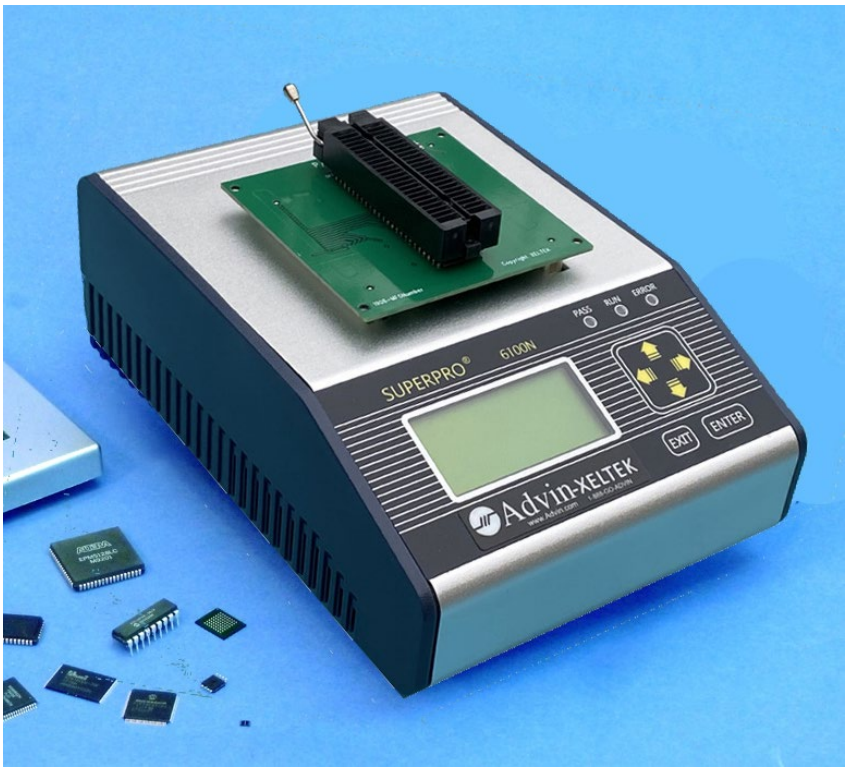
43. After the POST, the BIOS would run the "boot loader" which would initiate the boot process. EX1015, at 5. This was done in various ways on various computers, but typically the BIOS would read the Master Boot Record or "MBR" from the first disk drive on the computer. This MBR would be read into RAM, and the CPU would then proceed to run the computer instructions read from the MBR, which would in turn load the operating system.

44. On occasion a problem was found within the BIOS and users would want to update their BIOS to a later version or a repaired version of the BIOS. The ROM chip depicted above is seated in a "socket." Sockets made it easier for a

technician (or a tech-savvy computer owner) to swap one ROM for another: the technician would open the computer, use a plastic screwdriver to pry out the old ROM chip and then install the new chip by pressing it into the socket. This was (and remains today) a delicate procedure because a mistake could mean destroying not only the ROM, but other components on the motherboard.

45. A ROM, once manufactured, has fixed contents. It cannot be changed, overwritten, or have its contents altered. Therefore the only way to update its contents is to undertake the process described above. If the ROM is not socketed but instead soldered into the motherboard, changing the ROM becomes even more difficult and requires more skill on the part of the technician. If the computer's case cannot be opened in a non-destructive way (because, for example, the case is closed in a way that is not designed to ever be opened) then changing the ROM is essentially impossible: it cannot be electronically altered and it cannot be physically replaced.

46. Later versions of ROMs included PROMs (Programmable Read-Only Memories) that could be electronically written to one-time and would then become read-only. EX1015, at 14-15; EX1017, at 6-7; EX1026 at 19-20. The writing process took place in a special setting with a programming device used to conduct the initial write operation.



A PROM "universal programmer" device from Advin-XELTEK

47. After the PROM was mounted on the programming device and the data were written to the PROM, it would be removed and installed into a computer. After that no further writes would be possible and the only method of updating the PROM would be to program another chip and replace the first chip with it.

48. Next came the invention of the EPROM or "Erasable PROM." EX1015, at 13; EX1026, at 19-20. These chips were recognizable by the small window on the top of the chip; if ultraviolet light were shone into this window for a period of time (usually 20-30 minutes) it would erase the entire contents of the EPROM. Then a device like the one shown above would be used to write new contents into the EPROM.

An EPROM with the erasure window visible as a circle in the top center of the chip.

49. Again this process took place outside of the computer system the chip would ultimately reside in. To change the EPROM's contents (e.g., for a BIOS update), the technician would remove the EPROM from the computer system, place it under an ultraviolet lamp long enough to erase its contents, then reprogram the EPROM with new contents, and then finally re-install the EPROM into the computer. *See* EX1017, at 5; EX1026, at 19-20. When I was a teenager, I conducted these steps countless times in order to service the computers my father sold and maintained as part of his computer business.

50. The final step in this evolution relevant to the background here, is the EEPROM. This is an "Electronically Erasable Programmable Read-Only Memory" which can be erased in situ: in other words, there was no longer a need to physically remove the chip from the computer in order to erase its contents. EX1026, at 19-20. Additionally, individual bytes of the chip's memory could be erased and reprogrammed obviating the need to fully erase the entire chip's

contents and rewrite the entire memory each time (as was done with the EPROM). In some sense, the name EEPROM is misleading: it means essentially there is a memory chip that can be written to (via erasure and reprogramming) and yet is still called a "Read Only Memory." EX1015, at 7. A more familiar (and less confusing) name for this kind of memory is "flash." *See* EX1017, at 3.

2. Flash Memory

51. Flash memory is a specific type of EEPROM that was available by 2003 and indeed had become affordable enough to be used in consumer devices. Flash memory is readable and writeable and is still non-volatile (meaning that, like all ROMs discussed above, removing power would not result in data loss). *See* EX1015, at 6; EX1016, at 3; EX1017, at 3; EX1026, at 19-24.

52. Flash memory has the advantage of being fast, low power, compact and non-volatile, thereby serving as an alternative for conventional hard disk drives. The downsides are its minimum write area and the maximum number of writes before failure. Today flash memory is used in the form of so-called USB Drives, Thumb Drives, Flash drives and the like, which makes them a convenient method of moving files between computers or storing information on an external medium[4].

[4] Flash drives were commercially available in 2003, but not yet as widely used as they are today. Capacities and transfer rates have also gone up markedly in the last 20 years.

53. Solid State Drives ("SSD Drives") were manufactured using flash memory and deployed in various computers in place of a hard disk drive. In 2003, SSDs were relatively more expensive than conventional spinning hard disk drives of the same capacity, but SSDs were light weight, consumed less power, were more resilient to jarring and mechanical shocks (SSDs have no moving parts), and therefore much more appropriate as non-volatile storage in laptops and PDAs. Although there did exist very small conventional hard disks called "microdisks," flash memory was clearly the better choice for laptops and PDAs for the reasons stated above, in spite of their higher cost.

54. Finally, storing the BIOS in flash memory instead of in a conventional ROM meant that updates could be made to the BIOS and the BIOS could have configurable "settings" that a user could change.[5] *See* ; EX1026, at 27. One setting in the BIOS of a computer might be, for example, to indicate the "boot order:" perhaps the user wants to first attempt to boot from the CD-ROM and if that fails then the hard drive, etc.

3. Other Kinds of Memory

55. The class of non-volatile memories discussed above (ROM, PROM, EPROM, EEPROM and Flash) come in a "chip-based" form factor that either

[5] Prior to this the only low-level settings available to technicians were configured by turning DIP switches off or on (DIP switches are small hardware switches usually accessible only by opening the computer enclosure).

plugs into a socket or is soldered into a circuit. *See* EX1015, at 8 (defining non-volatile memory). These could in turn be part of a pluggable module such as a USB Flash drive, a security key, a console game cartridge, etc.

56. Another kind of chip-based memory is called Random Access Memory or "RAM." *See* EX1016, at 8-9; EX1026, at 3-4. This is high-speed high-density memory used during the runtime operation of the computer; RAM is both readable and writeable. RAM is "volatile memory" in the sense that when power is removed from the circuit containing the RAM, all contents in the memory are lost. RAM chips are commonly installed on the motherboard of a computer in sockets or in modules installed in motherboard sockets. If a computer cannot be opened, RAM cannot be added and if a computer already has all sockets filled with the highest-density RAM chips, no further RAM can be added. RAM is much faster than flash for reads and writes and therefore much more suitable for runtime use by programs. RAM is also not subject to the limitations of flash memory mentioned above: the minimum write is quite small and memory can be overwritten arbitrarily many times without any degradation to the underlying hardware.

A 2GB DDR2 RAM module circa 2002. The RAM chips themselves are soldered into the module, but the module itself can be plugged into the motherboard (and removed) by a technician using proper precautions. The reverse side of this module also has RAM chips mounted; this is therefore called a DIMM (Dual Inline Memory Module).

57. Regarding non-volatile memory, there are several other kinds of memory other than the chip-based memories discussed above. These can be either read-only or readable and writeable. An example of a read-only memory in this context would be a CD-ROM or DVD-ROM: these are optical media that are "burned" once with given contents and then no longer writeable thereafter. These media are suitable for distributing large amounts of data (such as a large database, software, movies, etc.) and require a special optical drive to be read. Many desktop computers in 2003 had such a drive, but it was relatively rare for smaller devices such as laptops or PDAs to support such a drive (which would normally have to be an external device connected to the computer through one of its interfaces; rarely some laptops did have integrated CD-ROM drives). CD-ROMs and DVD-ROMs had relatively low transfer speeds and high storage capacity.

58. For readable and writeable non-volatile memory there were several options. Tapes were used for long term archival (usually as a backup medium) and were slow high-density media that were impractical for random access given very

poor “seek times.” In other words, if the computer wanted to “jump around” to different locations on a tape, it would be impractically slow. CD-RW discs were like CD-ROMs but writeable (with very slow write times making them impractical to serve in place of hard drives). Floppy disks also used magnetic materials for read/write storage, but these disks supported random access and therefore were much more suitable for use by a computer wanting a practical secondary memory system. Floppy disks were designed to be removeable and came in different form factors including 8”, 5.25” and 3.5”.

The three most common sizes of floppy disks in use around 2003. The 8” and 5.25” disks have a visible slot where the read/write head of the disk drive would access the disk; the 3.5” disk had a sliding metal cover over this slot to better protect the disk against contamination, scratches or other damage that could corrupt the data on the disk.

59. A faster non-volatile read/write but non-removable magnetic storage system was known as a “hard disk.[6]” Like floppy disks, a hard disk storage system required that the magnetic medium had moving parts since the media had to spin

[6] The “hard disk” was so called because unlike the bendable mylar used in “floppy” disks, the hard disk used a rigid magnetic platter.

under the read/write head. Hard disk drives were built into computers and generally required a technician to replace or upgrade. Hard disk drives had higher capacities than floppy disks and were generally quite a bit faster and therefore usually would serve as the primary non-volatile storage means for many computers.

4. Computer Types and Memories Used

60. Desktop computers around 2003 commonly contained RAM, a ROM or Flash containing the BIOS, floppy drives and/or hard disk drives for long-term storage, and often a CD-ROM or DVD-ROM drive. Occasionally, they could contain an SSD drive instead of a hard drive, but SSD drives at the time were still more expensive for the same size hard disk drive, so this was uncommon.

61. Laptops around 2003 would contain RAM, a ROM or Flash containing the BIOS, and a hard disk drive. If a floppy drive were also available, it would be a 3.5" drive or it would be an external drive. SSD drives were becoming common instead of hard disk drives by 2003 due to the fact the price was low enough to appeal to consumers (in spite of still being higher than hard disk prices) and the advantages that SSD drives offered for laptops: lower power, lighter weight, and no moving parts that might be damaged from a jarring impact.

62. PDAs around 2003 would contain RAM, a ROM and/or Flash with startup code and operating system code. Given that PDAs were designed to be in

constant motion (i.e., in the hands or pockets of a human user) they usually had no moving parts. Although "microdrives" were designed for use as hard disks with moving parts that could be used in small form-factor computers, most PDA manufacturers preferred to use technology with no moving parts such as chip-based memories (RAM, ROM and Flash).

5. Restricting Access to Memory

63. There are two primary categories of techniques for restricting access to memory: hardware-based restrictions and software-based restrictions. A hardware-based restriction means that the hardware itself disables access to a memory system. For example, a ROM (or PROM or EPROM) is read-only and cannot be written to without physical alteration of the computer. This is a limitation imposed by the nature of the technology itself rather than a mechanism enforced by a piece of software. The only way to change what is stored in a computer's ROM would be to replace it with a different ROM altogether. In some cases, even replacing the ROM is not practical: for example, if the ROM is in a sealed case not designed to be opened.

64. Restricting access to other kinds of reprogrammable non-volatile memory (e.g., flash memory) is still possible, but because the memory is not physically resistant to modification like ROM, such protection must be accomplished via software-based restrictions. Since the memory itself is capable of

being written to, then denying write access requires that there be a software-based mechanism to enforce that denial. This kind of mechanism is often implemented by the operating system.

6. Disk Partitions

65. One example of a software-based mechanism is a disk partition. Some computer systems support the concept of "dividing up" or "partitioning" a secondary storage device (i.e., a hard disk or SSD) into pieces called "partitions."[7] Using special software, one could partition a disk into various non-overlapping subsets. EX1026 at 12.

66. In PC-type systems, the "partition table" would be stored in the MBR and record where each partition began and ended, along with the "partition type." A partition could be a "primary partition" meaning the computer could boot from it, or it could be an "extended partition." EX1026 at 12. Usually there could be at most one extended partition, but that partition could in turn be further subdivided into "logical partitions." In Linux systems, the user could create a "swap partition" used as a backup when RAM was full (Windows handled this differently). Windows and OS/2 had the concept of a "hidden partition" that would usually be used as a "recovery partition" in the event the operating system became corrupted

[7] The term used would depend on which system was being discussed, but the most common term was "partition."

and would not boot: a user could boot from the recovery partition and attempt to repair the system.

67. A "hidden partition" would not show up as a "logical drive" when using the operating system in a normal way. In Windows the main partition was usually assigned to a logical drive called "C:". Using file explorer, no contents within a hidden partition would appear under the folders contained on C:. Many systems allowed partitions (and any files stored therein) to be marked read-only. *See* EX1015, at 11; EX1017, at 4. This would prevent writes (i.e., changes) to the partition by users.

7. Controlled Software Environments

68. Certain devices tightly control access to memory by limiting the range of software that can be installed on the device and ensuring that no programs are available that get around access limits enforced by the operating system. When these systems work as intended, their software-based controls effectively transform a physically writable area of memory into "read-only" memory from the perspective of a user, much like the hardware-based restrictions discussed above.

69. To take a more recent and well-known example, consider the Apple iPhone[8]. The iPhone runs an operating system called iOS, and iOS strictly limits

[8] The iPhone did not exist in 2003, nor did any "smartphone" as we take the term to mean today. But I use it as an example here because most readers will be familiar with the device.

access to certain parts of its secondary memory (a flash drive). Apple further restricts the type of software or "apps" a user can install on her phone: all apps must be installed via the "App Store" and Apple strictly controls what software is available through the App Store. Apple does this for a variety of reasons, including ensuring that low-quality apps don't end up on user's phone, malicious apps are barred from download, apps that employ questionable practices (such as snooping or surreptitiously recording a user) are barred, but also so that apps that attempt to violate memory access restrictions are barred from download as well. Although some users in the past have found a way to "jailbreak" an iPhone and thereby install unauthorized apps, Apple responds quickly and vigorously to disable such jailbreaks and continue enforcing its rules to maintain a completely controlled operating system environment.

70. Taking another example that is perhaps less well-known but more relevant to the 2003 timeframe, Palm OS was another operating system that enforced access restrictions via the operating system and, provided someone could not overcome the security measures of Palm OS, strictly limited access to certain parts of memory. Palm OS was designed for Palm PDA devices and used flash memory for secondary storage; the Palm OS operating system was stored in flash, and the security of the device relied on a user's inability to modify portions of the flash, including the operating system itself. Occasionally, vulnerabilities were

discovered that allowed malicious users to circumvent these security measures, but to exploit these vulnerabilities generally required extraordinary measures and the use of tools outside of the Palm OS operating system. Additionally, OS designers took great efforts to eliminate any vulnerabilities as they were discovered, thereby returning the operating system code to being inaccessible to users, as intended. A pre-2003 example of this back-and-forth process (i.e., vulnerabilities being discovered and then being addressed by the OS designers) is illustrated in a 2001 paper titled *Security Analysis of the Palm Operating System and its Weaknesses Against Malicious Code Threats* (EX1010), which discusses hardware- and software-based recommendations to improve the protection of the Palm operating system and associated applications from tampering. For example, the paper discusses the need for "[s]ecurity processes…at the operating system level that are undetectable and inescapable," noting that if the flash memory is not "properly protected using the Software Protection and Boot-Block locking features provided by the Flash memory device, [the memory] can be altered." EX1010, 14-15.

8. Software-Based Controls with Privileged Access Permissions

71. While some software-based controls could only be circumvented—if at all—by users who identified unintended vulnerabilities, other software-based controls intentionally included paths for certain classes of users to gain access to protected areas of memory. Historically, the designers of PC-type operating

systems have often chosen to include such paths, presumably for commercial reasons. For instance, consumers who purchase a computing device will generally expect that, as the owners of that device, they should be granted permission to modify the device and/or its operating system as they see fit. Accordingly, to appease these consumers, designers of operating systems with software-based protections often chose to program their software to allow certain users (e.g., users with access privileges) permission to access and modify these areas but preventing other users from accessing and/or changing these protected areas of memory.

72. One example of a software-based mechanism that allowed workarounds for special classes of users was the Linux operating system around 2003: the Linux kernel[9] will mark certain areas of RAM as reserved for its own use; it will mark other areas as being used by a given program, and Program A is restricted from reading from or writing to the memory of Program B. This kind of restriction is enforced both for security reasons and to ensure that erroneous programs don't inadvertently corrupt the memory of other programs. In Linux, there are two main classes of user: a "normal" user and a "root" user. In Linux, the

[9] The "kernel" is the core of the operating system that has ultimate authority over all operations on the computer.

root user has effectively no limits to her authority, but normal users have a limited number of actions available to them, enforced by the Linux software.

73. In another example of a software-based mechanism, around 2003, Microsoft offered a number of operating systems including MS-DOS, various versions of Windows (including Windows 98, Windows 2000, Windows XP, Pocket PC 2002, Windows Mobile 2003, Windows Server 2003), and OS/2[10]. Each of these operating systems likewise made it possible for users to have an administrator-type account, which gave those users the ability to read and write to any memory on the machine.

V. THE '649 PATENT

74. The '649 patent discloses "[a] system and method for securing and tracking an electronic device." EX1001, Abstract. Specifically, the '649 patent concerns an "electronic device security and tracking system and method (ESTSM) that includes a plurality of hardware, software and firmware components that cooperate to allow tracking, disabling, and other interaction with the stolen electronic device." EX1001, 1:36-40.

75. The ESTSM generally includes two component types: an ESTSM-enabled client device and one or more ESTSM servers. In operation, the ESTSM-

[10] OS/2 was developed as a business-oriented operating system jointly with IBM and was seeing declining levels of use by 2003.

enabled client device (e.g., a computer or PDA) communicates via a network with the ESTSM server to achieve certain device-protections (i.e., ESTSM service(s)) to determine whether the user registered for ESTSM services and to perform tasks that secure and track the device. EX1001, 1:41-2:15. Communication between an **ESTSM device** with **ESTSM server** is illustrated in annotated Figure 56 below:

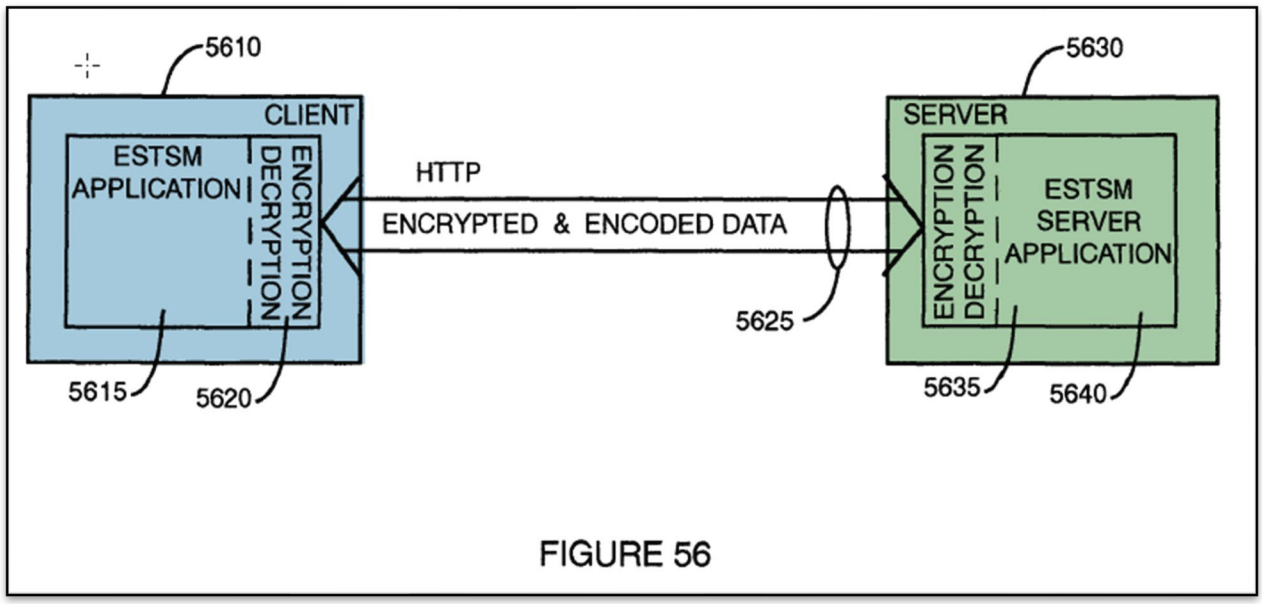


FIGURE 56

A. ESTSM Operation

76. The ESTSM device communicates with the ESTSM server over the Internet or through a message passing scheme, such as Short Messaging Service (SMS), Transmission Control Protocol/Internet Protocol (TCP/IP), or Multimedia Messaging Service (MMS). EX1001, 1:30-32, 10:45-53, 17:49-52, 19:18-22, 19:30-32, 20:1-4, 20:21-31, 23:29-33. The ESTSM server system may include

numerous servers, including web servers containing web pages and data. EX1001, 17:52-55, 19:23-26, 19:32-35, 20:4-7, 20:21-24.

1. Registration

77. To use the ESTSM services, a user must register the ESTSM device with the ESTSM security service. "If the electronic device is not registered for ESTSM services, then upon first time power-on and connection to the ESTSM server of the electronic device that includes ESTSM software and firmware, the user is prompted to register for different ESTSM services." EX1001, 1:48-52. A user also may register the device later by "selecting a menu option for registration or selecting an icon on the electronic device's desktop, or via World Wide Web pages from a remote system other than that ESTSM device itself." EX1001, 1:52-57, 8:2-7, 11:10-13.

78. During registration, "[a] user creates an account with ESTSM, specifies what ESTSM services he wishes to purchase, and provides user and billing information to complete the registration." EX1001, 7:18-22, 8:7-56. During registration of a mobile device, the user may provide "the mobile phone number, service provider, International Mobile Equipment Identifier (IMEI) number, and a phone description." EX1001, 32:33-38.

79. The **operations** for registration are highlighted in the annotated Figure 55 below.

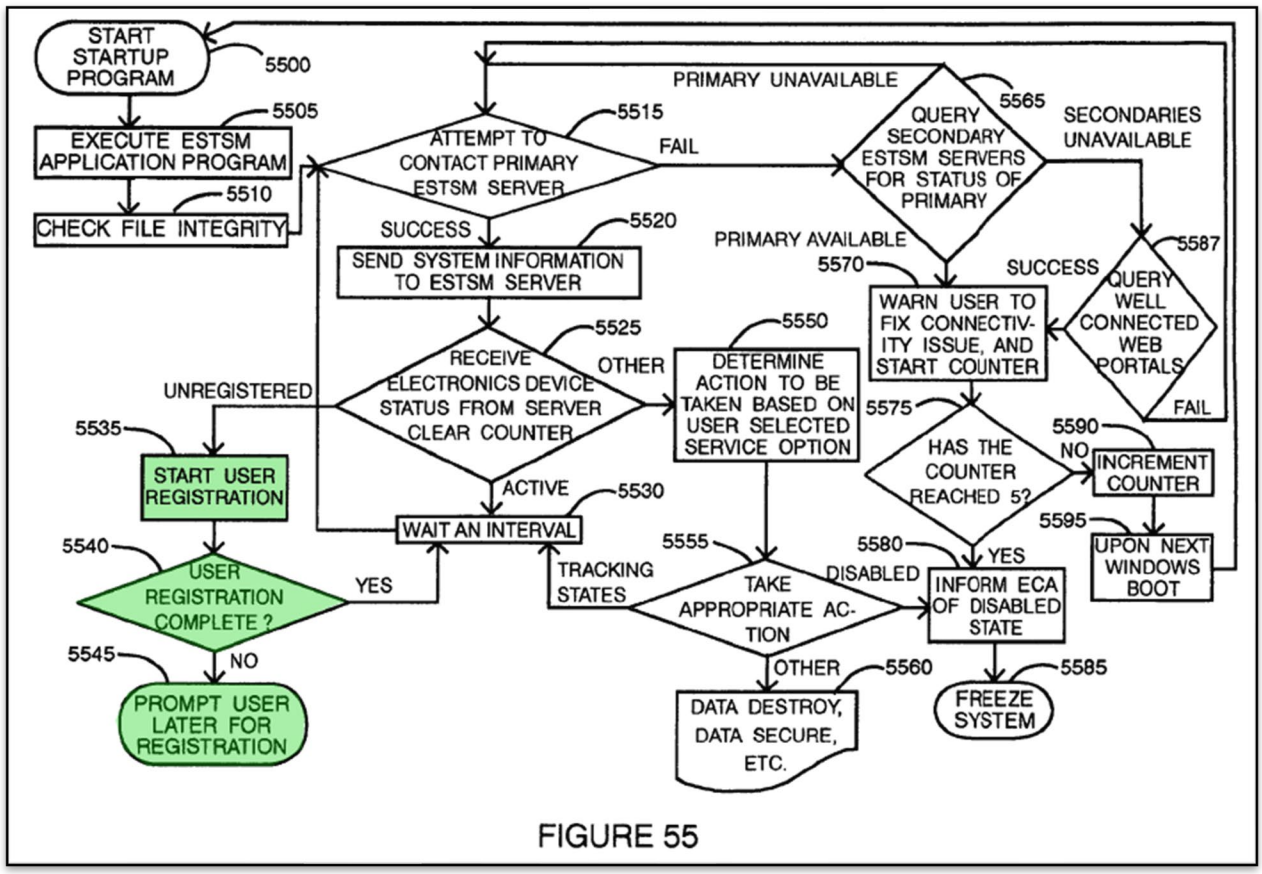


FIGURE 55

2. Device-Server Communication

80. Once registration is complete, the ESTSM device "periodically check[s]" with the ESTSM server over the Internet to determine whether the device has been reported stolen. EX1001, 26:11-17, *see also* 7:31-33, 26:11-17, 26:57-61, 60:60-63. "[T]he user can report the device as stolen" through the ESTSM system. EX1001, 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. For example, "the user may click on the button labeled 'Report Stolen' to start the process" at the ESTSM server. EX1001, 10:27-37, 2:31-37, 10:33-37. The ESTSM application contacts the primary

ESTSM server via the Internet. It sends an encrypted query that identifies the device by its system information, and, in response, it receives the device status with one or more command ("Cmd") to be performed by the ESTSM device. EX1001, 26:39-53. The application then "wait[s] an interval and again contact[s] the ESTSM server." EX1001, 26:61-63.

81. The ESTSM device can also send the server updated mobile device information. For example, the ESTSM application detects if any user information has been updated. EX1001, 33:60-66. If there is updated information, the ESTSM application notifies the ESTSM server of that new information and determines the current state of the mobile device. EX1001, 33:66-34:3. The application then waits for a message from the ESTSM server, which may be encrypted and encoded. EX1001, 34:3-6.

82. The **operations** for periodically establishing device-server contact—including the **operation for sending system information**—are highlighted in the annotated Figure 55 below.

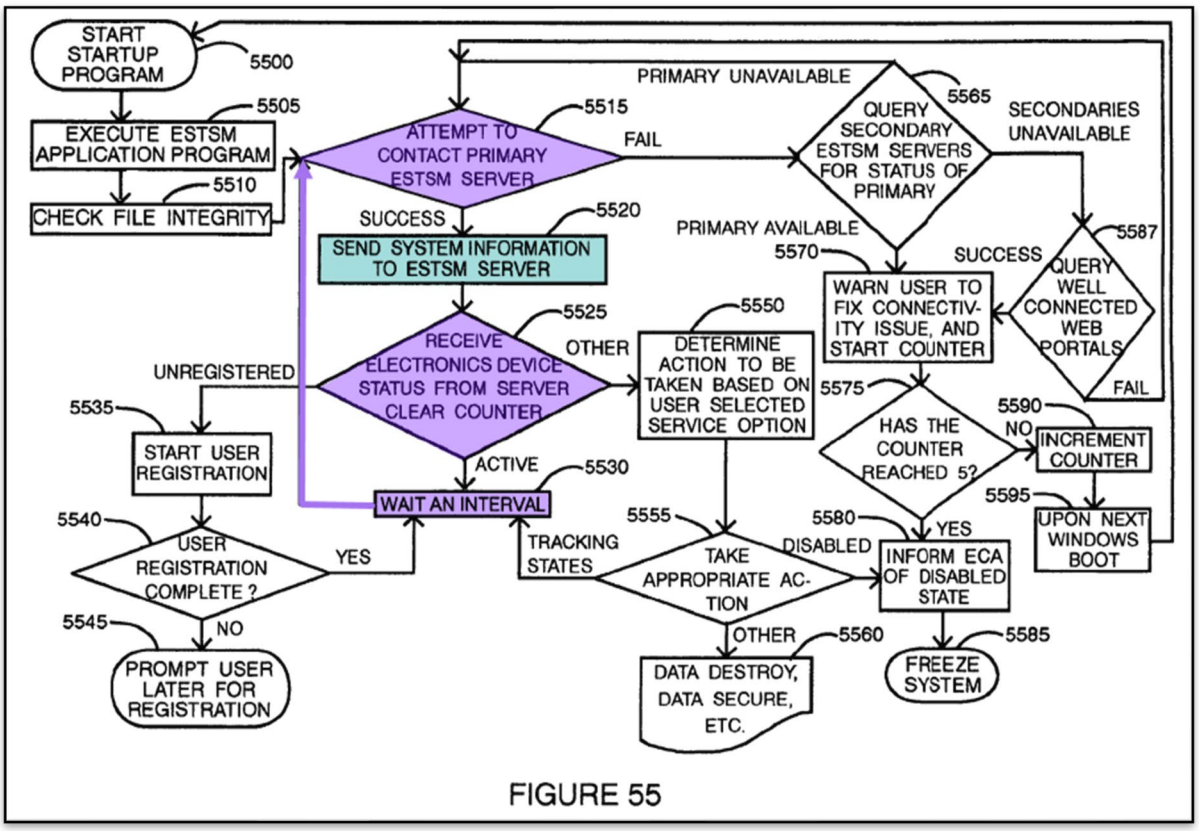


FIGURE 55

3. Security Notifications and Responses

83. "[I]f the application component [of the client device] detects that a new message has arrived [from the ESTSM server], message data is processed in block 7145." EX1001, 34:7-9; Fig. 71. Then, "[a] command is extracted from the message data in block 7160 . . . and is stored into the variable Cmd." EX1001, 34:9-10.

84. There are multiple potential commands that could be part of the message:

a. Register

85. "If the Cmd is 'REGISTER' as shown in block 7165, then the user has registered the mobile device for ESTSM services" and "[t]he ESTSM server is notified to change the mobile device state to 'ACTIVE' in block 7187 and the application component sets the current state to 'ACTIVE' in block 7185." EX1001, 34:11-15.

86. The user also may report the device as stolen or lost utilizing the ESTSM website. The user will log into the ESTSM website and report the device as stolen. EX1001, 7:25-27, 10:10-14, 10:29-32, 13:10-12, 15:61-63. "The user fills out the information on the web page to generate a theft incident report and the ESTSM site will log this report so that it may be given later to the appropriate authorities as proof of filing the theft incident report." EX1001, 10:33-37.

87. "If the device has been reported stolen, the application component along with the ESTSM server computer system will determine what services the user has registered for and will take the appropriate action (e.g. disable the device, communicate identifying information to the server, erase the storage device, recover data, encrypt data, etc.)." EX1001, 2:31-37; *see also* EX1001, 7:33-39, 17:55-61, 26:63-67.

b. Disable

88. "The ESTSM server may send a 'DISABLE' command 7170 if the mobile device is reported stolen or the user information module that may be a [Subscriber Identity Module] SIM card has been changed and the device identifier has not changed in the mobile device." EX1001, 34:18-22. If such a command is sent, "the mobile device is disabled 7192 and the application component sets the current state to 'DISABLE' in block 7190." EX1001, 34:15-18.

89. Once the device is put in the DISABLED state, "[t]he system is now in the locked state and can not be used," and "[i]f the system is recovered by the user, they will need to obtain the activation password to re-enable access to the electronic device." EX1001, 13:35-39. "The Application component of the electronic device disables the device 4045 and informs the ESTSM server computer system that the electronic device is in a disabled state 4050." EX1001, 15:35-38. "If the user has selected the disable electronic service, then the ESTSM application program will inform the ECA of electronic device disabled state 5580 and freeze the electronic device 5585," and "[t]he electronic device executing the ESTSM application program will send an encrypted message to the ESTSM server periodically while the system is connected to the Internet." EX1001, 26:67-27:6. If the electronic device is a mobile device, "[t]he ESTSM server may disable the mobile device . . . if the Subscriber Identity Module (SIM) card has been changed

and the device is reported stolen," "if the IMEI number has been changed and the device is reported stolen," or "[i]f the application component is not able to get the device identifier in block 7110." EX1001, 33:35-40, 33:47-50.

90. The **operations for disabling the device** based on the status response from the ESTSM are highlighted in the annotated Figures 55 and 71 below.

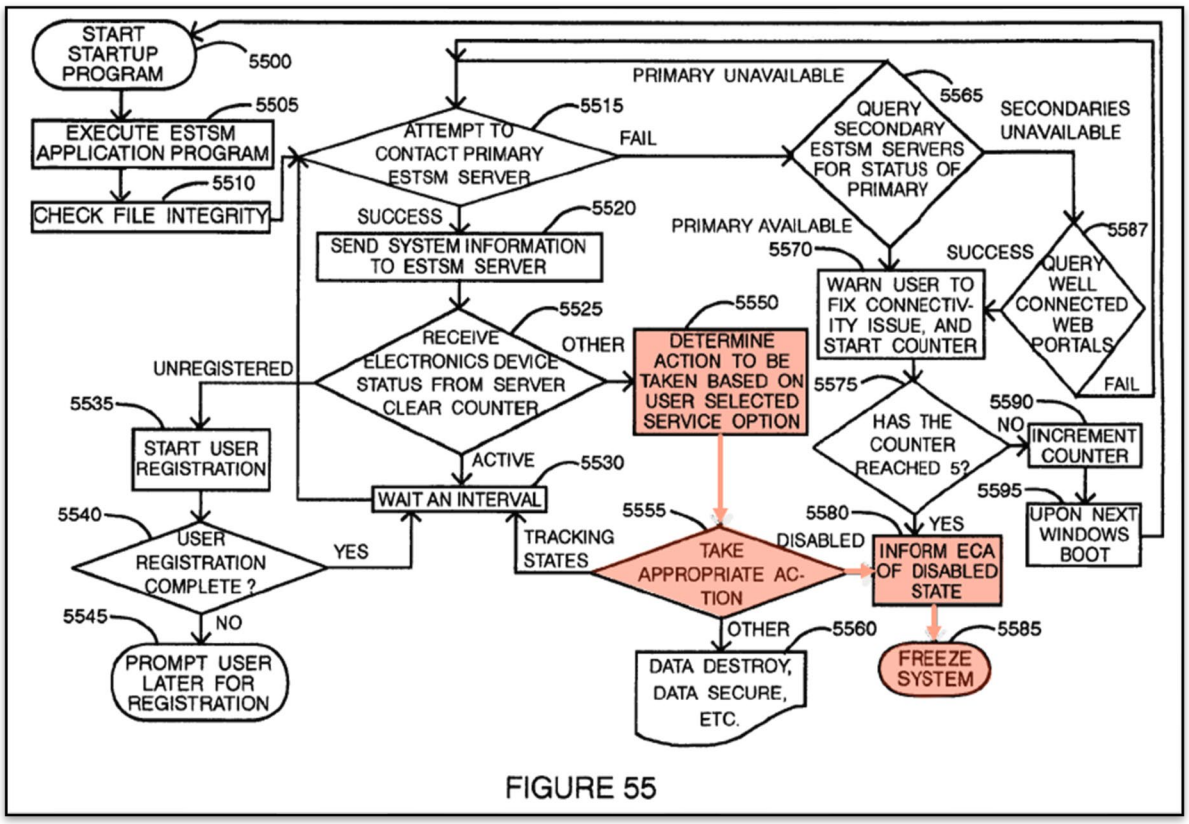


FIGURE 55

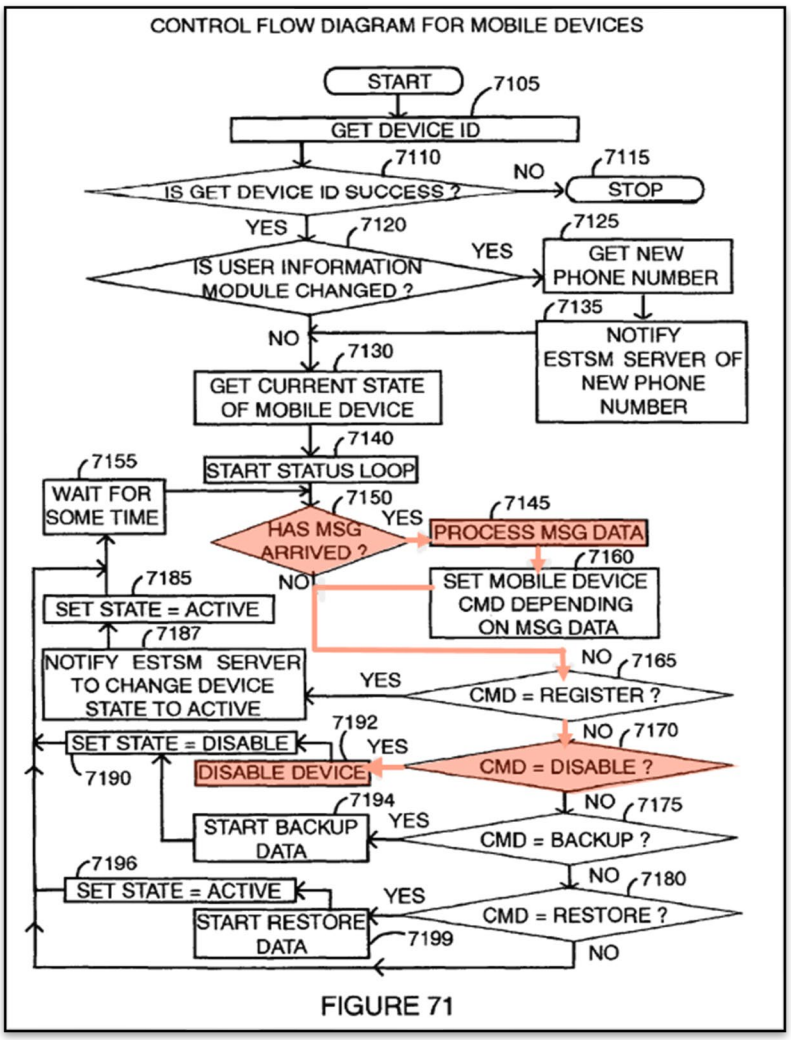


FIGURE 71

c. Backup

91. "If the Cmd is 'BACKUP' as shown in block 7175, the ESTSM server requests that the data on the mobile device be copied to the ESTSM server," "the ESTSM server begins to backup the data stored on the mobile device . . . requested [to be backed up] by the user during registration for the mobile device." EX1001, 34:22-28. "Thus, if during ESTSM registration the user had selected recovery of contacts and calendar data, these items will be backed-up." EX1001, 34:28-30.

92. Regarding the backup and recovery of data, "the ESTSM server computer system may inform the mobile device that it has been reported stolen and backup the data on the device" or "the ESTSM server may periodically back up the data on the device even if the mobile device has not been reported stolen." EX1001, 33:28-34; *see also* 34:57-60. "If the user during registration had selected the data recovery service, the mobile device is placed into 'BACKUP IN PROGRESS' state 7235 and data on the mobile device is backed-up to the ESTSM server." EX1001, 35:16-19. If that is successful, "the mobile device is placed into 'DISABLED DATA BACKUP' state 7240, data on the device is deleted, and the mobile device is disabled." EX1001, 35;19-22.

93. The **operations for backing up user data** based on the status response from the ESTSM are highlighted in the annotated Figures 55 and 71 below.

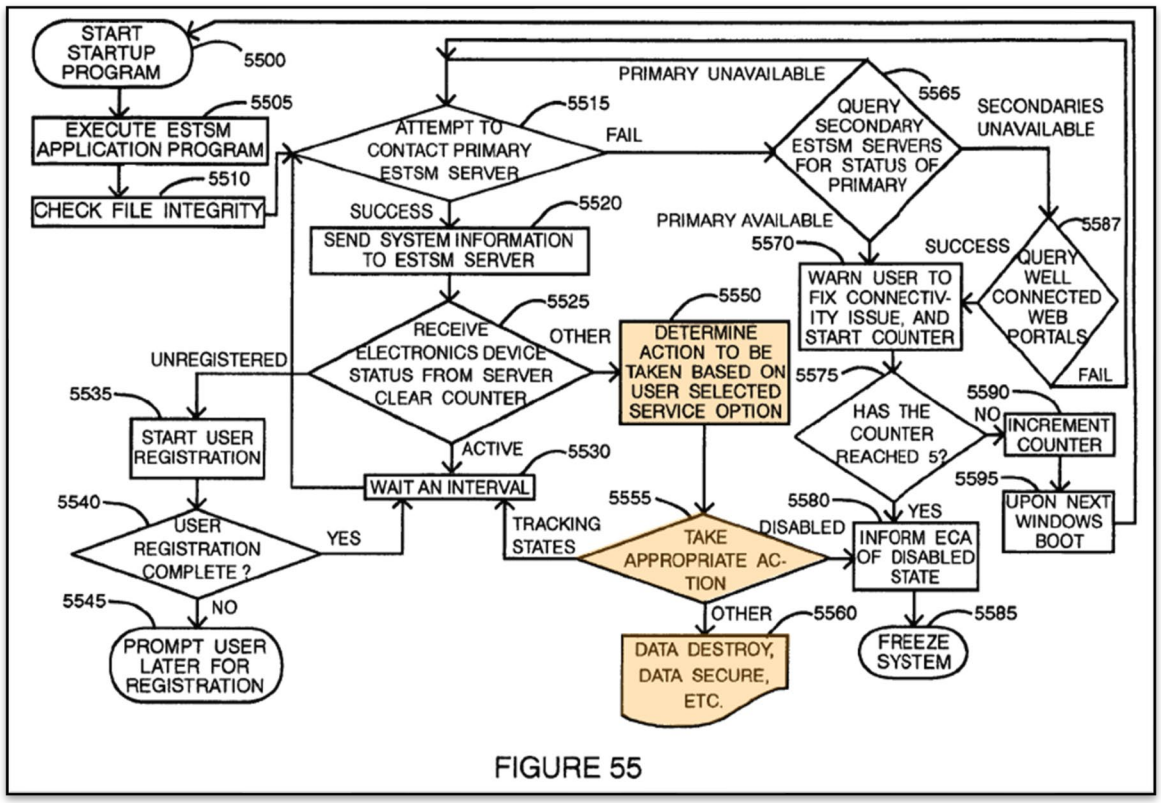

START STARTUP PROGRAM
5500
EXECUTE ESTSM APPLICATION PROGRAM
5505
CHECK FILE INTEGRITY
5510
ATTEMPT TO CONTACT PRIMARY ESTSM SERVER
5515
FAIL
PRIMARY UNAVAILABLE
QUERY SECONDARY ESTSM SERVERS FOR STATUS OF PRIMARY
5565
SECONDARIES UNAVAILABLE
SUCCESS
SEND SYSTEM INFORMATION TO ESTSM SERVER
5520
PRIMARY AVAILABLE
5570
WARN USER TO FIX CONNECTIVITY ISSUE, AND START COUNTER
SUCCESS
QUERY WELL CONNECTED WEB PORTALS
5587
FAIL
RECEIVE ELECTRONICS DEVICE STATUS FROM SERVER CLEAR COUNTER
5525
OTHER
DETERMINE ACTION TO BE TAKEN BASED ON USER SELECTED SERVICE OPTION
5550
UNREGISTERED
5535
START USER REGISTRATION
ACTIVE
WAIT AN INTERVAL
5530
HAS THE COUNTER REACHED 5?
5575
NO
INCREMENT COUNTER
5590
5595
UPON NEXT WINDOWS BOOT
5540
USER REGISTRATION COMPLETE ?
YES
NO
5545
PROMPT USER LATER FOR REGISTRATION
TRACKING STATES
5555
TAKE APPROPRIATE ACTION
DISABLED
5580
YES
INFORM ECA OF DISABLED STATE
OTHER
5560
DATA DESTROY, DATA SECURE, ETC.
FREEZE SYSTEM
5585

FIGURE 55

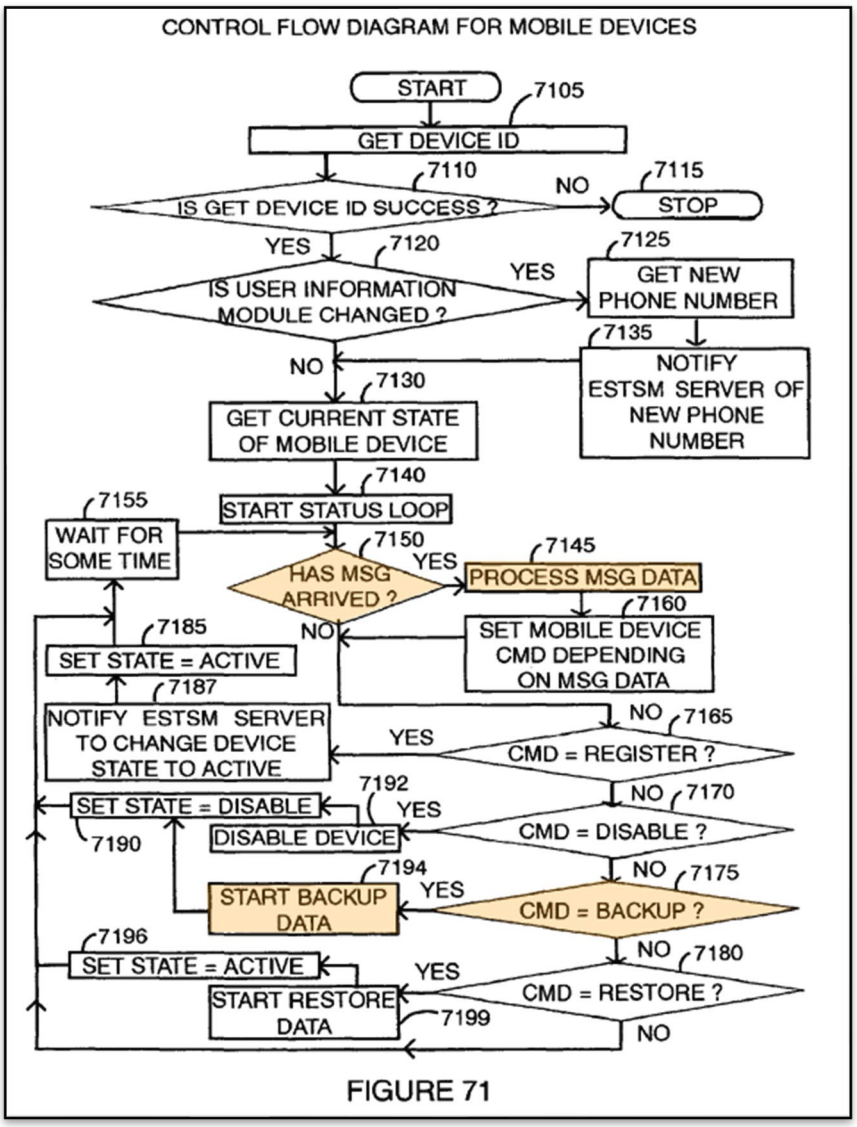


FIGURE 71

d. Delete

94. If the status is "ERASE HARDDISK," "the user selected 'Data Destroy Services' option when registering with the ESTSM." EX1001, 14:21-23. In this state, "the Application component on the electronic device erases the hard disk drive." EX1001, 16:2-5.

95. The **operations for deleting user data** based on the status response from the ESTSM are highlighted in the annotated Figure 55 below.

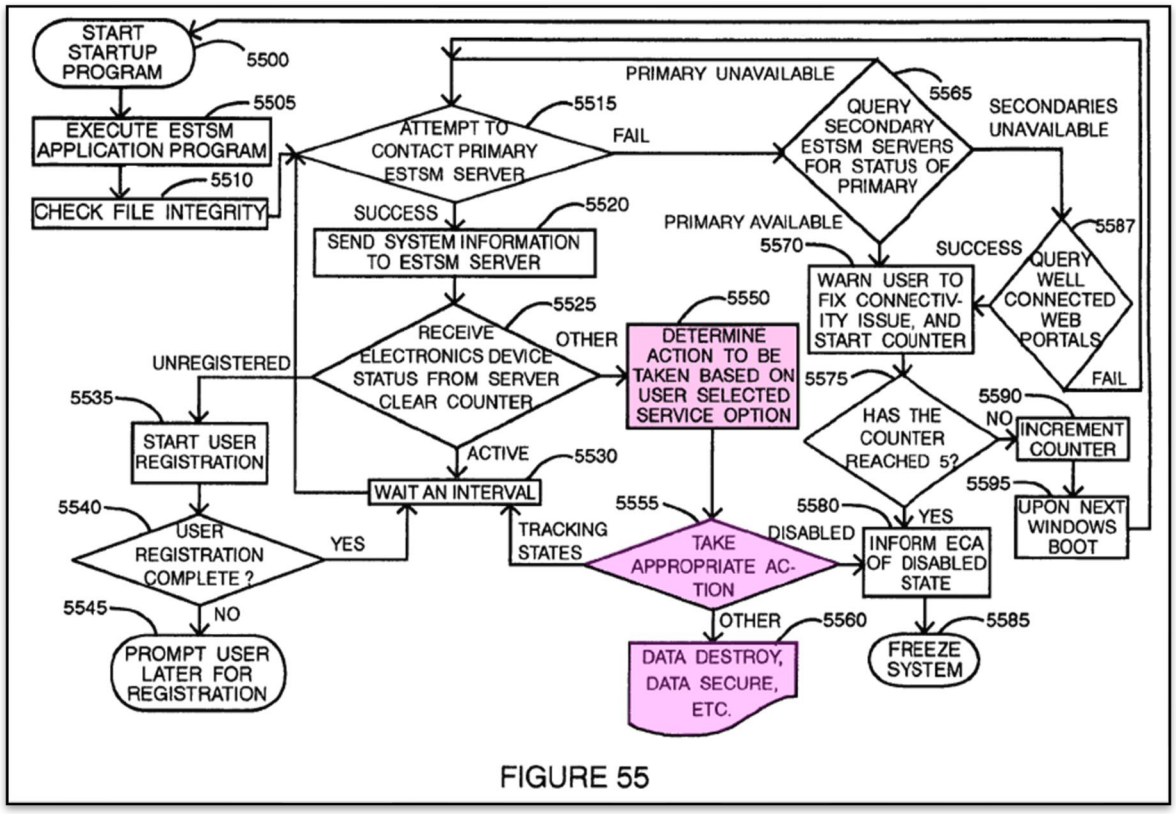


FIGURE 55

e. Restore

96. "If the Cmd is 'RESTORE' as shown in block 7180, 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," and once that is complete, "the ESTSM server places the mobile device into an active state" and "[t]he application component in the mobile device sets the current state to 'ACTIVE' in block 7196 and waits for some time 7155 before starting the status loop 7140." EX1001, 34:37-46.

97. “Once the mobile device has been recovered or the user has purchased a new mobile device and the user re-enables the device using the ESTSM website, an SMS message is sent from the server to the mobile device placing the device into an ‘ENABLE AFTER RECOVERY’ state 7245,” and “[t]he mobile device sends an SMS confirmation message to the ESTSM server indicating that it has received the re-enablement SMS message from the ESTSM server.” EX1001, 35:27-34. The device is then activated and “[t]he data that has been backed-up into the ESTSM server is restored into the new or re-enabled mobile device.” EX1001, 35:34-39.

98. The **operations for restoring user data to the device** based on the status response from the ESTSM are highlighted in the annotated Figures 55 and 71 below.

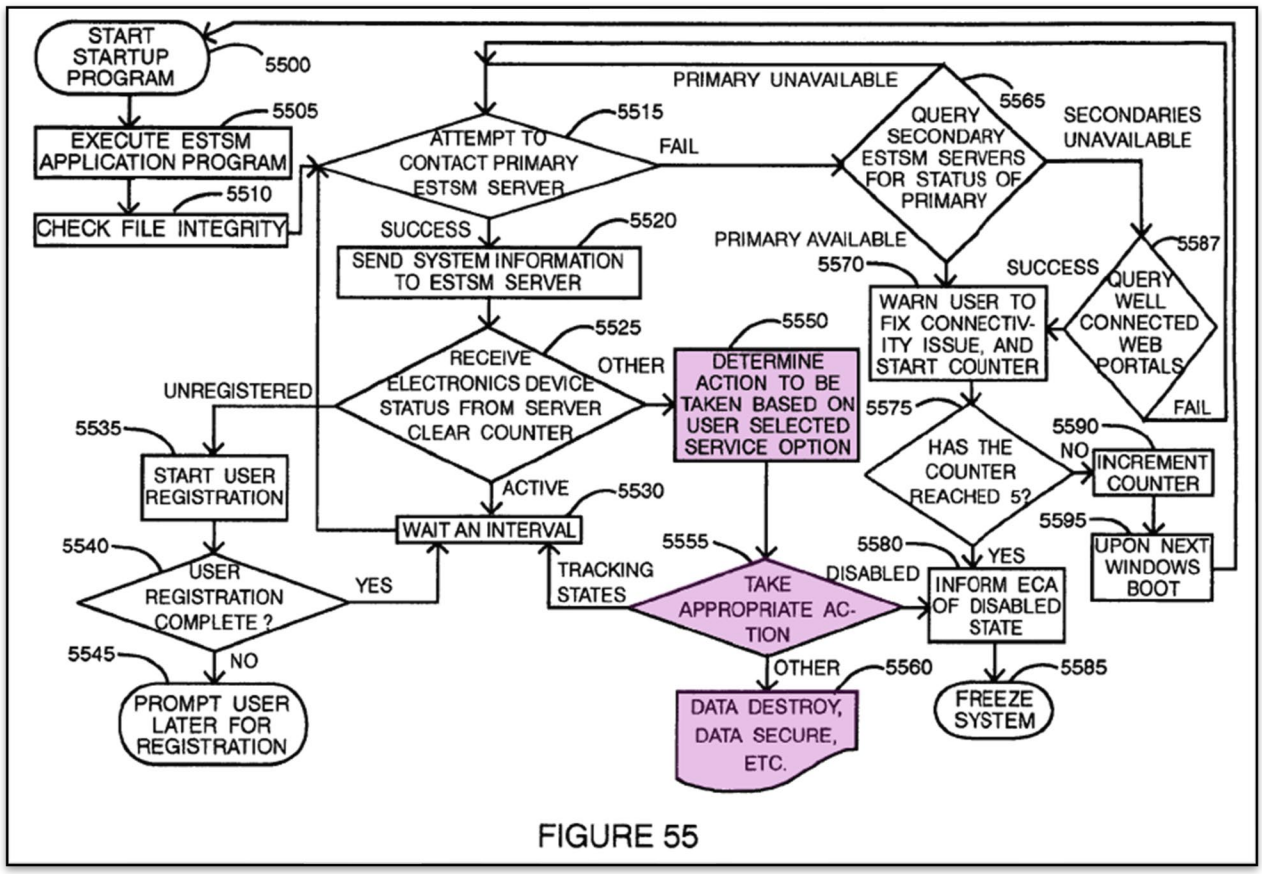

START STARTUP PROGRAM
5500
EXECUTE ESTSM APPLICATION PROGRAM
5505
CHECK FILE INTEGRITY
5510
ATTEMPT TO CONTACT PRIMARY ESTSM SERVER
5515
FAIL
PRIMARY UNAVAILABLE
QUERY SECONDARY ESTSM SERVERS FOR STATUS OF PRIMARY
5565
SECONDARIES UNAVAILABLE
SUCCESS
SEND SYSTEM INFORMATION TO ESTSM SERVER
5520
PRIMARY AVAILABLE
5570
WARN USER TO FIX CONNECTIVITY ISSUE, AND START COUNTER
SUCCESS
QUERY WELL CONNECTED WEB PORTALS
5587
FAIL
RECEIVE ELECTRONICS DEVICE STATUS FROM SERVER CLEAR COUNTER
5525
OTHER
DETERMINE ACTION TO BE TAKEN BASED ON USER SELECTED SERVICE OPTION
5550
UNREGISTERED
5535
START USER REGISTRATION
ACTIVE
5530
WAIT AN INTERVAL
5575
HAS THE COUNTER REACHED 5?
NO
5590
INCREMENT COUNTER
5595
UPON NEXT WINDOWS BOOT
5540
USER REGISTRATION COMPLETE ?
YES
TRACKING STATES
5555
TAKE APPROPRIATE ACTION
DISABLED
5580
YES
INFORM ECA OF DISABLED STATE
5545
NO
PROMPT USER LATER FOR REGISTRATION
OTHER
5560
DATA DESTROY, DATA SECURE, ETC.
5585
FREEZE SYSTEM

FIGURE 55

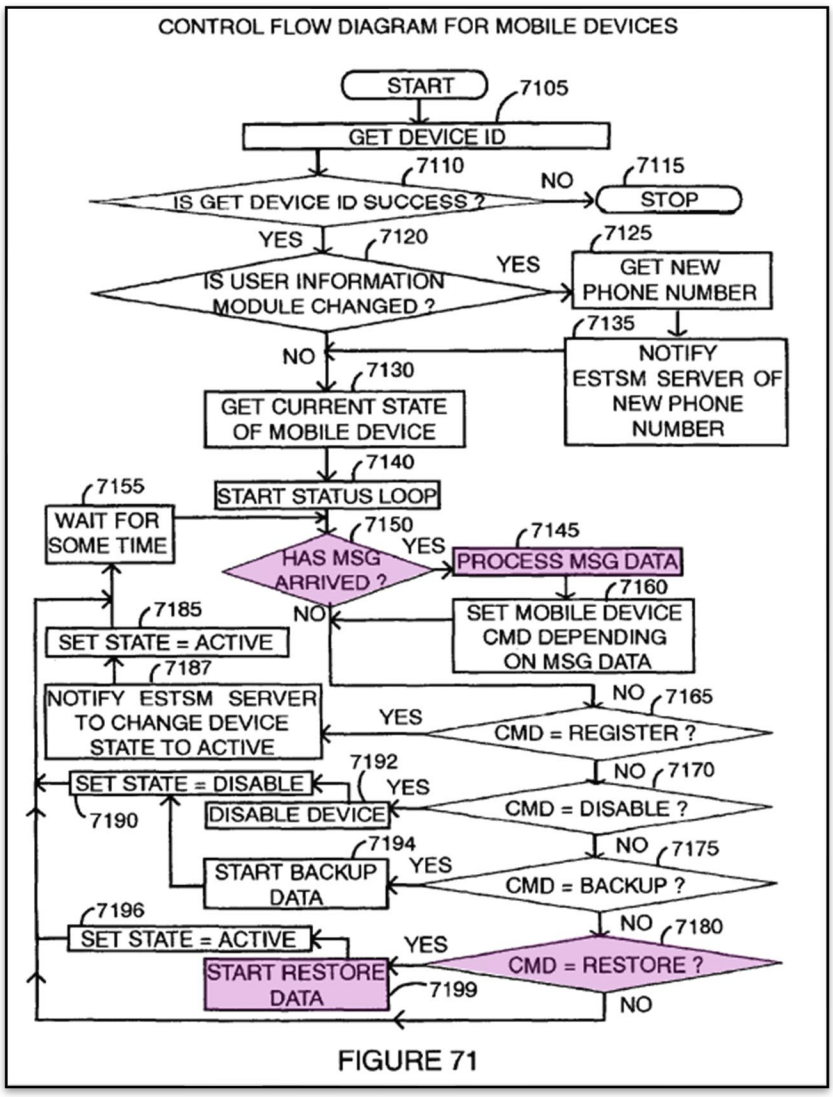


FIGURE 71

B. Memory Access Restrictions for Security Application

99. The ESTSM electronic device includes processing components and various types of memory. The device can be, for example, a "PDA" or "mobile phone that in some embodiments may be a cell phone, or Smart Phone" and that "may include a Flash memory 4500." 19:8-12. The device can further include "a central processing unit (CPU) 4902 coupled to a main memory array 4906 and to a variety of other peripheral computer system components[.]" 20:37-40. "The main

memory 4906 functions as the working memory for the CPU 4902 and generally includes a conventional memory device or array of memory devices in which program instructions and data are stored such as a volatile memory that runs programs and a non-volatile memory such as Read-Only Memory (ROM) or flash memory. The main memory array may comprise any suitable type of memory such as dynamic random access memory (DRAM) or any of the various types of DRAM devices…" 20:56-62. The device may further include a "BIOS ROM" which typically is a 'nonvolatile' memory device, which means that the memory contents remain intact even when the computer 4900 powers down. By contrast, the contents of the main memory 4906 typically are 'volatile' and thus are lost when the computer shuts down." 22:9-18.

100. The '649 patent teaches that the security application is maintained in a "secured environment" on the client device so that a "simple low level format of the hard disk drive" will not allow a user to "remove the application and bypass the security features." Abstract. To create this "secured environment" for the security application, the '649 patent discloses several techniques for protecting the application from tampering. In an example, the '649 describes storing the security application at least partially in a "system area" that "is not changeable by the user of the electronic device." 3:44-49. The system area may be a "flash memory" that "contain[s] ESTSM application programs," may be "non-viewable," and may be

"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* 18:13-41, 21, 55-59, 25:15-38, 31:29-43. The ESTSM may also utilize a "secure nonvolatile area that stores critical information present after electronic device power-off and accessible during electronic device power-on and boot." 2:61-66. This secure nonvolatile area may store a "small piece of code that resides in the system BIOS ROM image located in a secure nonvolatile area 4465." 17:62-64; *see also* 18:3-12. "The BIOS ROM 4494 is a memory device that stores commands which instruct the computer how to perform basic functions such as sending video data to the display or accessing data on hard floppy disk drives." 21:61-65. "The BIOS instructions also enable to load the operating system software system program into main memory during system initialization and transfer control to the operating system so the operating system can start executing[.]" 22:2-6. The '649 patent explains that these techniques "ensure[] that a thief cannot bypass or circumvent the ESTSM application from running." 2:66-3:5; *see also* 25:62-66 (ESTSM application is resilient even "if the thief deletes or tampers with ESTSM files, loads an application or service to try to bypass ESTSM operation, or in any other way tries to prevent ESTSM from running.").

C. Prosecution History of the ’649 Patent

101. The application that became the ’649 patent was filed on July 11, 2006 though it purports to claim priority to a provisional application No. 60/497,182, filed on August 23, 2003. EX1001, (60). I have not been asked to determine whether provisional application No. 60/497,182 contains written description support for the challenged claims of the ’649 patent and, instead, have been asked to assume for purposes of this declaration only, that the challenged claims are entitled to a priority date of August 23, 2003. However, none of my opinions in this declaration would be affected by the priority date of the ’649 patent being July 11, 2006 instead of the assumed date of August 23, 2003.

102. I have reviewed the prosecution history of the ’649 patent (EX1002). The as-filed application included 52 claims. EX1002, 61-68. After an initial rejection, those 52 claims were canceled and replaced with 27 new claims. EX1002, 326-336. Independent claim 53 became the first independent claim and recited, *inter alia*, an “electronic device” storing a “security application” operable to perform a series of operations including “enabling an owner…to register the mobile electronic device a security service,” “causing the mobile electronic device to automatically send identifying information for the mobile electronic device to the security service,” “accepting a theft report at the mobile electronic device from the security service,” and “in response to receiving the theft report, automatically

disabling at least one user function." EX1002, 326. The other independent claims recited similar limitations.

103. Prior to allowance, the applicant faced several rejections under §§101, 102, and 103. EX1002, 365, 461, 508. In one of these office actions, the examiner rejected then-pending independent Claim 53 for being anticipated by Komsi (2004/0110488, EX1013). EX1002, 465. The examiner stated that Komsi disclosed all limitations of the then-pending claim, which I've reproduced below:

> A mobile electronic device, comprising:
> a processor;
> one or more machine-readable storage media responsive to the processor; and
> a security application in at least one of the machine-readable storage media, wherein the
> security application is operable to perform operations comprising:
> 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;
> after the owner has registered the mobile electronic device with the security service, causing the mobile electronic device to automatically send identifying information for the mobile electronic device to the security service;
> after the owner has registered the mobile electronic device with the security service, accepting a theft report at the mobile electronic device from the security service, wherein the theft report comprises a message indicating that the owner of the mobile electronic device has reported a loss of the mobile electronic device; and
> in response to receiving the theft report, automatically disabling at least one user function of the mobile electronic device while still allowing the

security application in the mobile electronic device to communicate with the security service; and

wherein the mobile electronic device comprises a mobile phone; and

wherein the operation of automatically disabling at least one user function of the mobile electronic device comprises preventing a person from using the mobile phone for calls, while allowing the security application in the mobile phone to communicate with one or more servers.

EX1002, 392.

104. In response, the applicant amended Claim 53, to recite the following limitations:

wherein the one or more non-transitory machine-readable storage media comprises nonvolatile memory;

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 resides at least partially in the system area; and wherein the security application receives the theft report from at least one of the servers via the system area.

EX1002, 487-488.

105. In the remarks accompanying this amendment, the applicant argued that the newly added limitations were not disclosed by Komsi because Komsi "does not mention anything remotely pertaining to a system area that cannot be modified by a user." EX1002, 498.

106. In the subsequent office action, the examiner rejected the claims over Komsi 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.

107. The applicant responded to this §103 rejection by amending Claim 53 to recite "*causing the mobile electronic device to periodically communicate with the security service*" and argued that neither Komsi nor Hasebe disclosed such periodic communication with a security service. 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 Komsi's lost-device system with Hasebe's program in ROM. EX1002, 546-550.

108. The applicant received a notice of allowance only after an Examiner's Amendment in which Claim 53 was amended to recite limitations to those previously included in dependent Claim 54, such as "*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. Prior to its inclusion in Claim 53, Claim 54 had been rejected several times by the Examiner in view of the prior art to Claim 53 in view of Smith (2004/0003282). EX1002, 370, 469, 516.

D. The Challenged Claims

109. I have been asked to provide my opinions regarding claims 1-25 (the "challenged claims"). Section VII below includes a Claim Listing of claims 1-25 with annotations added to label claim limitations.

110. Independent Claims 1, 9, 17, and 25 contain substantially similar limitations for devices, systems, and methods for electronic device security. Each claim recites steps for registering an electronic device with a security service, sending information about the device to the service, periodically communicating with the service, receiving a notification from the service (e.g., a notification that the device is lost), disabling the device in response to the notification, and copying user data from the device to the security service server(s). Each claim further specifies that the security application/software for performing these operations is stored in an area of memory that is not modifiable by a user of the device. Claim 25 further adds steps relating to deleting user data from the device (e.g., in response to a report of the device being lost/stolen) and restoring user data to the device (e.g., following recovery of a lost/stolen device).

111. The dependent claims add conventional details of electronic communications and computer-security systems. For example, the claims that depend from the independent claims , are summarized as follows:

i. Claims 2, 10, and 18 recite negative limitations specifying that the notification received by the mobile phone does not include a third-party certification

ii. Claims 3-5, 11-13, and 19-21 recite conventional types of identifying information for a mobile phone operating in a wireless communications network, such as phone number, phone description, model number, and IMEI

iii. Claims 6, 14, and 22 specify a conventional format (namely, SMS) for sending and receiving messages in a mobile device network

iv. Claims 7, 15, and 23 mirror limitations of Independent Claim 25 and add steps for deleting user data from a mobile device (e.g., in response to a report of the device being lost/stolen)

v. Claims 8, 16, and 24 also mirror limitations of Independent Claim 25 and add steps for restoring user data to a mobile device (e.g., following recovery of a lost/stolen device)

112. These, and other conventional features added by other dependent claims, were well-known and POSITAs had reason to implement them in computer security systems and methods, meeting the challenged claims, as I discuss in Section VII.A-VII.D, below.

VI. CLAIM INTERPRETATION

113. I understand that determining whether a claimed invention is novel and non-obvious requires comparing the prior art to the claim. I discuss in the sections below the interpretations I have applied to certain claim terms, in accordance with the standards set forth in Section III above. For the reasons I discuss below in Sections VII.A-VII.D below, it is my opinion that the prior art I consider in those sections plainly disclose the claim limitations without having to determine the exact outer boundary of the claim terms' scope and meaning.

VII. THE CHALLENGED CLAIMS ARE UNPATENTABLE IN LIGHT OF THE PRIOR ART IDENTIFIED IN THE PETITION

114. I have been asked to provide my opinion concerning whether claims 1-25 of the '649 patent are anticipated by or would have been obvious to a POSITA in light of the prior-art. For the reasons explained below, it is my opinion that each of claims 1-25 is anticipated by and/or would have been obvious to a POSITA over the prior art discussed below.

A. Ground 1A: Claims 1-5, 7-13, 15-21, and 23-25 are Anticipated by and/or Would Have Been Obvious Over Andrews

1. Overview of Ground 1

115. For the reasons I discuss below in Sections VII.A.2-12, it is my opinion that claims 1-5, 7-13, 15-21, and 23-25 are anticipated by and/or would

have been obvious over Andrews (EX1005) in view of the knowledge of a person of ordinary skill at the time of the alleged invention of the ’649 patent.

2. Andrews (EX1005): WIPO Pub. No. WO2001084455

116. From its face, Andrews is an international application published under the Patent Cooperation Treaty (PCT) that published on November 8, 2001. Because Andrews was published in 2001, I understand that Andrews qualifies as prior art even if the challenged claims are entitled to the August 23, 2003 filing date of Provisional Application No. 60/497,182 (*see* ’649 patent, code (60)). I understand that Andrews was not cited or otherwise made of record during prosecution of the ’649 patent. *See* ’649 patent, code (56) (references cited).

117. Like the ’649 patent, Andrews discloses a security solution for portable electronic devices. In particular, Andrews discloses “computing devices” and “a portable computing device communication system and method.” Like the ’649 patent, Andrews identifies both that portable electronic devices have become “increasingly popular in recent years” Andrews, 1:7-8, and that “the portable nature of such devices makes them particularly susceptible to loss and theft” Andrews, 1:13-14. The risk of loss and theft is exacerbated by the fact that “the value of the data stored on a lost or stolen portable computing device may eclipse the value of the device itself” and, moreover, “may be of a sensitive nature,” such

that "public disclosure of the data may have detrimental consequences for its owner. Andrews, 1:17-19.

118. To address these and related problems, Andrews discloses a "communication system" that includes a "**host computer 12** and one or more **client computing devices 14**," as depicted in the annotated figures below. Andrews, 8:4-8.

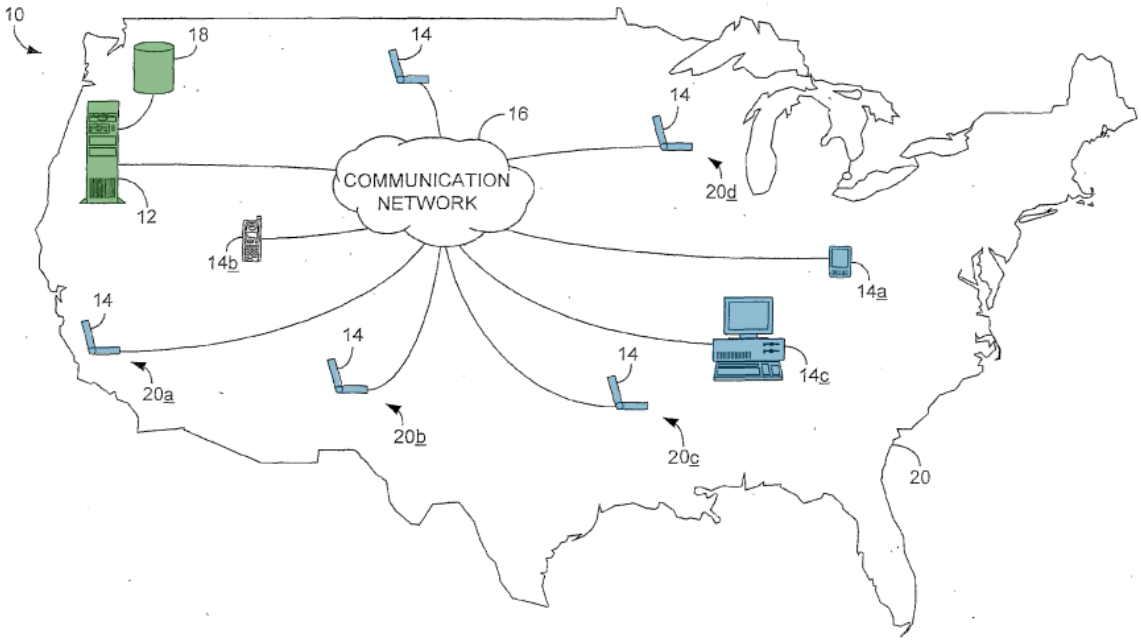


FIG. 1

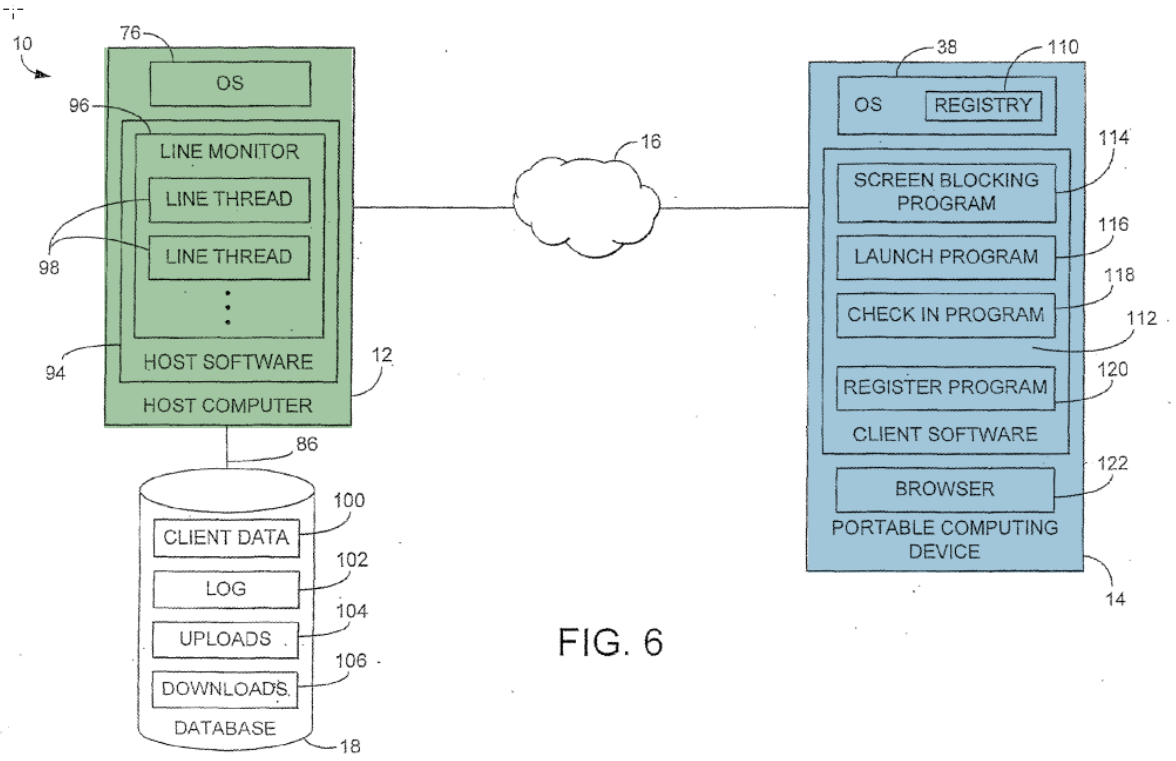


FIG. 6

119. Andrews's **client computing device 14** can be a "portable computing device 14 such as a laptop computer" or can be "personal data assistant (PDA) 14a, cellular phone 14b, or virtually any other portable computing device." Andrews, 8:18-9:7. To operate within Andrews's system, the device must be able to "establish contact with host computer 12 via communication network 16." Andrews, 8:18-9:7. The portable computing device contains conventional electronic components, such as "a central processing unit 22, memory 24, a mass storage device 26, each linked to a bus 28. The mass storage device may be a hard drive, CD ROM drive, magnetic disk drive, tape drive, or other device. Mass storage device 26 may also be flash memory, and/or device 14 may include

firmware 25, particularly where portable computing device 14 is a PDA or cellular phone." Andrews, 10:3-11. These components are depicted in Figure 2:

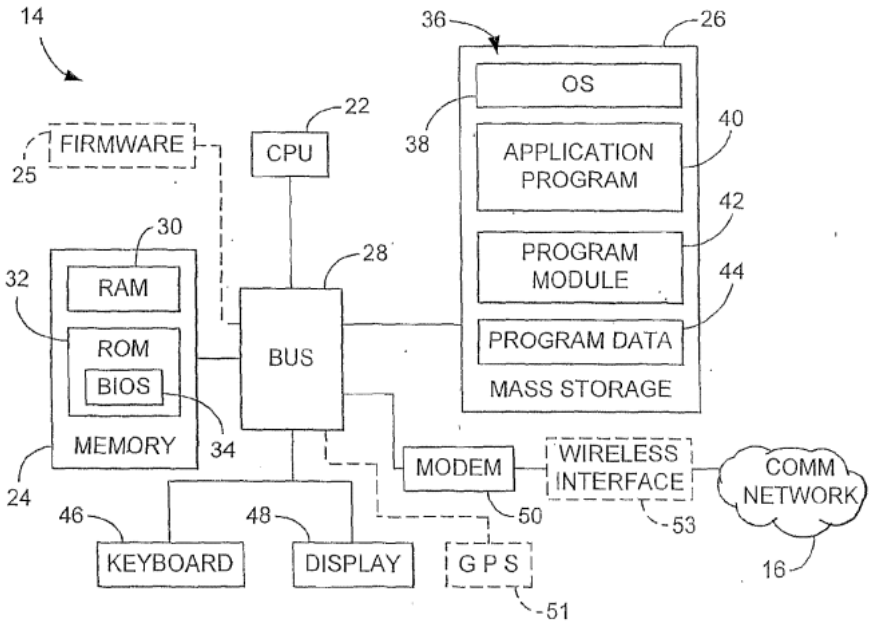


FIG. 2

120. Andrews's **host computer 12** similarly includes "a central processing unit 60, memory 62, and mass storage device 64 linked by a bus 66. Memory 62 typically includes random access memory (RAM) 68, read only memory (ROM) 70, and a basic input output system (BIOS) 72, which contains software routines necessary to start-up and operate 15 host computer 12. The mass storage device may be a hard drive, CD ROM drive, magnetic disk drive, tape drive, or other device. Computer-readable data 74, such as an operating system 76, application program 78, program module 80, and program data 82 are typically stored on mass storage device 64, or in memory 62." Andrews, 12:11-20. Additionally, the host computer is linked to database 18 via a network modem 84 20 linked to a computer

network 86." Andrews, 12:19-20. The "host computer 12 typically is configured to execute operating system 76, as well as host software 94." Andrews, 13:22-23. The host software is "configured to communicate with database 18. Database 18 is configured to store client data 100, a contact log 102, uploaded files 104 received from portable computing devices 14, and downloadable files 106 to be sent to portable computing devices 14 by host computer 12." Andrews, 14:9-12.

121. The client computing device and host computer are each linked to "communication network 16," which may be the "PSTN," "a wireless network, such as a cellular or satellite network," or a "computer network, such as the Internet." Andrews, 13:3-19.

122. Client computing device runs "client programs 112" or "client software 112." Andrews, 15:8-14. Client software may be a "security product," which typically "has features such as determining if a portable computing device is missing and retrieving and deleting data, tracking the location of the portable computing device, and locking up the portable computing device." Andrews, 34:10-13. The software may additionally be a "content distribution product" and, as such, may be used to "distribute messages and other content from host computer 12 to portable computing device 14[.]" Andrews, 34:13-15. 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." Andrews, 32:9-14.

123. Andrews's Figure 11, below, depicts the operation of the client software on the portable computing device when the software is implemented as a service of the operating system.

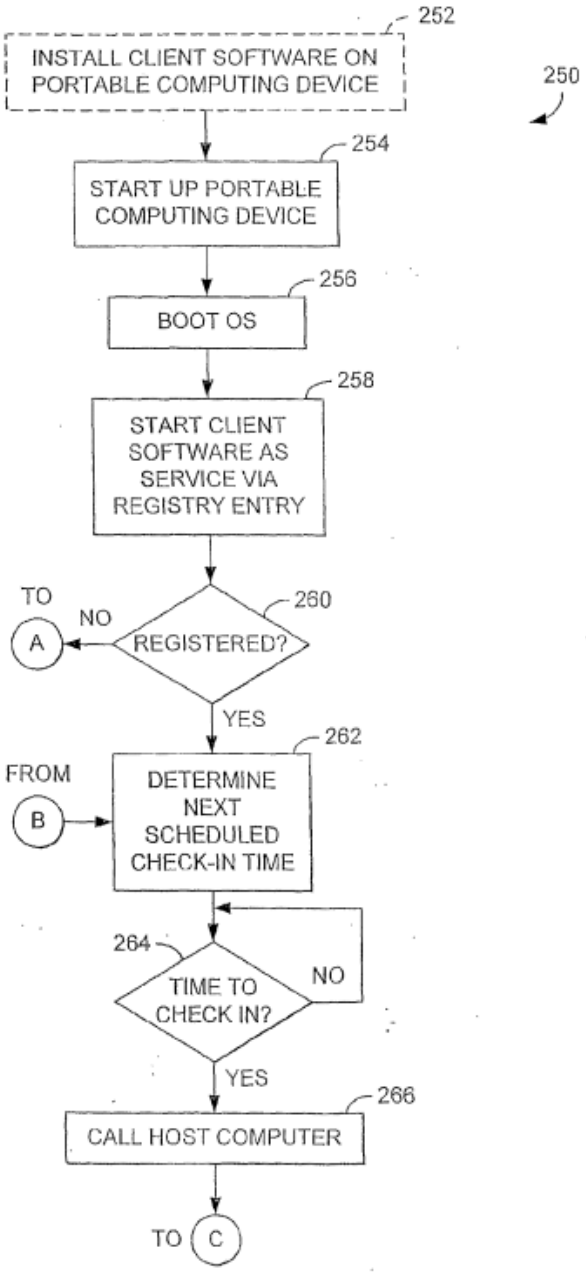


FIG. 11

124. First, at step 252, the software is installed on the protable computing device, typically by the "owner or user of the portable computing device . . . after purchasing the portable computing device. Andrews, 31:21-32:2. After the portable computing device starts up, the client software is started.

125. At 260, it is determined whether the client software is registered. Andrews, 32:15-16. If the device is not yet registered, the software runs a "registration program 120" that "receive[s] user information" and sends it to "host computer 12" for storage as part of "client data 100 on database 18." Andrews, 16:9-11, 33:21-34:6. The software additionally determines a hardware and software configuration for the device, which is likewise sent to host computer 12 for storage in database 18. Andrews, 24:16-21, 35:15-20, 16:11-14.

126. Once the device is registered, the software runs a "check-in program 118 that is configured to launch upon start-up" and that determines "whether it is time to check in" with the host computer. If so, the program "contact[s] host computer 12" via a network connection (e.g., telephone network, cellular network, or Internet). Andrews, 30:8-21; 33:2-6.

127. In response to checking in with the host computer, client software receives a "reported stats 148 of portable computing device 14." Andrews, 19:6-13. The reported status is stored in database 18 associated with the host computer 12. An "interest holder in portable computing device" can report the device status

"via a telephone call, email, online form, or virtually any other suitable communications method," at which point the status is stored in database 18. Andrews, 19:6-13; *see also* 27:16-21, 37:6-13.

128. "The reported status may be virtually any status, but is typically NORMAL, MISSING, LOST, STOLEN, UNAUTHORIZED USE, MESSAGE QUEUED, PAYMENT DUE, and/or DELINQUENT." Andrews, 19:14-16. The host computer 12 sends the reported status to the portable computing device, along with a "responsive action," which "may be virtually any action, and may for example include retrieving data from portable computing device 14, deleting data from portable computing device 14, restricting access to portable computing device 14, or determining a geographic location of portable computing device 14[.]" Andrews, 28:17-22, 30:13. The host computer 12 "instruct[s] portable computing device 14 to take responsive action 150." Andrews, 30:13.

129. In some cases, the responsive action will be "LOCK-UP DEVICE," which will "instruct portable computing device 14 to restrict user access to portable computing device 14." Andrews, 22:21-23:4. Restricting user access can be achieved by, e.g., "locking up the GUI 52 of the operating system 38 of portable computing device 14" and/or by "restricting the user's access privileges in another suitable manner," such as by using a "screen-blocking the program" that "prevents a user from interacting with the GUI to access the files and folders

contained on portable computing device 14." Andrews, 22:21-23:4; 45:6-46:3. In any event, "a password is required of the user to gain access to the portable computing device once the device is locked up." Andrews, 22:21-23:4.

130. Additionally or alternatively, the responsive action may be "RETRIEVE FILE," which will "instruct portable computing device 14 to transfer a file located by a predetermined file-to-retrieve indicator 164 to host computer 12 for storage as an upload 104 in database 18." Andrews, 21:16-23, 34:10-13. In some—but not necessarily all—cases, the RETRIEVE FILE action will be accompanied by a DELETE FILE action, which will "instruct portable computing device 14 to delete a file on portable computing device 14 located by a predetermined file-to-delete indicator 166." Andrews, 22:10-12, 40:14-19. The action may also include "DOWNLOAD FILE," which "causes host computer 12 to download a file to portable computing device 14." Andrews, 23:7-10, 42:15-20.

131. The operation of the host computer to send these—and other—responsive actions to the portable computing device for execution by the client software is depicted in the flowcharts of Figures 14-15 below:

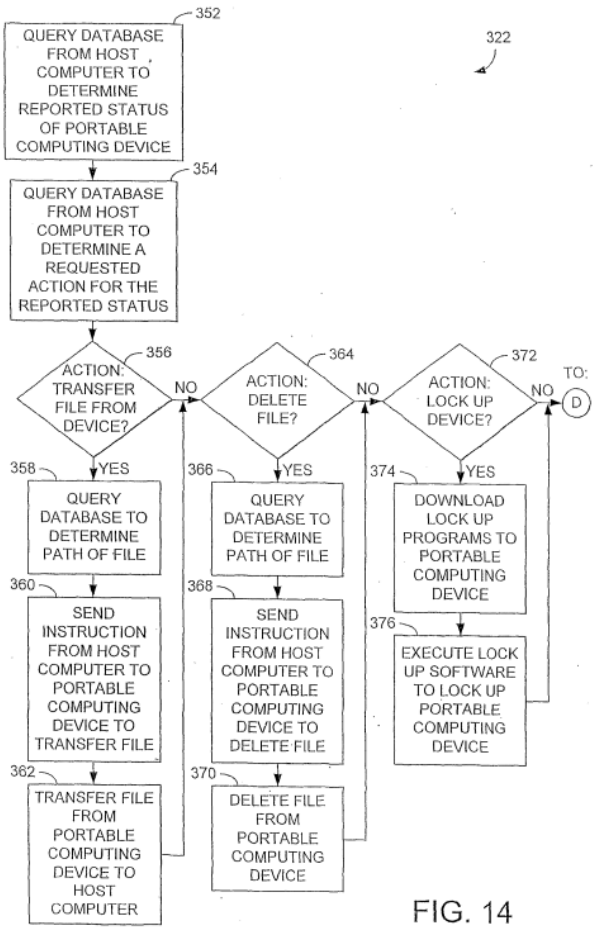


FIG. 14

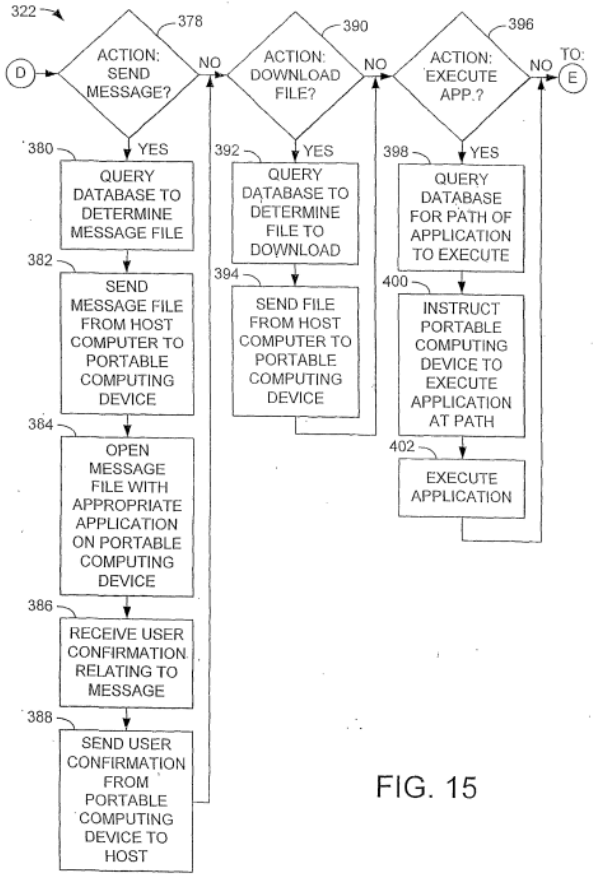


FIG. 15

3. Independent Claim 1

132. Claim 1 is reproduced below. Throughout my declaration, I use italics to denote language of the challenged claims. All bold font text is my own emphasis unless otherwise noted.

> *A mobile electronic device, comprising:*
> *a processor;*
> *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;*

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:

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;

causing the mobile electronic device to automatically send identifying information for the mobile electronic device to the security service;

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;

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;

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

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

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.

a. Preamble 1[pre]

133. The preamble of Claim 1 recites "*A mobile electronic device, comprising*." For the reasons I discuss below, Andrews discloses the subject matter of the preamble.

134. Andrews's client computing device 14 can be a "portable computing device 14 such as a laptop computer" or can be "personal data assistant (PDA) 14a, cellular phone 14a, or virtually any other portable computing device." Andrews, 8:18-9:7. Andrews's "portable computing device 14," which is the claimed *mobile electronic device*. Andrews, 8:4-9, 8:18-9:7.

b. Structural Limitations 1[A] and 1[B]

135. The Structural Limitations of Claim 1 recites "*a processor*" and "*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.*" For the reasons I discuss below, Andrews discloses the Structural Limitations.

136. Andrews's "portable computing device 14 typically includes a central processing unit 22." 10:3-4. A CPU is a *processor*, and it is therefore my opinion that Andrews discloses the *processor* of claim 1.

137. Andrews also discloses that the portable computing device includes "memory 24 [and] a mass storage device 26." Andrews, 10:3-14. As Andrews explains, "[m]ass storage device 26 may also be flash memory, and/or device 14 may include firmware 25," Andrews, 10:6-8, while "[m]emory 24 typically includes random access memory (RAM) 30, read only memory (ROM) 32, and a basic input output system (BIOS) 34." Andrews, 10:9-11.

138. As I discussed in Section IV.B, flash memory and ROM are each common, well-known types of *non-transitory machine-readable storage media* that are *non-volatile memory* and that would have been found in computing devices in 2003. Thus, it is my opinion that Andrews also discloses these memory limitations.

c. Security Application Limitation 1[C]

139. The Security Application Limitation of Claim 1 recites "*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*." For the reasons I discuss below, Andrews discloses the Security Application Limitation.

140. Andrews's portable computing device includes "**client software 112**" as depicted in Figure 6 below.

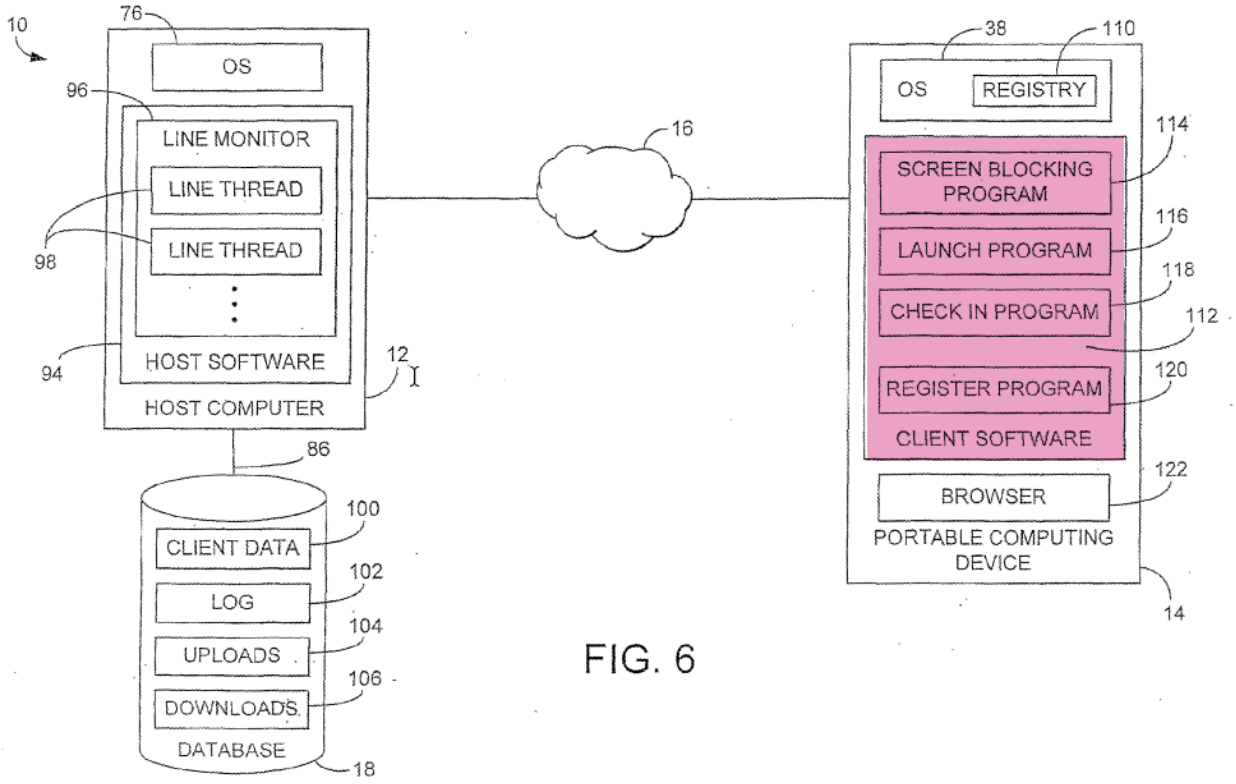


FIG. 6

141. Client software 112 includes one or more "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 on portable computing device 14." Andrews, 15:8-14. Client software can include a "security product," an "information distribution product," or "may be both." Andrews, 18:10-13. Client software that is a security product typically "has features such as determining if a portable computing device is missing and retrieving and deleting data, tracking the location of the portable computing device, and locking up the portable computing device." Andrews, 34:10-13.

142. In my opinion, Andrews's client software 112, at least when implemented as a security product on the portable client electronic device, is a *security application in at least one of the non-transitory machine-readable storage media*, as claimed.

d. Registration Limitation 1[D]

143. The Registration Limitation of Claim 1 recites "*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*." For the reasons I discuss below, Andrews discloses the Registration Limitation.

144. Andrews teaches that its "client software 112" "includes a **registration program 120**," as depicted in Figure 6 below. Andrews, 16:9-11.

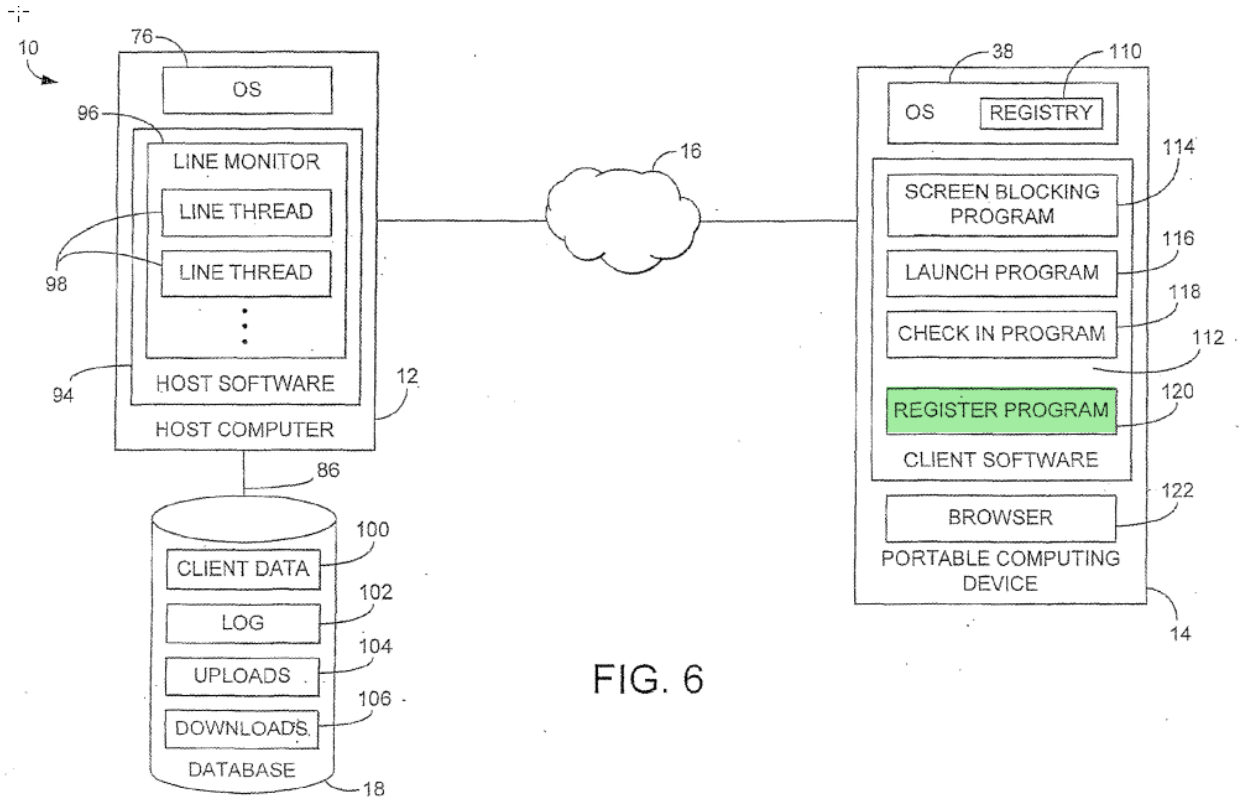


FIG. 6

145. The registration program is "configured to receive user information," which "is entered by the user via menu options on a registration menu." Andrews, 16:9-11; *see also* 19:1-5, 33:21-34:6. User information may include, *inter alia*, "user name 126, user address 140, [and] user email 144." Andrews, 34:16-35:1. The user information is "sent to host computer 12 for storage in database 18." Andrews, 19:1-5; *see also* 16:11-14 (registration program "transmit[s] to the host the gathered user information 125").

146. The software may be a "security product," which "has features such as determining if a portable computing device is missing and retrieving and deleting data,…and locking up the portable computing device." Andrews, 34:10-13. Upon

registration, the "host computer" assigns a "client ID" to the portable computing device. Andrews, 18:3-7.

147. After sending user information to host computer via registration program 120, the portable computing device receives—from host computer 12—"the registration information, as well as an associated client ID and contact schedule information," which, as discussed in greater detail below, enable the computing device to perform the security-service operations of Andrews. Andrews, 36:7-9.

148. Annotated Figure 12 below depicts the operation of **receiving registration information**, as well as the operations of **sending the registration information** to host computer for **storage in the host computer database**.

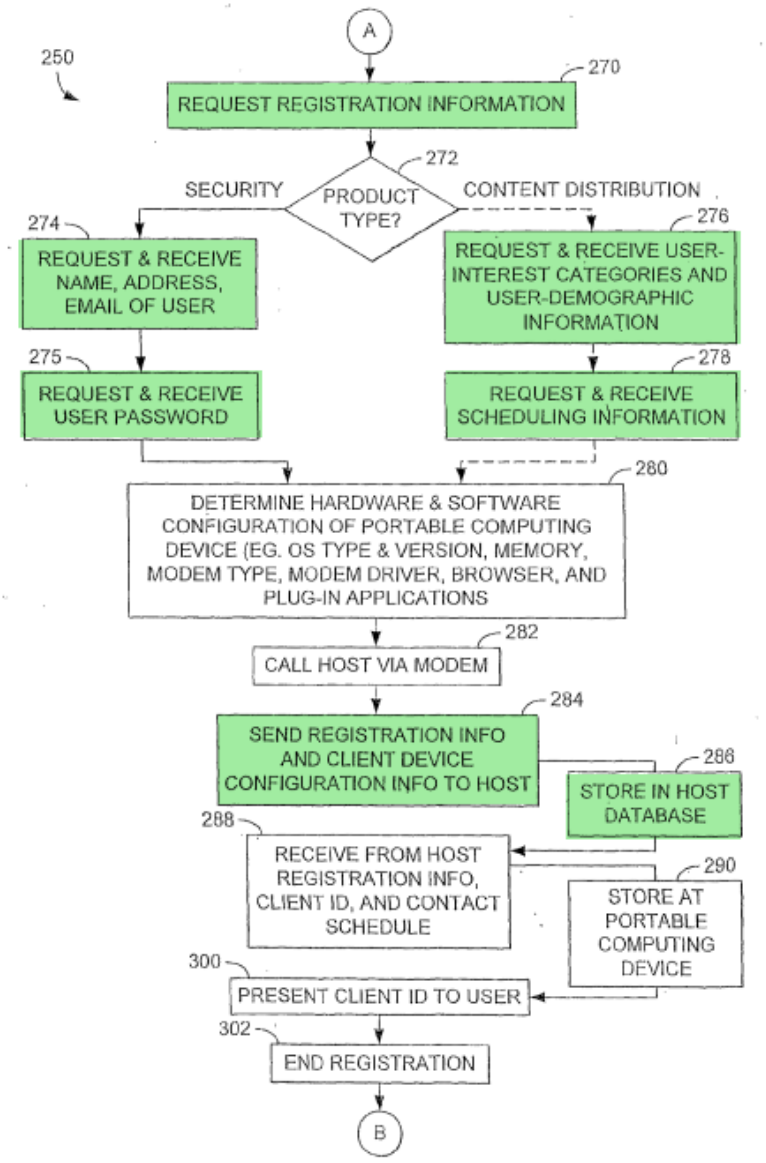


FIG. 12

149. In my opinion, Andrews discloses that the "client software 112"—and, more specifically, the registration program—*enables an owner of the device to request to register the* portable computing device with the host computer (and its associated database). Similarly, the user's submission of user information to the host computer using this registration program constitutes *receiving a request to*

register and *enabling an owner to register* the device with the host computer (and its associated database). In response to the owner's submission of registration information, the information is stored at the host computer, thereby registering the device. Andrews, 19:1-5; *see also* 16:11-14.

150. Furthermore, host computer 12 "includes a central processing unit 60 [and] memory 62," the memory "contain[ing] software routines necessary to start-up and operate host computer 12." Andrews, 12:11-15. The host computer is "linked to database 18 via a network modem 84." Andrews, 12:19-20. In operation, the host computer (in conjunction with its associated database) stores "host software" that causes the host computer to " communicate with database 18" to perform the operations of the security software, such as "stor[ing] client data 100, a contact log 102, uploaded files 104 received from portable computing devices 14, and downloadable files 106 to be sent to portable computing devices 14 by host computer 12." Andrews, 14:9-12. The operations of the host computer and host software are discussed throughout this declaration and include, e.g., periodically communicating with the client device (Section VII.A.3.d), sending a device status to the client device (Section VII.A.3.g), causing the client device to become disabled (Section VII.A.3.h), and causing the client device to copy, delete, and restore user data (Sections VII.A.3.i, VII.A.6.h, VII.A.6.i). *See also* Andrews,

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).

151. Therefore, in my opinion, the host computer running host software to implement the operations of the security software in conjunction with its associated database constitutes a *security service residing at least partially on one or more servers*. Accordingly, registration with the host computer (e.g., using the client software as discussed above) would constitute registration with the *security service* as claimed.

e. Sending Identifying Information Limitation 1[E]

152. The Sending Identifying Information Limitation of Claim 1 recites "*causing the mobile electronic device to automatically send identifying information for the mobile electronic device to the security service*." For the reasons I discuss below, Andrews discloses the Sending Identifying Information Limitation.

153. The registration program on Andrews's portable computing device sends "hardware and software configuration 168" to the host computer. Andrews, 16:11-14. The hardware and software configuration can include "a modem driver type[,]…a browser type, operating system type, available memory, available plug-in applications, and other parameters" of the computing device. Andrews, 24:16-19, 35:15-20. In my opinion, each of these pieces of information describes an

aspect of the client device and would, therefore, be *identifying information for the portable computing device*.

154. The portable computer sends this information to the host computer by "calling host computer 12 via the modem 50 of the portable computing device 14 through communications network" and "sending…the hardware and software configuration 168 of portable computing device 14." Andrews, 35:21-36:6. Like the user information, this device information is "stor[ed]…in the database 18 associated with host computer 12." Andrews, 35:21-36:6.

155. In my opinion, Andrews discloses sending this information to the host computer *automatically*, as claimed, because the client software can "detect[]" and send the information from the device to the host/server without being instructed by a user to do so. *See* Andrews, 24:16-21. Moreover, 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, which depicts the operations occurring *automatically* without any prerequisite user input or determination step:

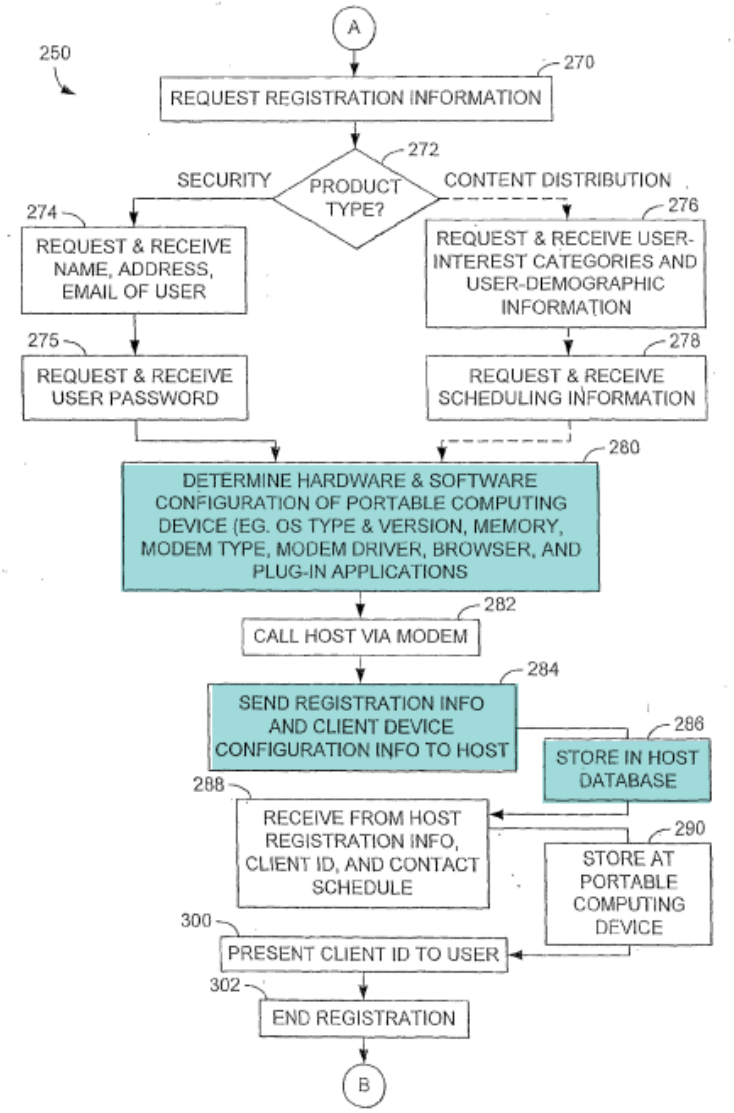


FIG. 12

156. Andrews also discloses sending a "product identifier 124" from the portable computing device (i.e., *mobile electronic device*) to the host computer (i.e., *security* service). Andrews, 18:3-13, 34:2-13. The product identifier is a "code assigned to the particular version of client software 112 on personal computing device 14," Andrews, 18:7-9, which is "stored within the client software" and is "transferred to host computer and stored…on database 18"

following registration, Andrews, 34:3-6. The product identifier typically indicates the type of client software (e.g., a security product, a content distribution product, or both) that is installed on the portable computing device. Andrews, 34:7-10. The registration program "gather[s]" the information and "transfer[s]" it to host computer automatically without any user instruction to do so. Andrews, 33:23-34:6. In my opinion, the product identifier would also be *identifying information for the mobile electronic device* that the device *automatically sends to the security service* as claimed.

f. Periodic Communication Limitation 1[F]

157. The Periodic Communication Limitation of Claim 1 recites "*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*." For the reasons I discuss below, Andrews discloses the Periodic Communication Limitation.

158. As discussed in Section VII.A.3.d, the computing device receives "contact schedule information" from the host computer following registration. Andrews, 36:7-9. Thereafter, "[c]lient software 112 is configured to periodically check in with host computer 12" based on this contact schedule information. Andrews, 15:19-16:8.

159. More specifically, client software "includes a **check-in program 118**," as depicted in annotated Figure 6 below. Andrews, 16:15-17:4.

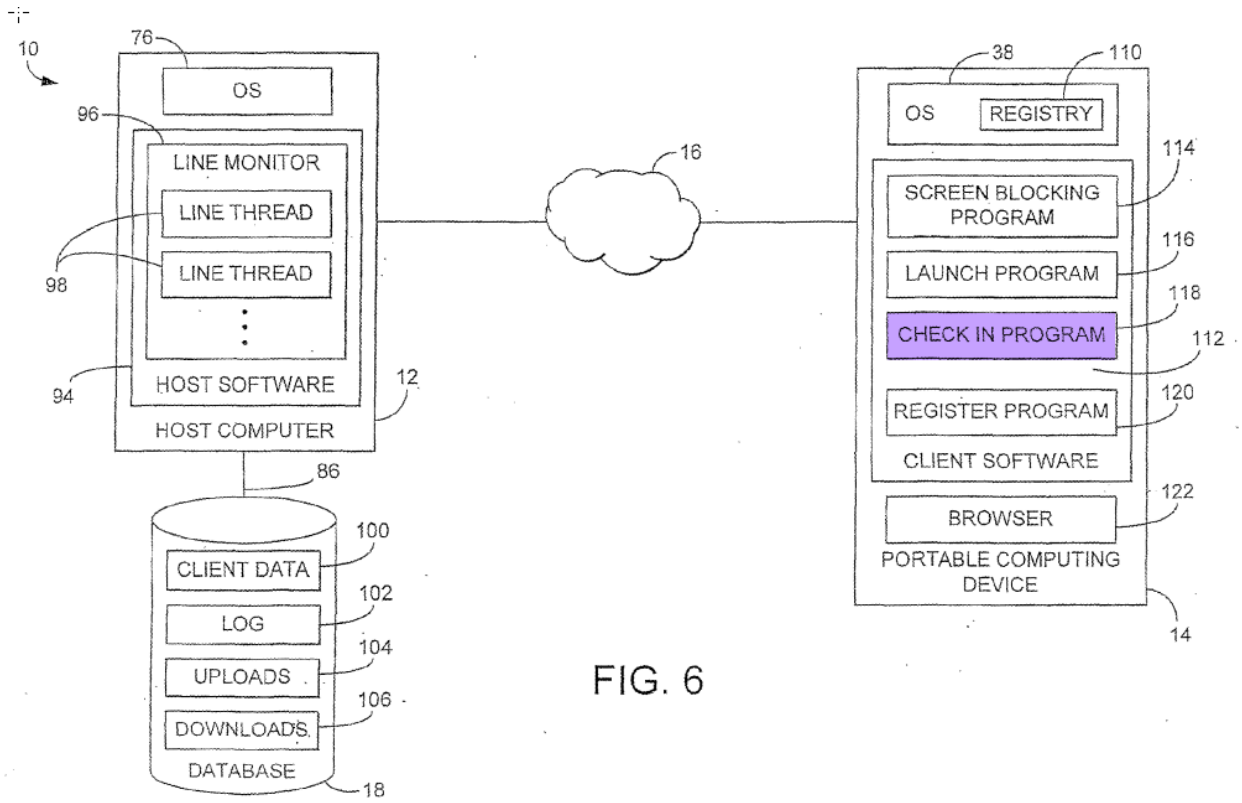


FIG. 6

160. The check-in program "is configured to launch upon start-up of portable computing device 14" and to wait until the "next scheduled check-in time" for the device, at which point the program "proceeds to establish a connection with host computer 12." Andrews, 16:15-17:4. "If it is time to check in, at 266 the method typically includes contacting host computer 12 from portable computing device 14." Andrews, 32:21-33:6.

161. The scheduled contact between the portable computing device and host computer occurs "periodically according to contact schedule 176." Andrews,

28:5-10. As Andrews explains, "contact schedule 176…may be a periodic or non-periodic schedule," such that "portable computing device 14 may be programmed with a contact schedule causing the device 14 to contact the host computer 12 on a monthly, daily, hourly, or random basis." Andrews, 27:3-6.

162. In response to the portable computing device checking in with (i.e., establishing contact with) the host computer, the host computer sends to the portable computing device a "reported status 148 of portable computing device 14," as will be discussed in greater detail in Section VII.A.3.g. Andrews, 19:6-13.

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

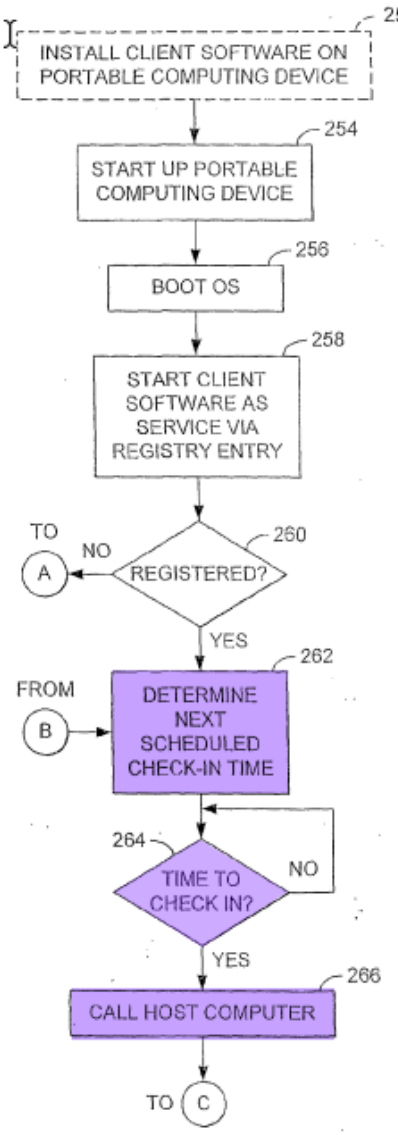


FIG. 11

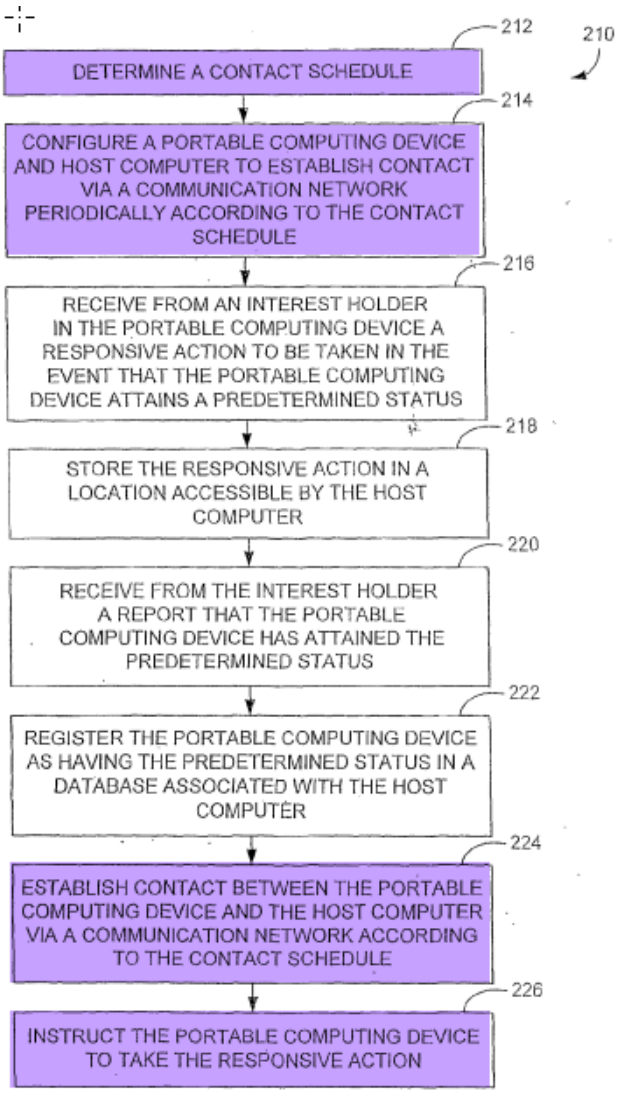


FIG. 9

164. "The contact is typically established via a telephone network such as the PSTN. Alternatively, the telephone network may be a wireless network such as a cellular or satellite network." Andrews, 28:11-16. "Contact is typically made via a telephone network, however wireless networks, such as satellite and cellular

networks, and/or computer networks, such as the Internet, may also be used[.]" Andrews, 30:8-21.

165. In my opinion, periodically contacting the host computer according to a periodic schedule and receiving, in response, a reported device status constitutes *periodically communicat[ing] with the security service*.

166. 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. *See also* Andrews, 32:15-20 (disclosing that the check-in operations will occur "[i]f the client software is registered").

167. Moreover, the "check-in program 118" is "configured to launch upon start-up of portable computing device 14." Andrews, 16:15-17:4. Because the check-in program launches upon start-up, it is my opinion that the check-in program is running—and, as a result, the periodic communication between client and server is occurring—whenever the device is *in a state other than a state in which the mobile electronic device is powered off*.

g. Security Notification Limitation 1[G]

168. The Security Notification Limitation of Claim 1 recites "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 understand that because of the use of the disjunctive "or" – only one of these alternatives need be satisfied by the prior art. Nevertheless, for the reasons I discuss below, Andrews discloses both alternatives of the Security Notification Limitation.

169. Andrews discloses that during operation of the check-in program on client software 112, 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 14," which is "a party who has an interest in the portable computing device, such as a corporate or individual owner of the device, a lessor, lender, or other financier of the device, or a user of the device." Andrews, 19:6-13. A reported status can be reported using "any [] suitable communications method," such as "via a telephone call, email, [or] online form." Andrews, 19:6-13.

170. Andrews identifies several example device statuses that may be reported to the portable computing device, including "NORMAL, MISSING, LOST, [and] STOLEN." Andrews, 19:14-16. As Andrews explains, "the status is MISSING when the portable computing device is missing from the possession of the interest holder," Andrews, 19:17-19, "the status of the device is LOST when

the interest holder knows that the device is missing because it was lost," Andrews, 20:1-3, and "the status of the device is STOLEN when the interest holder knows that the device is missing because it was stolen." Andrews, 20:1-3. In my opinion, the LOST status is *a message indicating that the owner of the mobile electronic device has reported a loss*, as claimed.

171. Furthermore, the status may be accompanied by a message "instructing the portable computing device" to "take [a] responsive action," which "may be virtually any action, and may for example include retrieving data from portable computing device 14, deleting data from portable computing device 14, restricting access to portable computing device 14, or determining a geographic location of portable computing device 14[.]" Andrews, 28:17-22; 30:12. In my opinion, a message instructing the device to restrict access to the device is *a message indicating that the owner of the mobile electronic device has…requested disabling of the mobile electronic device*, as claimed.

h. Device Disabling Limitation 1[H]

172. The Device Disabling Limitation of Claim 1 recites "*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*." For the reasons I discuss below, Andrews discloses the Device Disabling Limitation.

173. In certain instances, the responsive action received at the portable electronic device from the host computer is a "LOCK-UP DEVICE" instruction, which "will cause host computer 12 to instruct portable computing device 14 to restrict user access to portable computing device 14." Andrews, 22:21-23:4; *see also* 30:12, 34:10-13 ("Typically, the security product has features such as…locking up the portable computing device."), 40:20-41:11 ("[T]he method includes executing the lock-up programs to lock up portable computing device 14, thereby restricting user access to portable computing device 14."), 45:6-46:3 ("a method for restricting access to a computing device is shown generally at 450.…The screen-blocking program grabs the focus of the GUI 52 of the operating system 38 of portable computing device 14, and prevents a user from interacting with the GUI to access the files and folders…"). Restricting user access may be "achieved by locking up the GUI 52 of the operating system 38 of portable computing device 14," and/or by "restricting the user's access privileges in another suitable manner." Andrews, 22:21-23:4. In either example, the user may be required to enter a "password…to gain access to the portable computing device once the device is locked up." Andrews, 22:21-23:4.

174. In an example embodiment, Andrews describes a "method for restricting access to a computing device." The method "includes, at 452, installing a launch program 116 and a screen-blocking program 114 on a computing device,

such as portable computing device 14." Andrews, 45:6-13. "Launch program 116 is configured to be executed automatically upon installation and thereafter upon startup of portable computing device 14, as described above." Andrews, 45:14-16. "The screen-blocking program grabs the focus of the GUI 52 of the operating system 38 of portable computing device 14, and prevents a user from interacting with the GUI to access the files and folders contained on portable computing device 14." Andrews, 45:19-46:3.

175. In my opinion, restricting user access to a portable computing device by locking up the GUI and/or restricting user's access privileges, as taught in Andrews, constitutes disabling *at least one user function of the mobile electronic device*.

176. Additionally, in my opinion, Andrews discloses that the client software *still allow[s] the mobile electronic device to communicate with the security service*, as claimed. For instance, as shown in Figs 14-15, communication between the device and the host computer occurs even after the locking of the device. At **step 376**, the computing device "execute[s] lock up software to lock up [the] portable computing device." Subsequently, at **steps 382, 388, 394, 400, 414, 418, 422**, the computing device performs operations requiring communication with the host computer, such as receiving files and instructions from the host computer.

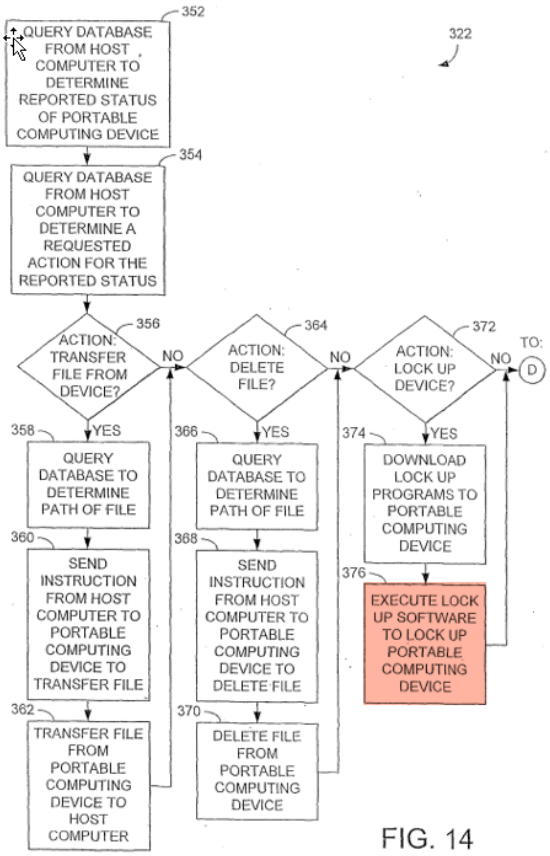

322
352
QUERY DATABASE FROM HOST COMPUTER TO DETERMINE REPORTED STATUS OF PORTABLE COMPUTING DEVICE
354
QUERY DATABASE FROM HOST COMPUTER TO DETERMINE A REQUESTED ACTION FOR THE REPORTED STATUS
356
ACTION: TRANSFER FILE FROM DEVICE?
NO
364
ACTION: DELETE FILE?
NO
372
ACTION: LOCK UP DEVICE?
NO
TO: D
YES
358
QUERY DATABASE TO DETERMINE PATH OF FILE
360
SEND INSTRUCTION FROM HOST COMPUTER TO PORTABLE COMPUTING DEVICE TO TRANSFER FILE
362
TRANSFER FILE FROM PORTABLE COMPUTING DEVICE TO HOST COMPUTER
366
QUERY DATABASE TO DETERMINE PATH OF FILE
368
SEND INSTRUCTION FROM HOST COMPUTER TO PORTABLE COMPUTING DEVICE TO DELETE FILE
370
DELETE FILE FROM PORTABLE COMPUTING DEVICE
374
DOWNLOAD LOCK UP PROGRAMS TO PORTABLE COMPUTING DEVICE
376
EXECUTE LOCK UP SOFTWARE TO LOCK UP PORTABLE COMPUTING DEVICE

FIG. 14

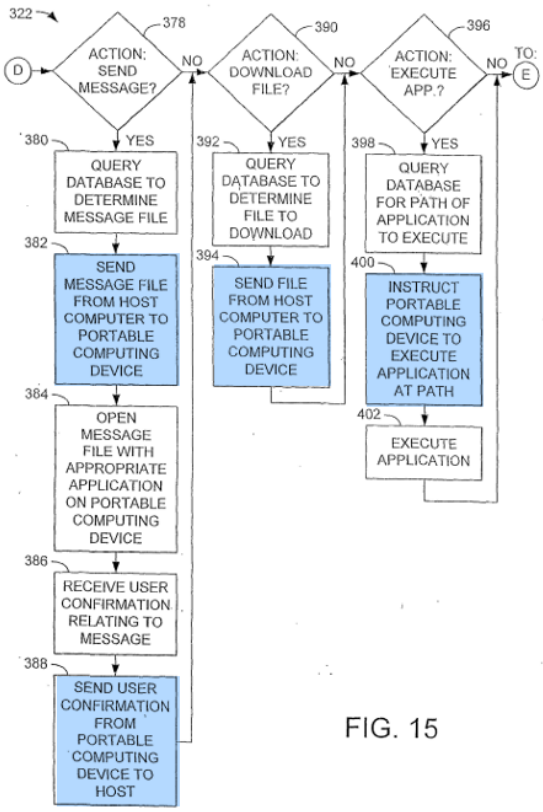

322
D
378
ACTION: SEND MESSAGE?
NO
390
ACTION: DOWNLOAD FILE?
NO
396
ACTION: EXECUTE APP.?
NO
TO: E
YES
380
QUERY DATABASE TO DETERMINE MESSAGE FILE
382
SEND MESSAGE FILE FROM HOST COMPUTER TO PORTABLE COMPUTING DEVICE
384
OPEN MESSAGE FILE WITH APPROPRIATE APPLICATION ON PORTABLE COMPUTING DEVICE
386
RECEIVE USER CONFIRMATION RELATING TO MESSAGE
388
SEND USER CONFIRMATION FROM PORTABLE COMPUTING DEVICE TO HOST
392
QUERY DATABASE TO DETERMINE FILE TO DOWNLOAD
394
SEND FILE FROM HOST COMPUTER TO PORTABLE COMPUTING DEVICE
398
QUERY DATABASE FOR PATH OF APPLICATION TO EXECUTE
400
INSTRUCT PORTABLE COMPUTING DEVICE TO EXECUTE APPLICATION AT PATH
402
EXECUTE APPLICATION

FIG. 15

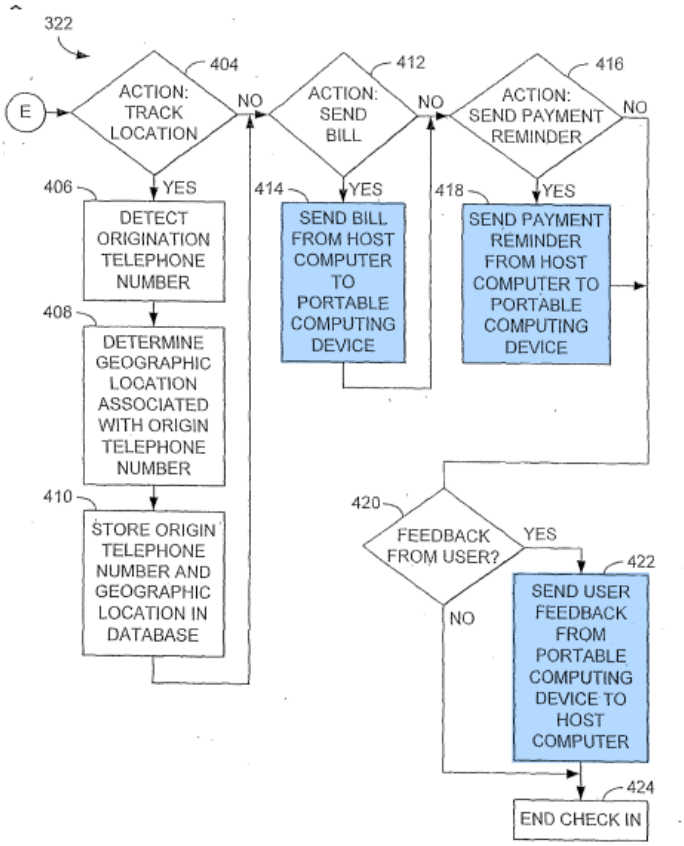


FIG. 16

177. Thus, in my opinion, even after the device has been disabled, the client software *still allow[s] the mobile electronic device to communicate with the security service*, as claimed.

i. Copying User Data Limitation 1[I]

178. The Copying User Data Limitation of Claim 1 recites "*automatically causing at least some user data to be copied from the mobile electronic device to at least one of the servers*." For the reasons I discuss below, Andrews discloses the Copying User Data Limitation.

179. Discussing the purpose of its device-protection system, Andrews explains that "the value of the data stored on a lost or stolen portable computing device" may be valuable and/or sensitive and, therefore, identifies the "recovery of the data stored [on the computer]" as a "high priorit[y] for owners whose portable computing devices are lost or stolen." Andrews, 1:17-22.

180. Accordingly, Andrews discloses that an owner of a "missing" portable computing device can use the security software installed on the device for "retrieving [] data" on the device. Andrews, 34:10-13. In particular, as discussed above, a portable computing device has a "reported status" and, in some cases, an accompanying instruction to take a "responsive action." *See* Section VII.A.3.g.

181. In certain instances, the responsive action may be a "RETRIEVE DATA" instruction, which "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." Andrews, 21:16-23; *see also* 38:23-39:16 (describing "RETRIEVE DATA" operation mode), 40:5-13 (describing "RETRIEVE FILE" action). Andrews refers to the files retrieved from the portable computing device as "uploaded files" and explains that these files include the "data retrieved from a missing portable computing device" as well as "user feedback data" and "user messages." 14:18-21. In my opinion, each of these categories of information is *user data*.

182. As Andrews explains, to "transfer" a file from the portable computing device to the host computer "does not necessarily mean to 'transfer and delete' the file." Andrews, 21:16-23. Thus, at the end of the "RETRIEVE" operation, it is possible that the retrieved file may remain on both the portable computing device and a copy of the file may be stored on the host computer database. In my opinion, to retrieve a file by creating a duplicate version stored at a different network location constitutes *causing at least some user data to be copied from the mobile electronic device to at least one of the servers*, as claimed.

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

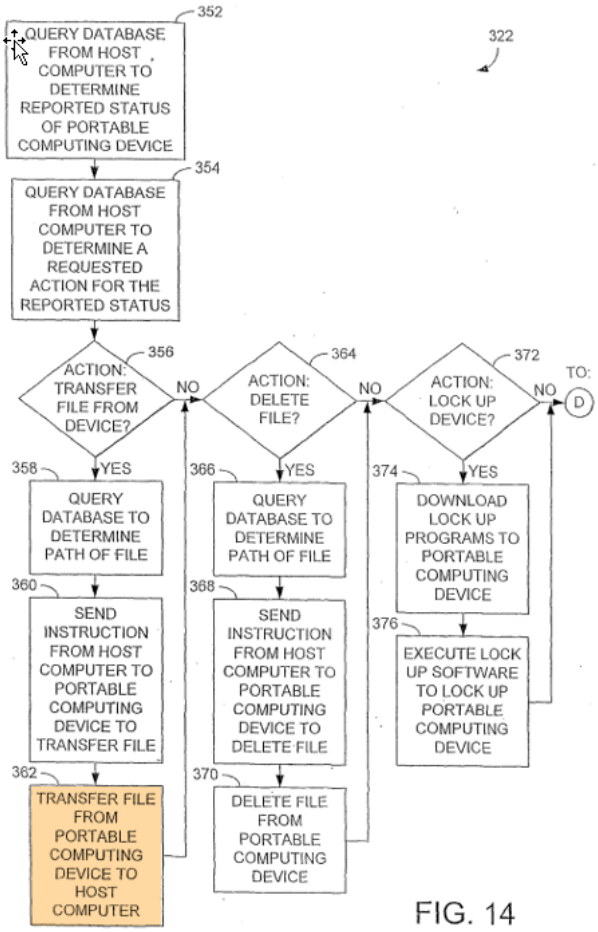


FIG. 14

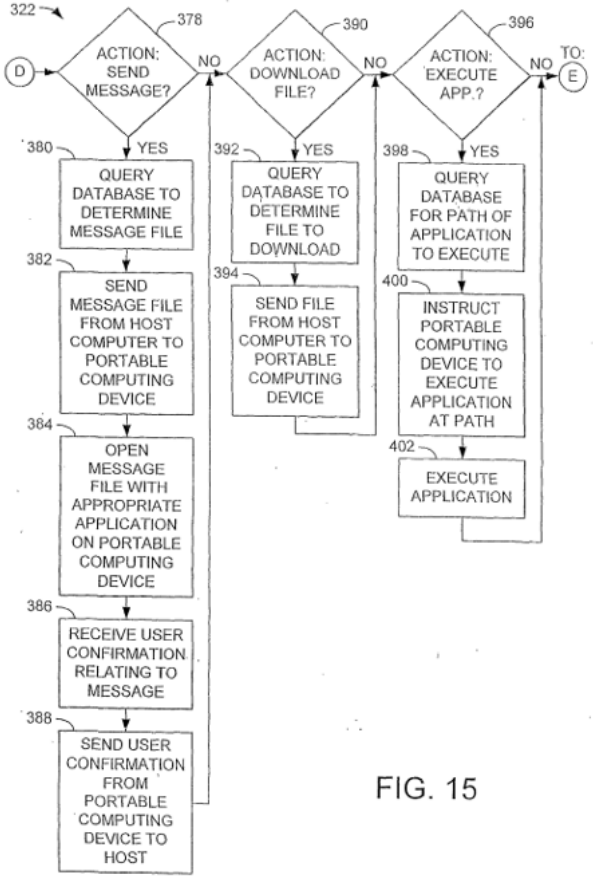


FIG. 15

184. Andrews also discloses that the RETRIEVE FILE command may be accompanied by a "file-to-retrieve indicator 164" specifying which file(s) should be transferred to the host computer. The "file-to-retrieve indicator 164 is a path to a file or folder on portable computing device 14." Andrews, 22:1-7; *see also* 40:5-13. In some cases, "the file to retrieve indicator 164 may be a string representing a partial or complete file name 164," which "instruct[s] the portable computing device 14 to search for the file based on the partial or complete file name, and then transfer the file to the host computer." Andrews, 22:1-6. Moreover, if the file

transfer operation is interrupted, the computing device is placed into a RETRIEVE DATA operation mode, which causes the device to "reconnect with host computer 12…to complete the data transfer" as soon as it is able to do so. Andrews, 38:23-39:16.

185. In my opinion, because the RETRIEVE FILE command and the accompanying file-to-retrieve indicator cause a portable computing device to identify and transfer one or more files without user intervention, the copying of user data in Andrews's system occurs *automatically*, as claimed.

j. Memory Area Limitation 1[J]

186. The Memory Area Limitation of Claim 1 recites "*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*." For the reasons I discuss below, Andrews discloses the Memory Area Limitation.

187. As discussed in Section IV.B, Andrews discloses that the portable computing device can include several different types of *memory*, including flash memory and ROM, which are types of *non-volatile memory*.

188. Andrews does not disclose that its client software must be installed in one particular manner or in one particular memory location. Rather, "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," Andrews, 15:3-11. For example, when installed in the ROM as described in Andrews, the client software can be part of the routines that are "executed on start-up of portable computing device 14." Andrews, 32:9-14.

189. As I explained in Section IV.B, ROM is *non-volatile memory* that *cannot be changed by a user*. A ROM is a memory chip that is installed in a computing device, including desktops, laptops, palm-tops, etc., usually on the main board (or "motherboard") of the computer, and usually at the time of manufacture. A CPU can "read" from the ROM, but cannot "write" to the ROM. If the CPU attempts to *write* to ROM, it won't work: a ROM is read-only and attempts to write to any address within its address space will fail. As explained in multiple technical dictionaries from 2002-2003, "new data cannot be entered" into ROM because the data stored on the ROM "cannot be altered," EX1016, at 6, meaning that "neither the user nor the computer can erase" its contents, EX1017, at 4.

190. Accordingly, in my opinion, when the client software is stored in "ROM 32 on portable computing device 14," as taught in Andrews, the client

software is *utiliz[ing] code residing at least partially in [a] system area…that cannot be modified by the user*, as claimed.

191. Additionally, it is my opinion that Andrews discloses the claimed *changeable area* of *non-volatile memory*. Andrews teaches that its client device includes a "hard drive" that can be "flash memory," which would be a standard component in a computing device such as a laptop computer or the like, as I discuss in Section IV.B. Andrews, 10:4-8; *see also* . As I discuss in my background section, a hard drive and flash memory are classic examples of changeable memory implemented in computing devices and used to persistently store files and data, such as files created by the user.

192. My understanding of Andrews is confirmed by the operation of Andrews's system. For example, Andrews's DELETE FILE and RETRIEVE FILE operations use a "file-to-retrieve"/"file-to-delete" indicator to identify "a path to a file or folder" to be retrieved/deleted. Andrews, 22:1-7. In my opinion, the "files" and/or "folders" discussed in this portion of Andrews clearly refer to files and folders stored in a changeable area of memory on the computing device. Indeed, Andrews's Figure 7 depicts an example of a file-to-retrieve indicator identifying a file path of file to be retrieved. Andrews, Fig. 7. The file path points to the location "C:\files\importantfile.doc," which I interpret to be a reference to the "C:" drive of a Windows operating system, which stores, among other things, the files and

folders created by users in a changeable area of their device's memory. Furthermore, my understanding that Andrews's file system is a *changeable area* within the meaning of the '649 patent is consistent with teachings of the '649 that the *changeable area* "may include a file system," Andrews, 20:14-17, and that the *changeable area* "acts like a file system," as shown in Figure 45 below:

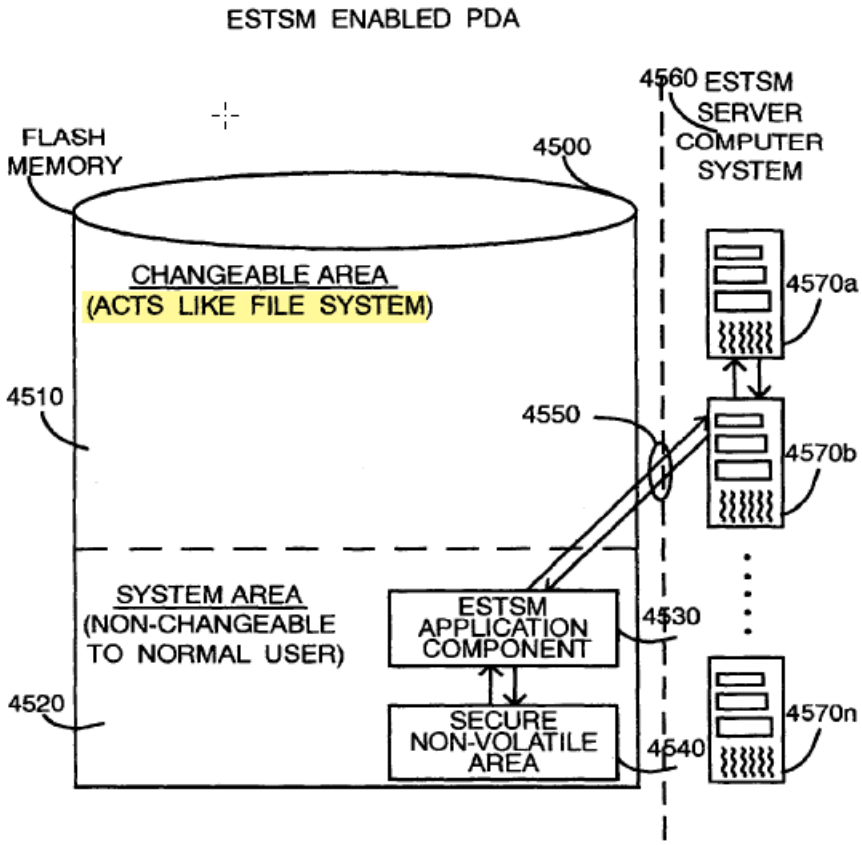


FIGURE 45

193. Moreover, Andrews's security application performs the security operations of Andrews's client software, as described in detail in connection with all other limitations of Claim 1 in the preceding sections.

194. As discussed above, Andrews's software is stored in ROM and cannot be modified. A POSITA would have understood that, during operation, Andrews's software is executed by the processor. A POSITA would have understood that during execution Andrews's software receives messages containing information from other components in the computer system and acts on those messages pursuant to the instructions stored in the ROM. Specifically, a POSITA would have understood that when a "reported status" is received from the host computer (e.g., as discussed in connection with the Periodic Communication Limitations (Section VII.A.3.f), Security Notification Limitations (Section VII.A.3.g), and Device Disabling Limitations (Section VII.A.3.h)), Andrews's client software is given access to data contained in the message and acts on the message by, e.g., updating the state of the software and causing the computer to perform the responsive action.

195. Thus, in my opinion, in the implementation where Andrews's client software is stored in ROM, Andrews's client software receives the reported device status from the host computer (i.e., *a notification from the security service from at least one of the servers*) via the ROM (i.e., *system area*), as claimed.

4. Independent Claim 9

196. Claim 9 is reproduced below.

The system of claim 1, wherein the personal alert device is operable to communicate with one or more nearby alert devices, to forward received

signals and/or alerts generated in response to the received signals among the personal alert device and the one or more nearby alert devices.

wherein the mobile electronic device comprises non-volatile memory;

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;

automatically sending identifying information for the mobile electronic device from the mobile electronic device to the security service;

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;

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;

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

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

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.

a. Preamble 9[pre]

197. The preamble of Claim 9 recites "*A method for providing security for a mobile electronic device, the method comprising*."

198. 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* at least insofar as Andrews's method includes performing an "action…in the event that the portable computing device becomes missing." Andrews, 3:2-5; *see also* 1:7-8, 1:13-14 (identifying loss/theft of portable electronic devices as problem to be addressed).

b. Structural Limitation 9[A]

199. The Structural Limitation of Claim 9 recites "*wherein the mobile electronic device comprises non-volatile memory*."

200. The Structural Limitation of Claim 9 is substantially similar to the Structural Limitation of Claim 1. Thus, it is my opinion that Andrews discloses the Structural Limitation of Claim 9 for the same reasons discussed in connection with Claim 1.

c. Registration Limitation 9[B]

201. The Registration Limitation of Claim 9 recites "*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*."

202. The Registration Limitation of Claim 9 is substantially similar to the Registration Limitation of Claim 1. Thus, it is my opinion that Andrews discloses the Registration Limitation of Claim 9 for the same reasons discussed in connection with Claim 1.

d. Sending Identifying Information Limitation 9[C]

203. The Sending Identifying Information Limitation of Claim 9 recites "*automatically sending identifying information for the mobile electronic device from the mobile electronic device to the security service*."

204. The Sending Identifying Information Limitation of Claim 9 is substantially similar to the Sending Identifying Information Limitation of Claim 1. Thus, it is my opinion that Andrews discloses the Sending Identifying Information Limitation of Claim 9 for the same reasons discussed in connection with Claim 1.

e. Periodic Communication Limitation 9[D]

205. The Periodic Communication Limitation of Claim 9 recites "*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*."

206. The Periodic Communication Limitation of Claim 9 is substantially similar to the Periodic Communication Limitation of Claim 1. Thus, it is my

opinion that Andrews discloses the Periodic Communication Limitation of Claim 9 for the same reasons discussed in connection with Claim 1.

f. Security Notification Limitation 9[E]

207. The Security Notification Limitation of Claim 9 recites "*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.*"

208. The Security Notification Limitation of Claim 9 is substantially similar to the Security Notification Limitation of Claim 1. Thus, it is my opinion that Andrews discloses the Security Notification Limitation of Claim 9 for the same reasons discussed in connection with Claim 1.

g. Device Disabling Limitation 9[F]

209. The Device Disabling Limitation of Claim 9 recites "*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*."

210. The Device Disabling Limitation of Claim 9 is substantially similar to the Device Disabling Limitation of Claim 1. Thus, it is my opinion that Andrews

discloses the Device Disabling Limitation of Claim 9 for the same reasons discussed in connection with Claim 1.

h. Copying User Data Limitation 9[G]

211. The Copying User Data Limitation of Claim 9 recites "*automatically causing at least some user data to be copied from the mobile electronic device to at least one of the servers*."

212. The Copying User Data Limitation of Claim 9 is substantially similar to the Copying User Data Limitation of Claim 1. Thus, it is my opinion that Andrews discloses the Copying User Data Limitation of Claim 9 for the same reasons discussed in connection with Claim 1.

i. Memory Area Limitation 9[H]

213. The Memory Area Limitation of Claim 9 recites "*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*."

214. The Memory Area Limitation of Claim 9 is substantially similar to the Memory Area Limitation of Claim 1. Thus, it is my opinion that Andrews discloses

the Memory Area Limitation of Claim 9 for the same reasons discussed in connection with Claim 1.

5. Independent Claim 17

215. Claim 17 is reproduced below.

An article of manufacture comprising:
a non-transitory machine-readable storage medium; and . . .
non-volatile memory in the mobile phone
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:
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;
automatically sending identifying information for the mobile electronic device from the mobile electronic device to the security service;
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;
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;
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
automatically causing at least some user data to be copied from the mobile electronic device to at least one of the servers;
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.

a. Preamble 17[pre]

216. The preamble of Claim 17 recites "*An article of manufacture comprising:*" For the reasons I discuss below, Andrews discloses the subject matter of the preamble.

217. Andrews discloses a "portable computing device 14." Andrews, 8:4-9, 8:18-9:7. The computing device "includes a…memory 24 [and] a mass storage device 26," Andrews, 10:3-14, each of which stores computer readable instructions and which—independently or in combination with the entirety of the computing device—constitutes an *article of manufacture*.

b. Structural Limitation 17[A]

218. The Structural Limitation of Claim 17 recites "*a non-transitory machine-readable storage medium; and . . . non-volatile memory in the mobile phone*."

219. The Structural Limitation of Claim 17 is substantially similar to the Structural Limitation of Claim 1. Thus, it is my opinion that Andrews discloses the Structural Limitation of Claim 17 for the same reasons discussed in connection with Claim 1.

c. Security Application Limitation 17[B]

220. The Security Application Limitation of Claim 17 recites "*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."

221. The Security Application Limitation of Claim 17 is substantially similar to the Security Application Limitation of Claim 1. Thus, it is my opinion that Andrews discloses the Security Application Limitation of Claim 17 for the same reasons discussed in connection with Claim 1.

d. Registration Limitation 17[C]

222. The Registration Limitation of Claim 17 recites "*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*."

223. The Registration Limitation of Claim 17 is substantially similar to the Registration Limitation of Claim 1. Thus, it is my opinion that Andrews discloses the Registration Limitation of Claim 17 for the same reasons discussed in connection with Claim 1.

e. Sending Identifying Information Limitation 17[D]

224. The Sending Identifying Information Limitation of Claim 17 recites "*automatically sending identifying information for the mobile electronic device from the mobile electronic device to the security service*."

225. The Sending Identifying Information Limitation of Claim 17 is substantially similar to the Sending Identifying Information Limitation of Claim 1. Thus, it is my opinion that Andrews discloses the Sending Identifying Information Limitation of Claim 17 for the same reasons discussed in connection with Claim 1.

f. Periodic Communication Limitation 17[E]

226. The Periodic Communication Limitation of Claim 17 recites "*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*."

227. The Periodic Communication Limitation of Claim 17 is substantially similar to the Periodic Communication Limitation of Claim 1. Thus, it is my opinion that Andrews discloses the Periodic Communication Limitation of Claim 17 for the same reasons discussed in connection with Claim 1.

g. Security Notification Limitation 17[F]

228. The Security Notification Limitation of Claim 17 recites "*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*."

229. The Security Notification Limitation of Claim 17 is substantially similar to the Security Notification Limitation of Claim 1. Thus, it is my opinion that Andrews discloses the Security Notification Limitation of Claim 17 for the same reasons discussed in connection with Claim 1.

h. Device Disabling Limitation 17[G]

230. The Device Disabling Limitation of Claim 17 recites "*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*."

231. The Device Disabling Limitation of Claim 17 is substantially similar to the Device Disabling Limitation of Claim 1. Thus, it is my opinion that Andrews discloses the Device Disabling Limitation of Claim 17 for the same reasons discussed in connection with Claim 1.

i. Copying User Data Limitation 17[H]

232. The Copying User Data Limitation of Claim 17 recites "*automatically causing at least some user data to be copied from the mobile electronic device to at least one of the servers*."

233. The Copying User Data Limitation of Claim 17 is substantially similar to the Copying User Data Limitation of Claim 1. Thus, it is my opinion that

Andrews discloses the Copying User Data Limitation of Claim 17 for the same reasons discussed in connection with Claim 1.

j. Memory Area Limitation 17[I]

234. The Memory Area Limitation of Claim 17 recites "*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.*"

235. The Memory Area Limitation of Claim 17 is substantially similar to the Memory Area Limitation of Claim 1. Thus, it is my opinion that Andrews discloses the Memory Area Limitation of Claim 17 for the same reasons discussed in connection with Claim 1.

6. Independent Claim 25

236. Claim 25 is reproduced below.

> *A method for providing security for a mobile electronic device, the method comprising:*
> *wherein the mobile electronic device comprises non-volatile memory;*
> *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;*
> *automatically sending identifying information for the mobile electronic device from the mobile electronic device to the security service;*
> *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;

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;

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

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

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;

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.

a. Preamble 25[pre]

237. The preamble of Claim 25 recites "*A method for providing security for a mobile electronic device, the method comprising:*" For the reasons I discuss below, Andrews discloses the subject matter of the preamble.

238. 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* at least insofar as Andrews's method includes performing an "action…in the event that the portable computing device becomes missing."

Andrews, 3:2-5; *see also* 1:7-8, 1:13-14 (identifying loss/theft of portable electronic devices as problem to be addressed).

b. Structural Limitation 25[A]

239. The Structural Limitation of Claim 25 recites "*wherein the mobile electronic device comprises non-volatile memory.*"

240. The Structural Limitation of Claim 25 is substantially similar to the Structural Limitation of Claim 1. Thus, it is my opinion that Andrews discloses the Structural Limitation of Claim 25 for the same reasons discussed in connection with Claim 1.

c. Registration Limitation 25[B]

241. The Registration Limitation of Claim 25 recites "*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*."

242. The Registration Limitation of Claim 25 is substantially similar to the Registration Limitation of Claim 1. Thus, it is my opinion that Andrews discloses the Registration Limitation of Claim 25 for the same reasons discussed in connection with Claim 1.

d. Sending Identifying Information Limitation 25[C]

243. The Sending Identifying Information Limitation of Claim 25 recites "*automatically sending identifying information for the mobile electronic device from the mobile electronic device to the security service*."

244. The Sending Identifying Information Limitation of Claim 25 is substantially similar to the Sending Identifying Information Limitation of Claim 1. Thus, it is my opinion that Andrews discloses the Sending Identifying Information Limitation of Claim 25 for the same reasons discussed in connection with Claim 1.

e. Security Notification Limitation 25[D]

245. The Security Notification Limitation of Claim 25 recites "*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*."

246. The Security Notification Limitation of Claim 25 is substantially similar to the Security Notification Limitation of Claim 1. Thus, it is my opinion that Andrews discloses the Security Notification Limitation of Claim 25 for the same reasons discussed in connection with Claim 1.

f. Device Disabling Limitation 25[E]

247. The Device Disabling Limitation of Claim 25 recites "*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."

248. The Device Disabling Limitation of Claim 25 is substantially similar to the Device Disabling Limitation of Claim 1. Thus, it is my opinion that Andrews discloses the Device Disabling Limitation of Claim 25 for the same reasons discussed in connection with Claim 1.

g. Copying User Data Limitation 25[F]

249. The Copying User Data Limitation of Claim 25 recites "*automatically causing at least some user data to be copied from the mobile electronic device to at least one of the servers*." For the reasons I discuss below, Andrews discloses the Copying User Data Limitation.

250. The Copying User Data Limitation of Claim 25 is substantially similar to the Copying User Data Limitation of Claim 1. Thus, it is my opinion that Andrews discloses the Copying User Data Limitation of Claim 25 for the same reasons discussed in connection with Claim 1.

h. Deleting User Data Limitation 25[G]

251. The Deleting User Data Limitation of Claim 25 recites "*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." For the reasons I discuss below, Andrews discloses the Deleting User Data Limitation.

252. As discussed above, Andrews explains that to "transfer" a file from the portable computing device to the host computer "does not necessarily mean to 'transfer and delete' the file." Andrews, 21:16-23. However, Andrews also discloses transferring and subsequently deleting files. Specifically, "the action DELETE FILE will cause host computer 12 to instruct portable computing device 14 to delete a file on portable computing device 14 located by a predetermined file-to-delete indicator 166." 22:10-12.

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

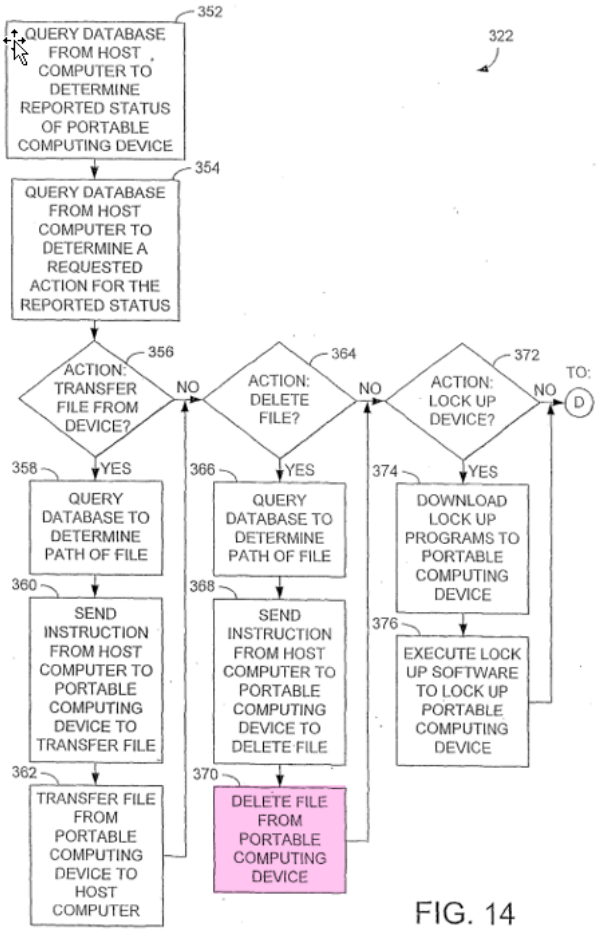


FIG. 14

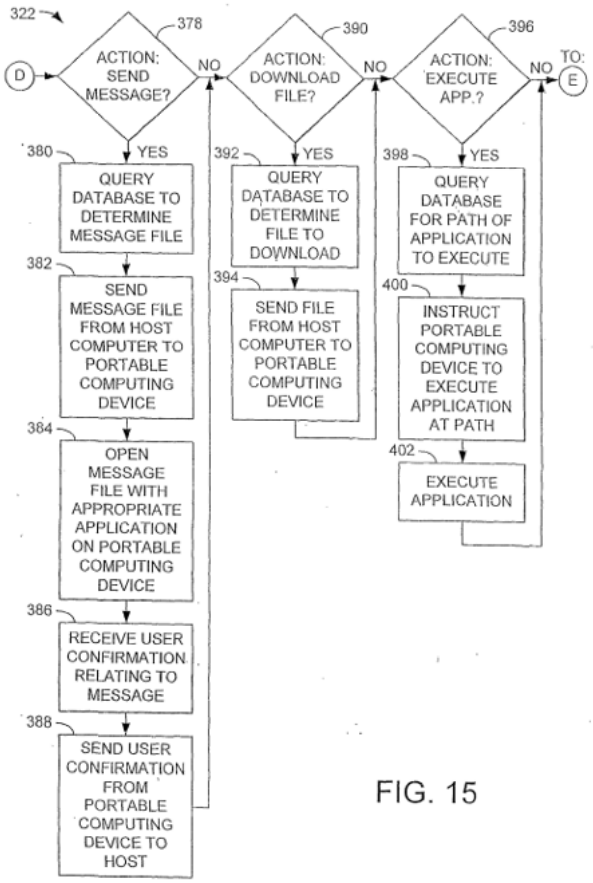


FIG. 15

254. Similar to the file-to-retrieve indicator 164 used in the RETRIEVE FILE operation, the file-to-delete indicator 166 is used during the DELETE FILE operation to provide an "indicator or path 166 of a file to delete," (e.g., "a folder, or group of files". Andrews, 40:14-19. The DELETE FILE command is sent from the host computer to the portable computing device and "instruct[s] portable computing device 14 to delete the file," which, in turn, causes the device to "delet[e] the file located at the path 166." Andrews, 40:14-19. In my opinion, the

DELETE FILE command therefore *caus[es]* files *to be deleted from the mobile electronic device*, as claimed.

255. Additionally, it is my opinion that the files being deleted from the portable computing device during the DELETE FILE operation could—and, in many cases, likely would—include at least some of the files copied to the server in the RETRIEVE FILE operation discussed above. Use of the commands in this way is disclosed by Andrews, which shows, in the 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

256. Therefore, in my opinion, Andrews discloses that the DELETE FILE operation can be used to delete *at least some user data…from the mobile electronic device*, as claimed.

i. Restoring User Data Limitation 25[H]

257. The Restoring User Data Limitation of Claim 25 recites "*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." For the reasons I discuss below, Andrews discloses the Restoring User Data Limitation.

258. In addition to the RETRIEVE FILE and DELETE FILE operations, Andrews also discloses a DOWNLOAD FILE operation, which "causes host computer 12 to download a file to portable computing device 14." Andrews, 23:7-10. When the requested action is to DOWNLOAD FILE, the host computer "instruct[s] the portable computing device to download the appropriate file from host computer 12 to portable computing device 14 via communication network 16." Andrews, 42:15-20.

259. In my opinion, downloading a file from host computer to portable computing device constitutes *causing* a file *to be copied from at least one of the servers to the mobile electronic device*, as claimed.

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

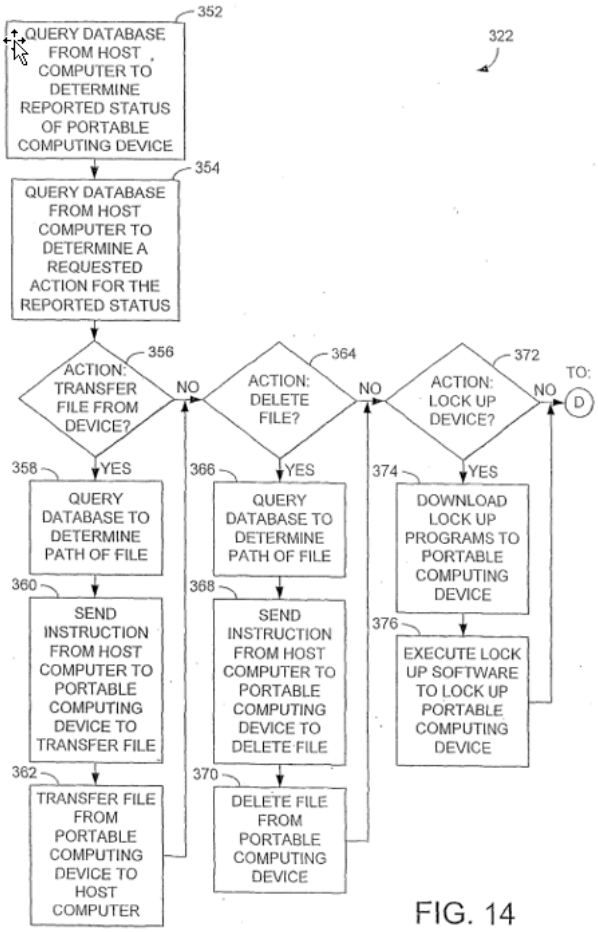


FIG. 14

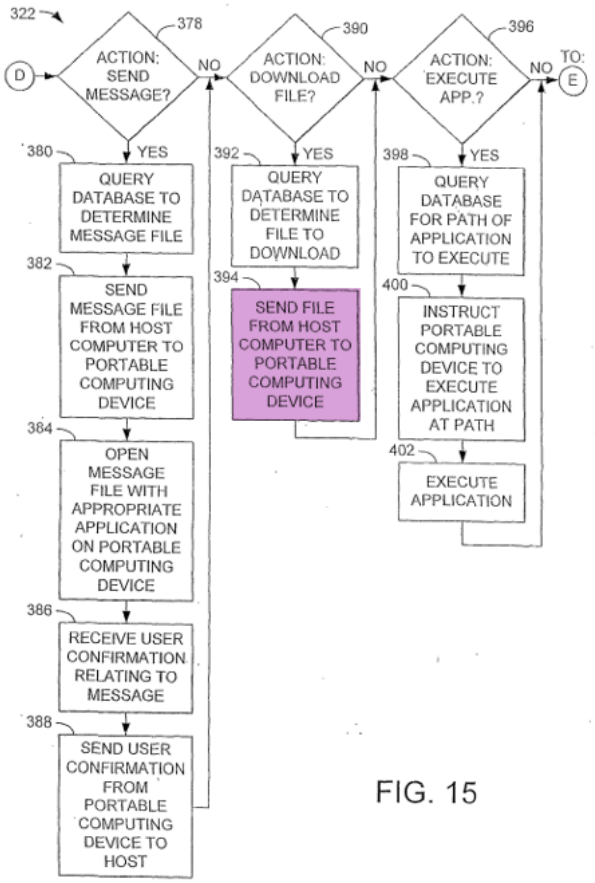


FIG. 15

261. Moreover, Andrews discloses that the responsive actions—such as RETRIEVE FILE, DELETE FILE, and DOWNLOAD FILE—can be "implemented singularly or in combination[.]" Andrews, 21:14-15. Indeed, Figures 14 and 15 show the operations performed by the portable computing device when it "determine[s] [its] reported status 148" based on the information received from the host computer. As shown in the annotated figures below, the portable computing device can perform multiple responsive actions in

combination, including (i) first, **RETRIEVE FILE**, (ii) second, **DELETE FILE**, and (iii) third, **DOWNLOAD FILE**.

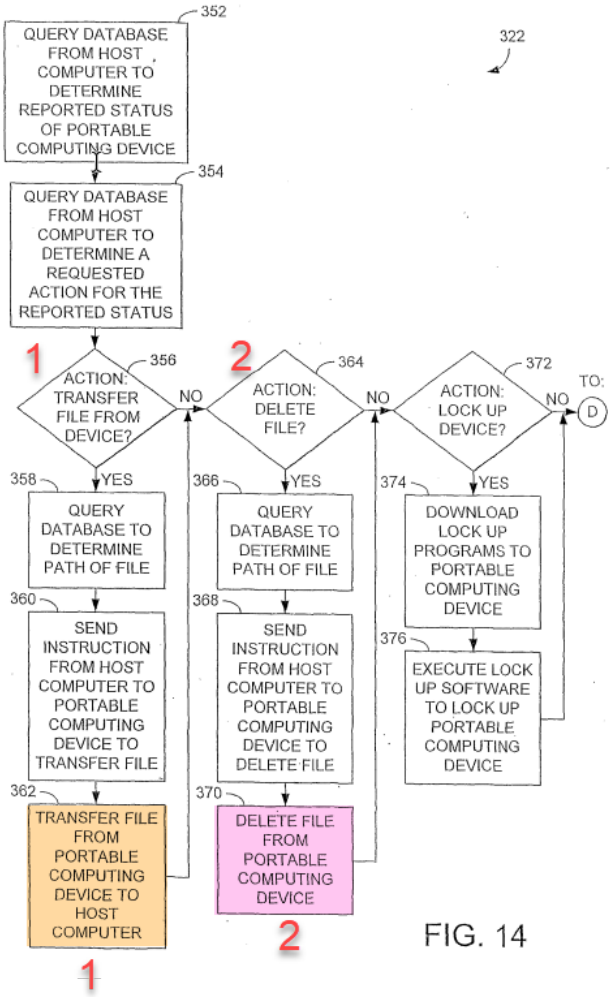


FIG. 14

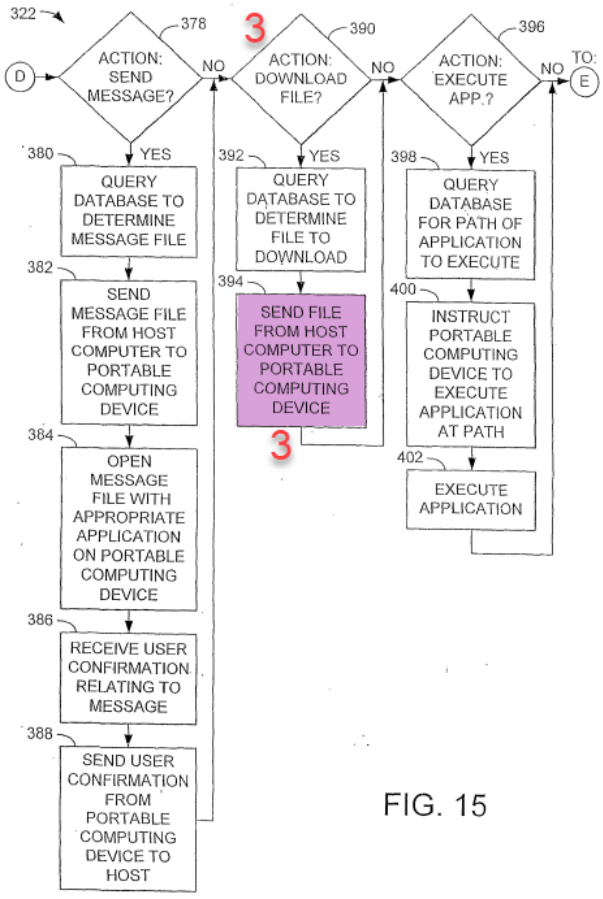


FIG. 15

262. In my opinion, Andrews therefore discloses that the DOWNLOAD FILE operation occurs after the at least some of the user data has been deleted from the mobile electronic device.

263. Andrews discloses that the "[d]ownloadable files 106 [] may include program data files" and "other file types." Andrews, 15:1-2. In my opinion, Andrews discloses that the DOWNLOAD FILE operation can be used to copy any type of file from the host computer to the portable computing device. The files copied from the host computer to the portable computing device could, therefore, include the user data previously uploaded to the host computer and deleted from the portable computing device. In my opinion, implementing the DOWNLOAD FILE in this manner would be one of the most beneficial uses of the DOWNLOAD FILE action because it would allow a user to restore any files deleted from the portable electronic device during the DELETE FILE operation to the device following recovery of the lost/stolen device. In my opinion, Andrews discloses 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.

j. Memory Area Limitation 25[I]

264. The Memory Area Limitation of Claim 25 recites "*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.*"

265. The Memory Area Limitation of Claim 25 is substantially similar to the Memory Area Limitation of Claim 1. Thus, it is my opinion that Andrews discloses the Memory Area Limitation of Claim 25 for the same reasons discussed in connection with Claim 1.

7. Dependent Claims 2, 10, 18

266. Claim 2 depends from claim 1, claim 10 depends from claim 9, and claim 18 depends from claim 17. These claims are substantially similar as shown in the comparison table below. For the reasons I discuss below, Andrews discloses these claims.

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

267. Claims 2, 10, and 18 each recite that the notification received by the electronic device of the Independent Claims "*includes no third-party certification*." The phrase "*third-party certification*" does not appear in the specification of the '649 patent. Without any specialized meaning in the context of the '649 patent, I understand this claim limitation to refer to a certification provided by a third party other than an interest holder in the device or the operator of the host computer security service.

268. Andrews 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. Rather, the reported status is "typically reported by an interest holder in portable computing device 14," such as a "corporate or individual owner of the device, a lessor, lender, or other financier of the device, or a user of the device." Andrews, 19:8-13. Likewise, the responsive action is selected by an interest holder. Andrews, 21:4-8. Accordingly, in my opinion, the message/command sent by the host computer to the portable computing device *includes no third-party certification*, as claimed.

8. Dependent Claims 3, 11, 19

269. Claim 3 depends from claim 1, claim 11 depends from claim 9, and claim 19 depends from claim 17. These claims are substantially similar as shown in the comparison table below. For the reasons I discuss below, Andrews discloses and/or renders obvious these claims.

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.*
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.
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.*

270. 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." These categories each provide certain information about the device with which they are associated. For example, a modem driver and modem type describe aspects of the modem. Similarly, the operating system type and version describes aspects of the operating system installed on the computer. In the circumstance where Andrews's portable electronic device is a mobile phone (e.g., cellular telephone), these categories would describe that phone and, therefore, in my opinion disclose a *phone description*. Andrews, 35:15-20.

271. Additionally, Andrews notes that beyond these expressly identified categories, the configuration information can include any "other hardware and software parameters." Andrews, 35:15-20. There are a number of categories of

information that falls within this broad classification of hardware/software "parameters." For instance, nearly every item of information about the hardware and software of a device would be described as a "parameter" of that device. Andrews's disclosure encompasses a wide range of these parameters, but in the specific context of Andrews's disclosure, there are certain conventional types of hardware/software parameters that would be particularly useful to send to the host computer to identify the device.

272. For a client device that is a "cellular telephone," it would have been conventional to include in the hardware/software parameters *a phone number*, *a phone service provider*, and *an International Mobile Equipment Identifier (IMEI) number*. These pieces of information would have been appropriate to include in the hardware/software parameters because every cellular telephone has its own phone number, phone service provider, and IMEI, which makes these categories of information useful in uniquely identifying a device in Andrews's system. Furthermore, Andrews specifically recognizes the benefits of storing a "cellular telephone number associated with a cellular modem of the portable computing device" at the host computer so that the host computer can use the number to establish contact with the device. Andrews, 28:11-16. Even if Andrews does not expressly state that this phone number is stored on the host computer after being

uploaded as part of the hardware/software parameters, this would have been one of the most efficient and straightforward ways of gathering that information.

273. My opinion that an *IMEI* is information typically used to identify a cellular telephone in a system for tracking mobile electronic devices is further corroborated by WIPO Pub. No. 96/36194, which teaches mobile phones operating in a "GSM system" and which teaches uploading "identity data" for the phone. EX1018, 13:5-25. The reference specifically identifies the device's "IMEI" as being the identity data that is "automatically" transmitted to a server every time the device contacts the network and which can be used by the network to confirm the device identity and ensure that the device is not stolen. EX1018, 13:5-25, 3:25-4:3.

274. Moreover, if Andrews is found not to disclose that its hardware/software configuration includes the claimed categories of identifying information, then it is my opinion that it would have been obvious to implement Andrews to include this conventional information. As discussed above, these categories of information are standard descriptors for any mobile phone operating on a mobile phone network. In fact, they were among a finite set of descriptors that could be used to describe any phone operating in that network and, as such, would have been obvious fields for a POSITA to include in hardware/software configuration parameters when registering a device with a network.

275. My opinion that these were standard descriptors used to identify cellular telephones is further corroborated by contemporaneous publications from the European Telecommunications Standards Institute—a global standards-setting organization—regarding the conventional operation of cellular phones (or, "mobile stations") in a cellular network. For example, GSM 02.07 (EX1022), a technical specification published in 1996 for the Global System for Mobile Communications (or, "GSM") identifies "IMEI" and "service provider indication" as being "mobile station features" used to identify devices "within the digital cellular telecommunications system." EX1022, p. 5, 13, 15. Similarly, GSM 02.16 (EX1023), published in 2000, describes IMEI as being "necessary in order to obtain knowledge about the presence of specific mobile station equipment in the network." EX1023, p. 7. Furthermore, GSM 03.03 (EX1024), published in 1996, describes an "identification plan for mobile subscribers in the GSM system" that is based on assigning phone numbers to the devices in the network. EX1024, p. 7.

276. 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).

9. Dependent Claims 4, 12, 20

277. Claim 1 depends from claim 3, claim 12 depends from claim 11, and claim 20 depends from claim 19. These claims are substantially similar as shown in the comparison table below. For the reasons I discuss below, Andrews discloses and/or renders obvious these claims.

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.*
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.*
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.*

278. The limitations of Claims 4, 12, and 20 are similar to those of Claims 3, 11, and 19. Specifically, whereas Claims 3, 11, and 19 recite sending three out of four items of information to the security service during registration, Claims 4,

12, and 20 recite sending two out of those four categories of information to the security service as part of the *identifying information*. As discussed above, it is my opinion that Andrews discloses sending the four categories of information recited in Claims 3, 11, and 19. Therefore, it is also my opinion that Andrews discloses sending two out of the four of these categories. It does not affect my opinion whether the information is send during registration or as part of the *identifying information* because, in Andrews, the hardware and software configuration can be send either during or after registration, thus meeting either claimed scenario.

10. Dependent Claims 5, 13, 21

279. Claim 5 depends from claim 3, claim 13 depends from claim 11, and claim 21 depends from claim 19. These claims are substantially similar as shown in the comparison table below. For the reasons I discuss below, Andrews discloses and/or renders obvious these claims.

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.*
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.
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.*

280. The limitations of Claims 5, 13, and 21 are similar to those of Claims 4, 12, and 20. Specifically, whereas Claims 4, 12, and 20 recite sending two out of those four categories of information recited in Claims 3, 11, and 19, Claims 5, 13, and 21 recite sending those same two categories of information, plus a *model number for the mobile electronic device*. In my opinion, Andrews discloses sending a *model number* for the same reasons it discloses sending a *phone number* and *IMEI* to the security service as part of the *identifying information*. That is, a POSITA would recognize these categories of information as being forms of hardware and software configuration information for a mobile electronic device. Additionally, Andrews expressly 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, in my opinion, is equivalent to a model number for the software on the device.

11. Dependent Claims 7, 15, 23

281. Claim 7 depends from claim 1, claim 15 depends from claim 9, and claim 23 depends from claim 17. These claims are substantially similar (i) to each other and (ii) to the Deleting User Data Limitation of Claim 25, as shown in the comparison table below. Accordingly, for the reasons discussed in Section VII.A.6.h relating to the Deleting User Data Limitation of Claim 25, Andrews discloses these claims.

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.*
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.*
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.*
25[G]	*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…*

12. Dependent Claims 8, 16, 24

282. Claim 8 depends from claim 7, claim 16 depends from claim 15, and claim 24 depends from claim 23. These claims are substantially similar (i) to each other and (ii) to the Restoring User Data Limitation of Claim 25, as shown in the comparison table below. Accordingly, for the reasons discussed in Section VII.A.6.i relating to the Restoring User Data Limitation of Claim 25, Andrews discloses these claims.

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.*
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.*
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.*
25[H]	*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*

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

1. Bonnett (EX1006): U.S. Patent Pub. No. 2003/0051090

a. Overview of Disclosure

283. From its face, Bonnett is a U.S. Patent Publication that published on March 13, 2003 from a patent application filed on July 17, 2002. Because Bonnett published in March 2003 from an application filed in 2002, I understand that Bonnett qualifies as prior art even if the challenged claims are entitled to the August 23, 2003 filing date of Provisional Application No. 60/497,182 (*see* '649 patent, code (60)).

284. Bonnett teaches techniques for securely upgrading a "program" in an "appliance." The program can be any "software, firmware, code, portions of code, data compilations, and/or a combination of these," Bonnett, [0019], that is "capable of contributing to one or more functions of [a computing device]." Bonnett, [0007].

285. Bonnett discloses techniques for managing the memory of the appliance in such a way that will ensure that the program is inaccessible (and not changeable) to users of that device. Bonnett, [0007].

286. Bonnett describes the purpose and effect of these techniques as follows:

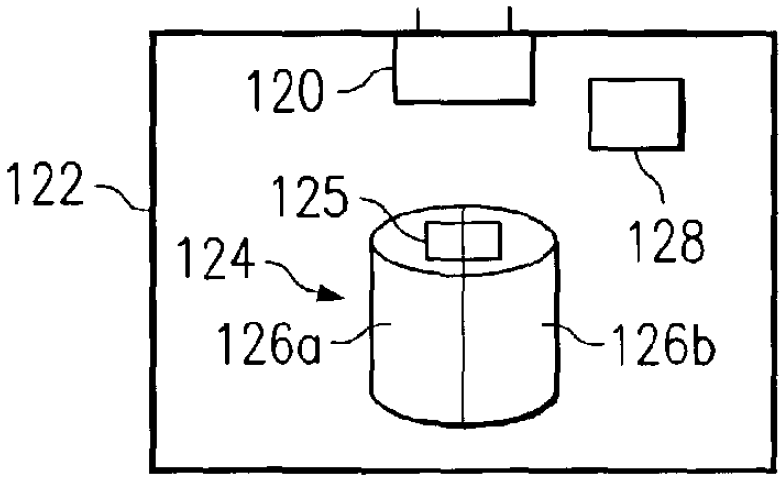
> Various embodiments substantially restrict access to portions of a program stored in a memory accessible to an appliance. Restricting access to programs and/or portions of a program can help prevent a user

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

Bonnett, [0011].

287. While Bonnett refers generally to an "appliance," Bonnett uses this term broadly to include any "device or combination of devices" that are "capable of performing a desired…computing functionality. Bonnett, [0018]. Bonnett provides several examples of appliances, including "a personal digital assistant (PDA), a cell phone, a digitized audio recorder/player, or any other digital or analog device." Bonnett, [0018].

288. To implement Bonnett's techniques, the computer program on the appliance is "stored on [a] memory device" of the appliance, which includes "any…suitable volatile or nonvolatile storage." Bonnett, [0031]. The memory "includes at least an open partition of memory 126a and at least a hidden partition of memory 126b." Bonnett, [0032]. The hidden partition (126b) and open partition (126a) of memory device (124) are depicted in cropped Figure 1 below:



289. The hidden partition is "inaccessible through the external interface." Bonnett, [0010]. Thus, to protect the above-described "programs," Bonnett teaches storing the program 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." Bonnett, [0032], [0037]. 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." Bonnett, [0036].

b. Bonnett Provisional

290. I understand that Bonnett claims priority to a provisional patent application 60/322,252 that was filed on September 10, 2001 ("Bonnett Provisional", EX1009). I have reviewed the Bonnett Provisional and have been asked to determine whether the disclosure of the Bonnett Provisional shows that

the patent applicant was in possession of the invention recited in Bonnett's Claim 1.

291. In my opinion, the Bonnett Provisional describes every aspect of Claim 1 as shown in the paragraphs below:

292. Bonnett's Claim 1 recites: "An appliance." In my opinion, the Bonnett Provisional describes this limitation in at least the following disclosure:

i. "Programmable portable electronic devices or appliances, such as digitized audio recorder/players can require field upgrade of their operating software." (EX1009, p. 3)

293. Bonnett's Claim 1 recites: "a memory comprising at least a hidden portion of memory operable to store at least a portion of a program capable of contributing to one or more functions of the appliance." In my opinion, the Bonnett Provisional describes this limitation in at least the following disclosure:

i. "This solution allows a single storage media that does not require removal from the appliance, thus reduces cost." (EX1009, p. 5)

ii. "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." (EX1009, p. 4)

iii. "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." (EX1009, p. 11)

294. Bonnett's Claim 1 recites: "a controller operable to process at least a portion of the program stored on the hidden portion of memory." In my opinion, the Bonnett Provisional describes this limitation in at least the following disclosure:

i. "The Internet Audio Applications team recently supported a DSP board design that incorporated a C54x based DSP, NAND flash memory, and USB capabilities." (EX1009, p. 11)

ii. "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." (EX1009, p. 11)

295. Bonnett's Claim 1 recites: "an external interface operable to provide access to at least an open portion of the memory." In my opinion, the Bonnett Provisional describes this limitation in at least the following disclosure:

i. “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.” (EX1009, p. 3)

ii. “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.” (EX1009, p. 4)

296. Bonnett’s Claim 1 recites: “wherein the hidden portion of memory is inaccessible through the external interface.” In my opinion, the Bonnett Provisional describes this limitation in at least the following disclosure:

i. “All but one of these sections are hidden from the host computer's operating system.” (EX1009, p. 4)

ii. “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.” (EX1009, p. 11)

iii. “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." (EX1009, p. 11)

2. The Andrews-Bonnett Combination

297. In my opinion, Andrews and Bonnett are analogous art because both relate to hardware and software solutions for improving security of computing systems.

298. It is my opinion that there would have been multiple reasons 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. This combination of Andrews and Bonnett is illustrated in the annotated figure below, which combines figures from both disclosures to show Andrews's client software being stored as Bonnett's program 225b in hidden partition 206b:

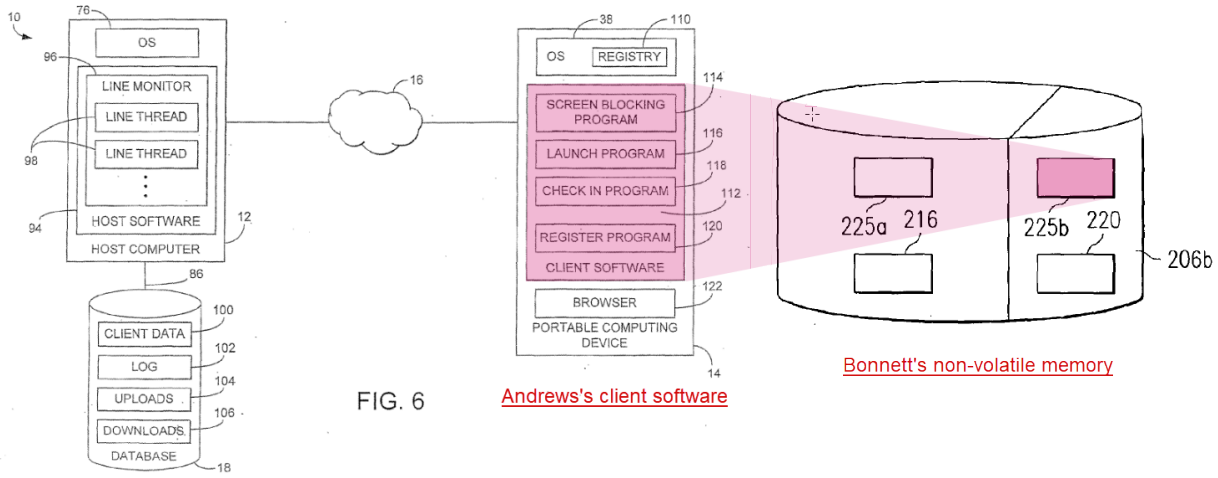


FIG. 6

299. First, Bonnett's intended purpose for its memory-management techniques aligns with the purposes of Andrews's security system. More specifically, the purpose of Bonnett's memory-management techniques is to protect software on a device, while the purpose of Andrews's security system is to protect the device itself. Bonnett accomplishes its objective by storing a program in a "hidden" portion of memory that is not accessible to a user. Bonnett, [0019]. Andrews accomplishes its objective by initiating responsive actions when the device is lost or stolen, including actions that make the device inoperable to a user. Andrews, 1:13-22. In my opinion, a POSITA would have understood these aligned teachings as a reason to combine the two and to store Andrews's device-protection systems using Bonnett's hidden partition to "prevent[] a user from deleting or corrupting . . . the program" and "protect[] . . . software stored on memory [of the] device." Bonnett, [0011], [0032], [0037].

300. Bonnett provides a broad solution that appears to be designed to be used in combination with other systems. The solution can be used to prevent users from accessing computer programs of any type on devices of any type. Thus, while Bonnett does not specifically suggest using its hidden partition to store a program meant for recovering 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 relevant to Andrews, such as when a user finds a lost/stolen device and is attempting to access its programs.

301. Bonnett describes the benefits of protecting programs in this way, teaching that it "can lead to an improved reliability" of the device upon which the protected program is stored. Bonnett, [0011], [0032], [0037]. Reliability is a benefit in a wide variety of situations, but a POSITA would have understood that reliability is particularly important for programs whose proper functioning is necessary for a device owner to recover a lost/stolen device. To improve the reliability of such a program, a POSITA would have 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).

302. Second, a POSITA would have been motivated to combine Andrews and Bonnett because protecting Andrews's client software by installing it in Bonnett's protected, hidden memory area 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.

303. When Andrews's client software contacts the host computer, it does so "surreptitiously" and "silently, without interrupting any activity of the user." Andrews, 31:21-32:8. This teaching would indicate to a POSITA that the Andrews software should by designed to avoid detection by an unauthorized user who, upon detecting the software, may attempt to disable, disrupt, or delete it. By utilizing Bonnett's techniques, though, a POSITA would be able to ensure that even if a user were to detect the software, it would still be protected against tampering.

304. 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." Andrews, 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." Andrews, 46:17-22. A POSITA would have understood Andrews to be teaching that a user might attempt to bypass the security software (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). 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.

305. 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." Andrews, 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)." Andrews, 10:3-14. Likewise, Bonnett teaches that its appliance's memory can be "any [] suitable volatile or nonvolatile storage." [0031]. Because both Andrews and Bonnett provide flexibility in where, how, and in what type of memory the relevant software/programs are stored, a POSITA would have had multiple options for how to specifically combine the two references, thus providing additional reason to pursue the combination.

306. 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.

307. For example, U.S. Patent No. 5,764,892 to Cain et al. ("Cain", EX1011) 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. Like Andrews-Bonnett, Cain's system is meant to be deployed on "smaller lost or stolen objects, particularly laptop computers, cellular telephones" and the like. EX1011, 1:38-42; And, like the Andrews-Bonnett system, Cain's system communicates with a remote server for the purpose of "facilitat[ing] the recovery of [a] stolen device." EX1011, Abstract.

308. Similarly, US2003/0126462 to Howard et al. ("Howard", EX1012) describes a system for "preventing use of a wireless device" – for example if the wireless device has been stolen – through the use of a security program (e.g., security protocol") stored in non-volatile memory. EX1012, [0017]-[0018]. More specifically, the security program "is operable to prevent execution of . . . one user application . . . when a message is received . . . indicat[ing] that the [] device is not in possession of a rightful user." EX1012, (54), Abstract. Howard also recognized the desirability of preventing modifications to the security program to "minimize[] the probability that the security protocols . . . will be circumvented by a malicious user." EX1012, [0019]. When the device is reported stolen, the "security protocol

110 writes a 'STOLEN' status in non-volatile memory" so that an unauthorized user cannot "circumvent the security mechanisms." EX1012, [0030].

309. 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 install Andrews's security software in Bonnett's hidden partition. As discussed above, Andrews teaches that its client software being stored in a variety of formats (e.g., hardware, software, firmware) and in a variety of types of memory (e.g., ROM, flash, hard drive). As I discuss in the technology background Section IV.B, using software-based memory-management techniques like hidden partitions was well-known and well-understood by POSITAs at the time of the invention. To combine Andrews and Bonnett in the proposed manner would therefore require using this background knowledge to (i) identify suitable non-volatile memory in the Andrews portable electronic device (e.g., memory 24 or mass storage 26), (ii) create a hidden partition in this memory, and (iii) install the Andrews client software in the hidden partition.

3. Independent Claim 1

a. Preamble 1[pre]

310. The preamble of Claim 1 recites "*A mobile electronic device, comprising*."

311. In the combination of Andrews and Bonnett described above, Andrews's client software would be stored on Andrews's portable client electronic device using Bonnett's disclosed techniques to store the software program in a hidden partition invisible and inaccessible to users. This combination would meet the preamble of Claim 1 for the same reasons as Andrews alone.

b. Structural Limitations 1[A] and 1[B]

312. The Structural Limitations of Claim 1 recites "*a processor*" and "*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.*"

313. In the combination of Andrews and Bonnett described above, Andrews's client software would be stored on Andrews's portable client electronic device using Bonnett's disclosed techniques to store the software program in a hidden partition invisible and inaccessible to users. This combination would meet the Structural Limitations of Claim 1 for the same reasons as Andrews alone.

c. Security Application Limitation 1[C]

314. The Security Application Limitation of Claim 1 recites "*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*."

315. In the combination of Andrews and Bonnett described above, Andrews's client software would be stored on Andrews's portable client electronic device using Bonnett's disclosed techniques to store the software program in a hidden partition invisible and inaccessible to users. This combination would meet the Security Application Limitation of Claim 1 for the same reasons as Andrews alone.

d. Registration Limitation 1[D]

316. The Registration Limitation of Claim 1 recites "*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*."

317. In the combination of Andrews and Bonnett described above, Andrews's client software would be stored on Andrews's portable client electronic device using Bonnett's disclosed techniques to store the software program in a hidden partition invisible and inaccessible to users. This combination would meet the Registration Limitation of Claim 1 for the same reasons as Andrews alone.

e. Sending Identifying Information Limitation 1[E]

318. The Sending Identifying Information Limitation of Claim 1 recites "*causing the mobile electronic device to automatically send identifying information for the mobile electronic device to the security service*."

319. In the combination of Andrews and Bonnett described above, Andrews's client software would be stored on Andrews's portable client electronic device using Bonnett's disclosed techniques to store the software program in a hidden partition invisible and inaccessible to users. This combination would meet the Sending Identifying Information Limitation of Claim 1 for the same reasons as Andrews alone.

f. Periodic Communication Limitation 1[F]

320. The Periodic Communication Limitation of Claim 1 recites "*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*."

321. In the combination of Andrews and Bonnett described above, Andrews's client software would be stored on Andrews's portable client electronic device using Bonnett's disclosed techniques to store the software program in a hidden partition invisible and inaccessible to users. This combination would meet the Periodic Communication Limitation of Claim 1 for the same reasons as Andrews alone.

g. Security Notification Limitation 1[G]

322. The Security Notification Limitation of Claim 1 recites "*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*."

323. In the combination of Andrews and Bonnett described above, Andrews's client software would be stored on Andrews's portable client electronic device using Bonnett's disclosed techniques to store the software program in a hidden partition invisible and inaccessible to users. This combination would meet the Security Notification Limitation of Claim 1 for the same reasons as Andrews alone.

h. Device Disabling Limitation 1[H]

324. The Device Disabling Limitation of Claim 1 recites "*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*."

325. In the combination of Andrews and Bonnett described above, Andrews's client software would be stored on Andrews's portable client electronic

device using Bonnett's disclosed techniques to store the software program in a hidden partition invisible and inaccessible to users. This combination would meet the Device Disabling Limitation of Claim 1 for the same reasons as Andrews alone.

i. Copying User Data Limitation 1[I]

326. The Copying User Data Limitation of Claim 1 recites "*automatically causing at least some user data to be copied from the mobile electronic device to at least one of the servers*."

327. In the combination of Andrews and Bonnett described above, Andrews's client software would be stored on Andrews's portable client electronic device using Bonnett's disclosed techniques to store the software program in a hidden partition invisible and inaccessible to users. This combination would meet the Copying User Data Limitation of Claim 1 for the same reasons as Andrews alone.

j. Memory Area Limitation 1[J]

328. The Memory Area Limitation of Claim 1 recites "*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."

329. Andrews-Bonnett includes Bonnett's memory device(s) 124, 212, which can be "any…nonvolatile storage" and which, in my opinion, are *non-volatile memory*. Bonnett, [0031], [0035]. In the combined system, this memory device includes Bonnett's open partition of memory 126a, 206a, which stores files "accessible to the user" and which, in my opinion, is a *changeable area that can be modified by a user*. Bonnett, [0036]. The combined system further includes Bonnett's hidden partition of memory 126b, 206b, which is "inaccessible to a user of appliance" and which, in my opinion, is a *system area that cannot be modified by the user* (e.g.,). Bonnett, Figs. 1-3, [0031]-[0033], [0036].

330. In Bonnett, the "hidden partition" of the memory is "operable to store one or more programs" and in the combined Andrews-Bonnett system 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. Accordingly, in my opinion, Andrews-Bonnett's client software is a *security application* that *utilizes code residing at least partially in the system area*.

331. Moreover, in the combined Andrews-Bonnett system, Andrews's client software would be otherwise unmodified and would, therefore, continue to perform the security operations described above in connection with the Security

Notification Limitations in Ground 1A. For example, the software would continue to receive a "reported device status" from the remote host computer that is "reported by an interest holder in portable computing device" to the host computer using "any suitable communications method," such as "via a telephone call, email, [or] online form." EX1005, 19:6-13.

332. Storing the client software in Bonnett's hidden partition would not affect these functions, and the software would continue to operate as described. As discussed above, while the software is stored in Bonnett's hidden partition, it cannot be modified. A POSITA would have understood that, during operation, Andrews's software is executed by the processor from memory. A POSITA would have understood that during execution Andrews's software receives messages containing information from other components in the computer system and acts on those messages pursuant to the software instructions in the hidden partition. Specifically, a POSITA would have understood that when a "reported status" is received from the host computer (e.g., as discussed in connection with the Periodic Communication Limitations (Section VII.A.3.f), Security Notification Limitations (Section VII.A.3.g), and Device Disabling Limitations (Section VII.A.3.h)), Andrews's client software is given access to data contained in the message and acts on the message by, e.g., updating the state of the software and causing the computer to perform the responsive action.

333. Thus, in my opinion, in the implementation where Andrews's client software is stored in Bonnett's hidden partition, the client software receives the reported device status from the host computer (i.e., *a notification from the security service from at least one of the servers*) via the hidden partition (i.e., *system area*), as claimed.

4. Independent Claim 9

a. Preamble 9[pre]

334. The preamble of Claim 9 recites "*A method for providing security for a mobile electronic device, the method comprising*."

335. In the combination of Andrews and Bonnett described above, Andrews's client software would be stored on Andrews's portable client electronic device using Bonnett's disclosed techniques to store the software program in a hidden partition invisible and inaccessible to users. This combination would meet the preamble of Claim 9 for the same reasons as Andrews alone.

b. Structural Limitation 9[A]

336. The Structural Limitation of Claim 9 recites "*wherein the mobile electronic device comprises non-volatile memory*."

337. The Structural Limitation of Claim 9 is substantially similar to the Structural Limitation of Claim 1. Thus, it is my opinion that the combination of Andrews and Bonnett discloses the Structural Limitation of Claim 9 for the same reasons discussed in connection with Claim 1.

c. Registration Limitation 9[B]

338. The Registration Limitation of Claim 9 recites "*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*."

339. The Registration Limitation of Claim 9 is substantially similar to the Registration Limitation of Claim 1. Thus, it is my opinion that the combination of Andrews and Bonnett discloses the Registration Limitation of Claim 9 for the same reasons discussed in connection with Claim 1.

d. Sending Identifying Information Limitation 9[C]

340. The Sending Identifying Information Limitation of Claim 9 recites "*automatically sending identifying information for the mobile electronic device from the mobile electronic device to the security service*."

341. The Sending Identifying Information Limitation of Claim 9 is substantially similar to the Sending Identifying Information Limitation of Claim 1. Thus, it is my opinion that the combination of Andrews and Bonnett discloses the Sending Identifying Information Limitation of Claim 9 for the same reasons discussed in connection with Claim 1.

e. Periodic Communication Limitation 9[D]

342. The Periodic Communication Limitation of Claim 9 recites "*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*."

343. The Periodic Communication Limitation of Claim 9 is substantially similar to the Periodic Communication Limitation of Claim 1. Thus, it is my opinion that the combination of Andrews and Bonnett discloses the Periodic Communication Limitation of Claim 9 for the same reasons discussed in connection with Claim 1.

f. Security Notification Limitation 9[E]

344. The Security Notification Limitation of Claim 9 recites "*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.*"

345. The Security Notification Limitation of Claim 9 is substantially similar to the Security Notification Limitation of Claim 1. Thus, it is my opinion

that the combination of Andrews and Bonnett discloses the Security Notification Limitation of Claim 9 for the same reasons discussed in connection with Claim 1.

g. Device Disabling Limitation 9[F]

346. The Device Disabling Limitation of Claim 9 recites "*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*."

347. The Device Disabling Limitation of Claim 9 is substantially similar to the Device Disabling Limitation of Claim 1. Thus, it is my opinion that the combination of Andrews and Bonnett discloses the Device Disabling Limitation of Claim 9 for the same reasons discussed in connection with Claim 1.

h. Copying User Data Limitation 9[G]

348. The Copying User Data Limitation of Claim 9 recites "*automatically causing at least some user data to be copied from the mobile electronic device to at least one of the servers*."

349. The Copying User Data Limitation of Claim 9 is substantially similar to the Copying User Data Limitation of Claim 1. Thus, it is my opinion that the combination of Andrews and Bonnett discloses the Copying User Data Limitation of Claim 9 for the same reasons discussed in connection with Claim 1.

i. Memory Area Limitation 9[H]

350. The Memory Area Limitation of Claim 9 recites "*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*." For the reasons I discuss below, the combination of Andrews and Bonnett discloses the Memory Area Limitation.

351. The Memory Area Limitation of Claim 9 is substantially similar to the Memory Area Limitation of Claim 1. Thus, it is my opinion that the combination of Andrews and Bonnett discloses the Memory Area Limitation of Claim 9 for the same reasons discussed in connection with Claim 1.

5. Independent Claim 17

a. Preamble 17[pre]

352. The preamble of Claim 17 recites "*An article of manufacture comprising:*"

353. In the combination of Andrews and Bonnett described above, Andrews's client software would be stored on Andrews's portable client electronic device using Bonnett's disclosed techniques to store the software program in a

hidden partition invisible and inaccessible to users. This combination would meet the preamble of Claim 17 for the same reasons as Andrews alone.

b. Structural Limitation 17[A]

354. The Structural Limitation of Claim 17 recites "*a non-transitory machine-readable storage medium; and . . . non-volatile memory in the mobile phone*."

355. The Structural Limitation of Claim 17 is substantially similar to the Structural Limitation of Claim 1. Thus, it is my opinion that the combination of Andrews and Bonnett discloses Structural Limitation of Claim 17 for the same reasons discussed in connection with Claim 1.

c. Security Application Limitation 17[B]

356. The Security Application Limitation of Claim 17 recites "*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*."

357. The Security Application Limitation of Claim 17 is substantially similar to the Security Application Limitation of Claim 1. Thus, it is my opinion that the combination of Andrews and Bonnett discloses the Security Application Limitation of Claim 17 for the same reasons discussed in connection with Claim 1.

d. Registration Limitation 17[C]

358. The Registration Limitation of Claim 17 recites "*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*."

359. The Registration Limitation of Claim 17 is substantially similar to the Registration Limitation of Claim 1. Thus, it is my opinion that the combination of Andrews and Bonnett discloses the Registration Limitation of Claim 17 for the same reasons discussed in connection with Claim 1.

e. Sending Identifying Information Limitation 17[D]

360. The Sending Identifying Information Limitation of Claim 17 recites "*automatically sending identifying information for the mobile electronic device from the mobile electronic device to the security service*."

361. The Sending Identifying Information Limitation of Claim 17 is substantially similar to the Sending Identifying Information Limitation of Claim 1. Thus, it is my opinion that the combination of Andrews and Bonnett discloses the Sending Identifying Information Limitation of Claim 17 for the same reasons discussed in connection with Claim 1.

f. Periodic Communication Limitation 17[E]

362. The Periodic Communication Limitation of Claim 17 recites "*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*."

363. The Periodic Communication Limitation of Claim 17 is substantially similar to the Periodic Communication Limitation of Claim 1. Thus, it is my opinion that the combination of Andrews and Bonnett discloses the Periodic Communication Limitation of Claim 17 for the same reasons discussed in connection with Claim 1.

g. Security Notification Limitation 17[F]

364. The Security Notification Limitation of Claim 17 recites "*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*."

365. The Security Notification Limitation of Claim 17 is substantially similar to the Security Notification Limitation of Claim 1. Thus, it is my opinion

that the combination of Andrews and Bonnett discloses the Security Notification Limitation of Claim 17 for the same reasons discussed in connection with Claim 1.

h. Device Disabling Limitation 17[G]

366. The Device Disabling Limitation of Claim 17 recites "*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*."

367. The Device Disabling Limitation of Claim 17 is substantially similar to the Device Disabling Limitation of Claim 1. Thus, it is my opinion that the combination of Andrews and Bonnett discloses the Device Disabling Limitation of Claim 17 for the same reasons discussed in connection with Claim 1.

i. Copying User Data Limitation 17[H]

368. The Copying User Data Limitation of Claim 17 recites "*automatically causing at least some user data to be copied from the mobile electronic device to at least one of the servers*."

369. The Copying User Data Limitation of Claim 17 is substantially similar to the Copying User Data Limitation of Claim 1. Thus, it is my opinion that the combination of Andrews and Bonnett discloses the Copying User Data Limitation of Claim 17 for the same reasons discussed in connection with Claim 1.

j. Memory Area Limitation 17[I]

370. The Memory Area Limitation of Claim 17 recites "*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.*"

371. The Memory Area Limitation of Claim 17 is substantially similar to the Memory Area Limitation of Claim 1. Thus, it is my opinion that the combination of Andrews and Bonnett discloses the Memory Area Limitation of Claim 17 for the same reasons discussed in connection with Claim 1.

6. Independent Claim 25

a. Preamble 25[pre]

372. The preamble of Claim 25 recites "*A method for providing security for a mobile electronic device, the method comprising:*"

373. In the combination of Andrews and Bonnett described above, Andrews's client software would be stored on Andrews's portable client electronic device using Bonnett's disclosed techniques to store the software program in a hidden partition invisible and inaccessible to users. This combination would meet the preamble of Claim 25 for the same reasons as Andrews alone.

b. Structural Limitation 25[A]

374. The Structural Limitation of Claim 25 recites "*wherein the mobile electronic device comprises non-volatile memory.*"

375. The Structural Limitation of Claim 25 is substantially similar to the Structural Limitation of Claim 1. Thus, it is my opinion that the combination of Andrews and Bonnett discloses the Structural Limitation of Claim 25 for the same reasons discussed in connection with Claim 1.

c. Registration Limitation 25[B]

376. The Registration Limitation of Claim 25 recites "*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*."

377. The Registration Limitation of Claim 25 is substantially similar to the Registration Limitation of Claim 1. Thus, it is my opinion that the combination of Andrews and Bonnett discloses the Registration Limitation of Claim 25 for the same reasons discussed in connection with Claim 1.

d. Sending Identifying Information Limitation 25[C]

378. The Sending Identifying Information Limitation of Claim 25 recites "*automatically sending identifying information for the mobile electronic device from the mobile electronic device to the security service*."

379. The Sending Identifying Information Limitation of Claim 25 is substantially similar to the Sending Identifying Information Limitation of Claim 1. Thus, it is my opinion that the combination of Andrews and Bonnett discloses the Sending Identifying Information Limitation of Claim 25 for the same reasons discussed in connection with Claim 1.

e. Security Notification Limitation 25[D]

380. The Security Notification Limitation of Claim 25 recites "*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*."

381. The Security Notification Limitation of Claim 25 is substantially similar to the Security Notification Limitation of Claim 1. Thus, it is my opinion that the combination of Andrews and Bonnett discloses the Security Notification Limitation of Claim 25 for the same reasons discussed in connection with Claim 1.

f. Device Disabling Limitation 25[E]

382. The Device Disabling Limitation of Claim 25 recites "*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*."

383. The Device Disabling Limitation of Claim 25 is substantially similar to the Device Disabling Limitation of Claim 1. Thus, it is my opinion that the combination of Andrews and Bonnett discloses the Device Disabling Limitation of Claim 25 for the same reasons discussed in connection with Claim 1.

g. Copying User Data Limitation 25[F]

384. The Copying User Data Limitation of Claim 25 recites "*automatically causing at least some user data to be copied from the mobile electronic device to at least one of the servers*."

385. The Copying User Data Limitation of Claim 25 is substantially similar to the Copying User Data Limitation of Claim 1. Thus, it is my opinion that the combination of Andrews and Bonnett discloses the Copying User Data Limitation of Claim 25 for the same reasons discussed in connection with Claim 1.

h. Deleting User Data Limitation 25[G]

386. The Deleting User Data Limitation of Claim 25 recites "*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*."

387.

i. Restoring User Data Limitation 25[H]

388. The Restoring User Data Limitation of Claim 25 recites "*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."

389.

j. Memory Area Limitation 25[I]

390. The Memory Area Limitation of Claim 25 recites "*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.*"

391. The Memory Area Limitation of Claim 25 is substantially similar to the Memory Area Limitation of Claim 1. Thus, it is my opinion that the combination of Andrews and Bonnett discloses the Memory Area Limitation of Claim 25 for the same reasons discussed in connection with Claim 1.

7. Dependent Claims 2, 10, 18

392. Claim 2 depends from claim 1, claim 10 depends from claim 9, and claim 18 depends from claim 17. These claims are substantially similar as shown in the comparison table provided above in Ground 1A.

393. The combination of Andrews and Bonnett meets the limitations of these claims for the same reasons as Andrews alone.

8. Dependent Claims 3, 11, 19

394. Claim 3 depends from claim 1, claim 11 depends from claim 9, and claim 19 depends from claim 17. These claims are substantially similar as shown in the comparison table provided above in Ground 1A.

395. The combination of Andrews and Bonnett meets the limitations of these claims for the same reasons as Andrews alone.

9. Dependent Claims 4, 12, 20

396. Claim 4 depends from claim 3, claim 12 depends from claim 11, and claim 20 depends from claim 19. These claims are substantially similar as shown in the comparison table provided above in Ground 1A.

397. The combination of Andrews and Bonnett meets the limitations of these claims for the same reasons as Andrews alone.

10. Dependent Claims 5, 16, 21

398. Claim 5 depends from claim 3, claim 16 depends from claim 11, and claim 21 depends from claim 19. These claims are substantially similar as shown in the comparison table provided above in Ground 1A.

399. The combination of Andrews and Bonnett meets the limitations of these claims for the same reasons as Andrews alone.

11. Dependent Claims 7, 15, 23

400. Claim 7 depends from claim 1, claim 15 depends from claim 9, and claim 23 depends from claim 17. These claims are substantially similar as shown in the comparison table provided above in Ground 1A.

401. The combination of Andrews and Bonnett meets the limitations of these claims for the same reasons as Andrews alone.

12. Dependent Claims 8, 16, 24

402. Claim 8 depends from claim 7, claim 16 depends from claim 15, and claim 24 depends from claim 23. These claims are substantially similar as shown in the comparison table provided above in Ground 1A.

403. The combination of Andrews and Bonnett meets the limitations of these claims for the same reasons as Andrews alone.

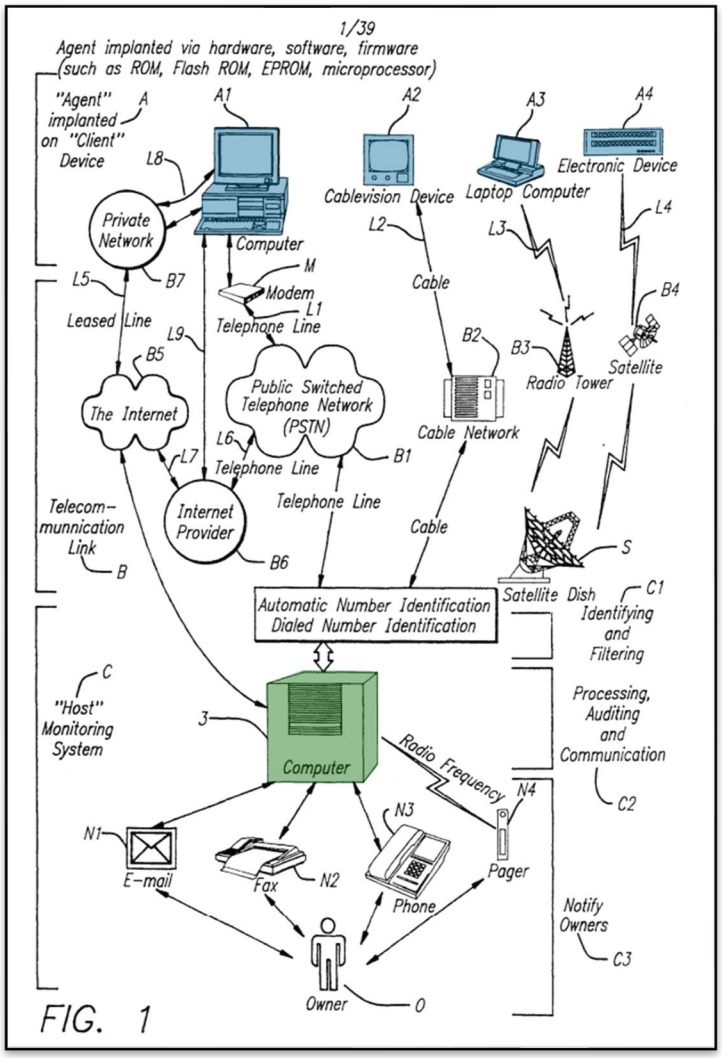
C. Ground 1C: Claims 1-5, 7-13, 15-21, and 23-25 Obvious over Andrews and Cotichini

1. Cotichini (EX1007): WIPO Pub. No. 1998/043151

404. From its face, Cotichini is an international application published under the Patent Cooperation Treaty (PCT) that published on October 1, 1998. Because Cotichini published in 1998, I understand that Cotichini qualifies as prior art even if the challenged claims are entitled to the August 23, 2003 filing date of Provisional Application No. 60/497,182 (*see* '649 patent, code (60)).

405. 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." Cotichini, (57).

406. Cotichini's system is very similar to those disclosed in the '649 patent and Andrews. For instance, as shown in the annotated Figure 1 below, Cotichini's system includes a one or more "**client device[s]**" that communicate via a network with a "**host monitoring system C**." Cotichini, 12:3-11.



407. Like in the ’649 patent and Andrews, Cotichini’s client device can be “laptop computer A3, or other type of electronic device A4 including a cellular telephone or personal digital assistant (PDA).” Cotichini, 12:12-15.

408. The “host monitoring system C sends and receives data packets from the client computer A1.” Cotichini, 12:17-18. The client device contacts the host computer periodically—“when a pre-defined time period has elapsed, or when a pre-determined event has occurred.” Cotichini, 21:4-6. The client device contains software (referred to as an “agent,” as discussed in greater detail below) that “contact[s] the host monitoring system C to report the identity, location, and other information relating to its associated client computer 10.” Cotichini, 20:3-6. The host computer uses this information to “determine whether the computer has been…reported lost or stolen,” Cotichini, 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 “placing either an automatic or manual call to the local authorities” or by initiating a “traceroute” to ascertain the location of the client device. Cotichini, 28:28-29:5, 30:24-33, 23:20-24:8, 31:29-32:27.

409. 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. Cotichini, 4:8-11. The agent operates

"without interfering with the regular operation of the device," Cotichini, 4:8-11, and is "designed to evade detection and resist attempts to disable it by an unauthorized user," Cotichini, 4:21-23. For instance, the software "remains hidden to the operating system," making it "tamper-proof." Cotichini, 36:13-16, 58:22-23.

410. The agent resists any attempts to modify or delete it, as explained in the excerpt from Cotichini below:

> The system remains transparent to an unauthorized user via implementation of well—known deflection methods. Attempts to read or write to the location where the Agent has been installed are deflected in Order to prevent discovery Of the agent. When read attempts are made to the Agent location the system generates meaningless bytes of data to be returned to the user. When 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. However, the data is not really stored, and thus the Agent is preserved. The Agent, in order to remain hidden to the user, will not interfere with any running applications unless designed to interfere.

Cotichini, 24:9-21.

411. 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." Cotichini, 4:24-32. Keeping the agent "hidden" in this manner also helps to "reduce the risk of [the agent] being disabled…" Cotichini, 2:27-30.

412. Cotichini describes various embodiments for implementing its agent. The agent can be " implemented in the firmware or software" of the client device, Cotichini, 19:25-26, can be "implemented in any component of" the device, "such as the DSP in a modem or the CPU in the computer," Cotichini, 19:26-29, and/or can be "implemented in the circuitry of any hardware device capable of establishing a communication link through sending and/or receiving packets of data," Cotichini, 19:29-20:2.

413. 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." Cotichini, 57:7-14. In operation, the "Agent is loaded from the ROM after the CPU registers are saved." Cotichini, 38:19-25. The agent is loaded before the operating system. *See* Cotichini, Fig. 14C, 25:15-23.

414. In another example, the agent is installed in the "partition boot sector" of the client device. In operation, the "computer 10 is powered on and the loading sequence begins." Cotichini, 37:1-11. After the "Power-On Self Test (POST) routine," the "partition boot sector is loaded" and "the agent is loaded with the operating system partition boot sector 94." Cotichini, 37:4-13, 38:8-13. The agent is loaded before the operating system. Cotichini, Fig. 14C.

415. In another example, the agent is a "Modem Agent" and is "installed into the 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." Cotichini, 42:16-21. The Modem agent can be "embedded into the modem Flash ROM or DSP by the manufacturer." Cotichini, 42:21-25. The modem agent operates "independent of the software running on the computer including the operating system," Cotichini, 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." Cotichini, 43:1-10. Specifically, even if a computer is "stripped for parts, the Modem Agent will still be able to be located." Cotichini, 43:1-10. This is particularly valuable when the Modem Agent is embedded "onto the motherboard of the computer" because the motherboard is the "most important component of the computer." Cotichini, 43:1-10.

416. The **Modem Agent** is depicted in example Figure 8A, which shows the Agent "installed into the Flash ROM" of the modem and shows that the modem is "coupled to the CPU 832" of the client device. Cotichini, 42:17-21, 43:21-22. The modem is further connected to a network (e.g., PSTN 813), which allows the modem to "communicate with the Host Monitoring System through the PSTN 813 at scheduled times without the involvement of the PC processor." Cotichini, 42:25-27.

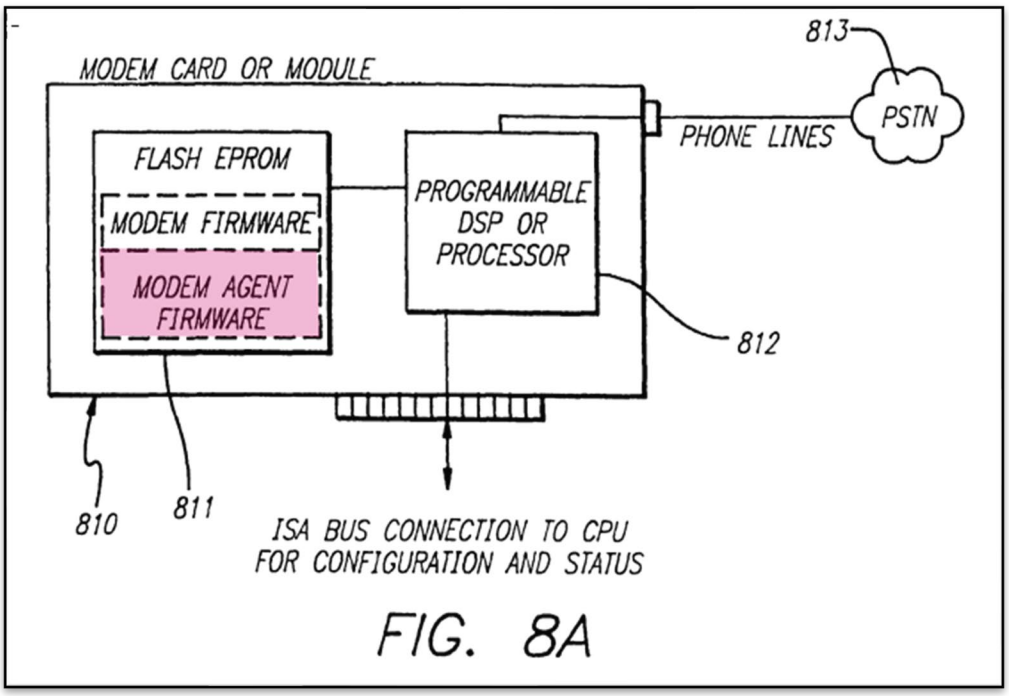


FIG. 8A

417. 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." Cotichini, 24:9-10. 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." Cotichini, 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 "the data is not really stored, and thus the Agent is preserved." Cotichini, 24:15-18.

2. The Andrews-Cotichini Combination

418. A POSITA would have had multiple reasons to combine Andrews and Cotichini, which both disclose security systems for remotely tracking a portable electronic device and are, for at least that reason, analogous art.

419. In my opinion, a POSITA would have had several reasons to combine Andrews and Cotichini by storing Andrews's security software so that it is hidden and unchangeable to a user using the methods taught by Cotichini's installation of a security agent. *See* Cotichini, 4:8-11, 4:21-23, 24:9-21, 36:13-16, 58:22-23 (describing installation of agent). Cotichini describes a number of techniques for installing software (or, in Cotichini's words, an "agent") in this manner (i.e., so that it is hidden and unchangeable by users), and a POSITA would have had reason several reasons to combine Andrews and Cotichini using any of the disclosed techniques.

420. First, a POSITA would have been motivated to combine Andrews and Cotichini for many of the same reasons discussed above for Andrews-Bonnett. 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." Andrews, 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)." Andrews, 10:3-14. As discussed for Andrews and Bonnett, the flexibility of Andrews's disclosure with respect to where and how its client software is installed provides compatibility between Andrews and Cotichini.

421. Andrews also teaches that when its client software contacts the host computer, it does so "surreptitiously" and "silently, without interrupting any activity of the user." Andrews, 31:21-32:8. And, if the user attempts to "reboot" the device, the security software "cause[s] screen-blocking program 114 to execute, thereby again restricting user access." Andrews, 46:17-22. This, too, applies to and motivates the combination of Andrews and Cotichini for the same reasons as Andrews and Bonnett because, like Bonnett, Cotichini offers mechanisms to protect software from a user's attempts to disable, delete, or bypass the software. Indeed, Cotichini discloses that its agent operates surreptitiously, further motivating the combination. Cotichini, 4:8-11, 4:21-22, 24:19-21 (agent operates "without interfering with the regular operation of the device," is "designed to evade detection," and "will not interfere with any running applications unless designed to interfere").

422. Second, a POSITA would have recognized the benefits of using Cotichini's secretive storage techniques to increase the chances that a finder or thief would not be able to delete Andrews's security software. Contemporaneous

publications like Cain and Howard describe systems for protecting a security program so that a user cannot prevent such security software from running and protecting the computer.

423. Moreover, Cotichini itself discloses a system for implementing a security program in a protected area of memory and describes the techniques used to achieve this protection as being "well-known." Cotichini, 24:9-10. Accordingly, Cotichini expressly motivates the combination of Andrews and Cotichini because it provides an independent reason to use Cotichini's software-protection techniques specifically in a system for recovering/tracking lost or stolen portable devices.

424. Third, a POSITA would have had a reasonable expectation of success in this combination. One reason that a POSITA would have had a reasonable expectation of success is that Cotichini provides several different ways to store an agent so that it may not be changed by a user, thus providing a POSITA the flexibility to pick the one(s) that would be most readily implemented in Andrews.

425. For instance, a POSITA would have had a reasonable expectation of success in combining Andrews and Cotichini by installing Andrews's security software in the same manner as Cotichini's "Modem Agent." 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]." Andrews, 11:10-15. Thus, to combine Andrews and Cotichini, a POSITA would have been able to install

Andrews's software as a Modem Agent on modem 50, where it would perform the same functions as performed in Andrews's independent system (e.g., contacting a host, sending identifying information, receiving notifications, etc.).

426. As another example, a POSITA would have had a reasonable expectation of success in combining Andrews and Cotichini by installing Andrews's security software in the same manner as Cotichini's "ROM Agent." Specifically, a POSITA would have been able to install Andrews's agent by "incorporat[ing]" it "into the ROM," as taught in Cotichini. Indeed, Andrews already discloses that its security software can be installed in the device ROM and loaded during start-up of the portable computing device. Andrews, 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. Cotichini, 38:19-25, Fig. 14C, 25:15-23. Thus, to combine Andrews and Cotichini in this manner would simply be an improvement upon a technique already disclosed in Andrews alone, and the combination would have been using a known technique (installing software in ROM) to improve similar systems (security systems for portable devices) in the same way (by installing software in memory that cannot be modified).

427. Beyond these two examples, every implementation described in Cotichini involves installing the security agent in a conventional area of computer

memory (e.g., a CPU, a hard drive, hardware, etc.), and Cotichini teaches that its system can be "added to existing computers without physical alteration." Cotichini, 57:7-8. Thus, it is my opinion that a POSITA would have had an expectation of success in combining Andrews and Cotichini using any of Cotichini's methods for storing a security agent such that it is unchangeable by users.

3. Independent Claim 1

a. Preamble 1[pre]

428. The preamble of Claim 1 recites "*A mobile electronic device, comprising*."

429. In the combination of Andrews and Cotichini described above, Andrews's client software would be installed on Andrews's portable client electronic device to be hidden and unchangeable to a user, as taught by Cotichini's installation of a security agent. This combination would meet the preamble of Claim 1 for the same reasons as Andrews alone.

b. Structural Limitations 1[A] and 1[B]

430. The Structural Limitations of Claim 1 recites "*a processor*" and "*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.*"

431. In the combination of Andrews and Cotichini described above, Andrews's client software would be installed on Andrews's portable client

electronic device to be hidden and unchangeable to a user, as taught by Cotichini's installation of a security agent. This combination would meet the Structural Limitations of Claim 1 for the same reasons as Andrews alone.

c. Security Application Limitation 1[C]

432. The Security Application Limitation of Claim 1 recites "*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*."

433. In the combination of Andrews and Cotichini described above, Andrews's client software would be installed on Andrews's portable client electronic device to be hidden and unchangeable to a user, as taught by Cotichini's installation of a security agent. This combination would meet the Security Application Limitation of Claim 1 for the same reasons as Andrews alone.

d. Registration Limitation 1[D]

434. The Registration Limitation of Claim 1 recites "*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*."

435. In the combination of Andrews and Cotichini described above, Andrews's client software would be installed on Andrews's portable client electronic device to be hidden and unchangeable to a user, as taught by Cotichini's

installation of a security agent. This combination would meet the Registration Limitation of Claim 1 for the same reasons as Andrews alone.

e. Sending Identifying Information Limitation 1[E]

436. The Sending Identifying Information Limitation of Claim 1 recites "*causing the mobile electronic device to automatically send identifying information for the mobile electronic device to the security service*."

437. In the combination of Andrews and Cotichini described above, Andrews's client software would be installed on Andrews's portable client electronic device to be hidden and unchangeable to a user, as taught by Cotichini's installation of a security agent. This combination would meet the Sending Identifying Information Limitation of Claim 1 for the same reasons as Andrews alone.

f. Periodic Communication Limitation 1[F]

438. The Periodic Communication Limitation of Claim 1 recites "*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*."

439. In the combination of Andrews and Cotichini described above, Andrews's client software would be installed on Andrews's portable client

electronic device to be hidden and unchangeable to a user, as taught by Cotichini's installation of a security agent. This combination would meet the Periodic Communication Limitation of Claim 1 for the same reasons as Andrews alone.

g. Security Notification Limitation 1[G]

440. The Security Notification Limitation of Claim 1 recites "*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*."

441. In the combination of Andrews and Cotichini described above, Andrews's client software would be installed on Andrews's portable client electronic device to be hidden and unchangeable to a user, as taught by Cotichini's installation of a security agent. This combination would meet the Security Notification Limitation of Claim 1 for the same reasons as Andrews alone.

h. Device Disabling Limitation 1[H]

442. The Device Disabling Limitation of Claim 1 recites "*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*."

443. In the combination of Andrews and Cotichini described above, Andrews's client software would be installed on Andrews's portable client electronic device to be hidden and unchangeable to a user, as taught by Cotichini's installation of a security agent. This combination would meet the Device Disabling Limitation of Claim 1 for the same reasons as Andrews alone.

i. Copying User Data Limitation 1[I]

444. The Copying User Data Limitation of Claim 1 recites "*automatically causing at least some user data to be copied from the mobile electronic device to at least one of the servers*."

445. In the combination of Andrews and Cotichini described above, Andrews's client software would be installed on Andrews's portable client electronic device to be hidden and unchangeable to a user, as taught by Cotichini's installation of a security agent. This combination would meet the Copying User Data Limitation of Claim 1 for the same reasons as Andrews alone.

j. Memory Area Limitation 1[J]

446. The Memory Area Limitation of Claim 1 recites "*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."

447. In my opinion, the Andrews and Cotichini combined system includes the claimed non-volatile memory. Above, I described a number of different implementations available to a POSITA combining Andrews and Cotichini. Each includes a non-volatile memory. For example, in the combination where Andrew's client software is installed in the same manner as Cotichini's Modem Agent, the software would be "embedded into the modem Flash ROM," which as I explained in my technology background Section IV.B is a form of non-volatile memory. Cotichini, 42:21-25.

448. Similarly, if Andrews's client software is installed in the same manner as Cotichini's ROM Agent, the software would be "incorporated into the ROM" of the device, which as I explained in my technology background Section IV.B is also a form of non-volatile memory. Cotichini, 57:7-14.

449. Likewise, if Andrews's client software is installed in the same manner as Cotichini's agent in the "partition boot sector," the software would be stored in the device's hard drive, which as I explained in my technology background Section IV.B is also a form of non-volatile memory. Cotichini, 37:4-13, 38:8-13.

450. Once installed as taught in each of the above-described ways disclosed in Cotichini, Andrews's software is protected from modification. As Cotichini explains:

> The system remains transparent to an unauthorized user via implementation of well—known deflection methods. Attempts to read or write to the location where the Agent has been installed are deflected in order to prevent discovery of the agent. When read attempts are made to the Agent location the system generates meaningless bytes of data to be returned to the user. When 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. However, the data is not really stored, and thus the Agent is preserved. The Agent, in order to remain hidden to the user, will not interfere with any running applications unless designed to interfere.

Cotichini, 24:9-21.

451. Thus, as Cotichini explains, the area of memory in which its agent is installed cannot be modified by a user. Accordingly, in the Andrews-Cotichini combination, in which the software is installed using the techniques disclosed in Cotichini, the security software is installed is a *system area* that cannot be rewritten (or, *modified*) *by a user*.

452. Moreover, in the described combination of Andrews and Cotichini, the client software receives a "reported device status" from the remote host computer in the same manner as discussed in connection with Andrews in Ground 1A. Andrews, 19:6-13; *supra* Sections VII.A.3.f-h. In the combined system, this software would, as discussed above, be installed in an area of memory "protected

by well-known deflection methods" that prevent modification of the agent. When performing these operations, the software is executed by a processor from this memory and, during execution, is given access to the reported device status sent from the host computer. Therefore, in my opinion, when the client software receives the device status from the host computer (i.e., *a notification from the security service*), it receives that status *via the system area* in which it is installed.

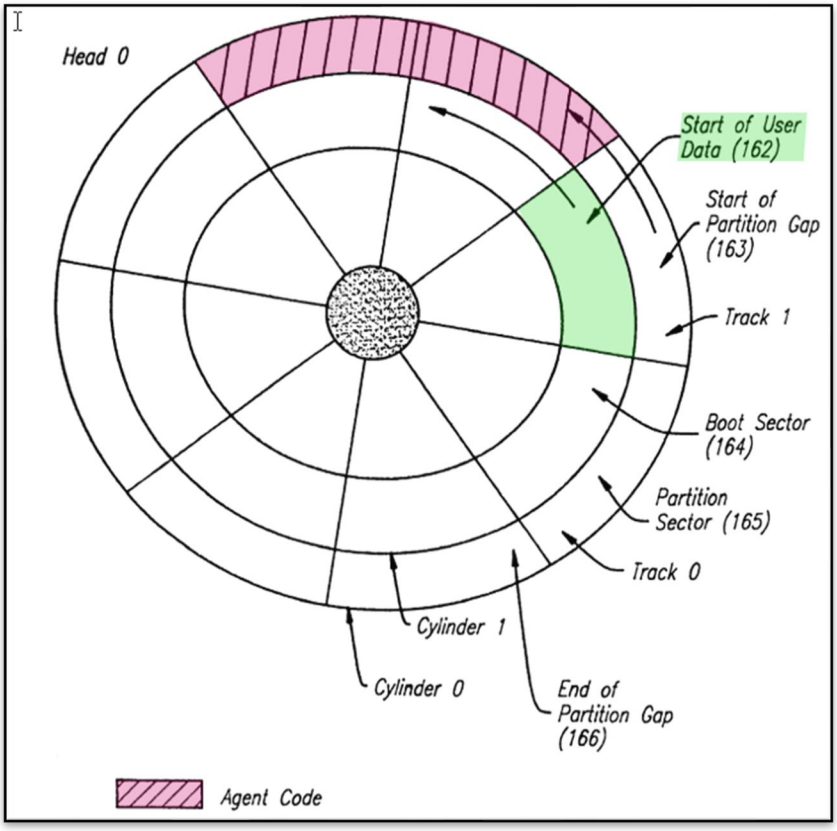
453. As one example of how the software receives the device status via the system area, consider the implementation where Andrews's software is installed in the same manner as Cotichini's Modem Agent. In this implementation, the client software would be installed in Andrews's modem 50, which, as Andrews teaches, is the device's "interface to the monitoring server" and which "communicat[es] with the host monitoring server directly," Andrews, 45:10-11, 46:13-14. In this implementation of Andrews-Cotichini, the modem agent would send and receive messages to and from the host computer during operation of the client software. When receiving the reported device status from the server via the modem in which the software is installed, the software would in my opinion receive *a notification from the security service…via the system area*.

454. In the combination of Andrews and Cotichini, the client device would also include a *changeable area* of non-volatile memory. Specifically, as discussed above in connection with the Memory Limitations of Ground 1A, Andrews

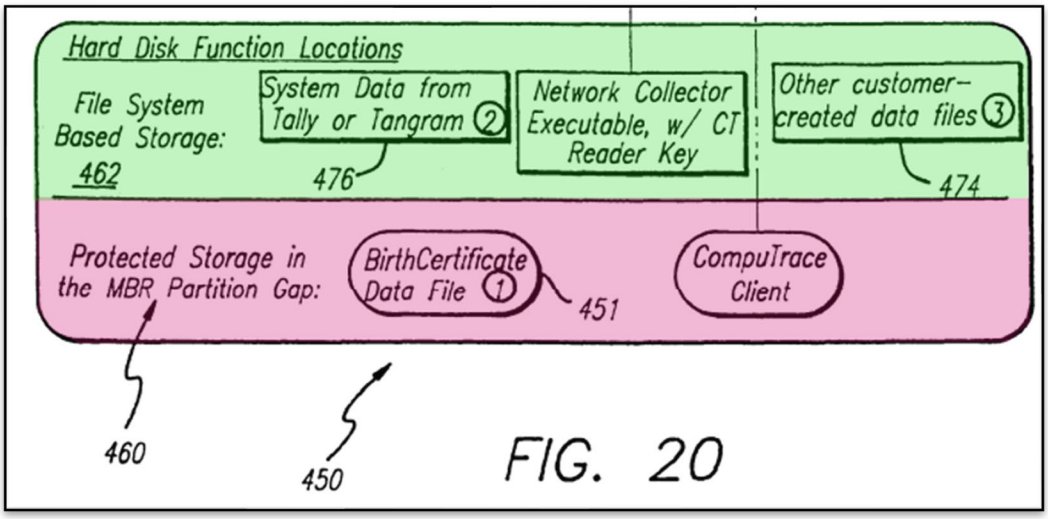
discloses a changeable area of memory in which the user's "files" and/or "folders" are stored. This area of memory stores files/folders that can be retrieved and deleted from the device by the host computer, as discussed above in connection with the RETRIEVE FILE and DELETE FILE operations in Ground 1A. This *changeable area* of memory would store files/folders like the example "C:\files\importantfile.doc" disclosed in Andrews. For the reasons discussed in Ground 1A, this area of memory remains changeable to a user to allow users to store and modify their personal files on the device.

455. Andrews's disclosure of a changeable area in which to store user files is consistent with the various implementations of Cotichini's agent. Specifically, Cotichini also discloses retaining a changeable area of memory alongside the protected area of memory storing the agent, which in my opinion would further support combining Andrews and Cotichini in a manner that preserves Andrews's changeable memory.

456. For example, Cotichini's Figure 14H depicts a hard disk containing both protected **Agent Code** and **User Data**:



457. Cotichini's Figure 20 also 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:



458. These examples in Cotichini demonstrate that Cotichini's agent-installation techniques are compatible with a computing device having multiple areas of memory, one of which is changeable and the other of which is a system area that cannot be modified by a user.

4. Independent Claim 9

a. Preamble 9[pre]

459. The preamble of Claim 9 recites "*A method for providing security for a mobile electronic device, the method comprising*."

460. In the combination of Andrews and Cotichini described above, Andrews's client software would be installed on Andrews's portable client electronic device to be hidden and unchangeable to a user, as taught by Cotichini's installation of a security agent. This combination would meet the preamble of Claim 9 for the same reasons as Andrews alone.

b. Structural Limitation 9[A]

461. The Structural Limitation of Claim 9 recites "*wherein the mobile electronic device comprises non-volatile memory*."

462. The Structural Limitation of Claim 9 is substantially similar to the Structural Limitation of Claim 1. Thus, it is my opinion that the combination of Andrews and Cotichini discloses the Structural Limitation of Claim 9 for the same reasons discussed in connection with Claim 1.

c. Registration Limitation 9[B]

463. The Registration Limitation of Claim 9 recites "*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*."

464. The Registration Limitation of Claim 9 is substantially similar to the Registration Limitation of Claim 1. Thus, it is my opinion that the combination of Andrews and Cotichini discloses the Registration Limitation of Claim 9 for the same reasons discussed in connection with Claim 1.

d. Sending Identifying Information Limitation 9[C]

465. The Sending Identifying Information Limitation of Claim 9 recites "*automatically sending identifying information for the mobile electronic device from the mobile electronic device to the security service*."

466. The Sending Identifying Information Limitation of Claim 9 is substantially similar to the Sending Identifying Information Limitation of Claim 1. Thus, it is my opinion that the combination of Andrews and Cotichini discloses the Sending Identifying Information Limitation of Claim 9 for the same reasons discussed in connection with Claim 1.

e. Periodic Communication Limitation 9[D]

467. The Periodic Communication Limitation of Claim 9 recites "*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*."

468. The Periodic Communication Limitation of Claim 9 is substantially similar to the Periodic Communication Limitation of Claim 1. Thus, it is my opinion that the combination of Andrews and Cotichini discloses the Periodic Communication Limitation of Claim 9 for the same reasons discussed in connection with Claim 1.

f. Security Notification Limitation 9[E]

469. The Security Notification Limitation of Claim 9 recites "*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.*"

470. The Security Notification Limitation of Claim 9 is substantially similar to the Security Notification Limitation of Claim 1. Thus, it is my opinion

that the combination of Andrews and Cotichini discloses the Security Notification Limitation of Claim 9 for the same reasons discussed in connection with Claim 1.

g. Device Disabling Limitation 9[F]

471. The Device Disabling Limitation of Claim 9 recites "*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*."

472. The Device Disabling Limitation of Claim 9 is substantially similar to the Device Disabling Limitation of Claim 1. Thus, it is my opinion that the combination of Andrews and Cotichini discloses the Device Disabling Limitation of Claim 9 for the same reasons discussed in connection with Claim 1.

h. Copying User Data Limitation 9[G]

473. The Copying User Data Limitation of Claim 9 recites "*automatically causing at least some user data to be copied from the mobile electronic device to at least one of the servers*."

474. The Copying User Data Limitation of Claim 9 is substantially similar to the Copying User Data Limitation of Claim 1. Thus, it is my opinion that the combination of Andrews and Cotichini discloses the Copying User Data Limitation of Claim 9 for the same reasons discussed in connection with Claim 1.

i. Memory Area Limitation 9[H]

475. The Memory Area Limitation of Claim 9 recites "*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*." For the reasons I discuss below, the combination of Andrews and Cotichini discloses the Memory Area Limitation.

476. The Memory Area Limitation of Claim 9 is substantially similar to the Memory Area Limitation of Claim 1. Thus, it is my opinion that the combination of Andrews and Cotichini discloses the Memory Area Limitation of Claim 9 for the same reasons discussed in connection with Claim 1.

5. Independent Claim 17

a. Preamble 17[pre]

477. The preamble of Claim 17 recites "*An article of manufacture comprising:*"

478. In the combination of Andrews and Cotichini described above, Andrews's client software would be installed on Andrews's portable client electronic device to be hidden and unchangeable to a user, as taught by Cotichini's

installation of a security agent. This combination would meet the preamble of Claim 17 for the same reasons as Andrews alone.

b. Structural Limitation 17[A]

479. The Structural Limitation of Claim 17 recites "*a non-transitory machine-readable storage medium; and . . . non-volatile memory in the mobile phone*."

480. The Structural Limitation of Claim 17 is substantially similar to the Structural Limitation of Claim 1. Thus, it is my opinion that the combination of Andrews and Cotichini discloses Structural Limitation of Claim 17 for the same reasons discussed in connection with Claim 1.

c. Security Application Limitation 17[B]

481. The Security Application Limitation of Claim 17 recites "*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.*"

482. The Security Application Limitation of Claim 17 is substantially similar to the Security Application Limitation of Claim 1. Thus, it is my opinion that the combination of Andrews and Cotichini discloses the Security Application Limitation of Claim 17 for the same reasons discussed in connection with Claim 1.

d. Registration Limitation 17[C]

483. The Registration Limitation of Claim 17 recites "*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*."

484. The Registration Limitation of Claim 17 is substantially similar to the Registration Limitation of Claim 1. Thus, it is my opinion that the combination of Andrews and Cotichini discloses the Registration Limitation of Claim 17 for the same reasons discussed in connection with Claim 1.

e. Sending Identifying Information Limitation 17[D]

485. The Sending Identifying Information Limitation of Claim 17 recites "*automatically sending identifying information for the mobile electronic device from the mobile electronic device to the security service*."

486. The Sending Identifying Information Limitation of Claim 17 is substantially similar to the Sending Identifying Information Limitation of Claim 1. Thus, it is my opinion that the combination of Andrews and Cotichini discloses the Sending Identifying Information Limitation of Claim 17 for the same reasons discussed in connection with Claim 1.

f. Periodic Communication Limitation 17[E]

487. The Periodic Communication Limitation of Claim 17 recites "*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*."

488. The Periodic Communication Limitation of Claim 17 is substantially similar to the Periodic Communication Limitation of Claim 1. Thus, it is my opinion that the combination of Andrews and Cotichini discloses the Periodic Communication Limitation of Claim 17 for the same reasons discussed in connection with Claim 1.

g. Security Notification Limitation 17[F]

489. The Security Notification Limitation of Claim 17 recites "*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*."

490. The Security Notification Limitation of Claim 17 is substantially similar to the Security Notification Limitation of Claim 1. Thus, it is my opinion

that the combination of Andrews and Cotichini discloses the Security Notification Limitation of Claim 17 for the same reasons discussed in connection with Claim 1.

h. Device Disabling Limitation 17[G]

491. The Device Disabling Limitation of Claim 17 recites "*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*."

492. The Device Disabling Limitation of Claim 17 is substantially similar to the Device Disabling Limitation of Claim 1. Thus, it is my opinion that the combination of Andrews and Cotichini discloses the Device Disabling Limitation of Claim 17 for the same reasons discussed in connection with Claim 1.

i. Copying User Data Limitation 17[H]

493. The Copying User Data Limitation of Claim 17 recites "*automatically causing at least some user data to be copied from the mobile electronic device to at least one of the servers*."

494. The Copying User Data Limitation of Claim 17 is substantially similar to the Copying User Data Limitation of Claim 1. Thus, it is my opinion that the combination of Andrews and Cotichini discloses the Copying User Data Limitation of Claim 17 for the same reasons discussed in connection with Claim 1.

j. Memory Area Limitation 17[I]

495. The Memory Area Limitation of Claim 17 recites "*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.*"

496. The Memory Area Limitation of Claim 17 is substantially similar to the Memory Area Limitation of Claim 1. Thus, it is my opinion that the combination of Andrews and Cotichini discloses the Memory Area Limitation of Claim 17 for the same reasons discussed in connection with Claim 1.

6. Independent Claim 25

a. Preamble 25[pre]

497. The preamble of Claim 25 recites "*A method for providing security for a mobile electronic device, the method comprising:*" For the reasons I discuss below, the combination of Andrews and Cotichini discloses the subject matter of the preamble.

498. In the combination of Andrews and Cotichini described above, Andrews's client software would be installed on Andrews's portable client electronic device to be hidden and unchangeable to a user, as taught by Cotichini's installation of a security agent. This combination would meet the preamble of Claim 25 for the same reasons as Andrews alone.

b. Structural Limitation 25[A]

499. The Structural Limitation of Claim 25 recites "*wherein the mobile electronic device comprises non-volatile memory.*"

500. The Structural Limitation of Claim 25 is substantially similar to the Structural Limitation of Claim 1. Thus, it is my opinion that the combination of Andrews and Cotichini discloses the Structural Limitation of Claim 25 for the same reasons discussed in connection with Claim 1.

c. Registration Limitation 25[B]

501. The Registration Limitation of Claim 25 recites "*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*."

502. The Registration Limitation of Claim 25 is substantially similar to the Registration Limitation of Claim 1. Thus, it is my opinion that the combination of Andrews and Cotichini discloses the Registration Limitation of Claim 25 for the same reasons discussed in connection with Claim 1.

d. Sending Identifying Information Limitation 25[C]

503. The Sending Identifying Information Limitation of Claim 25 recites "*automatically sending identifying information for the mobile electronic device from the mobile electronic device to the security service*."

504. The Sending Identifying Information Limitation of Claim 25 is substantially similar to the Sending Identifying Information Limitation of Claim 1. Thus, it is my opinion that the combination of Andrews and Cotichini discloses the Sending Identifying Information Limitation of Claim 25 for the same reasons discussed in connection with Claim 1.

e. Security Notification Limitation 25[D]

505. The Security Notification Limitation of Claim 25 recites "*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*."

506. The Security Notification Limitation of Claim 25 is substantially similar to the Security Notification Limitation of Claim 1. Thus, it is my opinion that the combination of Andrews and Cotichini discloses the Security Notification Limitation of Claim 25 for the same reasons discussed in connection with Claim 1.

f. Device Disabling Limitation 25[E]

507. The Device Disabling Limitation of Claim 25 recites "*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*."

508. The Device Disabling Limitation of Claim 25 is substantially similar to the Device Disabling Limitation of Claim 1. Thus, it is my opinion that the combination of Andrews and Cotichini discloses the Device Disabling Limitation of Claim 25 for the same reasons discussed in connection with Claim 1.

g. Copying User Data Limitation 25[F]

509. The Copying User Data Limitation of Claim 25 recites "*automatically causing at least some user data to be copied from the mobile electronic device to at least one of the servers*."

510. The Copying User Data Limitation of Claim 25 is substantially similar to the Copying User Data Limitation of Claim 1. Thus, it is my opinion that the combination of Andrews and Cotichini discloses the Copying User Data Limitation of Claim 25 for the same reasons discussed in connection with Claim 1.

h. Deleting User Data Limitation 25[G]

511. The Deleting User Data Limitation of Claim 25 recites "*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*."

512. In the combination of Andrews and Cotichini described above, Andrews's client software would be installed on Andrews's portable client electronic device to be hidden and unchangeable to a user, as taught by Cotichini's

installation of a security agent. This combination would meet the Deleting User Data Limitation of Claim 25 for the same reasons as Andrews alone.

i. Restoring User Data Limitation 25[H]

513. The Restoring User Data Limitation of Claim 25 recites "*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*."

514. In the combination of Andrews and Cotichini described above, Andrews's client software would be installed on Andrews's portable client electronic device to be hidden and unchangeable to a user, as taught by Cotichini's installation of a security agent. This combination would meet the Restoring User Data Limitation of Claim 25 for the same reasons as Andrews alone.

j. Memory Area Limitation 25[I]

515. The Memory Area Limitation of Claim 25 recites "*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.*"

516. The Memory Area Limitation of Claim 25 is substantially similar to the Memory Area Limitation of Claim 1. Thus, it is my opinion that the combination of Andrews and Cotichini discloses the Memory Area Limitation of Claim 25 for the same reasons discussed in connection with Claim 1.

7. Dependent Claims 2, 10, 18

517. Claim 2 depends from claim 1, claim 10 depends from claim 9, and claim 18 depends from claim 17. These claims are substantially similar as shown in the comparison table provided above in Ground 1A.

518. In the combination of Andrews and Cotichini described above, Andrews's client software would be installed on Andrews's portable client electronic device to be hidden and unchangeable to a user, as taught by Cotichini's installation of a security agent. This combination would meet Claims 2, 10, 18 for the same reasons as Andrews alone.

8. Dependent Claims 3, 11, 19

519. Claim 3 depends from claim 1, claim 11 depends from claim 9, and claim 19 depends from claim 17. These claims are substantially similar as shown in the comparison table provided above in Ground 1A.

520. The combination of Andrews and Cotichini meets the limitations of these claims for the same reasons as Andrews alone.

9. Dependent Claims 4, 12, 20

521. Claim 4 depends from claim 3, claim 12 depends from claim 11, and claim 20 depends from claim 19. These claims are substantially similar as shown in the comparison table provided above in Ground 1A.

522. The combination of Andrews and Cotichini meets the limitations of these claims for the same reasons as Andrews alone.

10. Dependent Claims 5, 16, 21

523. Claim 5 depends from claim 3, claim 16 depends from claim 11, and claim 21 depends from claim 19. These claims are substantially similar as shown in the comparison table provided above in Ground 1A.

524. The combination of Andrews and Cotichini meets the limitations of these claims for the same reasons as Andrews alone.

11. Dependent Claims 7, 15, 23

525. Claim 7 depends from claim 1, claim 15 depends from claim 9, and claim 23 depends from claim 17. These claims are substantially similar as shown in the comparison table provided above in Ground 1A.

526. In the combination of Andrews and Cotichini described above, Andrews's client software would be installed on Andrews's portable client electronic device to be hidden and unchangeable to a user, as taught by Cotichini's installation of a security agent. This combination would meet Claims 7, 15, 23 for the same reasons as Andrews alone.

12. Dependent Claims 8, 16, 24

527. Claim 8 depends from claim 7, claim 16 depends from claim 15, and claim 24 depends from claim 23. These claims are substantially similar as shown in the comparison table provided above in Ground 1A.

528. In the combination of Andrews and Cotichini described above, Andrews's client software would be installed on Andrews's portable client electronic device to be hidden and unchangeable to a user, as taught by Cotichini's installation of a security agent. This combination would meet Claims 8, 16, 24 for the same reasons as Andrews alone.

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

1. Hayward (EX1008): UK Pat. App. No. GB2369205A

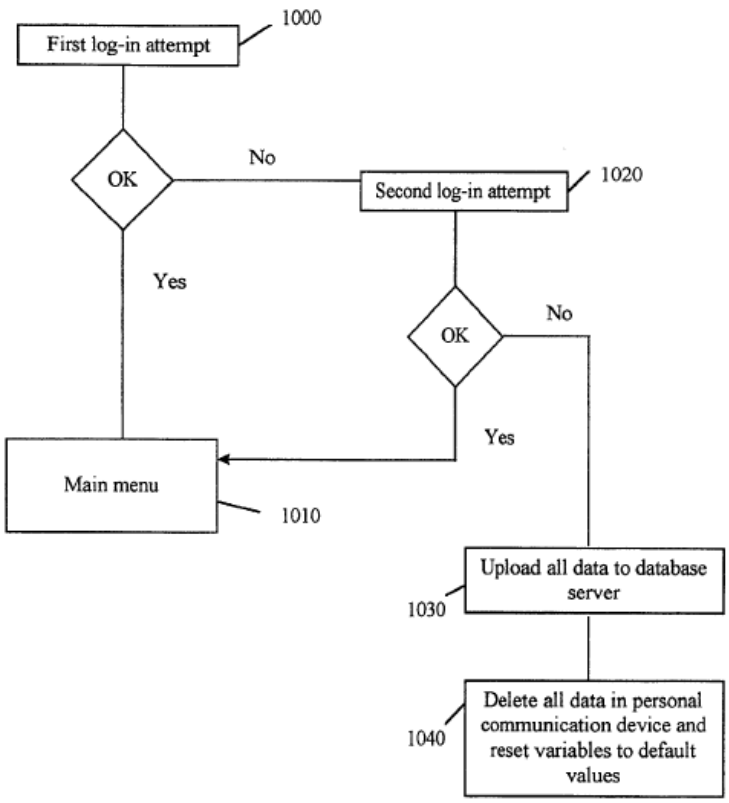
529. From its face, Hayward is a United Kingdom Patent Application that was filed on November 17, 2000. Because Hayward published in May 2002 from an application filed in November 2000, I understand that Hayward qualifies as prior art even if the challenged claims are entitled to the August 23, 2003 filing date of Provisional Application No. 60/497,182 (*see* '649 patent, code (60)). I understand that Hayward was not cited or otherwise made of record during prosecution of the '649 patent. *See* '649 patent, code (56) (references cited). during prosecution of the '649 patent. *See* '649 patent, code (56) (references cited).

530. Hayward discloses a "personal data device" storing "personal data" and "data protection software." Hayward, 1:23-2:4. The device may be a "mobile telephone" or "PDA." Hayward, 9:24-28. 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 10." Hayward, 20:28-21:2.

531. When a user "first log[s] into the personal data device," the user is required to "register the personal data device with the Internet database server." Hayward, 14:17-19. The "database server…performs an important function when a personal data device is missing." Hayward, 21:24-25. Specifically, a device may be "reported missing by contacting the database server via the Internet or telephone." Hayward, 21:27-28 When the database server receives such a report, it "seeks to contact the missing device…in a manner undetectable to a user, for example by sending a SMS message." Hayward, 21:25-30. When a device is reported missing, 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." Hayward, 22:5-9. In certain situations, the server may 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." Hayward, 22:9-12.

532. Additionally, using Hayward's data protection software, 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." Hayward, 23:17-19. In response to an unauthorized attempt to access the device, "the device deletes…all the data…in the personal data device." Hayward, 23:23-25. However, "before deleting the data, the device contacts the database server 50 and uploads, step 1030, at least any data to the database server that is necessary to create a current backup." Hayward, 23:25-27. Thereafter, "[a]n authorized user may, subject to proper authentication, subsequently reload the data from the backup into the personal data device." Hayward, 23:27-29.

533. The operation of this functionality in Hayward's data protection software is illustrated in Figure 11:



2. The Andrews-Cotichini-Hayward Combination

534. Like Andrews, Hayward is directed to techniques for protecting devices and the data stored therein and is, therefore, analogous art. In my opinion, a POSITA had multiple reasons to use Hayward's data-protection techniques in the Andrews security software. Specifically, POSITAs 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.

535. First, both Andrews and Hayward are directed to systems for protecting personal data on mobile electronic devices. Andrews teaches that the

"value of data stored on a lost or stolen portable computing device may eclipse the value of the device itself" and, furthermore, "may be of a sensitive nature." Andrews, 1:17-19. Thus, the "recovery of the data" is a "high priorit[y] for owners whose portable computing devices are lost or stolen." Andrews, 1:20-22. To address this problem, Hayward discloses "data protection software" with functionality that will help an owner of a device "protect[]" the data "from misuse" (Hayward, 10:27-28) by, *e.g.*, preventing unauthorized access to data (Hayward, 10:25-11:5, 13:27-14:8), deleting data that falls into the wrong hands (Hayward, 23:17-20, 23:29-31, 15:12-17), and copying data to a database server to allow for data recovery (Hayward, 22:30-23:12, 23:25-29).

536. Although Andrews-Cotichini would have provided device owners with the ability to protect their data by sending remote commands to copy, delete, and download data at their lost/stolen device, Hayward's data protection software adds an extra layer of protection by automatically backing up and deleting data from a device in response to unsuccessful attempts to access the device, while also allowing the same data to be restored to the device upon recovery by the owner. Implementation of Hayward's data-protection techniques would not have affected the storage of the Andrews client software as configured in the Andrews-Cotichini combined system because the implementation would have merely involved

programming additional functionality into the existing software, regardless of where it is stored.

537. 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).

538. In my opinion, a POSITA would have had a reasonable expectation of success in combining Andrews, Cotichini, and Hayward in this manner because Hayward discloses software-based data-protection techniques in a system that is substantially similar to the one disclosed in Andrews. Both systems include executing a computer program on a portable electronic device, such as a PDA. *Compare* Andrews, 8:18-9:7 *with* Hayward, 10:25-28, 15:28-31. In both systems, these devices communicate with a remote server system via a network. *Compare* Andrews, 15:19-16:8 *with* Hayward, 12:1-5. And in both systems, the devices send and receive user data to/from the remote server. *Compare* Andrews, 28:17-22 *with* Hayward, 14:9-33. It would have required only ordinary skill for POSITAs to program Andrews's client software to execute the data-protection steps performed by Hayward's data protection software.

3. Independent Claims 25

a. Deleting User Data Limitation 25[G]

539. The Deleting User Data Limitation of Claim 25 recites "*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*."

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." Hayward, 23:25-27. 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." Hayward, 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. Hayward, 23:23-27.

b. Restoring User Data Limitation 25[H]

541. The Restoring User Data Limitation of Claim 25 recites "*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*."

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." Hayward, 23:27-29.

4. Dependent Claims 6, 14, 22

543. Claim 6 depends from claim 1, claim 14 depends from claim 9, and claim 22 depends from claim 17. These claims are substantially similar as shown in the comparison table below. For the reasons I discuss below, the combination of Andrews, Cotichini, and Hayward discloses these claims.

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.*
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.*
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.*

544. In my opinion, the combined systems of Andrews, Cotichini, and Hayward discloses using an *SMS format* for the *notification* sent from Andrews's host computer to the client device. This disclosure is provided by Hayward, which teaches that 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." Hayward, 21:28-30.

545. In my opinion, when combining Andrews, Cotichini, and Hayward, a POSITA would have had reason to implement this teaching from Hayward in the combined system, such that the communications between the client device and host computer would be in an *SMS format* and would be handled by the claimed *SMS component residing in the system area*.

546. First, Hayward teaches that using an SMS message allows the server to send a notification that is "undetectable to a user." Hayward, 21:28-30. Because the Andrews, Cotichini, and Hayward combined system would be meant to be used to send responsive actions to a lost or stolen computing device, it would have been advantageous for the client-host communication to occur in a manner that is "undetectable to a user" so that the user in possession of a lost or stolen device would not be made aware of the background operation of the software. If a user of a lost/stolen device were made aware of the software, it might cause the user to attempt to disable or interrupt the operation of the software.

547. 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. 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. As a POSITA would have recognized, the advantages of using SMS messages include "the provision of information from any database server on the Internet to a user's PDA 'on the fly', the transmission of computer programs executable on a PDA, over the SMS, the installation of those programs on the PDA without user intervention, the transmission of text messages to a PDA of unlimited length and with receipt acknowledgment, and the sending of information to a PDA without a user request for that information[.]" EX1019, 7:7-16. These advantages would have been advantageous when combining Andrews, Cotichini, and Hayward because it would have defeated—or, at the very least, frustrated—the purpose of the system if host computer could not send commands to the portable electronic device to instruct the device to lock, delete data, backup data, etc. without a user request or intervention.

548. Moreover, in the combined Andrews, Cotichini, and Hayward system, it is my opinion that the *SMS component* would *resid[e] in the system area*. As discussed in connection with Ground 1C, one option for combining Andrews and

Cotichini combined system would have included installing Andrews's client software on Andrews's modem (like Cotichini's Modem Agent), which would continue to send and receives messages from the security service. To configure this system to send and receive messages in SMS format (which a POSITA would done for the reasons described above), a POSITA would simply need to configure the Andrews-Cotichini modem as an SMS modem capable of communicating with the GSM network, which would have been a routine and conventional implementation of Hayward's SMS teachings in Andrews-Cotichini.

5. Dependent Claims 7, 15, 23

549. Claim 7 depends from claim 1, claim 15 depends from claim 9, and claim 23 depends from claim 17. These claims are substantially similar as shown in the comparison table provided above in Ground 1A.

550. The limitations of Claims 7, 15, and 23 are substantially similar to the Deleting User Data Limitation of Claim 25. Thus, it is my opinion that the combination of Andrews, Cotichini, and Hayward discloses the limitations Claims 7, 15, and 23 for the same reasons discussed in connection with Claim 25.

6. Dependent Claims 8, 16, 24

551. Claim 8 depends from claim 7, claim 16 depends from claim 15, and claim 24 depends from claim 23. These claims are substantially similar as shown in the comparison table provided above in Ground 1A.

552. The limitations of Claims 8, 16, and 24 are substantially similar to the Restoring User Data Limitation of Claim 25. Thus, it is my opinion that the combination of Andrews, Cotichini, and Hayward discloses the limitations of Claims 8, 16, and 24 for the same reasons discussed in connection with Claim 25.

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

554. I declare under penalty of perjury that the foregoing is true and correct.

Dated: Jul 10 2023

John Black, Ph.D.

VIII. CLAIM LISTING

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.