PTO/SB/14 (11-08)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	130839.02101
	Application Number	
Title of Invention	RULES BASED ACTIONS FOR MOBILE DEVICE MANAGEMENT	

The application data sheet is part of the provisional or nonprovisional application for which it is being submitted. The following form contains the bibliographic data arranged in a format specified by the United States Patent and Trademark Office as outlined in 37 CFR 1.76.
This document may be completed electronically and submitted to the Office in electronic format using the Electronic Filing System (EFS) or the document may be printed and included in a paper filed application.

Secrecy Order 37 CFR 5.2

☐ Portions or all of the application associated with this Application Data Sheet may fall under a Secrecy Order pursuant to 37 CFR 5.2 (Paper filers only. Applications that fall under Secrecy Order may not be filed electronically.)

Applicant Information:

Applicant 1 Remove

Applicant Authority ◉ Inventor ○ Legal Representative under 35 U.S.C. 117 ○ Party of Interest under 35 U.S.C. 118

Prefix	Given Name	Middle Name	Family Name	Suffix
	Jatin		MALIK	

Residence Information (Select One) ○ US Residency ◉ Non US Residency ○ Active US Military Service

City	Bangalore	Country Of Residence[i]	IN
Citizenship under 37 CFR 1.41(b)[i]	IN		

Mailing Address of Applicant:

Address 1	30-303, Mantri Residency		
Address 2	Bannerghatta Road, Opp Meenakshi Temple		
City	Bangalore	State/Province	
Postal Code	560076	Country[i]	IN

Applicant 2 Remove

Applicant Authority ◉ Inventor ○ Legal Representative under 35 U.S.C. 117 ○ Party of Interest under 35 U.S.C. 118

Prefix	Given Name	Middle Name	Family Name	Suffix
	Ratnesh		SINGH	

Residence Information (Select One) ○ US Residency ◉ Non US Residency ○ Active US Military Service

City	Bangalore	Country Of Residence[i]	IN
Citizenship under 37 CFR 1.41(b)[i]	IN		

Mailing Address of Applicant:

Address 1	1104 Sobha Jasmine		
Address 2	Green Glen Layout, Bellandur		
City	Bangalore	State/Province	
Postal Code	560103	Country[i]	IN

Applicant 3 Remove

Applicant Authority ◉ Inventor ○ Legal Representative under 35 U.S.C. 117 ○ Party of Interest under 35 U.S.C. 118

Prefix	Given Name	Middle Name	Family Name	Suffix
	Rajakumar		BOPALLI	

Residence Information (Select One) ○ US Residency ◉ Non US Residency ○ Active US Military Service

City	Bangalore	Country Of Residence[i]	IN

PTO/SB/14 (11-08)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	130839.02101
	Application Number	
Title of Invention	RULES BASED ACTIONS FOR MOBILE DEVICE MANAGEMENT	

Citizenship under 37 CFR 1.41(b) [i]	IN		
Mailing Address of Applicant:			
Address 1	Flat #305, C-block		
Address 2	Samhita Rainbow MTB, Thubarahalli		
City	Bangalore	**State/Province**	
Postal Code	560066	**Country** [i]	IN

All Inventors Must Be Listed - Additional Inventor Information blocks may be generated within this form by selecting the **Add** button. Add

Correspondence Information:

Enter either Customer Number or complete the Correspondence Information section below.
For further information see 37 CFR 1.33(a).

☐ **An Address is being provided for the correspondence Information of this application.**

Customer Number	86308		
Email Address	bwdocket@pepperlaw.com	Add Email	Remove Email

Application Information:

Title of the Invention	RULES BASED ACTIONS FOR MOBILE DEVICE MANAGEMENT		
Attorney Docket Number	130839.02101	**Small Entity Status Claimed**	☒
Application Type	Nonprovisional		
Subject Matter	Utility		
Suggested Class (if any)		**Sub Class (if any)**	
Suggested Technology Center (if any)			
Total Number of Drawing Sheets (if any)	10	**Suggested Figure for Publication (if any)**	

Publication Information:

☐ Request Early Publication (Fee required at time of Request 37 CFR 1.219)

☐ **Request Not to Publish.** I hereby request that the attached application not be published under 35 U.S. C. 122(b) and certify that the invention disclosed in the attached application **has not and will not** be the subject of an application filed in another country, or under a multilateral international agreement, that requires publication at eighteen months after filing.

Representative Information:

Representative information should be provided for all practitioners having a power of attorney in the application. Providing this information in the Application Data Sheet does not constitute a power of attorney in the application (see 37 CFR 1.32).
Enter either Customer Number or complete the Representative Name section below. If both sections are completed the Customer Number will be used for the Representative Information during processing.

Please Select One:	◉ Customer Number	○ US Patent Practitioner	○ Limited Recognition (37 CFR 11.9)

PTO/SB/14 (11-08)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	130839.02101
	Application Number	
Title of Invention	RULES BASED ACTIONS FOR MOBILE DEVICE MANAGEMENT	

Customer Number	86308

Domestic Benefit/National Stage Information:

This section allows for the applicant to either claim benefit under 35 U.S.C. 119(e), 120, 121, or 365(c) or indicate National Stage entry from a PCT application. Providing this information in the application data sheet constitutes the specific reference required by 35 U.S.C. 119(e) or 120, and 37 CFR 1.78(a)(2) or CFR 1.78(a)(4), and need not otherwise be made part of the specification.

Prior Application Status	Pending		Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
	non provisional of	61/503729	2011-07-01

Additional Domestic Benefit/National Stage Data may be generated within this form by selecting the **Add** button. Add

Foreign Priority Information:

This section allows for the applicant to claim benefit of foreign priority and to identify any prior foreign application for which priority is not claimed. Providing this information in the application data sheet constitutes the claim for priority as required by 35 U.S.C. 119(b) and 37 CFR 1.55(a).

Remove

Application Number	Country [i]	Parent Filing Date (YYYY-MM-DD)	Priority Claimed
			○ Yes ◉ No

Additional Foreign Priority Data may be generated within this form by selecting the **Add** button. Add

Assignee Information:

Providing this information in the application data sheet does not substitute for compliance with any requirement of part 3 of Title 37 of the CFR to have an assignment recorded in the Office.

Assignee 1 Remove

If the Assignee is an Organization check here. ☒			
Organization Name	Fiberlink Communications Corporation		
Mailing Address Information:			
Address 1	1787 Sentry Park West		
Address 2	Building 18, Suite 200		
City	Blue Bell	**State/Province**	PA
Country [i] US		Postal Code	19422
Phone Number		Fax Number	
Email Address			

Additional Assignee Data may be generated within this form by selecting the **Add** button. Add

Signature:

A signature of the applicant or representative is required in accordance with 37 CFR 1.33 and 10.18. Please see 37 CFR 1.4(d) for the form of the signature.

PTO/SB/14 (11-08)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	130839.02101
	Application Number	
Title of Invention	RULES BASED ACTIONS FOR MOBILE DEVICE MANAGEMENT	

Signature	/Jay R. Mitchell, Reg. No. 54,316/			Date (YYYY-MM-DD)	2012-07-02
First Name	Jay	Last Name	Mitchell	Registration Number	54316

This collection of information is required by 37 CFR 1.76. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 23 minutes to complete, including gathering, preparing, and submitting the completed application data sheet form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

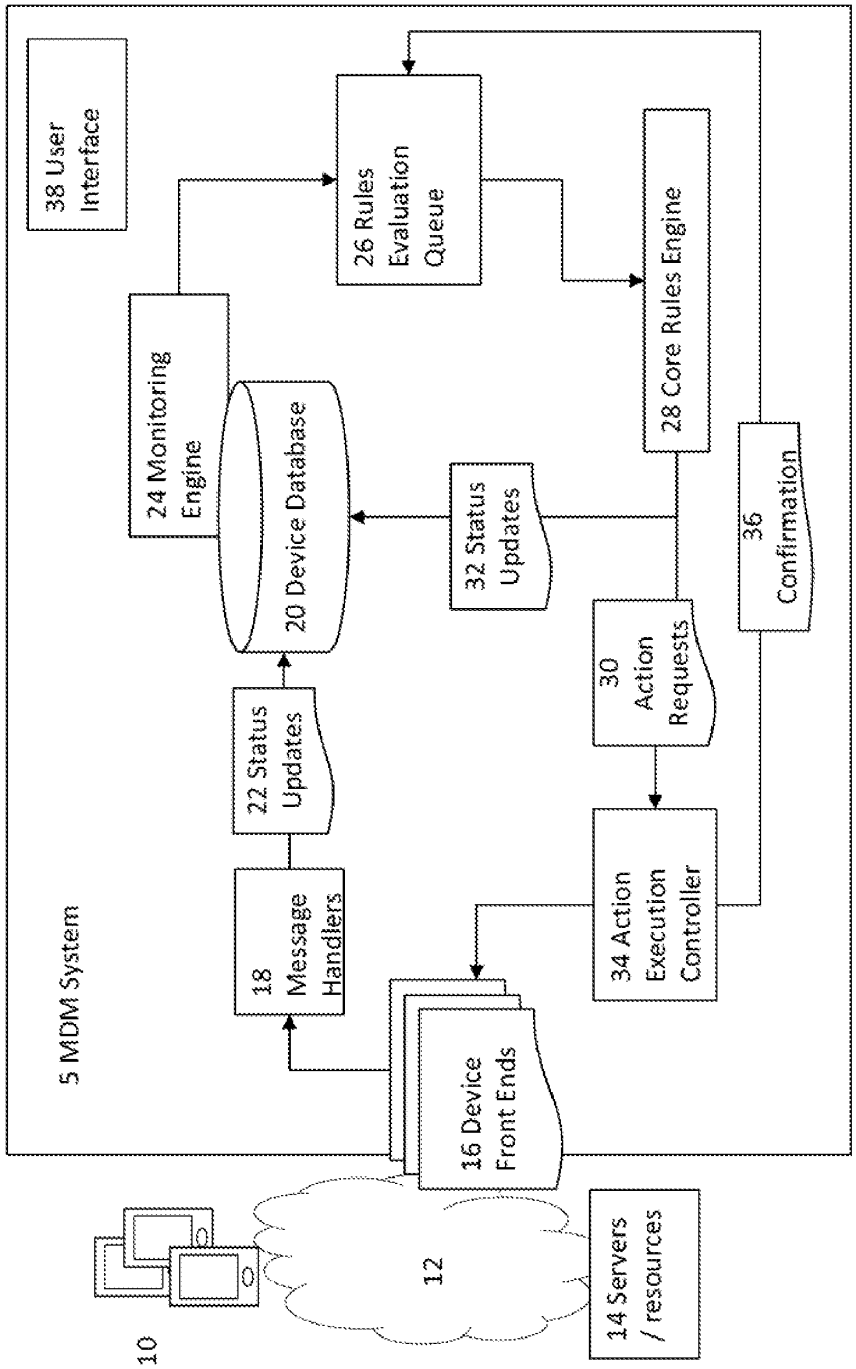

5 MDM System
38 User Interface
26 Rules Evaluation Queue
28 Core Rules Engine
24 Monitoring Engine
20 Device Database
32 Status Updates
36 Confirmation
30 Action Requests
22 Status Updates
18 Message Handlers
34 Action Execution Controller
16 Device Front Ends
12
14 Servers / resources
10

FIG. 1

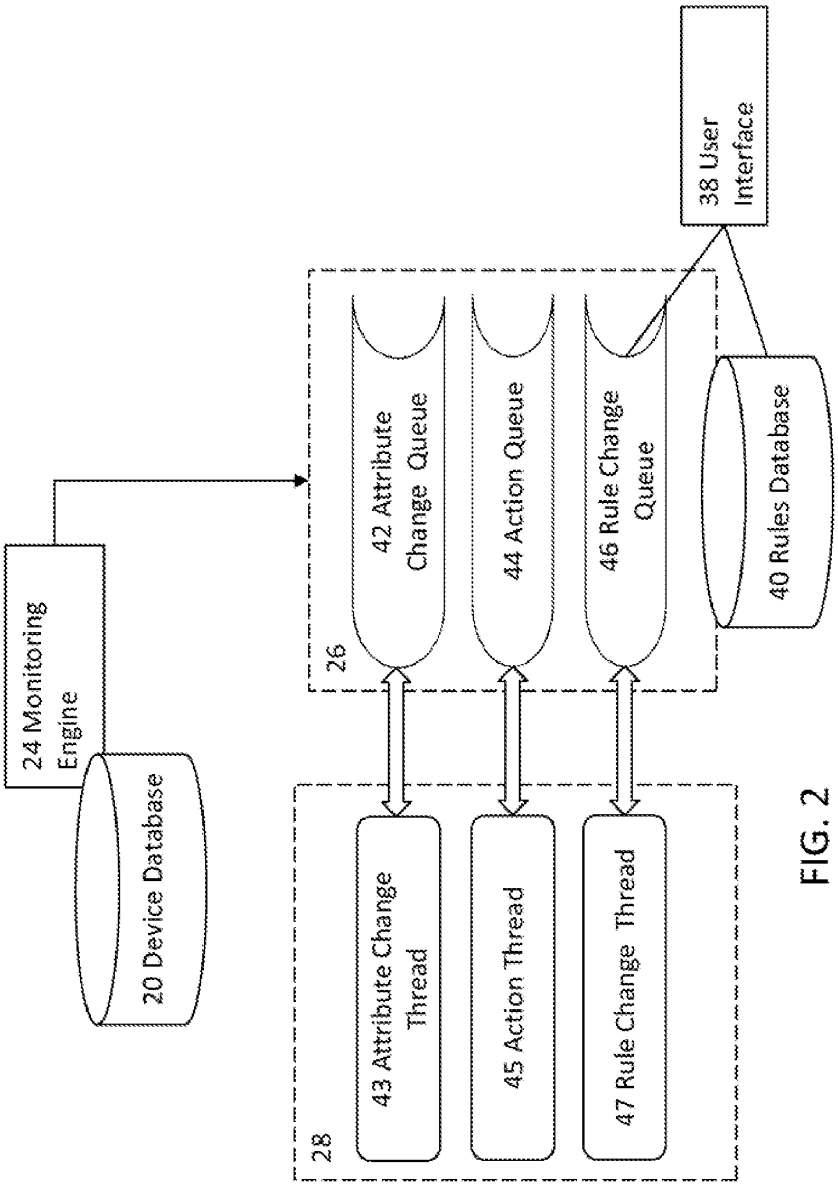

24 Monitoring Engine
20 Device Database
26
42 Attribute Change Queue
44 Action Queue
46 Rule Change Queue
38 User Interface
40 Rules Database
28
43 Attribute Change Thread
45 Action Thread
47 Rule Change Thread

FIG. 2

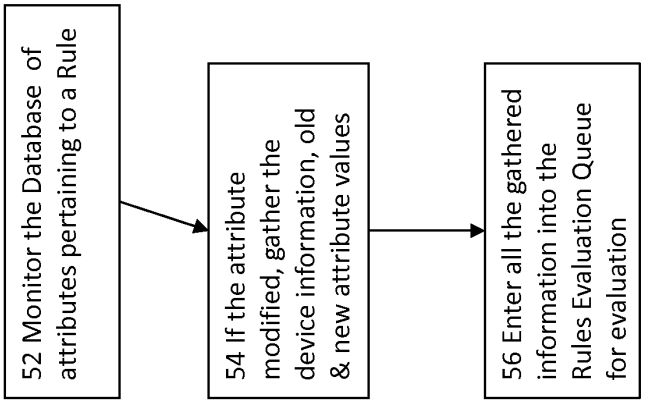

50
52 Monitor the Database of attributes pertaining to a Rule
54 If the attribute modified, gather the device information, old & new attribute values
56 Enter all the gathered information into the Rules Evaluation Queue for evaluation

FIG. 3

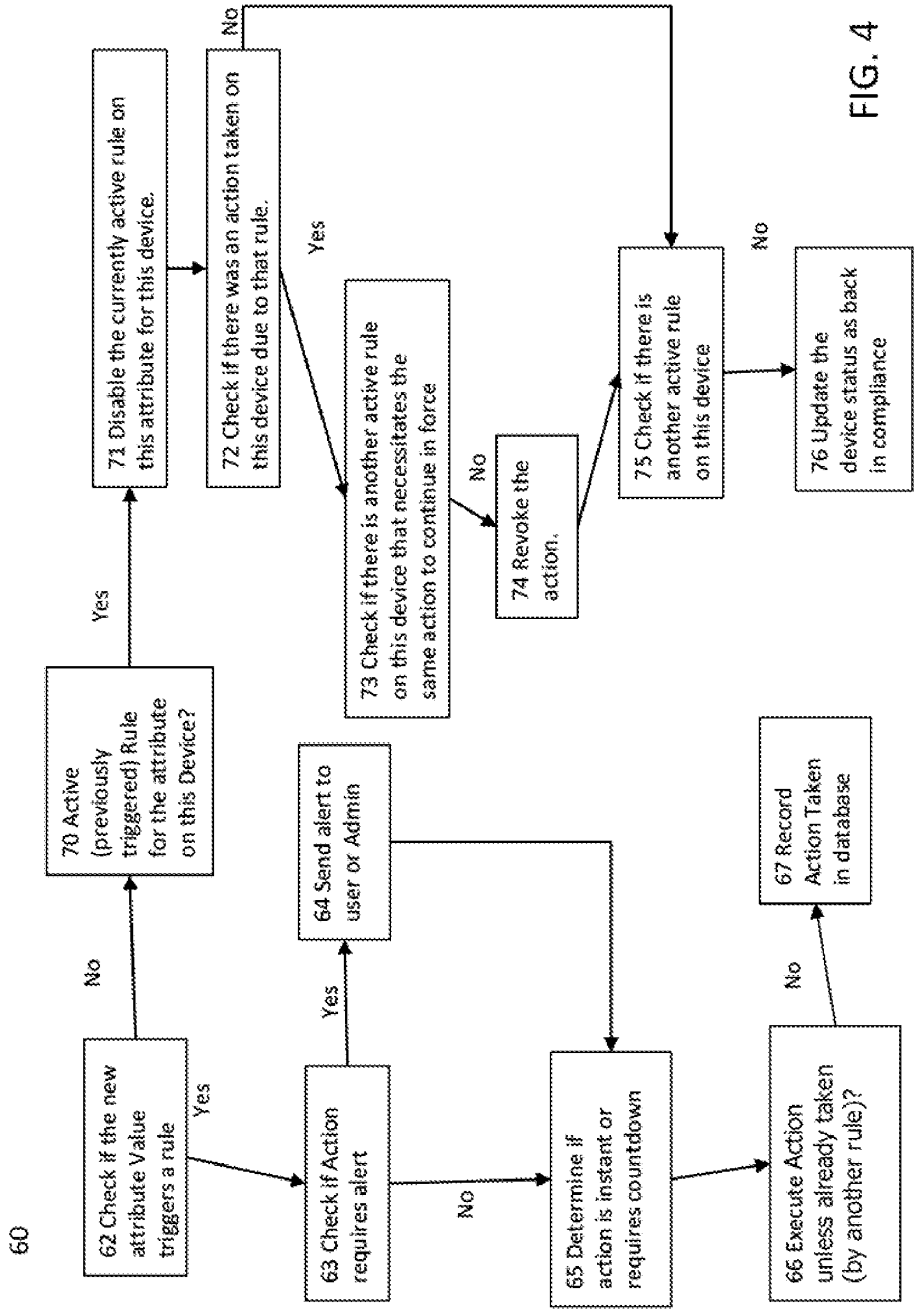

60
62 Check if the new attribute Value triggers a rule
No
Yes
70 Active (previously triggered) Rule for the attribute on this Device?
Yes
71 Disable the currently active rule on this attribute for this device.
72 Check if there was an action taken on this device due to that rule.
No
Yes
73 Check if there is another active rule on this device that necessitates the same action to continue in force
No
74 Revoke the action.
75 Check if there is another active rule on this device
No
76 Update the device status as back in compliance
63 Check if Action requires alert
Yes
64 Send alert to user or Admin
No
65 Determine if action is instant or requires countdown
66 Execute Action unless already taken (by another rule)?
No
67 Record Action Taken in database

FIG. 4

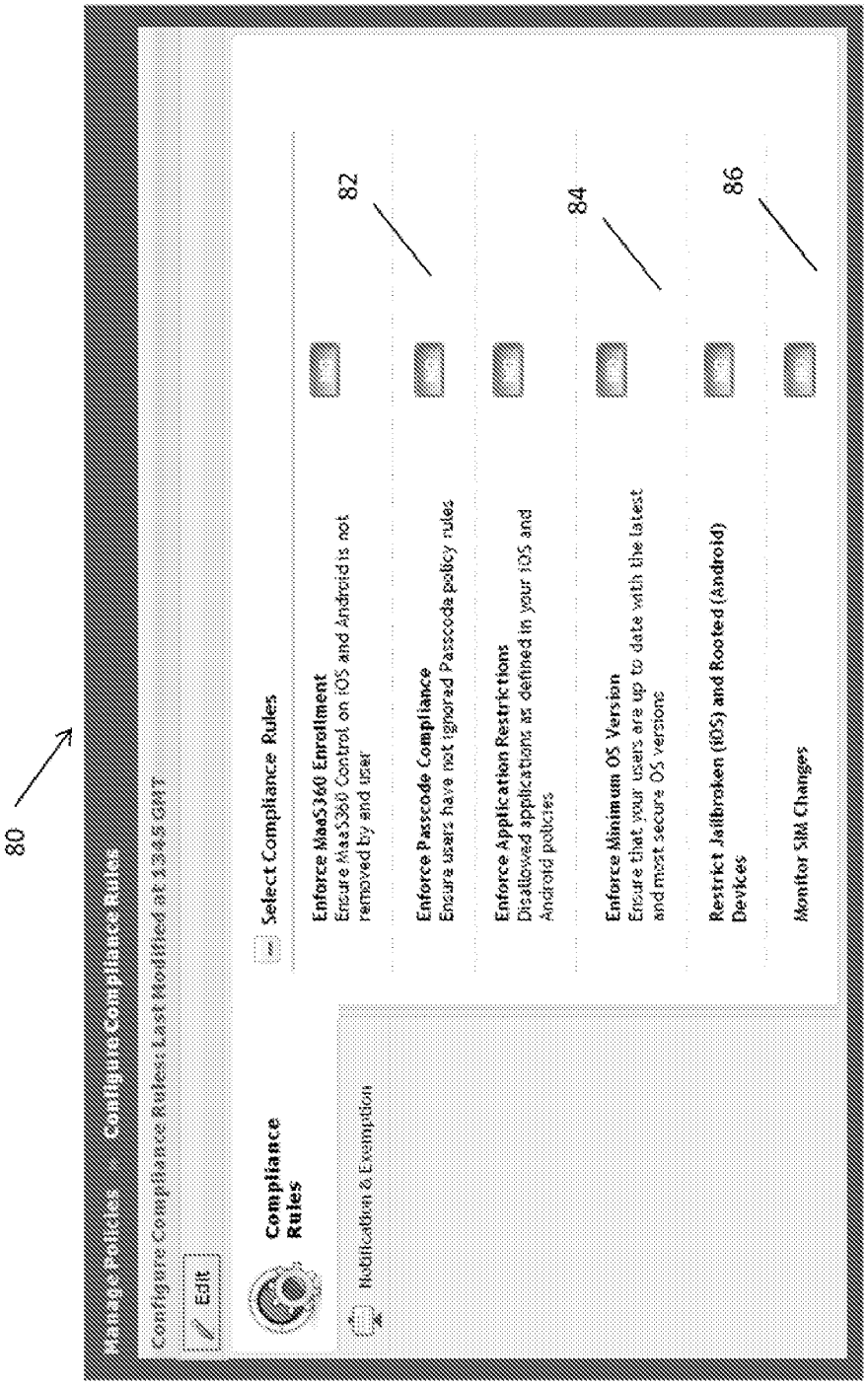

80
Manage Policies
Configure Compliance Rules
Configure Compliance Rules Last Modified at 13:45 GMT
Edit
Compliance Rules
Notification & Exemption
Select Compliance Rules
Enforce MaaS360 Enrollment
Ensure MaaS360 Control on iOS and Android is not removed by end user
82
Enforce Passcode Compliance
Ensure users have not ignored Passcode policy rules
Enforce Application Restrictions
Disallowed applications as defined in your iOS and Android policies
84
Enforce Minimum OS Version
Ensure that your users are up to date with the latest and most secure OS versions
Restrict Jailbroken (iOS) and Rooted (Android) Devices
86
Monitor SIM Changes

FIG. 5

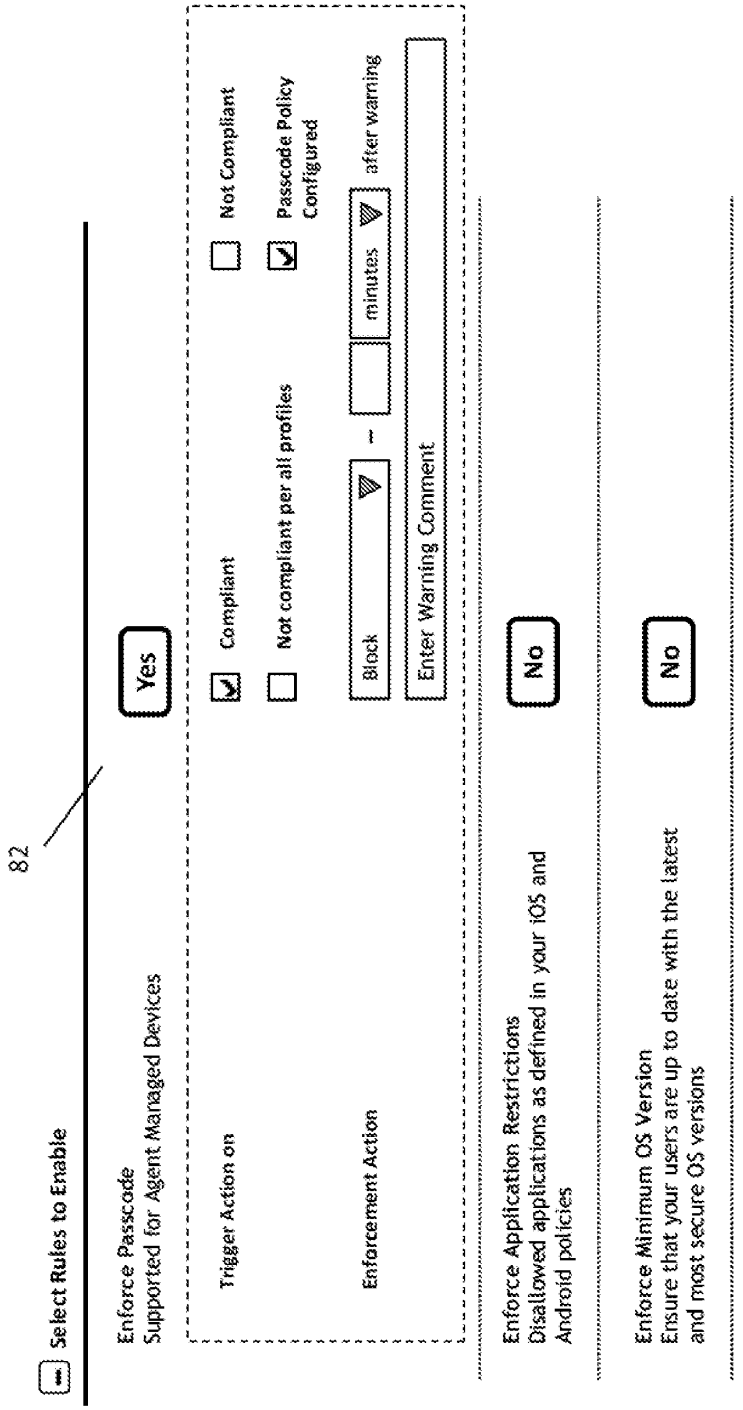

82
Select Rules to Enable
Enforce Passcode
Supported for Agent Managed Devices
Yes
Trigger Action on
Compliant
Not compliant per all profiles
Not Compliant
Passcode Policy Configured
Enforcement Action
Block
minutes
after warning
Enter Warning Comment
Enforce Application Restrictions
Disallowed applications as defined in your iOS and Android policies
No
Enforce Minimum OS Version
Ensure that your users are up to date with the latest and most secure OS versions
No

FIG. 6

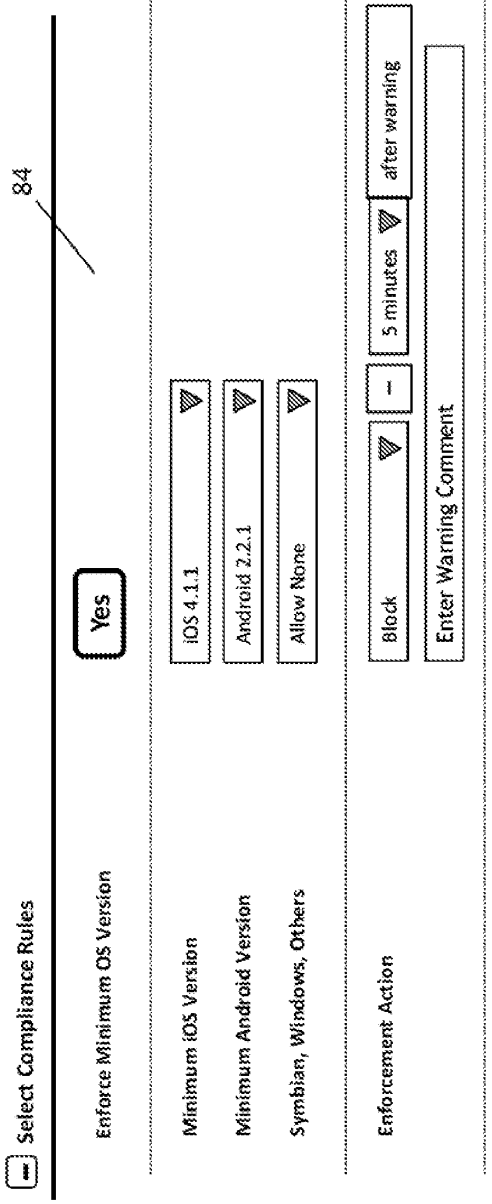

84
Select Compliance Rules
Enforce Minimum OS Version
Yes
Minimum iOS Version
iOS 4.1.1
Minimum Android Version
Android 2.2.1
Symbian, Windows, Others
Allow None
Enforcement Action
Block
5 minutes
after warning
Enter Warning Comment

FIG. 7

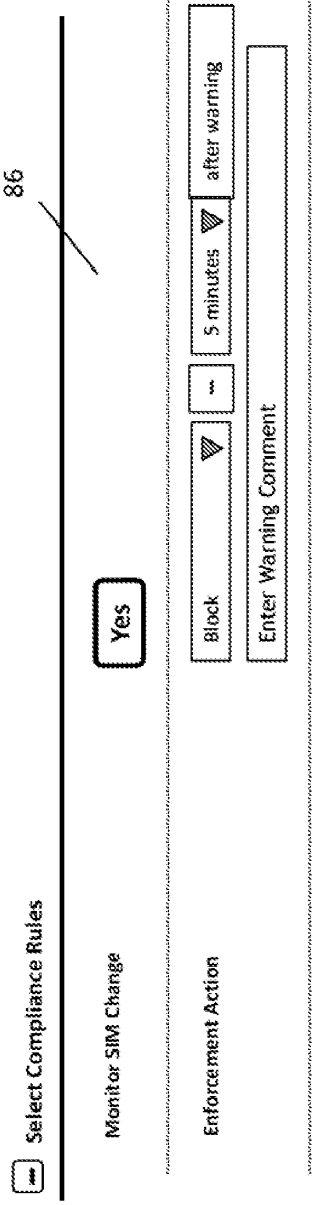

86
Select Compliance Rules
Monitor SIM Change
Yes
Enforcement Action
Block
5 minutes
after warning
Enter Warning Comment

FIG. 8

Administrator List for alert deliveries
Enter email addresses to be alerted on for actions taken
Enter email address
Enter email address
Exemption List
Select Group that you want to be exempt from Enforcement actions Actions will not be executed on Devices in this group. You can also manually maintain this list by individually marking the Device attribute "Special Devices" as "Yes".

FIG. 9

FIG. 10

Select Enforcement Rules

Enforce MaaS360 Enrollment

Ensure iOS and Android devices are enrolled in MDM and advanced management of the device has not been disabled or removed by the user.

Enforce OS Versions

Ensure that your managed devices are up to date with the required OS versions. Please note that version check may be invalid on Rooted or Jailbroken devices.

Enforce Remote Wipe Support

Ensure managed devices support remote wipe capabilities.

Enforce Encryption Support

Ensure managed devices support designated levels of encryption.

Enforce Application Compliance

Ensure devices are in compliance with application management requirements (required, disallowed & white list policies). Application compliance is based on policy settings assigned to managed devices.

Restrict Jailbroken (iOS) and Rooted (Android) Devices

Ensure managed devices are not jailbroken or rooted. The MaaS360 Application is required for Jailbreak detection on iOS devices.

Restrict Corporate Resources for Blocked Devices

Ensure that devices blocked on your mail server can not access corporate resources such as Wi-Fi or VPN.

FIG. 11

90
Select Geo-Fencing Rule(s)
Enable Geo-Fencing
Enforce the device to stay checked-in at all times. You need to have defined locations before enabling this rule. You can define new locations by using the Manage Locations workflow.
Enforcement Action
Alert Administrator
Alert User and Administrator
Block
Restrict Device
Change Policy
Wipe
Message (maximum 250 characters)
92
Select Expense Monitoring Rules
Monitor Roaming Mobile Data Usage
Monitor and notify users and administrators when roaming mobile data usage on the device exceeds defined thresholds.
Monitor In-Network Mobile Data Usage
Monitor and notify users and administrators when in-network mobile data usage on the device exceeds defined thresholds.

RULES BASED ACTIONS FOR MOBILE DEVICE MANAGEMENT

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] This application claims priority to U.S. provisional application Serial No. 61/503,729 filed July 1, 2011, entitled "Rules based Actions for Mobile Device Life Cycle Management System," which is incorporated herein by reference in its entirety.

TECHNICAL FIELD

[0002] The present invention relates generally to methods and systems for providing mobile device management and more specifically providing remote management of mobile devices at a server using rules based actions.

BACKGROUND

[0003] The general trend in corporate network management is the addition of mobility of users of the corporate network. Whereas traditional corporate networks have included a LAN and local desktop devices, the recent trend has been the introduction of mobile devices, such as smart phones, that are used by employees to work and access corporate resources remotely. While allowing users to work remotely is desirable within an organization, from an IT perspective the mobility of users can present certain challenges.

[0004] A common challenge in organizations that allow mobile access to users is the need for reliable security solutions. For example, users within an organization may use several different platforms for accessing resources within a network. Users may use smart phones, such as

Blackberries, iPhones, and Android devices, tablet computing devices, such as iPads or similar offerings with other mobile operating systems, laptops, or home desktops. The diversity of devices and operating systems employed by these devices can make it difficult to ensure security when users access computing resources within an organization's network. Furthermore, as mobile devices become more powerful and ubiquitous, users typically utilize a single device for both business and pleasure. Device users demand the ability to customize their devices, including their own personal preferences, data, and applications – many of which may be counter to the security or management goals of an organization.

[0005] Unlike traditional network management where devices share common operating system features, such as a network of desktops that all use a common Microsoft Windows operating system, mobile devices often utilize different operating systems, each of which may have different capabilities from a management and security standpoint. For example, for the last decade, corporate users commonly used Blackberry devices from Research in Motion ("RIM"), which allowed uniform remote access to status information and some actions via the Blackberry Enterprise Server ("BES"). New popular devices, such as those from Apple and manufactures that utilize Android and Windows Mobile, approach management and security differently, providing differing levels of out-of-the box management functionality. As these devices become part of the corporate ecosystem, IT managers are taxed with managing and/or providing security against threats related to a spectrum of devices. It is generally infeasible for most IT managers to develop expertise in each of the different rapidly-changing mobile platforms to manage these devices. There remains a need to simplify the management and configuration of these mobile devices by an IT manager.

SUMMARY

[0006] Applicants have recognized and appreciated that certain problems with the prior art can be solved by utilizing a server-based rules-based action framework. A server can include a plurality of front ends the gather status and configuration information about each of a plurality of mobile devices, which include devices from different mobile platforms. At the server, software processes monitor status information and respond automatically to changes, causing appropriate rules to be evaluated to determine if one is triggered. Each rule includes conditions and an action pre-selected by an administrator, which will automatically be initiated. Rules may be defined using a user interface, allowing an administrator to define rules in a simple manner without requiring the administrator to define how to collect status information from various mobile platforms, allowing rules to work across multiple platforms and simplifying the administrative process.

[0007] One embodiment is directed to a method for providing device management services, including steps of gathering, status information from a network, related to each of a plurality of mobile devices, each mobile device utilizing one of a plurality of different mobile operating systems and storing the status information in an electronic database accessible to a server. The method then evaluates a first compliance state of at least one of the mobile devices from the status information using a plurality of administrator-defined rules; and initiates at least one action defined by the user-defined rules in response to the step of evaluating. The step of evaluation is performed by a server automatically, in response to changes in the status information.

Petitioner Ex 1002, p. 18
Zimperium v. Taasera, IPR2024-00007

[0008] According to one aspect of some embodiments, the action is selectable from a plurality of actions, comprising by blocking access to the at least one of the mobile devices to a corporate resource. The action may also include blocking e-mail access for the at least one of the mobile devices, wiping information from the at least one of the mobile devices, or warning a user of the at least one of the mobile devices that further action may be taken. According to another aspect of some embodiments, the step of gathering status information, for the at least one mobile device, includes gathering information from that mobile device and at least one other source on the network. According to still another aspect of some embodiments, the method includes the step of subsequently evaluating a second compliance state of at least one of the mobile devices to determine if the at least one action should be revoked. In yet another aspect of some embodiments, the plurality of different mobile operating systems includes Android and iOS. In yet another aspect of some embodiments, the status information collected includes location information about the mobile device.

[0009] Another embodiment is directed to a method for providing device management services including steps of making a determination that an attribute of a mobile device has changed and evaluating the attribute, by a processor at a server in response to the determination, to determine if it triggers at least one of a plurality of administrator defined rules, which indicates that the attribute is out of compliance. If the attribute is out of compliance, and the method automatically initiates, by the server, an action defined by the at least one of a plurality of administrator defined rules. The attributes are stored in a data store accessible to the server that includes substantially real-time data pertaining to a plurality of attributes of a plurality of mobile devices, comprising devices having different mobile operating systems.

[0010] According to one aspect of some embodiments, the step of automatically initiating an action includes warning a user of the mobile device that the device is out of compliance and subsequently causing the action to be performed if the attribute remains out of compliance after a period of time defined in the rule. According to another aspect of some embodiments, the method includes the step of automatically revoking the action if the attribute is brought back into compliance and may include determining if another of the plurality of rules is triggered. According to still another aspect of some embodiments, the method includes the step of gathering the plurality of attributes for at least one of the plurality of mobile device by gathering attribute information from that mobile device and at least one other source on a network. In yet another aspect of some embodiments, the plurality of different mobile operating systems includes Android and iOS. In yet another aspect of some embodiments, the attribute collected includes location information about the mobile device.

[0011] Another embodiment is directed to a system for providing device management services including a data store configured to be accessible by a server and computer readable instructions for execution on the server, configured to make a determination that an attribute of a mobile device stored in the data store has changed. The instructions are further configured to evaluate the attribute, in response to the determination, to determine if it triggers at least one of a plurality of administrator defined rules, which indicates that the attribute is out of compliance and automatically initiate an action defined by the at least one of a plurality of administrator defined rules if the attribute is out of compliance. The data store is configured to include substantially real-time data pertaining to a plurality of attributes of a plurality of mobile devices, comprising devices having different mobile operating systems.

[0012] According to one aspect of some embodiments, the computer readable instructions include instructions configured to present a user interface to an administrator to allow selection of at least one attribute and one available action to define the at least one of the plurality of administrator defined rules. According to another aspect of some embodiments, at least one of the action includes warning a user of the mobile device that the device is out of compliance and causing subsequent action to be performed if the attribute remains out of compliance after a period of time defined in the at least one rule. According to yet another aspect of some embodiments, the computer readable instructions further comprise instructions configured to automatically revoke the action if the attribute is brought back into compliance.

[0013] According to still another aspect of some embodiments, the computer readable instructions include instructions configured to gather the plurality of attributes for at least one of the plurality of mobile device by gathering attribute information from that mobile device and at least one other source on a network. According to another aspect of some embodiments, the plurality of different mobile operating systems comprises at least Android and iOS. In yet another aspect of some embodiments, the attribute collected includes location information about the mobile device.

[0014] It should be appreciated that all combinations of the foregoing concepts and additional concepts discussed in greater detail below (provided that such concepts are not mutually inconsistent) are contemplated as being part of the inventive subject matter disclosed herein. In particular, all combinations of claimed subject matter appearing at the end of this disclosure are contemplated as being part of the inventive subject matter disclosed herein.

BRIEF DESCRIPTION OF THE DRAWINGS

[0015] The accompanying drawings are not intended to be drawn to scale. In the drawings, each identical or nearly identical component that is illustrated in various figures is represented by a like numeral. For purposes of clarity, not every component may be labeled in every drawing. In the drawings:

[0016] FIG. 1 is a system diagram of an exemplary mobile device management (MDM) system for use with certain embodiments of the present invention;

[0017] FIG. 2 is a system diagram of an exemplary mobile device management (MDM) system for use with certain embodiments of the present invention;

[0018] FIG. 3 is a flowchart of an exemplary method to monitor mobile device attributes for use with certain embodiments of the present invention;

[0019] FIG. 4 is a flowchart of an exemplary method to execute rules-based actions for use with certain embodiments of the present invention;

[0020] FIG. 5 is a screenshot of available rules that may be configured by an administrator for use with certain embodiments of the present invention;

[0021] FIGs. 6, 7, and 8 are exemplary templates for configuring rules-based actions for use with certain embodiments of the present invention;

[0022] FIG. 9 is a screenshot of exemplary settings for use with certain embodiments of the present invention;

[0023] FIG. 10 is a screenshot of available rules that may be configured by an administrator for use with certain embodiments of the present invention; and

[0024] FIG. 11 is screenshot of exemplary templates for configuring rules-based actions for use with certain embodiments of the present invention.

DETAILED DESCRIPTION OF EXEMPLARY EMBODIMENTS

[0025] The present invention solves many issues of managing a plurality of mobile devices by providing a server-based rules system for gathering status and configuration information related to each mobile device being managed and applying administrator-defined rules to automatically carry out actions to assist in managing the devices. By enforcing rules at the server level, rules can be uniformly defined and applied without requiring an administrator to have special expertise with each mobile platform. While subsets of the mobile devices can each have differing operating systems, a front end of the server can be adapted to handle the nuance of interacting with each mobile device and may be further configured to interact with a plurality of sources to develop a more complete view of each mobile device and to further to carry out actions on the device to enforce the rule. Status and configuration information (collectively "status information") gathered about each mobile device can be placed in a datastore. This status information can be monitored for changes by one or more processes on the server. Changes to the status information of each device can be placed in one or more queues for application of rules. Certain conditions may bring the device out of compliance, and according to the administrator-defined rules, corrective action can be automatically taken on the device (such as by displaying a warning message to the user) or on the server (such as by restricting access to corporate resources at the server). In some embodiments, the administrator's interaction with the

system may be limited to defining server-enforced rules, without burdening the administrator with the details of the server's interaction with the devices to gather information and take actions. The can result in a system that can be more easily scaled and adapted to a plurality of mobile operating systems without complicating the administrative experience. As a result, a mobile device management ("MDM") system can adapt to changes in mobile platforms and allow less specialized (or busy) IT personnel to manage a plurality of mobile devices in an automated manner. Mobile devices can include, in some embodiments, smart phones, such as BlackBerries, iPhones, and Android devices, tablet computing devices, such as iPads or similar offerings with other mobile operating systems or other portable computing devices, such as laptops.

[0026] In some embodiments, an MDM system provides features that allow an administrator to easily handle the entire lifecycle of a mobile device. As used herein, an administrator is any user that interacts with the MDM system to define and select rules or who actively participates in the monitoring or management of the mobile devices through an MDM system. For example, by gathering information from each mobile device that accesses a corporate network, mobile device inventory can be monitored to provide real-time inventory information. In some embodiments, an administrator can access the system for at-a-glance details of the overall status of the devices that access the network. In some embodiments, a dashboard can be presented that lists all devices registered with the network (which may or may not currently be online), including the ability to click to drill down into the status of each device or to provide a statistical snapshot of the device status information. For example, a dashboard can show the number of iOS device registered, the version of the operating system ("OS"), the number that are running file-sharing

applications, and the number that have enabled a 4 digit passcode to authenticate the user. In some embodiments, administrator can select a group of devices or individual devices and obtain more detailed information.

[0027] Examples of the information that can be gathered about each mobile device include, but are not limited to: the device model and manufacture information; applications (commonly referred to as "apps") installed on the device; certificates on the device; user profile information; the character of any passcode used to authenticate a user (e.g. whether a password/passcode is used and the relative strength of that password, such as the number of characters); operating system of the device; information regarding whether the device operating system has been tampered with by the user (e.g. an iOS device has been jailbroken, or an android device has been rooted); and the data usage (e.g. the amount of MB or GB used for a given billing period, the amount data used while roaming, or the relative amount compared to a data plan used by the user – which may be useful for monitoring or controlling costs where an organization pays for data usage).

[0028] In addition to gathering information about each device that can be used for monitoring device status, an exemplary MDM system can include management features that allow configuration of mobile devices and the resources they access. For example, an MDM system may communicate with certain mobile device operating system components or applications on the mobile device to change settings to comply with certain corporate policies. For example, after a device user registers his device, the MDM system can instruct the user (via any suitable message, including an email or pop-up message) to download an app to access the corporate

email server, which can be remotely configured or come preset with the appropriate settings to access the email server. Furthermore, the MDM system may interact with apps on the mobile device, other servers that the device accesses, corporate resources, or the OS, via remote procedure calls or network requests to change settings. These settings can alter the way the mobile device accesses or interacts with other resources on the network. An exemplary MDM system can remotely change configuration settings related to the mobile device. It should be noted that the specific character of configuration information available to the MDM system may vary by mobile device platform (i.e. iOS platform device, Android platform device, Blackberry platform devices, windows mobile/phone devices). Similarly, in some embodiments, the type of configuration information can be substantially the same across platforms, while the method for configuring the devices varies by platform. For example, a BlackBerry device may be configured to set up email and data access by interaction between the MDM server and the Blackberry Enterprise Server ("BES"), while an Android device may be configured by interaction between the MDM server and a client app on the device, which may in turn change settings in the OS utilizing APIs provided by the OS.

[0029] Examples of configuration settings that may be managed by the MDM system include, but are not limited to: email settings, VPN access settings, user profiles, Wi-Fi profiles, authentication certificates used by the device to securely access corporate resources.

[0030] The MDM system also can provide security or resource management functionality. For example, the MDM system can apply security or management policies to the status information retrieved from mobile devices. By applying policies, certain actions can be taken on

devices, depending on their status. These actions can include security actions, such as restricting access to corporate resources when a device is out of compliance. In some embodiments, policies can be of a resource management character. For example, a policy may observe the data usage of a mobile device and determine if too much data is being used. In cases where data usage exceeds a normal usage pattern, an administrator can be notified or a user can be warned that he is approaching his data limit.

[0031] Examples of security policies that may be used by the MDM system can include, but are not limited to: requiring users have a passcode to access their device, including defining the minimum passcode strength required; restricting access to devices that have been routed or are running certain apps (e.g., blacklisted apps, such as file-sharing apps); requiring that the user run certain apps, such as security apps or access clients; remotely wiping the device back to factory settings or wiping a portion of data stored on the device when a device appears compromised or is reported missing; and limiting access of devices that run versions of a mobile OS or on supported OSs. It should be noted that limiting access can include preventing access, restricting access, changing the nature of the access, or providing access to certain resources, while limiting access to other resources, etc. examples of resource management policies that may be used with the MDM system include, but are not limited to: alerting the user or an administrator; preventing email access from the device; restricting access to corporate Wi-Fi, VPN etc.; restricting access to corporate documents on the device; removing all corporate content and configuration from the device; and removing all personal and corporate data and settings from the device.

[0032] While the exemplary MDM systems are described as server-based, it should be appreciated that the system can be implemented on a plurality of servers, including cloud-based systems which may deploy the system on a plurality of servers on a dynamic basis, allowing for greater scalability. Any portion of the exemplary MDM systems can be executed on one or more processors, which may be separate from the processors executing other portions of the MDM system. A system may be implemented as part of the local IT infrastructure of a corporate environment or as part of a third party solution employed by the organization. The components of an MDM system on a server include software operating on one or more processor. This software can include software instructions, written in any suitable manner stored on non-transient computer readable media, such as optical, magnetic, or solid-state memory devices. For example, the systems and methods described with respect to FIGs. 1-4 can include software instructions operating on one or more processors.

[0033] As used herein, a corporate network should be considered a term for any network used by an organization that includes resources, such as Exchange servers, that need to be configured behind a firewall. Generally, a corporate network will include at least one local area network that is used by the organization. This can include campus networks used by universities or other institutions or networks used by corporations or small businesses. The corporate network may be large or small, and some networks may be maintained by a local IT staff. A corporate network can further be composed of multiple networks that interact with shared corporate computing resources, such as BlackBerry Enterprise servers (BES). In some embodiments corporate networks are synonymous with customer premises. It should also be understood that references to corporate, corporations, organizations, etc., may be interchangeable and are not

intended to be limited to commercial business organizations. While many of the embodiments described herein are described with reference to corporate environments, these embodiments are merely illustrative and can also apply to the computing environment of any organization that has a need for remote management of network resources via a cloud-based approach.

[0034] Corporate resources can include any of the resources, such as servers, data, credentials, e-mail and exchange services that may be part of, or accessed by, the corporate network. Corporate resources can include those resources that may be ordinarily made available to users of mobile devices when the mobile devices are in compliance with security and management policies. When a mobile device is brought out of compliance with these policies, restricting access to all or a subset of corporate resources may be an appropriate action as defined by the rules based policies. When a mobile device returns to compliance, an appropriate action may include restoring access to the resources may be an appropriate action.

[0035] By providing rules based actions and MDM system, some embodiments may have certain advantages over conventional IT management. For example, security and compliance of mobile devices can be substantially automated. Each mobile device can be required to enroll with the MDM system before accessing corporate resources. Enrolled mobile devices can then be automatically managed by the MDM system using rules based actions. This can result in reduced cost of managing mobile device infrastructure. Because rules based actions can be applied automatically, IT managers can be freed up to fulfill other roles in the organization. Furthermore, rules based actions can provide a simplified front-end for managing mobile devices that may require less training and expertise of IT personnel. For example, an IT manager may

not need to know the details of how Apple's iOS platform accesses device status information and enforces policy rules, but he may be able to identify the desired policies for enforcing on iOS devices, or mobile devices, in general.

[0036] A server-based MDM system can apply policies to information gathered from multiple sources and gathered in multiple ways. A server-based MDM system allows gathering information from sources other than just the device, which can be tailored to the mobile device platform. It should be appreciated that the MDM system may use one or more app on a mobile device to assist in gathering information for applying policies at the server, depending on the mobile platform. Because the system applies policies at a server, in some embodiments, the device capabilities and the method by which the server gathers information about a device can be separated from the logic that applies the policies, allowing powerful policies to be created uniformly for multiple mobile device platforms, while the application details of applying the policy to multiple device may vary. For example, while one mobile operating system may allow an app on the device that performs compliance analysis of the device status, another mobile operating system may not. By moving the compliance testing and action decision to the server, the MDM system may gather information from the devices in any manner suitable for the type of device being monitored. At the server, rules may then be applied more uniformly across device platforms.

[0037] While embodiments of the MDM system are contemplated to adapt to any appropriate mobile device platform, it may be helpful to understand an MDM system in the context of exemplary known mobile platforms. For example, RIM's BES for BlackBerry devices provides

a centralized resource in the form of an enterprise server that maintains status information about BlackBerry devices registered with the BES. The BES can push notifications to BlackBerry devices and request and maintain status information for his devices. The MDM system may interact with the BES to gather status information pertaining to the device.

[0038] Android devices, on the other hand, do not necessarily communicate with an enterprise server. Status information can be gathered from an Android device by using an app on the phone/mobile device, which communicates with the device's OS via an API, to gather or maintain status information while running. Remote procedure calls can be used by an MDM server to communicate with the app on the mobile device. An app may also be able to change certain settings on the device, such as Wi-Fi, e-mail, and network settings. The app may also respond to notifications from the MDM server to display messages to the user. An app may require that a user agrees to authorize the app at installation, which may allow the app to register with the operating system to access sensitive status information about the device.

[0039] Devices using Apple's iOS may require that the MDM system interact with a server provided by Apple. Apple's server may act as a trusted party for remote procedure calls, acting as a proxy for status requests from the MDM system to the mobile device. When a user enrolls his mobile device with the MDM system, the mobile device may download a certificate from Apple that can be used to authenticate communication to and from the mobile device. The MDM system may communicate through the Apple server to change configuration settings on the mobile device or to request that the device send status information to the MDM server.

[0040] The MDM system may require that users enroll or register with the MDM system to put the device into a managed state, whereby the MDM system can collect status information about the mobile device and enforce policies by sending certain actions to the device, such as remote wipe actions (including erasing all information from a device, or selectively erasing a portion of the information, such as sensitive date). An exemplary enrollment may include sending the user a webpage, e-mail, or SMS message, or having the user download an app. In response to the message or app, the user may be directed to a URL where configuration information and security certificates can be downloaded. Once certificates are downloaded from a certificate authority the identity of the mobile device can be trusted. This may also allow the communication with the mobile device to be encrypted for added security.

[0041] It should be noted that information about mobile devices can be gathered directly from the mobile device in certain instances, or from a third-party server, such as the BES server. In addition, status information about network access may be gathered from any corporate resources that the device is accessing. Similarly, third-party authorities may provide identity information, such as when a user logs into a device using his Google credentials.

[0042] Furthermore, actions can be taken with respect to the device by interacting with any of these components. For example, if an action requires a remote wipe of the device, the action may be taken by sending a remote procedure call to the device, including sending it to an app or to the operating system of the device to carry out the responsive wipe of information. Similarly, actions resulting in limiting access to corporate resources can be taken at the device, such as by changing configurations of any client apps on the phone to limit access to a remote resource, or

at a server which may be part of the corporate network or corporate resource. For example, when a user's device is out of compliance, a VPN server may limit access to corporate data when a user logs on to the VPN. Remote configuration performed by the MDM system can include remotely changing configuration information on the user device or on any chosen corporate resource.

[0043] By providing a rules-based management system that the server, a simplified administrative experience can be provided, which may be agnostic from the administrative standpoint to the type of mobile device being managed. Rules allow the administrator to define certain status conditions, such as installation of blacklisted apps, that trigger a responsive action. The action may be an action defined by the administrator that is appropriate to the out-of-compliance condition. For example, the action can include warning the user via an e-mail or pop-up message that he is not allowed to use certain applications on devices that access corporate resources. The rules may include further responsive actions if the out of compliance condition continues, such as sending alerts to IT administrators that the user has failed to uninstall blacklisted app. This can allow administrators to directly interact with the user to get the offending application uninstalled. This may be suitable response where the device operating system does not provide the ability to remotely uninstall specific applications. Similarly, a rule may be defined such that after a certain period of time since the user was first warned, access from mobile device to a corporate resource can be restricted or blocked at the device or server level.

[0044] FIG. 1 demonstrates the components of an exemplary embodiment of an MDM system 5. MDM system 5 interacts with mobile devices 10 through network 12. Network 12 can include any reasonable network, including the Internet. MDM system 5 may also interact with servers and other resources 14 on the Internet. Servers and resources 14 can include resources that interact with mobile devices 10, such as BES servers, corporate resources, or third-party servers. Mobile devices 10 may access servers and resources 14 as part of their normal behavior while being managed by MDM system 5. For example, servers and resources 14 may include an Exchange server for providing email access to mobile devices 10. During normal in-compliance operation, the mobile devices can freely access email in this manner; during out of compliance operation, such access may be restricted according to one or more rules.

[0045] MDM system 5 can interact with mobile devices 10, and servers and resources 14 via any suitable number of device front ends 16. Device front ends 16 can be specialized software components that have been configured to interact with certain types of mobile devices. For example, a device front end related to an Apple iOS device is configured to work with Apple's server and the mobile device to gather any requested status information from the mobile device. Similarly, a device front end can be configured to work with an Android device, which may include the ability to communicate with an app running on the device. By providing a plurality of device front ends 16, software device front ends can easily be added to the MDM system 5 as mobile device platforms change or as an organization chooses to support new platforms. It should be appreciated that device front ends 16 include software and/or hardware components sufficient to communicate over network 12 to mobile devices 10, and servers and resources 14.

Furthermore, device front ends 16 may also be configured to support the execution of actions that result from rules-based policies on the MDM system 5.

[0046] Device front ends 16 act as interfaces to gather status information pertaining to mobile devices 10, across network 12. In some embodiments, device front ends 16 regularly poll mobile devices 10, and servers and resources 14 to obtain status information on a periodic basis. In some embodiments, a portion of status information can also be regularly pushed from devices or servers on network 12 to the device front ends 16. When the device front ends 16 retrieve mobile device status information, this information is sent to message handlers 18. Message handlers 18 can include software components, such as one or more module, application, or thread. Message handlers 18 collect incoming data about mobile devices, format this status information into a usable form (which may include parsing and normalizing device information for uniformity across platforms), and forward this information to device database 20. It should be appreciated that message handlers 18 may include a plurality of handlers, each adapted to handle devices of a given mobile device platform. In some embodiments, each of message handlers 18 and device front ends 16 can be combined into a single software component.

[0047] Upon processing mobile device status information, message handlers 18 provide real-time status updates 22 to be stored and organized as records in device database 20. Device database 20 may include one or more records for each mobile device registered with MDM system 5. Using status updates 22, device database 20 can update these records and provide substantially real-time information about the status of mobile devices 10. Device database 20 can provide persistent storage of mobile device status information allowing an administrator to

access status information about mobile devices 10, even when a device is offline. Device database 20 can include one or more data stores that include one or more software objects suitable for interfacing with one or more memory devices, including hard drives, flash drives, shared memory, cloud-based memory, etc. Furthermore, old status information in device database 20 can be compared to incoming status updates 22 to determine which attributes of a mobile device have changed on a substantially real-time basis. Accordingly, device database 20 can maintain status information about mobile devices enrolled with the MDM system as a series of device attributes that are updated on a substantially real-time basis.

[0048] In some embodiments, device database 20 can be used as part of the rules-based policy components of MDM system 5, which are shown in FIG. 1, as well as used for maintaining real-time inventory of mobile devices 10. Other components not shown in FIG. 1 may interact with device database 20 to retrieve inventory information for any monitoring purpose desired by an IT administrator. Accordingly, in some embodiments, device database 20 can be used as a database for storing a snapshot of the mobile device inventory (e.g. those devices enrolled for use of the corporate resources).

[0049] Monitoring engine 24 can be a software component that is configured to interact with device database 20 to observe changes in status information. Monitoring engine 24 may receive pushed updates from device database 20 to inform the monitoring engine that a device attribute has changed. This can allow actions to be taken on device attributes immediately. In some embodiments, monitoring engine 24 regularly polls device database 20 to determine what, if any, device attributes related to mobile devices 10 have changed. In some embodiments, monitoring

engine 24 determines if any attributes that are the subject of a rules-based policy have changed. In these embodiments, monitoring engine 24 is configured to observe certain attributes for changes after a policy related to those attributes has been added by an IT administrator. In some embodiments, monitoring engine 24 is preconfigured to look for changes to commonly used attributes, and may be further configured to look for certain attributes in response to administrator-defined rules. An exemplary algorithm that is carried out by monitoring engine 24 is shown in FIG. 3.

[0050] The monitoring engine 24 denotes any relevant changes in attributes of mobile devices in the rules evaluation queue 26. The rules evaluation 26 queue provides an interface between the monitoring engine 24, and the core rules engine 28. Mobile device status changes may wait in rules evaluation queue 26 until core rules engine 28 is free to process this information. Rules evaluation queue 26 may be any software component that maintains memory structures suitable for storing device status updates for access by core rules engine 28. In some embodiments, by using a rules evaluation queue, changes may be handled in a scalable manner. In some embodiments, the number of mobile devices 10 being monitored by MDM system 5 can be sufficiently large that updates to status information may arrive faster than core rules engine 28 may be able to process for limited periods of time.

[0051] Furthermore, in some embodiments, rules evaluation queue 26 provides a means for keeping track of compliance changes for mobile devices 10. In some embodiments, core rules engine 28 also places resulting actions (or information pertaining to actions) in rules evaluation queue 26. This can allow core rules engine 28 to monitor past actions and pending actions, along

with new changes in status information of mobile devices. This can also allow the rules evaluation queue to provide information to core rules engine 28 regarding pending actions.

[0052] Core rules engine 28 is a software component responsible for evaluating device compliance with administrator-defined rules. These rules can include policy-based actions responsive to the compliance state of a mobile device with the policy rules. Core rule engine 28 retrieves device status information from rules evaluation queue 26 and applies administrator defined logic in the form of rules. The rules can define acceptable values for device attributes. Based on these values the core rules engine can determine whether a mobile device is out of compliance and depending on the attribute that is out of compliance, the core rules engine can select a responsive action as defined by the rules. In some embodiments, core rules engine 28 processes rules and initiates actions automatically, in real time in response to device attribute changes, without needed confirmation from an administrator.

[0053] In some embodiments, rules evaluation queue 26 is responsible for comparing device attribute values to administrator defined acceptable values. The rules evaluation queue can then present its determination regarding whether the device is out of compliance and of the reason for the out of compliance status to core rules engine 28. In these embodiments, core rules engine 28 can apply rules to the device attributes without needing to separately make a determination of whether the attribute is in compliance. In these embodiments, the core rules engine can then apply rules logic to the compliance state of the device, with the device attribute information preprocessed by the rules evaluation queue 26. This can facilitate scalability, as core rules engine 28 can begin with knowledge of whether a given attribute is in compliance or not.

[0054] For example, and administrator may determine that mobile devices that run file-sharing apps present a risk to corporate resources. The administrator may create a rule that causes a warning message to appear on a user's mobile device, if he is running a file-sharing app. The rule may also send an e-mail to the administrator. If a user installs a file-sharing app on his mobile device, device front ends 16 will determine that the file-sharing app has been installed and note this app in the device database 20. Monitoring engine 24, will determine that a list of apps installed on the device has changed and that the administrator is interested in what types of apps) are installed on mobile devices enrolled with MDM system 5 (or that the administrator is interested in certain apps. Monitoring engine 24 will then note the change in the mobile device status, placing an entry in rules evaluation queue 26 that reflects that the file-sharing app has been installed on the user device. Rules evaluation queue 26 or core rules engine 28 can compare the application to a list of blacklisted apps to determine if the newly installed app brings the device out of compliance. Core rules engine 28 may then apply a rule to the new compliance status of the device. The rule may state that if the device is out of compliance because it is running a file-sharing app, then a message should be sent to the user and the administrator. Core rules engine 28 will then execute this rule and will request that the action take place.

[0055] When an action is needed, according to a rule executed by core rules engine 28, the core rules engine can send one or more action requests 30 to an action execution controller 34. Action execution controller 34 may be a software module that is configured to facilitate the execution of actions. For example, an action that requires sending a warning to a user may require that action execution controller 34 interacts with an e-mail server to send an e-mail message to the user of the mobile device. Alternatively, the message may require that action

execution controller 34 communicate with an app or the operating system of the mobile device. Action execution controller 34 may use device front ends 16 to communicate with the device. Similarly, actions related to wiping part or all of the memory of a device can be facilitated by action execution controller 34, using device front and 16 to communicate with the operating system of the mobile device across network 12 to initiate a remote data wipe. Other examples of actions that may be facilitated by action execution controller 34 can include interacting with servers and resources 14 to restrict the devices access at the server level. Other actions as described throughout can also be facilitated by action execution controller 34.

[0056] Upon evaluation of the rules by core rules engine 28, device database 20 may be updated to reflect any changes in the compliance status of the mobile device. Similarly, upon taking an action on a mobile device, core rules engine 28 may note the action in device database 20. Core rules engine 28 may send status updates 32 to device database 20 to maintain a record of actions and compliance state changes of the device.

[0057] In some embodiments, there may be a delay between action requests 30 and the actual completion of the action by the action execution controller 34. For example, if a device is off-line, it may be several hours or days before an action could be completed. Upon completion of the action, action execution controller 34 can send a confirmation 36 to rules evaluation queue 26. By placing the confirmation 36 into rules evaluation queue 26, core rules engine 28 can consider the final execution of the action. In some embodiments, rules can be defined that consider as input the action state of the device. For example, if a user is newly warned that his device is out of compliance, a rule may state that within two hours of the warning, the device

should be restricted from accessing corporate resources if the user has not resolved the issue. Similarly, the core rules engine may consider a different action. For example, according to a rule, if confirmation of the originally planned action does not arrive within a predetermined time, such as 24 hours, an appropriate action may to be to restrict access to corporate resources at the server level in case the device has somehow gotten out of a managed state.

[0058] In some embodiments, MDM system 5 includes a user interface 38 that allows an IT administrator to view real-time device status information stored in device database 20, and to define rules for automatically taking actions on devices based on this status information. Accordingly, depending on the implementation, user interface 38 may interact with any or all of the components of MDM system 5. In some embodiments, user interface 38 interacts with core rules engine 28 to define a set of rules that will be enforced by core rules engine 28. Core rules engine 28 may include appropriate data stores for maintaining the rules defined by the user via user interface 38. In some embodiments, these rules may also be changed via configuration files or the like. User interface 38 can include software instructions and rendering information such as pictures, HTML, style sheets, flash files, and the like, which may be used to instruct a computer controlled by the administrator to display an interface, such as the interfaces depicted in FIGs. 5-11. It should be appreciated that the interface may include one or more websites or portals that may be remotely accessed.

[0059] MDM system 5 may be implemented on one or more computing devices. This may include, in some embodiments, a cloud-based implementation, whereby different components of MDM system 5 reside on different computers on a network, or are replicated across different

computers on a network to provide flexible scalability. It should be appreciated that these computing devices may include hardware and software executing on a processor that perform the roles discussed with respect to FIG. 1. Each component of the MDM system can be a separate software module, part of a shared software module, and can include one or more threads for carrying out the role of each component that execute on one or more processors in a suitable processing environment, such as a Linux or Window-based server environment.

[0060] FIG. 2 shows a detailed view of the rules evaluation queue 26 and core rules engine 28 for use with some embodiments of the present invention. In these embodiments, user interface 38 is used to define rules in a rules database 40, which may be accessed by core rules engine 28 and rules evaluation queue 26. Rules evaluation queue 26 includes three primary queues. Attribute change queue 42 can be used to process changed attribute values. These values can be used to determine the current state of compliance of a mobile device. The attribute change queue 42 provides an input to core rules engine 28 for determining which actions may be applicable based on administrator defined rules. A corresponding thread, attribute change thread 43, runs as part of core rules engine 28. This thread is responsible for monitoring attributes in attribute change queue 42. Attribute change thread 43 may then apply the rules from the rules database 40 to determine if an action needs to be taken.

[0061] If an action needs to be taken, action thread 45 will work with attribute change thread 43 to initiate a resulting action. Action thread 45 will place pending actions in action queue 44, which can be part of rules evaluation queue 26. Action queue 44 can include a list of past

actions and pending actions, which may be useful for core rules engine 28 to determine appropriate subsequent actions.

[0062] Rule change queue 46 can be used for new or edited rules defined by an administrator using user interface 38. For example, when an administrator defines a new rule, it may be necessary to reevaluate each mobile device enrolled in the network to determine if the new rule requires an action. Corresponding rule change thread 47 of the core rules engine can monitor rule change queue 46 and can evaluate the rule and each mobile device based on information stored in the device database 20. Similarly, resulting actions from rule change thread 47 can be handled by action thread 45. The details of the operation of core rules engine 28, in some embodiments, are disclosed with respect to FIG. 4.

[0063] When monitoring engine 24 determines that an important attribute in the device database 20 has changed, monitoring engine 24 will place this new attribute value into attribute change queue 42. This attribute change can then be immediately (or after its place in the queue is reached) evaluated by the attribute change thread 43, resulting in new actions to be taken based on rules in rules database 40. These actions may be handled as discussed with respect to FIG. 1 and recorded in action queue 44.

[0064] FIG. 3 shows an exemplary algorithm 50 that may be used by monitoring engine 24. At step 52, monitoring engine 24 monitors device database 20 for attributes related to rules defined by an administrator. These attributes may be all or a subset of available status information pertaining to each device. Step 52 may occur at regular intervals (e.g. polling), or in response to each update for each device in device database 20. At step 54, monitoring engine 24

determines if the attribute has been modified. If the device attribute has been modified, monitoring engine 24 will gather information about the device, including, in some embodiments, both the old attribute value and the new attribute value. In some embodiments, additional attribute information pertaining to the advice will also be captured. At step 56, the gathered information is placed into the rules evaluation queue 26 for evaluation by the core rules engine, such that rules-based actions may be initiated in response to the new attribute values.

[0065] FIG. 4 shows an exemplary algorithm 60 for use with some embodiments of core rules engine 28. At step 62, the core rules engine views and attribute in the attribute change queue 42. This attribute is then compared to attribute values defined in rules to determine if the new attribute value triggers an action according to one or more of the rules. At step 63, the resulting action is considered, and a determination is made whether the action requires an alert or not. If an alert is required, according to the rule, an alert will be sent to the user of the mobile device and/or an administrator as specified in the rule at step 64.

[0066] If no alert is required (or once an alert has been sent and an additional action is needed, according to the rule), an appropriate action can be taken. Exemplary actions that may be taken are discussed throughout this specification. At step 65, the core rules engine determines whether an action can be taken immediately, or whether the rule requires waiting for a predetermined amount of time (e.g. a grace period). In some embodiments, the rule may specify an action having a countdown or predetermined timeframe during which corrective action may be taken by the user. For example, if a user's mobile device is newly out of compliance, he may be warned that his device is out of compliance and be given two hours to fix the problem. If a

grace period is appropriate, at step 65, a countdown can be started so that a corrective action can be taken when the countdown expires. Action queue 44 may be used to facilitate actions for which a countdown has begun.

[0067] Once any grace period has expired (or the action should be immediately taken under the rule), the action can be taken. However, in some situations, actions may have already been taken against a device, such as actions taken by other rules already triggered. It may not be desirable or feasible to repeat an action. At step 66, the core rule engine determines if an action has not yet been taken, and if not, will take that action, as defined by the rule.

[0068] At step 67, once an action has been initiated, the action request can be recorded in the database, such as device database 20. In some embodiments, pending actions may be placed in action queue 44 and confirmation can subsequently be received to verify that the action has indeed occurred. In some embodiments, once an action has been taken on a mobile device, attributes related to the compliance date and the action taken can be updated in device database 20, so that these actions can be considered in the future.

[0069] If an attribute changes to a value that is in compliance, algorithm 60 may proceed to step 70. At step 70, previously triggered rules relating to the attribute are considered. These rules are said to be active. For example, if a user previously had installed a file-sharing app and his e-mail access was restricted, when the user removes the offensive application, algorithm 60 may proceed to step 70. At step 70, core rules engine 28 may consider that the rule that previously blocked the users e-mail access is no longer triggered by the new attribute value. Core rules engine 28 may then begin the process of restoring the user's e-mail access. If there

are no active rules for the newly changed attribute, core rules engine 28 can proceed to the next attribute in the attribute change queue.

[0070] If the new attribute value results in a more compliant device, core rules engine 28 may proceed to step 71. At step 71, core rules engine 28 can disable (e.g., reset) the currently active rule that had been previously been applied to the now compliant attribute.

[0071] At step 72, the core rules engine considers whether or not the previous attribute value had resulted in an action on the mobile device. For example, if a previous attribute value made the device noncompliant with a rule regarding e-mail access, the rule may previously have resulted in action, whereby the users e-mail access was restricted. If the new attribute value, according to the rule, should not result in the same action, core rules engine 28 can consider whether to revoke (i.e., undo) the previous action. For example, for a newly compliant device that previously had its e-mail access restricted, it may be appropriate to revoke this restriction and restore e-mail access to the device.

[0072] At step 73, core rules engine 28 considers whether there are any other reasons for the action associated with the previously active rule. For example, there may be multiple noncompliant attributes for a mobile device that have resulted in blocking a user's e-mail access. Step 73 allows the core rules engine to determine whether or not that e-mail access may be restored now that one of the noncompliant attributes is in compliance. Step 73 considers the previously recorded actions for this mobile device and determines if there are other rules that have taken (or previously attempted to take) the action now sought to be revoked.

[0073] In some embodiments, step 73 benefits from recording of actions at step 67. In some embodiments, redundant actions may also be recorded at step 67, without repeating the action. For example, once a noncompliant device's e-mail access has been blocked, a subsequent rule that also would result in blocking the e-mail access may be recorded in a database without repeating a step of blocking the e-mail access, which is already blocked.

[0074] If there are no other rules that explain the previous action, the previous action can be revoked at step 74. In the example of restricted e-mail access, e-mail access can be restored by communicating over a network to e-mail server to once again allow the mobile device to receive e-mail messages.

[0075] At step 75, core rules engine 28 considers whether there are any other rules that have been triggered on this device that indicate the device is noncompliant. This step can allow the device to be restored to a fully compliant state once no rules are triggered. For example, a device whose e-mail access has now been restored may be still noncompliant with other rules related to corporate data access or access to other resources. At step 75 other rules pertaining to the device and previously recorded actions related to other rules can be considered. If there are no other rules that are triggered on the device, core rules engine 28 can update the device database to indicate that the device is now fully compliant with all rules.

[0076] FIG. 5 shows an exemplary screen shot for a user interface 80 provided to an administrator for managing rules used by MDM system 5. Using a web based interface or an application, and administrator may login to the MDM system and be presented with a variety of types of available compliance rules. These compliance rules can present preconfigured

templates that may be used to set up common security or management rules. In this example, and administrator may require that devices be enrolled with the MDM system (called MaaS360 in this example) to be granted access to corporate resources. Enrollment may require that the user agree to a "terms of use" policy and register his identity and the identity of his device with the MDM system an install a certificate to authenticate the user. The user may also be required to grant permissions to the MDM system to resources and the user's mobile device. This can allow the MDM system to configure resources and monitor and configure the user's device. In some mobile platforms, such as the Android platform, the user may also be required to download an app that provides added functionality for the MDM system to access the user's device and configuration information.

[0077] Rule 82 may be used to ensure that a user is securing his mobile device using a pass code. An administrator may click a button associated with the enforce passcode compliance template to configure and enforce a passcode rule. Additional rules that may be available through user interface 80 can include templates to configure application restrictions, such as identifying blacklisted applications, templates to enforce minimum OS versions for the mobile device to ensure that the users mobile device is running a recent version of a mobile operating system as shown in template 84, a template for limiting the ability of rooted or jail-broken mobile devices from accessing corporate resources (which can ensure that users do not have root access to his device, which may indicate the device is a higher risk device or is difficult to manage securely), and a template to restrict device access when the device has recently changed the SIM card being used, such as template 86.

[0078] Other available rule templates may include a template for enforcing control and management that verifies that the mobile OS is authentic and functioning properly, a template for monitoring the roaming state and data usage of the device, a template for requiring that data on the mobile device related to corporate resources is encrypted, a template for identifying conditions and configuring the device for remote wipe capabilities, and a template for restricting access to corporate resources. When the device does not have sufficient permissions to access e-mail resources. Other action based rule templates may include any suitable rules for performing the functions of an MDM system, as discussed throughout this application.

[0079] FIG. 6 shows the user interface for configuring passcode rule 82. By clicking a button associated with the template in interface 80, a template may appear in the user interface to allow the administrator to configure the specifics of the enforced passcode rule. This template may have two sections: a trigger section and an enforcement section. By selecting boxes in the trigger section, an administrator may identify whether the rule should be applied to compliant devices or noncompliant devices (e.g., those devices that do not have a passcode set up). Most rules discussed throughout have assumed a rule applies to a noncompliant device. In some embodiments, a rule may be triggered by a compliant device, such as a rule that configures a service only when a device has come into compliance. The administrator may also select a passcode policy, such as a policy that identifies the minimum passcode strength required to be compliant. The selected policy may be a preconfigured policy or a custom policy defined by the administrator, in some embodiments.

[0080] In an enforcement section of the template, the type of action to be taken in response to the selected trigger can be identified. An administrator may select a drop-down box that gives the available options for actions. For example, an administrator may choose to block the device from a selected corporate resource. He may also select a grace period and a warning message (which may be tailored to the rule) to be displayed to a user of out of compliance device before the action occurs. This may enable the user to bring his device back into compliance before an action takes place.

[0081] FIG. 7 shows a template 84 that may be selected to enforce minimum OS versions required for a mobile device to access corporate resources. By selecting a button in user interface 80, an administrator can bring up a template to create a rule that excludes devices with certain operating systems or older versions of operating systems. In some embodiments, the template can be divided into two sections, a trigger section and enforcement section. Here, a trigger section allows the administrator to select the minimum version of multiple operating systems. A separate drop-down menu can be provided for iOS, Android, Symbian, Windows Phone, or other mobile device OSs. An enforcement section may allow the administrator to select appropriate enforcement actions if the rule is triggered. This may include blocking the mobile device's access to certain corporate resources, and may include providing a grace period and warning message to the user. In some embodiments, the enforcement action may also allow an alert to be sent to the administrator automatically when the device is out of compliance with the rule.

[0082] FIG. 8 shows an exemplary template 86 for configuring a rule that restricts access when a device has changed SIM cards. A mobile device that has switched SIM cards may be an indication that the device has been stolen. By selecting a button from user interface 80, the administrator may be presented with a template for defining the rule. In some embodiments, where the triggering condition is defined by the type of rule, the template may include only an enforcement section that allows the administrator to define the type of action to take when the device is out of compliance.

[0083] In some embodiments, and administrators may configure e-mails to be sent to administrators when devices become noncompliant. Furthermore, administrators may also identify certain devices that should be exempt from certain actions. For example, a VIP of an organization, such as CEO may not want to have his e-mail access disabled without an administrator speaking to him first. In certain situations, the relationship of an individual mobile device to the organization may be unique and warrant exemptions from rules that may otherwise get in the way of an organization's business. FIG. 9 presents a user-interface that may be suitable for configuring some of the settings. The interface may allow administrators to define administrative e-mail addresses to receive alerts related to device compliance issues. The interface may also allow certain devices to be selected to be exempt from rules.

[0084] In some embodiments, the device database may include a log of all actions taken on a device during a predefined period, such as a six-month period. This log may be used by administrators to view actions taken on devices, rather than (or in addition to) relying on separate e-mails for each device way rules triggered. This can be used for determining a pattern of

behavior. Similarly, log files may be e-mailed to administrators, rather than sending individual e-mails relating to each device and each rule triggered.

[0085] FIG. 10 shows an exemplary screen shot for another embodiment user interface provided to an administrator for managing rules used by MDM system 5. Using a web based interface or an application, and administrator may login to the MDM system and be presented with a variety of types of available compliance rules. These compliance rules can present preconfigured templates that may be used to set up common security or management rules. In this example, and administrator may require that devices be enrolled with the MDM system (called MaaS360 in this example) to be granted access to corporate resources.

[0086] Additional rules that may be available through the user interface of FIG. 10 can include templates to enforce minimum OS versions for the mobile device to ensure that the users mobile device is running a recent version of a mobile operating system, templates to create a rule to remotely wipe a device (e.g. when the device is extremely out of compliance or appears to be stolen, such as when the device has recently changed the SIM card being used or is reported missing), a template to require that data on the device is encrypted, a template to configure application restrictions, such as identifying blacklisted applications, a template for limiting the ability of rooted or jail-broken mobile devices from accessing corporate resources (which can ensure that users do not have root access to his device, which may indicate the device is a higher risk device or is difficult to manage securely), and a template to restrict device access to specific corporate resources.

[0087] FIG. 11 shows templates that may be selected to enforce other rules that may be suitable to monitoring inventory and controlling data charges. For example, a template 90 may be used to define geo-fencing rules. Geo-fencing rules may restrict a device's functionality based on the location of the device. For example, a device may have data access restricted if out of the country to save cost or change the device's access permissions when the device is operating while at a company facility versus when the device is at an untrusted location, such as an airport or another city. To apply a geo-fencing rule, an MDM system can gather location information about a device and compare that information to compliance criteria. Location information may include GPS information from the device that indicates a geographic location, Wi-Fi information, reflecting an IP address to indicate location, or network information, such as the carrier information, which may reflect the general or specific location of the device or nearest cell-tower. Compliance may be based on a whitelist, a blacklist, and/or a lookup or calculation from the location information to determine an estimate of the physical location of the device.

[0088] Furthermore, the device may be required to check in with the MDM system on a regular basis to ensure that geo-fencing remains up-to-date. A device that fails to check in may have access to resources restricted at the server level. Available actions may include alerting both the user of the device and/or an administrator, restricting the device's access to certain sensitive resources, blocking access to all resources, changing policies on the device, or wiping the device.

[0089] Template 92 may be used to monitor data usage. When these rules are selected, alerts may be sent to the user and/or the administrator that a user is approaching data limits. These

limits may be separate for in-network data usage and for out-of-network data usage, which may be billed at a more expensive rate.

[0090] Table 1 shows an exemplary list of the types of rules that may be selected by an administrator, the attributes considered by the rule for determining compliance, and the available actions that may be selected by the administrator when the rule is triggered.

[0091] Table 1

Rule Type	Attribute/Comments	Available Actions
Enforce Minimum Operating System Version	Operating System > OS Version	Alert, Block, Wipe, Selective Wipe, Change Policy
Enforce Remote Wipe Support	Security Compliance > Remote Wipe Support	Alert, Block, Selective Wipe, Change Policy
Enforce Full Encryption Support	Security Compliance > Hardware Encryption	Alert, Block, Wipe, Selective Wipe, Change Policy
Enforce Applications Compliance	Security Compliance > Policy Compliance State	Alert, Block, Wipe, Selective Wipe, Change Policy
Restrict Jailbroken or Rooted Devices	Security Compliance > Device Rooted and Security Compliance > Device Jailbroken	Alert, Block, Wipe, Selective Wipe, Change Policy
Monitor SIM Changes	Network Information > SIM (ICCID) ID	Alert
Enforce Management and Control	Hardware Inventory > Managed Status	Alert, Block, Wipe
Restrict Corporate Resources for devices blocked on	Security Compliance > Mailbox Approval State	Alert, Wipe, Selective Wipe, Change Policy

mail server		
Monitor Roaming Changes	Network Information > Roaming	Alert, Block, Wipe, Selective Wipe, Change Policy
Enable Geo-fencing	Location Information	Alert, Block, Wipe, Selective Wipe, Change Policy
Monitor Roaming data usage	Roaming data used as per billing plan	Alert, Alert Administrator only and Alert User only.
Monitor In-network data usage	In network data usage as per billing plan	Alert, Alert Administrator only and Alert User only.
Enforce Passcode	Enforce Passcode > Passcode	Alert, Block, Wipe, Selective Wipe, Change Policy

Appendix A: Examples of Data Formats

[0092] The following are examples of the data formats that can be used for storing information about mobile devices in the mobile device database 20.

[0093] An exemplary list of the core/generic attributes for describing mobile device 10 is shown in Table 2.

[0094] Table 2

Attribute	**Description**	**Data Type**
Device ID	Unique ID of the Device in the 3rd party application	String
Is New	Flag that indicates whether the device is new and whether its data is being uploaded for the first time.	Boolean - Yes / No
Device Name	Name of the device	String
Serial Number	IMEI or ESN for the device	String

(IMEI/ESN)	depending on whether the device supports GSM or CDMA	
Email Address	Corporate Email address of the user of the device. Typically this is used to register the device.	String
Username	AD Username of the user of the device – Typically this is used to register the device.	String
Domain	Domain of the user of the device	String
Installed Date Time (GMT)	Activation date/time of the device in the 3rd party application. This should be in GMT	Timestamp
Last Reported Time (GMT)	Last Sync date/time of the device in the 3rd party application. This should be in GMT	Timestamp
Platform	Device Platform – One of following values – iOS, Android, Windows Mobile, Windows Phone 7, Symbian, Palm, BlackBerry, Others	Enumeration
Source	Name of the 3rd party application that is providing the data	String

[0095] An exemplary list of the attributes for hardware, including corporate servers and the hardware on the customer premises for hosting the cloud extension agents is shown in Table 3 and Table 4. Table 3 shows the static or basic data associated with hardware, while Table 4 shows dynamic data associated with the hardware that is likely to change on incremental state changes.

[0096] Table 3

Attribute	**Description**	**Data Type**
Device ID	Unique ID of the Device in the 3rd party application	String
Device Type	Possible device types – Desktop, Laptop, Server, Smartphone, Tablet or Others	Enumeration
Manufacturer	Manufacturer of the device	String

Model	Model Name of the device	String
Model ID	Model ID of the device	String
Platform Serial Number	Platform specific serial of the device. For ex: Apple Serial Number, PIN, etc.	String
UDID	UDID or UUID of the device	String
Operating System	Operating System and Major Version of the device. For ex: iOS 4	String
Operating System Version	Full Operating System version including the build number	String
Software Platform Version	Software Platform version (specific to BlackBerry)	String
Modem Firmware Version	Specific to iOS, Modem Firmware Version	String
Total Internal Storage	Total internal memory of the device in GB	Float
Total External Storage	Total external (SD card) memory of the device in GB	Float
RAM	RAM on the device (in MB)	Integer
Screen Width	Screen width of the device	Float
Screen Resolution	Screen resolution of the device	String
Screen Language	Screen Language of the device	String
Time zone	Current time zone offset of the device. Ex: +0530	String
Last Reported Time (GMT)	Last Sync date/time of the device in the 3rd party application. This should be in GMT	Timestamp

[0097] Table 4

Attribute	**Description**	**Data Type**
Device ID	Unique ID of the Device in the 3rd party application	String
Available Internal Storage	Free internal memory of the device in GB	Float
Available External Storage	Free external memory of the device in GB	Float
Total Application Data	Total size of data across all applications on the device	Float
Battery Level	Current battery level (in percentage) of the device	Float
Battery Condition	Current condition of the device battery	String
Last Reported Time (GMT)	Last Sync date/time of the device in the 3rd party application. This should be in GMT	Timestamp

[0098] An exemplary list of the attributes related to security and compliance status of a mobile device is shown in Table 5. In addition, information related to the particular states of the device related to Exchange ActiveSync or BES attributes may be stored.

[0099] Table 5

Attribute	**Description**	**Data Type**
Device ID	Unique ID of the Device in the 3rd party application	String
Jailbroken or Rooted Device	Applicable to iOS and Android devices. Indicates whether the device is Jailbroken, in case of an iOS device or whether it is Rooted, in case of an Android device	Boolean
Device Password Status	Whether the Password is required to use the device and what is the status of the device with regards to Password policy Compliant Not Enabled Not Compliant per all requirements Not Compliant per Profiles Passcode Policy Configured Passcode Policy Not Configured Not Available	Enumeration
Minimum Password Length	Minimum length of the password enforced on the device	Integer
Password Quality	Quality of the password enforced Numeric Alphabetic Alpha-numeric	Enumeration
Maximum Time to Lock	Time in minutes after which the device will automatically lock	Integer
Maximum Failed Password Attempts for Wipe	Number of failed password attempts after which the device will automatically wipe	Integer
Encryption Status	Encryption Status of the device No Encryption File-level Encryption (iOS only) Block-level Encryption (iOS only) File & Block-level Encryption (iOS only) Partial Encryption	Enumeration

	Encryption Complete	
Policy Name	Name of the policy enforced on the device	String
Policy ID	A unique identified for the policy on the device	String
Policy Version	Currently enforced version of the policy	Integer
Last Policy Update Date/Time	Last date/time when any policy update was given to the device. This should be in GMT	Timestamp
Policy Compliance Status	Whether the device is in compliance per applied policies. Possible values: In-Compliance, Out-of-Compliance	Enumeration
Is Remote Wipe Supported	Whether remote wipe is supported by the device	Boolean
Device Wiped	Status of wipe action sent to the device. Possible values: Pending, Complete	Enumeration
Last Wipe Applied Date/Time	Date/time when Wipe was applied. In case multiple wipe commands can be sent to the device (like in case of Exchange server), this should be the last date/time for the wipe. This should be in GMT	Timestamp
Last Time Message Received by Device	Last time message was received by the device	Timestamp
Last Time Message Sent from Device	Last time message was sent from the device	Timestamp
Auto-Backup Configured	Whether automatic backup is configured for the device	Boolean
Auto-Backup Frequency	Frequency of automatic backup Daily Weekly Monthly Others	Enumeration
Last Successful Backup Time	Last time there was a successful backup from the device	Timestamp
Auto-Backup Exclusions	Items excluded from automatic backup Messages PIM Data MMC Data	Enumeration
Allow User to install applications	Allow the user to install applications	Boolean
Last Reported Time (GMT)	Last Sync date/time of the device in the 3rd party application. This should be in GMT	Timestamp

[00100] Having thus described several aspects of at least one embodiment of this invention, it is to be appreciated various alterations, modifications, and improvements will readily occur to those skilled in the art. Such alterations, modifications, and improvements are intended to be part of this disclosure, and are intended to be within the spirit and scope of the invention. Accordingly, the foregoing description and drawings are by way of example only.

Petitioner Ex 1002, p. 60
Zimperium v. Taasera, IPR2024-00007

CLAIMS

What is claimed is:

1. A method for providing device management services comprising steps of:

gathering, from a network, status information related to each of a plurality of mobile devices, each mobile device utilizing one of a plurality of different mobile operating systems;

storing the status information in an electronic database accessible to a server;

evaluating a first compliance state of at least one of the mobile devices from the status information using a plurality of administrator-defined rules; and

initiating at least one action defined by the user-defined rules in response to the step of evaluating,

wherein the step of evaluation is performed by a server automatically, in response to changes in the status information.

2. The method of claim 1, wherein the at least one action is selectable from a plurality of actions, comprising blocking access by the at least one of the mobile devices to a corporate resource.

3. The method of claim 1, wherein the at least one action is selectable from a plurality of actions, comprising blocking e-mail access for the at least one of the mobile devices.

4. The method of claim 1, wherein the at least one action is selectable from a plurality of actions, comprising wiping information from the at least one of the mobile devices.

5. The method of claim 1, wherein the at least one action is selectable from a plurality of actions, comprising warning a user of the at least one of the mobile devices that further action may be taken.

6. The method of claim 1, wherein the step of gathering status information, for the at least one mobile device, comprises gathering information from that mobile device and at least one other source on the network.

7. The method of claim 1, further comprising the step of subsequently evaluating a second compliance state of at least one of the mobile devices to determine if the at least one action should be revoked.

8. The method of claim 1, wherein the plurality of different mobile operating systems comprise at least Android and iOS.

9. The method of claim 1, wherein the status information comprises location information about each mobile device.

10. A method for providing device management services comprising steps of:

making a determination that an attribute of a mobile device has changed;

evaluating the attribute, by a processor at a server in response to the determination, to determine if it triggers at least one of a plurality of administrator defined rules, which indicates that the attribute is out of compliance; and

automatically initiating, at the server, an action defined by the at least one of a plurality of administrator defined rules if the attribute is out of compliance,

wherein the attribute is stored in a data store accessible to the server, that includes substantially real-time data pertaining to a plurality of attributes of a plurality of mobile devices, comprising devices having different mobile operating systems.

11. The method of claim 10, wherein the step of automatically initiating an action comprises warning a user of the mobile device that the device is out of compliance and subsequently causing the action to be performed if the attribute remains out of compliance after a period of time defined in the at least one rule.

12. The method of claim 10, further comprising the step of automatically revoking the action if the attribute is brought back into compliance.

13. The method of claim 12, wherein the step of automatically revoking the action comprises determining if another of the plurality of rules is triggered.

14. The method of claim 10, further comprising the step of gathering the plurality of attributes for at least one of the plurality of mobile device by gathering attribute information from that mobile device and at least one other source on a network.

15. The method of claim 10, wherein the plurality of different mobile operating systems comprise at least Android and iOS.

16. The method of claim 10, wherein the attribute comprises location information about the mobile device.

17. A system for providing device management services comprising:

a data store configured to be accessible by a server;

computer readable instructions for execution on the server comprising instructions configured to:

make a determination that an attribute of a mobile device stored in the data store has changed;

evaluate the attribute, in response to the determination, to determine if it triggers at least one of a plurality of administrator defined rules, which indicates that the attribute is out of compliance; and

automatically initiate an action defined by the at least one of a plurality of administrator defined rules if the attribute is out of compliance,

wherein the data store is configured to include substantially real-time data pertaining to a plurality of attributes of a plurality of mobile devices, comprising devices having different mobile operating systems.

18. The system of claim 17, wherein the computer readable instructions further comprise instructions configured to present a user interface to an administrator to allow selection of at least one attribute and one available action to define the at least one of the plurality of administrator defined rules.

19. The system of claim 18, wherein at least one of the actions comprises warning a user of the mobile device that the device is out of compliance and causing subsequent action to be performed if the attribute remains out of compliance after a period of time defined in the at least one rule.

20. The system of claim 17, wherein the computer readable instructions further comprise instructions configured to automatically revoke the action if the attribute is brought back into compliance.

21. The system of claim 17, wherein the computer readable instructions further comprise instructions configured to gather the plurality of attributes for at least one of the plurality of mobile device by gathering attribute information from that mobile device and at least one other source on a network.

22. The system of claim 17, wherein the plurality of different mobile operating systems comprise at least Android and iOS.

23. The system of claim 17, wherein the attribute comprises location information about the mobile device.

Petitioner Ex 1002, p. 65
Zimperium v. Taasera, IPR2024-00007

ABSTRACT

Utilizing a server-based rules-based action framework, methods and systems gather status and configuration information about each of a plurality of mobile devices, which include devices from different mobile platforms. At the server, software processes monitor status information and respond automatically to changes, causing administrator-selected rules to be evaluated to determine if an action should automatically be initiated.

Petitioner Ex 1002, p. 66
Zimperium v. Taasera, IPR2024-00007

Electronic Patent Application Fee Transmittal

Application Number:	
Filing Date:	
Title of Invention:	RULES BASED ACTIONS FOR MOBILE DEVICE MANAGEMENT
First Named Inventor/Applicant Name:	Jatin MALIK
Filer:	Jay R. Mitchell/Samantha Rizzo
Attorney Docket Number:	130839.02101

Filed as Small Entity

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Utility filing Fee (Electronic filing)	4011	1	95	95
Utility Search Fee	2111	1	310	310
Utility Examination Fee	2311	1	125	125
Pages:				
Claims:				
Claims in excess of 20	2202	3	30	90
Miscellaneous-Filing:				
Petition:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Miscellaneous:				
			Total in USD ($)	620

Electronic Acknowledgement Receipt

EFS ID:	13157898
Application Number:	13540142
International Application Number:	
Confirmation Number:	4198
Title of Invention:	RULES BASED ACTIONS FOR MOBILE DEVICE MANAGEMENT
First Named Inventor/Applicant Name:	Jatin MALIK
Customer Number:	86308
Filer:	Jay R. Mitchell/Samantha Rizzo
Filer Authorized By:	Jay R. Mitchell
Attorney Docket Number:	130839.02101
Receipt Date:	02-JUL-2012
Filing Date:	
Time Stamp:	16:31:36
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	$620
RAM confirmation Number	3289
Deposit Account	500436
Authorized User	JONES,MICHAEL K.
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees) Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)	

Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)					
File Listing:					
Document Number	**Document Description**	**File Name**	**File Size(Bytes)/ Message Digest**	**Multi Part /.zip**	**Pages (if appl.)**
1	Application Data Sheet	2101ADS1.pdf	1089337 684f48d072cc19dadebd4bf15ec5bd7800135b3b	no	5
Warnings:					
Information:					
2	Drawings-only black and white line drawings	2101FIGS1.pdf	1487718 323dec609b5e8a3d47eaf005d9ecc6618326c129	no	10
Warnings:					
Information:					
3		2101Appl.pdf	240835 f8de8188aaf5184649454ca2d113c88b0c591362	yes	51

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Specification	1	45
	Claims	46	50
	Abstract	51	51

Warnings:					
Information:					
4	Fee Worksheet (SB06)	fee-info.pdf	36554 992f3fd1c79e0a3a459343f7b3d88be915e13516	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	2854444		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Electronic Acknowledgement Receipt

EFS ID:	13157898
Application Number:	13540142
International Application Number:	
Confirmation Number:	4198
Title of Invention:	RULES BASED ACTIONS FOR MOBILE DEVICE MANAGEMENT
First Named Inventor/Applicant Name:	Jatin MALIK
Customer Number:	86308
Filer:	Jay R. Mitchell/Samantha Rizzo
Filer Authorized By:	Jay R. Mitchell
Attorney Docket Number:	130839.02101
Receipt Date:	02-JUL-2012
Filing Date:	
Time Stamp:	16:31:36
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	$620
RAM confirmation Number	3289
Deposit Account	500436
Authorized User	JONES,MICHAEL K.
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees) Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)	

Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)					
File Listing:					
Document Number	**Document Description**	**File Name**	**File Size(Bytes)/ Message Digest**	**Multi Part /.zip**	**Pages (if appl.)**
1	Application Data Sheet	2101ADS1.pdf	1089337 684f48d072cc19dadebd4bf15ec5bd7800135b3b	no	5
Warnings:					
Information:					
2	Drawings-only black and white line drawings	2101FIGS1.pdf	1487718 323dec609b5e8a3d47eaf005d9ecc6618326c129	no	10
Warnings:					
Information:					
3		2101Appl.pdf	240835 f8de8188aaf5184649454ca2d113c88b0c591362	yes	51

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Specification	1	45
	Claims	46	50
	Abstract	51	51

Warnings:					
Information:					
4	Fee Worksheet (SB06)	fee-info.pdf	36554 992f3fd1c79e0a3a459343f7b3d88be915e13516	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	2854444		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

DocCode - SCORE

SCORE Placeholder Sheet for IFW Content

Application Number: 13540142 Document Date: 7/2/2012

The presence of this form in the IFW record indicates that the following document type was received in electronic format on the date identified above. This content is stored in the SCORE database.

- Drawings – Other than Black and White Line Drawings

Since this was an electronic submission, there is no physical artifact folder, no artifact folder is recorded in PALM, and no paper documents or physical media exist. The TIFF images in the IFW record were created from the original documents that are stored in SCORE.

To access the documents in the SCORE database, refer to instructions developed by SIRA.

At the time of document entry (noted above):

- Examiners may access SCORE content via the eDAN interface.
- Other USPTO employees can bookmark the current SCORE URL (http://es/ScoreAccessWeb/).
- External customers may access SCORE content via the Public and Private PAIR interfaces.

Form Revision Date: February 8, 2006

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY.DOCKET.NO	TOT CLAIMS	IND CLAIMS
13/540,142	07/02/2012	3651	620	130839.02101	23	3

CONFIRMATION NO. 4198

86308
Pepper Hamilton LLP
400 Berywn Park
899 Cassatt Road
Berwyn, PA 19312-1183

FILING RECEIPT

OC000000055380644

Date Mailed: 07/17/2012

Receipt is acknowledged of this non-provisional patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. **If an error is noted on this Filing Receipt, please submit a written request for a Filing Receipt Correction. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections**

Applicant(s)

Jatin MALIK, Bangalore, INDIA;
Ratnesh SINGH, Bangalore, INDIA;
Rajakumar BOPALLI, Bangalore, INDIA;

Assignment For Published Patent Application

FIBERLINK COMMUNICATIONS CORPORATION, Blue Bell, PA

Power of Attorney: None

Domestic Priority data as claimed by applicant

This appln claims benefit of 61/503,729 07/01/2011

Foreign Applications (You may be eligible to benefit from the **Patent Prosecution Highway** program at the USPTO. Please see http://www.uspto.gov for more information.)

If Required, Foreign Filing License Granted: 07/13/2012

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 13/540,142**

Projected Publication Date: To Be Determined - pending completion of Missing Parts

Non-Publication Request: No

Early Publication Request: No
** **SMALL ENTITY** **

Title

RULES BASED ACTIONS FOR MOBILE DEVICE MANAGEMENT

Preliminary Class

198

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at http://www.uspto.gov/web/offices/pac/doc/general/index.html.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, http://www.stopfakes.gov. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4158).

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as

set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign AssetsControl, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

SelectUSA

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation and commercialization of new technologies. The USA offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to encourage, facilitate, and accelerate business investment. To learn more about why the USA is the best country in the world to develop technology, manufacture products, and grow your business, visit SelectUSA.gov.

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number: 13/540,142

APPLICATION AS FILED - PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY FEE($)
BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	95		N/A	
SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A	310		N/A	
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	125		N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	23 minus 20 =	* 3	x 30 =	90	OR		
INDEPENDENT CLAIMS (37 CFR 1.16(h))	3 minus 3 =	*	x 125 =	0.00			
APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).			0.00			
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))				0.00			
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL	620		TOTAL	

APPLICATION AS AMENDED - PART II

		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY ADDITIONAL FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE($)
AMENDMENT A	Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
	Application Size Fee (37 CFR 1.16(s))									
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE($)	ADDITIONAL FEE($)	OR	RATE($)	ADDITIONAL FEE($)
AMENDMENT B	Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
	Application Size Fee (37 CFR 1.16(s))									
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".
The "Highest Number Previously Paid For" (Total or Independent) is the highest found in the appropriate box in column 1.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
13/540,142	07/02/2012	Jatin MALIK	130839.02101

CONFIRMATION NO. 4198

86308
Pepper Hamilton LLP
400 Berywn Park
899 Cassatt Road
Berwyn, PA 19312-1183

FORMALITIES LETTER

OC000000055380645

Date Mailed: 07/17/2012

NOTICE TO FILE MISSING PARTS OF NONPROVISIONAL APPLICATION

FILED UNDER 37 CFR 1.53(b)

Filing Date Granted

Items Required To Avoid Abandonment:

An application number and filing date have been accorded to this application. The item(s) indicated below, however, are missing. Applicant is given **TWO MONTHS** from the date of this Notice within which to file all required items below to avoid abandonment. Extensions of time may be obtained by filing a petition accompanied by the extension fee under the provisions of 37 CFR 1.136(a).

- The oath or declaration is missing.
  A properly signed oath or declaration in compliance with 37 CFR 1.63, identifying the application by the above Application Number and Filing Date, is required.
  Note: If a petition under 37 CFR 1.47 is being filed, an oath or declaration in compliance with 37 CFR 1.63 signed by all available joint inventors, or if no inventor is available by a party with sufficient proprietary interest, is required.

The applicant needs to satisfy supplemental fees problems indicated below.

The required item(s) identified below must be timely submitted to avoid abandonment:

- A surcharge (for late submission of filing fee, search fee, examination fee or oath or declaration) as set forth in 37 CFR 1.16(f) of $**65** for a small entity in compliance with 37 CFR 1.27, must be submitted.

SUMMARY OF FEES DUE:

Total fee(s) required within **TWO MONTHS** from the date of this Notice is $**65** for a small entity
- $**65** Surcharge.

Petitioner Ex 1002, p. 80
Zimperium v. Taasera, IPR2024-00007

Replies should be mailed to:

Mail Stop Missing Parts
Commissioner for Patents
P.O. Box 1450
Alexandria VA 22313-1450

Registered users of EFS-Web may alternatively submit their reply to this notice via EFS-Web.
https://sportal.uspto.gov/authenticate/AuthenticateUserLocalEPF.html

For more information about EFS-Web please call the USPTO Electronic Business Center at **1-866-217-9197** or visit our website at http://www.uspto.gov/ebc.

If you are not using EFS-Web to submit your reply, you must include a copy of this notice.

/hnguyen/

Office of Data Management, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

Petitioner Ex 1002, p. 81
Zimperium v. Taasera, IPR2024-00007

DOCKET NO. 130839.02101 **PATENT**

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: **Jatin MALIK et al.**

Title: **RULES BASED ACTIONS FOR MOBILE DEVICE MANAGEMENT**

Application No.: **13/540,142** Group Art Unit: **3651**

Filed: **July 2, 2012** Examiner: **To Be Determined**

Confirmation: **4198** Filed by EFS on: **September 6, 2012**

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

RESPONSE TO NOTICE TO FILE MISSING PARTS OF NON-PROVISIONAL APPLICATION

Responsive to the Notification dated July 17, 2012, enclosed is a copy of the executed Declaration in compliance with 37 C.F.R. § 1.53 (b) along with the required surcharge fees.

The Commission for Patents is hereby authorized to charge any deficiency or credit any overpayment to Deposit Account 50-0436.

Respectfully Submitted,

By: /Michael K. Jones, Reg. #41100/
Michael K. Jones
Registration No. 41,100

Dated: **September 6, 2012**
PEPPER HAMILTON LLP
3000 Two Logan Square
Eighteenth and Arch Street
Philadelphia, PA 19103-279
Telephone: (215) 981-4405
Facsimile: (610) 640-7835

Doc Code: Oath
Document Description: Oath or declaration filed

PTO/SB/01 (04-09)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

DECLARATION FOR UTILITY OR DESIGN PATENT APPLICATION (37 CFR 1.63)

☐ Declaration Submitted With Initial Filing OR ☑ Declaration Submitted After Initial Filing (surcharge (37 CFR 1.16(f)) required)

Attorney Docket Number	130839.02101
First Named Inventor	Malik, Jatin
COMPLETE IF KNOWN	
Application Number	13/540142
Filing Date	2012-07-02
Art Unit	TBD
Examiner Name	TBD

I hereby declare that: (1) Each inventor's residence, mailing address, and citizenship are as stated below next to their name; and (2) I believe the inventor(s) named below to be the original and first inventor(s) of the subject matter which is claimed and for which a patent is sought on the invention titled:

RULES BASED ACTIONS FOR MOBILE DEVICE MANAGEMENT

(Title of the invention)

the application of which

☐ is attached hereto

OR

☑ was filed on (MM/DD/YYYY) 07/02/2012 as United States Application Number or PCT International Application Number 13/540,142 and was amended on (MM/DD/YYYY) _____ (if applicable).

I hereby state that I have reviewed and understand the contents of the above identified application, including the claims, as amended by any amendment specifically referred to above.

I acknowledge the duty to disclose information which is material to patentability as defined in 37 CFR 1.56, including for continuation-in-part applications, material information which became available between the filing date of the prior application and the national or PCT international filing date of the continuation-in-part application.

Authorization To Permit Access To Application by Participating Offices

☑ If checked, the undersigned hereby grants the USPTO authority to provide the European Patent Office (EPO), the Japan Patent Office (JPO), the Korean Intellectual Property Office (KIPO), the World Intellectual Property Office (WIPO), and any other intellectual property offices in which a foreign application claiming priority to the above-identified patent application is filed access to the above-identified patent application. See 37 CFR 1.14(c) and (h). This box should not be checked if the applicant does not wish the EPO, JPO, KIPO, WIPO, or other intellectual property office in which a foreign application claiming priority to the above-identified patent application is filed to have access to the above-identified patent application.

In accordance with 37 CFR 1.14(h)(3), access will be provided to a copy of the above-identified patent application with respect to: 1) the above-identified patent application-as-filed; 2) any foreign application to which the above-identified patent application claims priority under 35 U.S.C. 119(a)-(d) if a copy of the foreign application that satisfies the certified copy requirement of 37 CFR 1.55 has been filed in the above-identified patent application; and 3) any U.S. application-as-filed from which benefit is sought in the above-identified patent application.

In accordance with 37 CFR 1.14(c), access may be provided to information concerning the date of filing the Authorization to Permit Access to Application by Participating Offices.

This collection of information is required by 35 U.S.C. 115 and 37 CFR 1.63. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 21 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

PTO/SB/01 (04-09)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

DECLARATION — Utility or Design Patent Application

Claim of Foreign Priority Benefits

I hereby claim foreign priority benefits under 35 U.S.C. 119(a)-(d) or (f), or 365(b) of any foreign application(s) for patent, inventor's or plant breeder's rights certificate(s), or 365(a) of any PCT international application which designated at least one country other than the United States of America, listed below and have also identified below, by checking the box, any foreign application for patent, inventor's or plant breeder's rights certificate(s), or any PCT international application having a filing date before that of the application on which priority is claimed.

Prior Foreign Application Number(s)	Country	Foreign Filing Date (MM/DD/YYYY)	Priority Not Claimed	Certified Copy Attached? YES	NO
			☐	☐	☐
			☐	☐	☐
			☐	☐	☐
			☐	☐	☐

☐ Additional foreign application number(s) are listed on a supplemental priority data sheet PTO/SB/02B attached hereto.

PTO/SB/01 (04-09)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

DECLARATION — Utility or Design Patent Application

Direct all correspondence to: ☑ The address associated with Customer Number:	86308	OR	☐ Correspondence address below	
Name				
Address				
City	State	Zip		
Country	Telephone	Email		

WARNING:

Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identity theft. Personal information such as social security numbers, bank account numbers, or credit card numbers (other than a check or credit card authorization form PTO-2038 submitted for payment purposes) is never required by the USPTO to support a petition or an application. If this type of personal information is included in documents submitted to the USPTO, petitioners/applicants should consider redacting such personal information from the documents before submitting them to the USPTO. Petitioner/applicant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1.213(a) is made in the application) or issuance of a patent. Furthermore, the record from an abandoned application may also be available to the public if the application is referenced in a published application or an issued patent (see 37 CFR 1.14). Checks and credit card authorization forms PTO-2038 submitted for payment purposes are not retained in the application file and therefore are not publicly available. Petitioner/applicant is advised that documents which form the record of a patent application (such as the PTO/SB/01) are placed into the Privacy Act system of records DEPARTMENT OF COMMERCE, COMMERCE-PAT-7, System name: *Patent Application Files*. Documents not retained in an application file (such as the PTO-2038) are placed into the Privacy Act system of COMMERCE/PAT-TM-10, System name: *Deposit Accounts and Electronic Funds Transfer Profiles*.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under 18 U.S.C. 1001 and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

NAME OF SOLE OR FIRST INVENTOR:	☐ A petition has been filed for this unsigned inventor
Given Name (first and middle [if any])	Family Name or Surname
Jatin	MALIK
Inventor's Signature:	Date

Residence: City	State	Country	Citizenship
Bangalore		IN	IN

Mailing Address

30-303, Mantri Residency, Bannerghatta Road, Opp Meenakshi Temple

City	State	Zip	Country
Bangalore	KARNATAKA	560076	IN

☑ Additional inventors or a legal representative are being named on the 1 supplemental sheet(s) PTO/SB/02A or 02LR attached hereto

PTO/SB/02A (07-07)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

DECLARATION

ADDITIONAL INVENTOR(S)
Supplemental Sheet

Name of Additional Joint Inventor, if any:	☐ A petition has been filed for this unsigned inventor		
Given Name (first and middle (if any))	Family Name or Surname		
Ratnesh	SINGH		
Inventor's Signature Ratnesh Singh		Date 31st Aug 2012	
Bangalore Residence: City	State	IN Country	IN Citizenship
1104 Sobha Jasmine Green Glen Layout, Bellandur Mailing Address			
Bangalore City	State	560103 Zip	IN Country

Name of Additional Joint Inventor, if any:	☐ A petition has been filed for this unsigned inventor		
Given Name (first and middle (if any))	Family Name or Surname		
Rajakumar	BOPALLI		
Inventor's Signature		Date 31st AUG 2012	
Bangalore Residence: City	State	IN Country	IN Citizenship
Flat #305, C-block Samhita Rainbow MTB, Thubarahalli Mailing Address			
Bangalore City	State	560066 Zip	IN Country

Name of Additional Joint Inventor, if any:	☐ A petition has been filed for this unsigned inventor		
Given Name (first and middle (if any))	Family Name or Surname		
Inventor's Signature		Date	
Residence: City	State	Country	Citizenship
Mailing Address			
City	State	Zip	Country

This collection of information is required by 35 U.S.C. 115 and 37 CFR 1.63. This information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 21 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

Electronic Patent Application Fee Transmittal

Application Number:	13540142
Filing Date:	02-Jul-2012
Title of Invention:	RULES BASED ACTIONS FOR MOBILE DEVICE MANAGEMENT
First Named Inventor/Applicant Name:	Jatin MALIK
Filer:	Michael Kenneth Jones/Samantha Rizzo
Attorney Docket Number:	130839.02101

Filed as Small Entity

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Late filing fee for oath or declaration	2051	1	65	65
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
			Total in USD ($)	**65**

Electronic Acknowledgement Receipt

EFS ID:	13669708
Application Number:	13540142
International Application Number:	
Confirmation Number:	4198
Title of Invention:	RULES BASED ACTIONS FOR MOBILE DEVICE MANAGEMENT
First Named Inventor/Applicant Name:	Jatin MALIK
Customer Number:	86308
Filer:	Michael Kenneth Jones/Samantha Rizzo
Filer Authorized By:	Michael Kenneth Jones
Attorney Docket Number:	130839.02101
Receipt Date:	06-SEP-2012
Filing Date:	02-JUL-2012
Time Stamp:	16:08:29
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	$65
RAM confirmation Number	3274
Deposit Account	500436
Authorized User	JONES,MICHAEL K.
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees) Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)	

Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees)	
Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Applicant Response to Pre-Exam Formalities Notice	2101ResponseMP.pdf	72916 36567333360078bd234e4fc26d516b1fe97dce9af	no	1
Warnings:					
Information:					
2	Oath or Declaration filed	2101DEC1.pdf	931553 fe9ab2108758b6a8d9cc6d4dc7ac1c6d4b28e07e	no	4
Warnings:					
Information:					
3	Fee Worksheet (SB06)	fee-info.pdf	30244 8eab64d33e60ce510fd15cbb3bf3db3b55cc3aa2	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	1034713		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number: 13/540,142

APPLICATION AS FILED - PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY FEE($)
BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	95		N/A	
SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A	310		N/A	
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	125		N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	23 minus 20 =	* 3	x 30 =	90	OR		
INDEPENDENT CLAIMS (37 CFR 1.16(h))	3 minus 3 =	*	x 125 =	0.00			
APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).			0.00			
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))				0.00			
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL	620		TOTAL	

APPLICATION AS AMENDED - PART II

		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY ADDITIONAL FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE($)
AMENDMENT A	Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
	Application Size Fee (37 CFR 1.16(s))									
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE($)	ADDITIONAL FEE($)	OR	RATE($)	ADDITIONAL FEE($)
AMENDMENT B	Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
	Application Size Fee (37 CFR 1.16(s))									
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".
The "Highest Number Previously Paid For" (Total or Independent) is the highest found in the appropriate box in column 1.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY.DOCKET.NO	TOT CLAIMS	IND CLAIMS
13/540,142	07/02/2012	3651	685	130839.02101	23	3

CONFIRMATION NO. 4198

UPDATED FILING RECEIPT

86308
Pepper Hamilton LLP
400 Berywn Park
899 Cassatt Road
Berwyn, PA 19312-1183

Date Mailed: 09/14/2012

Receipt is acknowledged of this non-provisional patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. **If an error is noted on this Filing Receipt, please submit a written request for a Filing Receipt Correction. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections**

Applicant(s)

Jatin MALIK, Bangalore, INDIA;
Ratnesh SINGH, Bangalore, INDIA;
Rajakumar BOPALLI, Bangalore, INDIA;

Assignment For Published Patent Application

FIBERLINK COMMUNICATIONS CORPORATION, Blue Bell, PA

Power of Attorney: None

Domestic Priority data as claimed by applicant

This appln claims benefit of 61/503,729 07/01/2011

Foreign Applications (You may be eligible to benefit from the **Patent Prosecution Highway** program at the USPTO. Please see http://www.uspto.gov for more information.)

Permission to Access - A proper **Authorization to Permit Access to Application by Participating Offices** (PTO/SB/39 or its equivalent) has been received by the USPTO.

If Required, Foreign Filing License Granted: 07/13/2012

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 13/540,142**

Projected Publication Date: 01/03/2013

Non-Publication Request: No

Early Publication Request: No
**** SMALL ENTITY ****

Title

RULES BASED ACTIONS FOR MOBILE DEVICE MANAGEMENT

Preliminary Class

198

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at http://www.uspto.gov/web/offices/pac/doc/general/index.html.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, http://www.stopfakes.gov. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4158).

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as

set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign AssetsControl, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

SelectUSA

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation and commercialization of new technologies. The USA offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to encourage, facilitate, and accelerate business investment. To learn more about why the USA is the best country in the world to develop technology, manufacture products, and grow your business, visit SelectUSA.gov.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
13/540,142	07/02/2012	Jatin MALIK	130839.02101

CONFIRMATION NO. 4198

86308
Pepper Hamilton LLP
400 Berywn Park
899 Cassatt Road
Berwyn, PA 19312-1183

PUBLICATION NOTICE

Title:RULES BASED ACTIONS FOR MOBILE DEVICE MANAGEMENT

Publication No.US-2013-0007245-A1
Publication Date:01/03/2013

NOTICE OF PUBLICATION OF APPLICATION

The above-identified application will be electronically published as a patent application publication pursuant to 37 CFR 1.211, et seq. The patent application publication number and publication date are set forth above.

The publication may be accessed through the USPTO's publically available Searchable Databases via the Internet at www.uspto.gov. The direct link to access the publication is currently http://www.uspto.gov/patft/.

The publication process established by the Office does not provide for mailing a copy of the publication to applicant. A copy of the publication may be obtained from the Office upon payment of the appropriate fee set forth in 37 CFR 1.19(a)(1). Orders for copies of patent application publications are handled by the USPTO's Office of Public Records. The Office of Public Records can be reached by telephone at (703) 308-9726 or (800) 972-6382, by facsimile at (703) 305-8759, by mail addressed to the United States Patent and Trademark Office, Office of Public Records, Alexandria, VA 22313-1450 or via the Internet.

In addition, information on the status of the application, including the mailing date of Office actions and the dates of receipt of correspondence filed in the Office, may also be accessed via the Internet through the Patent Electronic Business Center at www.uspto.gov using the public side of the Patent Application Information and Retrieval (PAIR) system. The direct link to access this status information is currently http://pair.uspto.gov/. Prior to publication, such status information is confidential and may only be obtained by applicant using the private side of PAIR.

Further assistance in electronically accessing the publication, or about PAIR, is available by calling the Patent Electronic Business Center at 1-866-217-9197.

Office of Data Managment, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99**)		
	Application Number	13540142
	Filing Date	2012-07-02
	First Named Inventor	Malik, Jatin
	Art Unit	2447
	Examiner Name	Hwang, Joon H.
	Attorney Docket Number	130839.02101

U.S.PATENTS						
Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					
If you wish to add additional U.S. Patent citation information please click the Add button.						

U.S.PATENT APPLICATION PUBLICATIONS						
Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20100242088		2010-09-23	THOMAS	
	2	20080114862		2008-05-15	MOGHADDAM ET AL.	
	3	20070266422		2007-11-15	GERMANO ET AL.	
	4	20070206552		2007-09-06	YAQUB ET AL.	
If you wish to add additional U.S. Published Application citation information please click the Add button.						

FOREIGN PATENT DOCUMENTS								
Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99**)		
	Application Number	13540142
	Filing Date	2012-07-02
	First Named Inventor	Malik, Jatin
	Art Unit	2447
	Examiner Name	Hwang, Joon H.
	Attorney Docket Number	130839.02101

	1	2011022053	WO	A1	2011-02-24	NAIMAN ET AL.		☐

If you wish to add additional Foreign Patent Document citation information please click the Add button

NON-PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1		☐

If you wish to add additional non-patent literature document citation information please click the Add button

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99**)		
	Application Number	13540142
	Filing Date	2012-07-02
	First Named Inventor	Malik, Jatin
	Art Unit	2447
	Examiner Name	Hwang, Joon H.
	Attorney Docket Number	130839.02101

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☐ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Michael K. Jones, Reg. No. 41100/	Date (YYYY-MM-DD)	2013-05-20
Name/Print	Michael K. Jones	Registration Number	41100

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
24 February 2011 (24.02.2011)

PCT

(10) International Publication Number
WO 2011/022053 A1

(51) International Patent Classification:
G06F 21/22 (2006.01)

(21) International Application Number:
PCT/US2010/002264

(22) International Filing Date:
18 August 2010 (18.08.2010)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
61/274,528 18 August 2009 (18.08.2009) US

(72) Inventors; and
(71) Applicants : **NAIMAN, Errol, David** [US/US]; 24701 Raymond Way, Lake Forest, CA 92630 (US). **CRABBS, David, Edwin** [US/US]; 31491 Via Santa Maria, San Juan Capistrano, CA (US).

(74) Agents: **VALAUSKAS, Charles, C.** et al.; Valauskas Corder LLC, 150 South Wacker Drive, Suite 620, Chicago, IL 60606 (US).

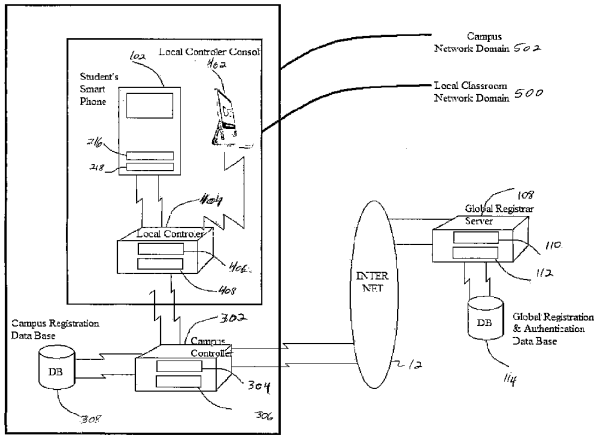
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report (Art. 21(3))*

(54) **Title**: SYSTEM AND METHODS FOR DEVICE MANAGEMENT

Fig 5



(57) **Abstract**: A method for device management includes steps of downloading a device control application to one or more hand held devices, registenng the one or more hand held devices with the global registry, authentication and compliance service, and establishing a communication session between the one or more hand-held devices and local device control equipment The method also has steps of creating the communication session between the one or more hand held devices and the local device control equipment, verifying the registration and compliance status of the one or more hand held devices, and monitonng the use of one or more approved applications and hand held devices including one or more restnctions in the use of the one or more hand held device and their features and functions

WO 2011/022053 A1

SYSTEM AND METHODS FOR DEVICE MANAGEMENT

This application claims the benefit of U.S. Provisional Application No. 61/274,528 filed August 18, 2009, which is hereby incorporated by reference.

FIELD OF THE INVENTION

The present invention relates generally to a system and methods for controlling hand held computer devices with communication features including a personal digital assistant (PDA), smart phone, tablet (iPad) or similar devices. More specifically, the present invention is directed to a system and methods for dynamically establishing, monitoring, and controlling hand held computer devices irrespective of the particular system used to operate the devices.

BACKGROUND OF THE INVENTION

The monitoring, managing, and controlling of hand held computer devices provided to individual users is a desirable capability for those having ultimate responsibility for these devices. A hand held computing devices as used in this application can be wireless devices, such as any mobile device or smart mobile device, a personal data assistant (PDA), a smart hand-held computing device, a cellular telephone, a book reader, a tablet (e.g. iPad like device), laptop or netbook computer, hand held computer game console, a MP3 player, or similar hand held computer devices. For purposes of this application, the business or individual or individuals having ultimate responsibility for such devices can be the device owner, an employer, the parent, or the guardian of the user and will be generally identified in the following as

Petitioner Ex 1002, p. 101
Zimperium v. Taasera, IPR2024-00007

the owner. Individuals and entities that wish to control the use of devices when on their premises or in their domain of control are identified in this application as a "policy control authority". For example, if a policy control authority is a parent of children having access to different mobile devices or smart mobile devices under a single family membership, then certain restrictions on the use of the mobile device may be desirable. The parent may wish to limit the time of day when the child can text to prevent texting on weekdays during night hours throughout a school year. Other individuals, institutions, and business entities may also desire to control how such devices are utilized on their premises. For example, educational institutions may desire that limited access to device services that are available in a classroom setting, such as phone services or texting services. Different instructors may desire different option availability of hand held computer device applications for different courses, sections of their courses, and/or for different tests. Students at earlier stages of a course or in lower grade levels may be restricted from using some of the functions of a calculator application operating on the device during exams, etc., whereas later in the course or in upper grade levels may be expected to use such application functions during an exam to solve more advanced mathematical or scientific problems. Generally, a problem exists with respect to the ability to place different restrictions on the use of a hand held computer devices with respect to location, time, and specific users in different environments by different commercial and non-commercial enterprises.

The field of hand held computer device management is often referred to as Mobile Device Management (MDM). Generally, known systems have been focused on business MDM and government MDM. Such systems are directed to the support and

Petitioner Ex 1002, p. 102
Zimperium v. Taasera, IPR2024-00007

security services of mobile devices owned by a particular enterprise with a focus often on access to enterprise data and systems. In these systems, the managers make device control decisions imposed by entities providing the devices to users. The managers also determine the control policies and management services that apply to the devices. Such known MDM systems provide very little flexibility in the management of devices based on location, time, or enterprise by which the hand held computer devices may be controlled when the enterprise is other than the subscribing company. The management and control techniques used with known MDM systems do not foster interoperability with competing entities and systems, and are often an obstacle to important uses of the device and desired applications. Existing MDM systems are generally not able to manage and control end-user applications using different types of computer systems, operating systems, and applications software, interconnected by different types of local and wide area networks for hand held device users not subscribed to a particular MDM system.

Interoperability limitations of MDM systems have resulted in the loss of the availability of many useful applications, for example, limited or no control of devices when they are used in different locations (under the management and control of different control authorities) or in different social, educational, or business environments.

However, a known problem of these MDM systems is that they are closed MDM systems and permit only one control authority. For purposes of this application, closed MDM systems are ones that require all of the devices controlled by the system to have a membership with the MDM system. Membership can take the form of, for example, employee/employer, service member and a unit of the Armed Forces, or an

Petitioner Ex 1002, p. 103
Zimperium v. Taasera, IPR2024-00007

independent contractor relationship which are referred to as organizational relationships. The management of devices is established by a policy control authority inputting data into the MDM system and policies are made obligatory to all of the members subscribing to the service – control of the device is mandatory and imposed by fiat. The control of the devices is further limited by a geographic boundary of the MDM system. Other MDM systems operating by different control authorities in adjacent geographic regions typically do not operate with non-members of the subscribed to MDM system.

Current systems do not make important architectural distinctions among enterprises and functions that permit flexible control regimes. The systems require that the device owner and policy control authority have an organizational relationship, if not be the same entity. Device provisioning or initiating of the device for communication with a network is provided under the control of the enterprise as are also authentication of a device, establishment of control policies for the device, and administration of the control policies. The control authorities all have an organizational relationship with device users, and most often the control authorities share a common management policy-making apparatus. This limits how devices can be controlled by a policy since only devices of users in those organizational relationships are controlled by the policy.

Other known problems with existing hand held computing devices are that such devices are dynamic and are typified by changes to their operating characteristics that occur from time to time without authorization from a security system or an enterprise information technology department or controller. A hand held computer device that is compliant with a MDM system can be readily changed to present a security risk

Petitioner Ex 1002, p. 104
Zimperium v. Taasera, IPR2024-00007

subsequent to registration. For example, application software can be easily added to the devices from an application store or other less reliable or controlled sources. Hand held computer devices can be "jail broken" and otherwise "hacked" introducing software imitating ("or spoofing") legitimate educational applications. A device can be reset eliminating the device control software from the device without the permission or knowledge of the enterprise. Such "hacking and spoofing" could facilitate cheating or other unauthorized operations in, for example, a testing or other high security environment.

It is clear that there is a demand for a system and methods that allows hand held computer devices to be operated such that the above organizational relationship is not required to control hand held computer devices, such that the devices have their functions subject to the control of multiple control authorities, and such that the devices be able to operate in educational and other environments so that the devices are not jail broken, hacked, or spoofed. The present invention satisfies these various demands.

SUMMARY OF THE INVENTION

The present invention relates generally to a method and system for controlling hand held computer devices with communication features, and methods for dynamically establishing, monitoring and controlling the devices' behavior based on location and time. The present invention also pertains to interoperable control regimes and policies established by separate control authorities which may be independent of the device owner. These control regimes may be layered and may also coexist and cooperate

Petitioner Ex 1002, p. 105
Zimperium v. Taasera, IPR2024-00007

providing multiple benefits to the device owner, its user and the enterprises that implement and operate the device control regime.

Mobile Device Management (MDM) provides the ability to improve mobile device functionality by updating firmware, changing configurations, and managing software over the air (OTA). MDM may also provide the ability to retrieve information from a device for troubleshooting and analysis. The present MDM system can optimize mobile device functionality and ensure better interoperation with a different service provider's network.

From a topological point of view, the system is open to subscription by any device owner who chooses to voluntarily subscribe and have their device managed and to opt-in and have their device controlled. The device owner benefits from the multiple independent entities who implement control regimes. The system is open to any enterprises (inclusive of households) who implement MDM device control within the boundaries of the enterprise's premises.

In one embodiment of the present invention, the locus of such Open MDM (OMDM) control is limited to the geographic boundaries of the participating household's or enterprise's location or locations. Once the device is located outside the boundaries of those locations, the device-management regime restores the device to an un-controlled state or to a default control policy established by the user (or their parents or guardian in the case of minor children).

One embodiment of the present invention has an open architecture that separates the provision, authentication of a subscribed user, establishment of control

Petitioner Ex 1002, p. 106
Zimperium v. Taasera, IPR2024-00007

policies, and administration of the control policies into logically independent components.

OMDM can be implemented to provide substantial benefits in a variety of applications that include but are not limited to schools, homes, airlines in flight, movie theaters, testing authorities, etc. One advantage of the present invention is the open opt-in feature. Another advantage of the present invention is the multi-entity multi-policy independent device control feature.

One embodiment of the invention can provide "enterprise device management"-like services for those that may not be associated, for example, with a large enterprise with a sophisticated information technology (IT) department. Such embodiment may provide voluntary device management that renders hand-held computer devices more useful and more accepted. For the small business owner or for the operator of public services and facilities, the present embodiment can provide device management controls over a public who do not need to share a common employer or other association and who opt-in for device-management. Users get more benefits and better quality of service without a control authority ever needing to take physical possession of their devices.

Voluntary opt-in device-management allows households and enterprises to adopt standard control policies. The hand-held computing devices can be controlled on entry into the enterprise based on at least one of the following: global positioning satellite (GPS) coordinates; Near Field Communications (NFC) technologies and applications and/or standard policy profiles stored on a user's device at the time the device was

Petitioner Ex 1002, p. 107
Zimperium v. Taasera, IPR2024-00007

registered and provisioned; or information provided in the device controller as described in the educational application below.

In one embodiment, a device control policy based on time and location could be created in a smart phone application that has global positioning satellite services available.

In one embodiment, a device control policy based on time and location could be implemented in a background process in a smart phone that listens for device controller communications, accepts and implements device control policy received from a device controller, enforces device control polices based on white (approved) and black (prohibited) lists while communicating and reporting to the device controller as required.

For high security test applications corresponding to educational standardized tests, a policy control authority can use multiple redundant approaches that provide automated device management, control, and alerts to notify the policy control authority about possible out of compliance events. These could include applications related to test registration, check in procedures, GPS information, and local controller operation. The degree of security can be arbitrarily set by a policy control authority based on selected implementations that one skilled in the art would be able to construct from the description that follows.

BRIEF DESCRIPTION OF THE DRAWINGS

The preferred embodiments of the invention will be described in conjunction with the appended drawings provided to illustrate and not to the limit the invention, where like designations denoted like elements, and in which:

Petitioner Ex 1002, p. 108
Zimperium v. Taasera, IPR2024-00007

FIG. 1 shows an architecture diagram of an Open Mobile Device Management (OMDM) system in an illustrative embodiment incorporating features of the present invention;

FIG. 2A and 2B show component diagrams of a system for a user to subscribe to the OMDM system, download device management software and have their device information registered in a global device management database in an illustrative embodiment incorporating features of the present invention;

FIG. 3 shows a component diagram of an OMDM system for setting up or modifying device control policies governing approved applications and services to run on a hand held computer device in an illustrative embodiment incorporating features of the present invention;

FIG. 4 shows a component diagram of an OMDM system for setting, establishing or modifying local device management policies governing approved applications to run on a hand held computer device in an illustrative embodiment incorporating features of the present invention;

FIG. 5 shows a component diagram of an OMDM system for registering a new hand held computer device, periodic device compliance monitoring and authentication of the device, and updating an enterprise registration database in an illustrative embodiment incorporating features of the present invention;

FIG. 6 shows a flow chart of a hand held computer device "no-click log-in" process in an illustrative embodiment incorporating features of the present invention, and

Petitioner Ex 1002, p. 109
Zimperium v. Taasera, IPR2024-00007

FIG 7 shows a flow chart of device control monitoring, event logging and alert processes in an illustrative embodiment incorporating features of the present invention.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

A system and methods for controlling usage of a hand held computing device such as a wireless device, such as a personal data assistant, a smart hand-held computing device, a smart phone, a cellular telephone, a book reader, a tablet (e.g. devices similar to the Apple iPad), a laptop or netbook computer, hand held computer game console or MP3 player or similar computer devices is disclosed.

Use of hand held computer devices encompasses outgoing and incoming communication channels as well as application usage. Outgoing or incoming communication channels may include cellular phone networks, cellular phone data services, and 802.11 x (Wi-Fi 33) and 802.15 x (Bluetooth) networking services and the like.

Restrictions on use of device functions can include, but are not limited to, specific hand held computing device applications, use of web browser or other web access and file transfer technology, electronic mails, telephone calls, text messaging, MP3 player, video player, camera usage, computer and video games, etc. and the myriad of applications available from a variety of sources including the iPhone and Android application stores and the like.

For the purposes of this invention, a policy is a set of restrictions regarding which features of a hand held computer device will be available for use within specific time periods, geographic locations, or other parameters. These restrictions may relate to

Petitioner Ex 1002, p. 110
Zimperium v. Taasera, IPR2024-00007

hardware and software features, functions and services such as access to WIFI, 3G, Bluetooth, camera, files, etc., that may be used, and also to general features such as persistence of state between separate usages of software applications. A control domain can be a physical location such as a home, school, college campuses, retail facilities such as stores, gyms, etc., industrial offices, corporate offices, military bases or facilities, public facilities (e.g. airports, arenas, stadiums, theatres, churches, mosques, synagogues, or other religious facilities), etc.

For the purposes of this invention, control policies or policies are those that can limit the use of the following: software; services-specific hardware supported services such as camera, phone, texting and/or other network connections and services; access to files; persistence of the state of user applications; and a subset of features and functions an approved application can provide during a control session or in a particular context. A context can be, for example, a test item, course module, or similar item. Control policies may be implemented to invoke a function to wipe files created during a control session or in other circumstances.

The following embodiments illustrate the definition of control policies with reference to an embodiment relating to use in an educational setting. Control policies as defined in this application have multiple applications in multiple industries so that the description provided here is not meant to limit the generality nor scope of the present invention.

Control policies can be implemented by specifying white list items and black list items. White list items will mean for purposes of this application those features, functions, applications and tools, etc. that a user can use in the specific time or place or

Petitioner Ex 1002, p. 111
Zimperium v. Taasera, IPR2024-00007

as otherwise controlled such as on exams as described below. Black list items will mean for purposes of this application those features, functions, applications and tools, etc. that are off-limit and prohibited for use. Embodiments of the present invention provide an easy to use tool for instructors to establish, add to, modify and delete items to the white list and black list.

Multiple control policies can exist in a particular time and location. In one embodiment, an instructor can assign students to different groups and each group can have a different control policy. This allows instructors to accommodate different lessons or lesson versions for different groups of students having different needs and/or capabilities that are simultaneously located in the same classroom.

In one embodiment, employees and clients can be assigned to groups for the purpose of providing each of them different privileges or benefits. In another embodiment, a customer loyalty program application may provide different services, privileges and pricing to customers based on their group membership.

Other embodiments may allow a member of a grocery store's customer loyalty program to have their device equipped with a conformable shopping list application. The member's device could communicate with the grocery store's "policy server" applications that provided weekly specials, special pricing for loyalty program members, suggested items of interest, and/or a map through the store so that the customer could minimize the time and effort required to do their shopping. These applications could also include a check-out and payment function that utilized NFC technology and applications.

Petitioner Ex 1002, p. 112
Zimperium v. Taasera, IPR2024-00007

In one embodiment, students can be assigned to different groups to suit the needs of the instructor's lesson plan and/or their individualized education program (IEP) as mandated by Federal government regulations.

A broad policy may be selected for a curriculum and testing site, where an instructor could further define which program features and functions were available for use in the class, section of a course or during an exam. These could be used in conjunction with the policy group feature defined above to ensure compliance government IEP requirements.

In one embodiment, the control policy feature could be employed in an electronic test administration application that could vary the features and functions of an educational tool such as a graphing calculator on an item-by-item basis, scramble test items, multiply choice item parameters, scramble answer alternatives or test sections, etc., so that no two adjacent students have the same test item and so that no two tests were exactly the same. This is important to educators and test administrators who might wish to deploy the present invention with an electronic test administration application to take advantage of hand held computer devices for use in standardized tests.

Turning now with reference to the drawings, FIG. 1 is a diagram that provides a general overview of the alternate uses and implementation of embodiments of the invention. Subsequent drawings show embodiments of a specific educational application, but such particular application should not be inferred to diminish the generality of the invention's application that spans both the public and private sectors.

Petitioner Ex 1002, p. 113
Zimperium v. Taasera, IPR2024-00007

In the following description, numerous specific details are set forth in order to provide a more thorough disclosure of embodiments of the invention. It will be apparent to one skilled in the art that the embodiments disclosed may be practiced without all of the specific details provided for each embodiment. In some instances, well-known features may have not been described in detail so as not to obscure the features disclosed. Moreover, it is envisioned that features in the various embodiments may be used in other embodiments as is known to those skilled in the art.

In particular, almost every device manufacturer provides facilities and services that aid in MDM. Examples of such services are the wide spread implementation of Microsoft Exchange Active Sync Device Management or implementations based on technologies like the SyncML MDM standard sponsored by the multi-enterprise Open Mobile Alliance (OMA). The SyncML MDM standard is a variant of Extensible Markup Language (XML) and its use in the applications anticipated in embodiments of the invention are well known to those skilled in the art.

In one embodiment, the invention will serve as the basis for a Device Management module for an OMA hand held standard. The embodiment will promote multiplatform implementation of MDM technologies and provide an industry standard promoting interoperability.

In the following description like reference numbers designate like or corresponding parts throughout the several views. The illustrations are for the purpose of describing a preferred embodiment of the invention and are not intended to limit the invention thereto.

Petitioner Ex 1002, p. 114
Zimperium v. Taasera, IPR2024-00007

As discussed above, FIG. 1 illustrates a first embodiment of the present invention which is an open MDM system, shown generally as 10. In this embodiment, the open MDM system 10 has a plurality of enterprises connected to one another via an internet connection 12. The enterprises illustrated in the FIG. 1 embodiment are an educational institution 14, fitness center 16, corporation 18, movie theater 20, church 22, and airplane 24. In other embodiments, one or more other types of enterprises can be substituted for one or more of the above-described enterprises. For example, other embodiments of the invention may include residential housing, military installations, etc.

FIG. 1 illustrates independent hand held computer devices 26 of various users that can be connected to the internet 12. These users can voluntarily opt-in to the system 10 by subscription and have MDM control which is independent of the limited control provided by original equipment manufacturers. More specifically, in certain embodiments of the present invention, the present system is not manufacturer specific in terms of MDM control, but instead spans the breath of device manufacturers to provide a global hand held computer device management control system 10. The embodiment of system 10 is open to subscription by any user of the devices 26 who voluntarily chooses to have their device managed and opt-in to have their device controlled by the system 10. Since the embodiment of system 10 is globally managed, an advantage of subscribing to the present system is that control is not limited according to specific boundaries, such as geographical boundaries. The present embodiment of system 10 maintains control of a device and restores a device to an un-controlled state or pre-established default control policy once the device is external to a specific geographical boundary or boundaries. A Global Device Management Services

Petitioner Ex 1002, p. 115
Zimperium v. Taasera, IPR2024-00007

facility 28 provides registration, compliance and authentication services to various hand held computer devices; it may also provide one or more of the devices with downloads for the required hand-held device control application. Authentication services are particularly important, since a major benefit is the global service's frequent verification of the authenticity of the hand held device's device control software. The global service also provides registration support for local device controllers, facilitating their registration of client devices as described herein. A connection to the internet from various local device control servers and from the Global Device Management Services facility is preferably via a wired connections, such as connection 30. However, it is contemplated that most hand held devices will connect via a wireless facility with the present system.

As best seen in FIG. 2A, an embodiment of a system now identified as 100 for providing network security for hand held computer devices is shown. The system 100 of the embodiment shown in FIG. 2A is directed towards a user that is a student of an educational institution. The system includes at least one hand held computer device, such as a student smart phone 102 having electronic data storage and software operability and capable of (operable for) wireless communication on a network, shown generally as 104.

The network 104 includes the internet connection 12 and also a wireless data network 106 constructed and configured for wireless communication between the at least one mobile device 100 and at least one device control server 108. The device control server 108 further includes a multi-layered and/or multi-mode security system operable thereon to provide platform-independent security for controlling the device's

Petitioner Ex 1002, p. 116
Zimperium v. Taasera, IPR2024-00007

capabilities and operation. Application and device control software and policies 110 are also stored on the server 108, and synchronized with the smart phone 102. Additionally, subscription and registration software 112 are stored on the server 108 in this embodiment.

As shown in FIG 2B, an embodiment of the smart phone 102 is selected by a user to have device control software 216 and application software 218 installed thereon. Upon completion of these installations, the smart phone 102 is registered in a global registration data base 114 shown in FIG. 2A. The device control software 216 and device control policies controls the smart phone's functions when the smart phone is within the limits of a MDM and subject to its local device control server and control policies. Such control enterprises can be, for example, the enterprises 14-24 shown in FIG. 1. Enforcement of the security policies set by the security software results in the smart phone 102 being able to access the network 104 and data, applications and device services associated with the network only if the user agrees to operate the smart phone 102 in compliance with the policies established by enterprises subscribed to the system. In one embodiment, it is envisioned that the enterprises would subscribe to the system 100 for a specified fee and create policies related to each specific enterprise's device control needs. Other embodiments may have enterprises being able to establish policies with payment of a fee, and device users paying fees for a subscription to global registry and authentication service 100.

FIG. 3 illustrates an example of a subscribing enterprise establishing MDM control policies specific to that enterprise. In this example, an educational institution is shown as an enterprise. A campus device control administrative officer is selected by

Petitioner Ex 1002, p. 117
Zimperium v. Taasera, IPR2024-00007

the educational institution to operate an educational institution's policy console 300. More specifically, the campus device control administrator logs on to the educational institution's policy console 300 and accesses preferably via a secured connection a campus control server 302 which stores a MDM policy management module 304. The MDM policy management module 304 provides a web page interface to policy creation logic that facilitates establishment of an educational institution MDM policy. Policies can be implemented by using templates that are pre-populated with the most common policies typical for the type of enterprise. Thus, in the present example there can be templates specifically tailored for college, high school, or elementary school. Policy values predetermined by the templates can be modified by a campus security officer accessing drop down lists and radio buttons. In some instances, the campus device control administrator may wish to make the policy values global in scope for the educational institution. One such policy value might be preventing any modification to a rule that prohibits the use of cameras in locker rooms of the educational institution. In other instances, however, the campus device control administrator might select other less restrictive policy values if the educational institution desired more relaxed policies for other types of rules, such as camera use in a cafeteria or outside campus buildings. Alternatively or in addition, it may be desired to delegate some or all authority to a class instructor to modify a specific policy for that instructor's classes with or without restriction. In essence, the campus device control administrator can selectively impose a global policy value on specific policies of the educational institution, imposed less restrictive policy values, or authorize localized control of policy values to specific policies during log on of the educational institution's policy console 300. Once the

Petitioner Ex 1002, p. 118
Zimperium v. Taasera, IPR2024-00007

overall campus policy has been established which assigns policy values to each of the educational institutions policies, then a data management module 306 stored on the campus control server 302 may assist such that the MDM policy is recorded in a campus database 308. The campus database 308 is connected to the data management module 306 preferably by a secured connection. The campus database 308 can further include storage for all class databases of the educational institution, or alternatively such class device control policies databases can be stored in separate databases connected to the campus database 308 as is known to those skilled in the art.

FIG. 4 illustrates and embodiment of a process by which an educational instructor of the educational institution may modify a default campus policy implemented by a campus security officer in a local area. A student smart phone 102, selected by a user to have device control software 216 and application software 218 installed thereon, enters a zone 400. By way of example, the zone 400 can be a classroom of the educational institution. A local policy console 402 and local controller 404 are also located in the zone. The local controller is preferably wirelessly connected to the local policy console 402 and smart phone 102.

Other smart phones (not shown) for other students may be similarly connected to the local controller 404 and subject to the same restrictions of use imposed upon the smart phone 102. However, even more localized (i.e., groups of student or even student specific) restrictions may be imposed should further device control flexibility be desired.

Petitioner Ex 1002, p. 119
Zimperium v. Taasera, IPR2024-00007

Generally, the system permits the educational instructor to log on to the local console 402 and access, preferably via a secured connection, the local controller 404 which stores a local MDM policy management module 406. The local MDM policy management module 406 provides a web page interface to policy creation logic that facilitates establishment of a local class MDM policy or policies. Policies can be implemented by using localized templates that are pre-populated with the most common local policies typical for the type of local environment within the specific enterprise.

The local controller 404 also has a local data management module 408 in this embodiment stored on the local controller. The local controller 404 communicates with the campus controller 302. The campus controller 302 communicates with the campus database 308 as discussed above with reference to FIG. 3.

Although the local console 402 and local controller 404 in this embodiment are shown being located within the zone 400, it is envisioned that one or both of these components could be located in an area outside the zone. For example, the local controller 404 could be in a storage area adjacent to the classroom. Moreover, the local controller 404 could be designed to operate with a plurality of zones (e.g., multiple classrooms).

FIG. 5 illustrates a process by which an educational institution's local MDM controllers 404 (one controller shown for brevity) constantly monitor for any new hand held computer device 100 requesting network service via a local registration verification module 406. For a local classroom network domain 500 and a campus network domain 502, each controller 404 compares a respective device identity with the devices registered with the educational institution by sending an inquiry to the campus controller

Petitioner Ex 1002, p. 120
Zimperium v. Taasera, IPR2024-00007

302 and its registration module 304 which searches the campus registration data base 308. If registered, the registration module 304 sends the local registration verification module 406 a message indicating that the device is registered.

If not registered locally, the campus registration module 304 interrogates the new hand held computer device 100 for its global registration information. Upon receipt of the global registration information, the campus registration module 304 interrogates a global registration server 108 running a registration authentication module 110 and the global registration data base 114 to authenticate the new hand held computer device 102.

If registered, the global registration server 108 returns appropriate compliance and registration records to the campus controller 302 and the campus registration module 304 creates a new registration record for the device 102 and adds it to the campus' master registration data base granting it permission to use the school's campus network. The campus registration module 304 then sends a message to the local registration verification module 406 to notify the local registration verification module that the hand held computer unit 102 is registered and compliant.

If the global device registration authentication module 304 does not find a registration for the hand held computer device 102, then the global device registration authentication module returns a message of non-registration to the educational institution. The educational institution then issues an alert to the local control console 402.

Referring now to FIG. 6, a flow chart illustrates the log in and monitoring of a hand held computer device in an educational environment for an embodiment of the

Petitioner Ex 1002, p. 121
Zimperium v. Taasera, IPR2024-00007

present invention. A student brings a hand held computer device that has been properly provisioned and registered with the educational institution onto the educational institution at start step 600. The device controller starts at step 602. A local controller's listener module listens (i.e., monitors whether the mobile device has entered a domain) for the mobile device at step 604. Step 606 determines if the mobile device is detected, and if not the device controller keeps listening at step 604. If yes indicating that the device is detected, device login is initiated at step 608 and the local controller first requests the registration and compliance status of the hand held computer device. Next, in step 610 the device transmits registration information. The device control software, if present, sends the registration and compliance information to the local controller. If not present, the device control software issues an alert at step 612. The local controller validates the registration at step 614. If the device is registered, the local controller completes the login process and then initiates the device control and management logic at step 616. (See FIG. 7). If the device is not registered, then the local controller issues an alert at step 618.

Turning now to FIG. 7, a flow chart of the device control and management logic is illustrated for an embodiment of the present invention. Once the device is determined to be registered, the local controller begins device monitoring at step 702. The local controller then issues an appropriate control policy to the hand held computer device at step 704. The device next implements a policy at step 706 and then reports compliance with the policy at step 708. The device is logged as compliant in step 710. The local controller next starts periodic device monitoring at step 712, which includes polling the hand-held computing device periodically to ensure that the approved device

Petitioner Ex 1002, p. 122
Zimperium v. Taasera, IPR2024-00007

management application is running, and in control of the device at step 714. If the local controller does not receive a proper response from a poll at step 714, then the local controller re-checks for compliance at step 712 and issued an alert at step 720. If compliance of the device is reported at step 714, then compliance is logged at step 718 in an event logged and monitoring is continued at step 712. Step 720 issues an alert to a local security official noting the time and tracking a duration and/or non-compliance which is stored in a session event database and which the local controller logs in the event log database at step 718.

If a student desires to run a task (educational application, game, etc.) such will be monitored by the device's resident control software at step 714. If such tasks are not compliant with the enterprise policy, the control software will kill or prevent operation of the application and the non-compliant behavior will be reported at step 714 and an alert will be issued at step 720.

In one embodiment of the present invention, the registration process identifies the GPS coordinates of all enterprises near the device being registered and downloads those to the hand held computer device. The GPS coordinates can be stored in a file and up loaded during registration, or alternatively, a user can identify an educational institution or other enterprise and if unknown provide the enterprise's address. Based on the enterprise location information, the control program continually monitors the device's location. When the device is within a predetermined distance of the enterprise during a first visit, the device can enter listener mode on the preferred control program security communication service (G3 Data, 802.11x, 802.15x, etc.). When a connection to a local networking service has been established, then the hand held computing

Petitioner Ex 1002, p. 123
Zimperium v. Taasera, IPR2024-00007

device commences the local registration process as described above. Periodically, it is envisioned that an enterprise interrogates its global registry to verify on-going compliance of all devices registered in the enterprise's master registration database. In the unlikely event of an unrecoverable failure of an enterprise's master registration database, it is also envisioned that the enterprise can rebuilt its enterprise database from the global master database.

In another embodiment, the hand held device and local device control servers employ NFC technology and applications to perform the log in and registration processes described above.

Once a user starts a hand held device that has been properly provisioned and registered with the enterprise, then the hand held device runs a proprietary service that begins a communication session with the local device controller. Upon receiving the session request, the local device controller first verifies the registration and compliance status of the requesting hand-held computing device as described above.

Once a device is found registered and compliant, the local controller then grants service and initiates monitoring. The monitoring includes polling the hand-held computing device periodically to ensure that the approved application is running and in control of the device. If the local controller does not receive a proper response from a poll, then the local controller issues an alert to a local security official noting the time and tracks the duration or apparent non-compliance which it stores in a session event database.

Petitioner Ex 1002, p. 124
Zimperium v. Taasera, IPR2024-00007

If a user desires to run another task such as an educational application, the device will start a new application if and only if it is permitted by the device control policy resident on the hand held device.

An example of the present invention for a single tasking operating system with low level access is now provided with reference to a student entering an educational domain. Once the student starts an application that has been properly provisioned and registered with the educational institution, the application runs a proprietary service that begins a communication session with the local controller. Upon receiving the session request, the local controller first verifies the registration and compliance status of the requesting hand-held computing device. The local controller then verifies that the application requesting service is permitted by the local policy then extant. Upon successful verifications in the above first and second steps, the local controller then permits service and initiates monitoring in a third step. Upon an unsuccessful verification in the third step, the local controller issues an alert to the local security official and logs the event into the local controller's event database. The monitoring includes polling the hand-held computing device periodically to ensure that the approved application is running and in control of the device. While the session is live, the hand-held computing device answers the polling request with data detailing the applications and services active on the device. The local controller files these polling status reports in an auditable device control record for each such device. If the local controller does not receive a proper response from a polling request, then the local controller issues an alert to the local security official noting the time and tracking the duration or apparent non-compliance which are stored in a session event database. If a

Petitioner Ex 1002, p. 125
Zimperium v. Taasera, IPR2024-00007

student terminates one application and decides to run another approved application compliant with the security service according to the present invention, then the process goes to the third step above.

A second example of the present invention for a multi-tasking operating system with low level access is now provided with reference to a student entering an educational domain. Once the student starts the application that has been properly provisioned and registered with the educational domain, then the application runs a proprietary device control low level service that begins a communication session with a local controller. Upon receiving the session request, the local controller first verifies the registration and compliance status of the requesting hand-held computing device. The local controller then verifies that the application requesting service is permitted by the local policy then extant. Upon successful verifications in the above first and second steps, the local controller then grants service and initiates monitoring. The monitoring includes polling the hand-held computing device periodically to ensure that the approved application is running and in control of the device. The local controller can update the list of approved services and applications as it receives policy modifications from an authorized security official. While the session is live, the hand held computing device answers the polling request with data detailing the applications and services active on the device supplied by the low level device control service. The low level service may employ either active or passive control strategies or both. Active control strategies enable only functions approved by the local security policy. Passive control strategies deny service to any request that is not on the policy approved services and applications. The local controller files these polling status reports in an auditable device

Petitioner Ex 1002, p. 126
Zimperium v. Taasera, IPR2024-00007

control record for each such device. If the local controller does not receive a proper response from a poll, then the local controller issues an alert to the local security official noting the time and tracking the duration or apparent non-compliance which is stored in a session event database. If the student initiates another task, then the local controller would examine the approved applications and services as contained in local controller's local copy of the policy. If the task is contained in a local copy of the policy on the local controller, then the local controller would permit the task or service to operate on the device, otherwise the local controller would deny the request.

There are many exemplary implementations were a hierarchy of an open mobile device management network could be reduced or increased in levels. One embodiment would be high security test administration as required by the Educational Testing Service (ETS) for standardized tests such as the ACT, SAT, etc. In these embodiments every test site could be configured such that a test site is an OMDM enterprise. Such OMDM enterprises could interrogate a global registry to determine registration status, and if needed, the OMDM enterprises could create temporary registrations for the duration of a test for unregistered devices present at the test site. Such temporary registrations could be entered into the global device registry. Another embodiment would not record such "ad hoc" registrations in the global database.

Another embodiment is home device management for minor children or others. Such an embodiment would only need a central controller. In this embodiment, multiple polices could be implemented and tailored to the device management needs for each child. In other embodiments, multiple device management policies could be established for multiple classes of controlled hand held computer devices based on the

Petitioner Ex 1002, p. 127
Zimperium v. Taasera, IPR2024-00007

characteristics of the device owner and/or other characteristics of the device owner's profile.

An exemplary embodiment is described for standardized test sites. This embodiment is an example of multiple ad hoc embodiments that pertain to any authorized use or uses specified in a policy. This embodiment is a specific case illustrative of the more general ad hoc embodiments. The present invention may be used in this embodiment to control and monitor mobile calculating devices during the administration of standardized examinations. In this embodiment, a user arrives at a test site with a mobile device, and the user must register the device as a condition of being able to take the examination. The registration by the user is done ad hoc at the test site, and involves making a positive connection between the hand held computer device and a local security controller managed by the test administrator. The user will be using his mobile device as a graphing calculator. The purpose of the registration process is to turn off unauthorized functionality of the device for the duration of the exam, and to monitor the device at regular intervals to verify that the device remains in compliance, with unauthorized functionality of the device remaining disabled until the user leaves the test site.

In this embodiment, the user may be given a login identity. Once logged on, the security controller acquires and stores the mobile device's identification. The log on process may be implemented as a feature of the graphing calculator application on the mobile device. During the login transaction, an encrypted packet containing the security policy is downloaded to the mobile device and used to facilitate subsequent compliance monitoring transactions, each of which is also encrypted. The security policy in this

Petitioner Ex 1002, p. 128
Zimperium v. Taasera, IPR2024-00007

case can include a time interval (i.e., the duration of the exam), a geographic location (i.e., the test site), and a list of unauthorized functions to be disabled while the policy remains in effect (e.g., incoming/outgoing calls, text messaging, camera, voice recorder, blue tooth, wireless communication with anything other than the local security controller, applications other than the graphing calculator, etc.).

The hand held computer device is considered to be compliant for the specified time interval as long as the device remains in the specified geographic location, responds correctly each time the local security controller queries the device's status, and all unauthorized functions are verified disabled during each query. Otherwise, the hand held computer device is designated as non-compliant, and the local security controller takes an appropriate action to notify the exam administrator. The default state is non-compliant, so the mobile device is automatically non-compliant prior to registration at the exam site and after the compliance policy expires at the end of the exam, or whenever the device leaves the exam site.

All compliance monitoring transactions can be logged by the security controller, which can provide a full audit trail for each hand held computer device registered at the test site. The local security monitor can also be the global security monitor in this scenario, since the local security monitor is the sole source of compliance policy for the administration of the exam.

In another embodiment, the invention will provide a "no-click sign-on" process by continuously monitoring network traffic using traffic detection and analysis technology. This allows detection of traffic from unregistered devices and the signaling of an alarm indicating traffic from unregistered devices even if a hand held computer device does

Petitioner Ex 1002, p. 129
Zimperium v. Taasera, IPR2024-00007

not have a monitoring application installed. This embodiment would monitor traffic on all relevant wireless frequencies and all relevant protocols such as but not limited to 802.11 (Wi-Fi), 802.15 (Bluetooth), 802.16 (WiMax) and Carrier provided Wireless Cellular Data services such as but not limited to "3G" and "4G."

When a device comes into a domain secured by the invention it will attempt to interrogate the device. The interrogation will only succeed if the device has the invention's authentic monitoring software installed, and is properly registered. The device will respond to the interrogation with its registration status. Failure to respond will indicate non-compliance.

If the newly arrived mobile device reports that it is registered, then the local device controller will interrogate the local registration and authentication database registry, and if necessary, the global registration and authentication database registry, to validate that the particular mobile computing device is registered, and also that the control software is authentic and compliant. This is accomplished by comparing the registration data received from the hand held computing device with that contained in the registry, including such information as to authenticate the control software. This process allows a registered, authenticated and compliant hand held computer device to complete the login process without the device's user having to take any action. In a preferred embodiment, this could provide automatic attendance taking in a class room.

A controlling device is provided with hardware and software that allows it to control use of the hand held computing device. The controlling device is, for instance, a wireless access device, a special hardware machine implementing key supervisory and control functions, telephone, a PDA, or personal computer comprising an application

Petitioner Ex 1002, p. 130
Zimperium v. Taasera, IPR2024-00007

which provides a way to control the wireless access device. In one embodiment, the application runs on a controlling entity's wireless access point device.

Alternatively or in addition, the policy management application may be a web-based application where parameters are established using common web based user controls such as drop down lists, radio buttons and the like.

In another embodiment, the policy management application may interact with the local security official in a structured dialogue. The system and method may for example be used by a controlling entity (Controller) such as a parent, to control or manage use of a child's cellular telephone, a school administrator or their delegated security official to set campus policies controlling students use of their smart devices, a classroom teacher or an exam proctor or the like to set local policies that are more or less restrictive than the campus policy, or an International testing agency to ensure the uniform implementation of its exam security policies and procedures.

For standardized tests, the testing agency can develop a standard policy which can be disseminated globally to all local control devices. Alternatively, the testing authorities may be directly supplied verified compliant local control devices that they can distribute under the security methods they use for their test materials.

The present invention provides for a multi-layered policy regime. In an educational setting, a campus policy sets the defaults for a campus. In some instances, those policy settings are absolute and cannot be modified. Local policies established by instructors for their classes can more or less restrictive than the campus policy. Special policy provisions can be made for certain testing authorities during their testing. For example, testing authorities can establish policies that supersede campus policies.

Petitioner Ex 1002, p. 131
Zimperium v. Taasera, IPR2024-00007

These policies could be distributed via a central service to the appropriate locations or by the agencies directly.

In one embodiment, the present invention permits restrictions based on time by identifying periods when the child or student may make use of the hand held computer device. For example, telephone calls may be restricted based on time of day, such as during class, or day of the week, such as weekdays or weekends when different policies might apply.

In another embodiment, the present invention permits restrictions based on location. For example, the enterprise controller might establish different policies for locker rooms and language labs.

The identified time restrictions are stored in an enterprise control database accessed by the authorized hand held computer devices. Teachers, proctors, etc. can modify the enterprise policies as they deem appropriate if permitted by their authorization level and enterprise policy.

In one embodiment, the local controller devices communicate with security software on the hand held computer devices to either affirmatively enable or disable (or both) the applications and services that the device can employ or run.

In another embodiment, students and or their parents opt-in to device control by acquiring software for their device and registering their hand held computer devices with a central registry. During the software installation and registration process on the devices, certain unique parameters are established that permit the registry to validate the authenticity and continued compliance of the devices.

Petitioner Ex 1002, p. 132
Zimperium v. Taasera, IPR2024-00007

In an embodiment, the registry periodically audits the continued compliance of the device. Moreover, the registry and compliance service will be provided on a subscription basis.

In another embodiment, when a foreign device (i.e., new device external to a domain) comes into a domain secured by the present invention's controllers, such controllers will interrogate the new device. The foreign device will report a registration status, with a failure to respond indicating non-compliance. If the foreign device reports that it is compliant, then the local controller will interrogate the global registration and authentication database registry to validate that the particular hand-held computing device is registered and compliant. This is done by comparing data received from the foreign device with that contained in the global registration and authentication registry.

If the foreign device is not registered in the global registration and authentication registry, or not in compliance an alert will be sent to the local control official. If the foreign device is compliant, then the foreign device will be registered with the enterprise device registration data base.

In one embodiment for examination situations, hand held computer devices can be validated at the examination site prior to administering of the test.

In another embodiment, instructors could be provided with lists of approved devices detected with the associated student names. The teachers could further implement a campus policy for non-controlled devices which were being used in unauthorized ways.

Petitioner Ex 1002, p. 133
Zimperium v. Taasera, IPR2024-00007

In another embodiment, a campus can have a registration procedure so that students would be required to have their devices provisioned and authenticated as being compliant.

In yet another embodiment, compliance and control procedures would not invoke privacy issues since such procedures would be self-selected by parents, guardians, or students on an explicit opt-in procedure and as explicitly detailed in an end user license agreement (EULA). Unauthorized searches of the device owner's files would not be allowed unless there was significant evidence of illicit use of the device or possession of lost or stolen property. Such evidence could be produced by the present invention's audit and verification procedures that the device owner had explicitly authorized.

A situation where a device operator's authorization might not be present would be where an instrument was, for example, lost or stolen and used without an owner's permission. In one embodiment, the present invention could indicate new phones coming into a domain. Teachers or other officials might decide to investigate if the name in the registry and the student using the device did not match. Lost or stolen devices could also be reported to the registry and alerts could be dispatched to local officials indicating that a specific device was reported as lost or stolen.

In the case of a borrowed hand held computer device, use by an authorized person could optionally be governed by the terms of the owner's software license as detailed by the terms and conditions of the EULA.

In a single tasking operating system which does not provide facilities to directly interrogate low level system management facilities, one embodiment of the present invention can have device control affected by a layer upon which an educational

Petitioner Ex 1002, p. 134
Zimperium v. Taasera, IPR2024-00007

application operates, and would continually report the controlling device status. Failure to report a status to the controller would create compliance alert. The communication between the controller and the device control software would be encrypted and contain information that would be unique and not easily replicated by hacked software or spoofing.

In a further embodiment, in a multitasking environment with low level system management access, device control can be achieved by a low level control program that would monitor, control, and report system status providing audit trails and compliance alerts. Communication with the controlling device could be in a manner similar to that described above.

While the present inventions and what is considered presently to be the best modes thereof have been described in a manner that establishes possession thereof by the inventors and that enables those of ordinary skill in the art to make and use the inventions, it will be understood and appreciated that there are many equivalents to the exemplary embodiments disclosed herein and that myriad modifications and variations may be made thereto without departing from the scope and spirit of the inventions, which are to be limited not by the exemplary embodiments but by the appended claims.

Petitioner Ex 1002, p. 135
Zimperium v. Taasera, IPR2024-00007

WHAT IS CLAIMED IS:

1. A method for device management comprising the steps of:

downloading a device control application to one or more hand-held devices;

registering the one or more hand-held devices within a global registry service;

requesting a communication session between the one or more hand-held devices and a local device control policy server;

creating the communication session between the one or more hand-held devices and the local device control policy server;

verifying the registration and compliance status of the one or more hand-held devices;

granting service to one or more approved applications including one or more restrictions from the local device control policy server to the one or more hand held devices;

monitoring compliance of the one or more hand held devices with the device control policy resident on those devices;

issuing non-compliance alerts to the policy control administrators; and

logging events into a database of the local device control policy server.

2. The method of Claim 1, wherein said requesting, creating, verifying, granting, monitoring, and logging steps operate independent of device user interaction upon initiation of the creating the communication session step.

Petitioner Ex 1002, p. 136
Zimperium v. Taasera, IPR2024-00007

3. The method of Claim 1, wherein the one or more restrictions are based on time.

4. The method of Claim 1, wherein the one or more restrictions are based on location.

5. The method of Claim 1, wherein the one or more restrictions are based on sensor information available on a mobile device that implements control policies.

6. The method of Claim 1, wherein said sensor information comprises motion sensor data.

7. The method of Claim 1, further comprising a step of determining whether the one or more hand devices are unregistered.

8. The method of Claim 7, wherein an alarm is generated for unregistered hand held devices.

Petitioner Ex 1002, p. 137
Zimperium v. Taasera, IPR2024-00007

9. The method of Claim 1, wherein said monitoring step further includes the steps of:

polling the one or more hand-held devices to ensure that the device control software is running, that only zero, or one or more approved applications and services are running and that no prohibited applications and services are running;

providing data regarding the one or more hand-held devices;

generating one or more status reports; and

filing the one or more status reports in an auditable control record.

10. A system for network security for hand held computer devices comprising:

a local policy management server configured to connect to an internet network and having one or more registration modules stored thereon;

a device control console connected to the local policy management server and configured to facilitate user entry of local device control policies;

a database connected to the local device control policy server and configured to store registrations of one or more hand held computer devices; and

a global registration server connected to the local device control policy server via a network, the global registration server configured to determine if the hand held computer device is registered globally on the global registration server.

11. The system of Claim 10, wherein said registration modules comprises at least an authentication registration module configured to authorize registrations for a local entity.

Petitioner Ex 1002, p. 138
Zimperium v. Taasera, IPR2024-00007

12. The system of Claim 10, further comprising a local controller connected to the local device control policy server.

13. The system of claim 12, wherein the local controller has at least one registration module configured to verify registration of the one or more hand held computer devices with the local device control policy server.

14. The system of Claim 12, further comprising a local controller console connected to the local controller, the local controller console configured to facilitate user entry of local policy data unless entry of the local policy data is restricted by the policy stored on the enterprise registration database.

15. The system of Claim 14, wherein the local controller initiates determination of registration of the one or more hand held computer devices upon the devices entering a local network domain within an enterprise network domain, and if the devices are unregistered, then transmitting a request for registration to the enterprise controller to determine whether the devices are registered with the local device control policy server.

16. The system of Claim 15, wherein if the devices are unregistered with the enterprise controller, then the enterprise controller transmits a request to the global registration server to determine whether the devices are registered globally.

Petitioner Ex 1002, p. 139
Zimperium v. Taasera, IPR2024-00007

17. The system of Claim 16, wherein upon determination that the devices are registered globally, then a request is transmitted to the enterprise controller requesting local registration and enterprise registration of the globally registered devices.

18. The system of claim 17, wherein an alert is provided to at least the local console upon a determination that the one or more hand held devices are lacking a global registration.

Petitioner Ex 1002, p. 140
Zimperium v. Taasera, IPR2024-00007

Fig. 1

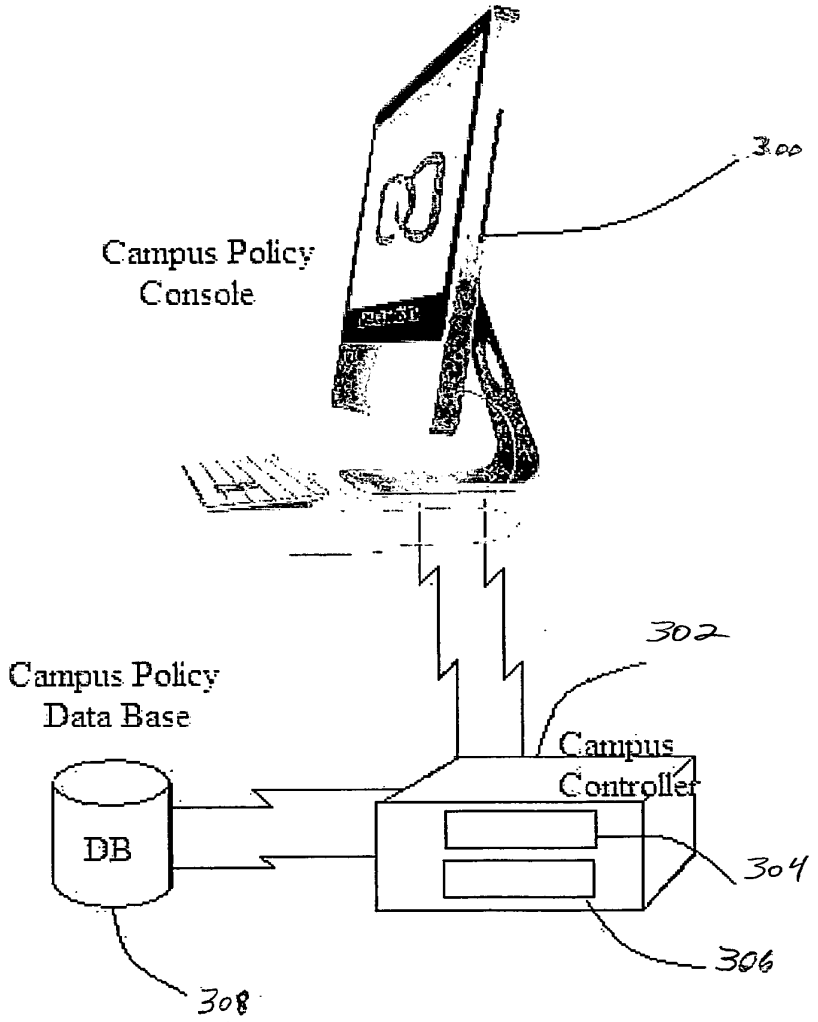
Petitioner Ex 1002, p. 141
Zimperium v. Taasera, IPR2024-00007

Fig 2A

Students Phone w/SW & Reg

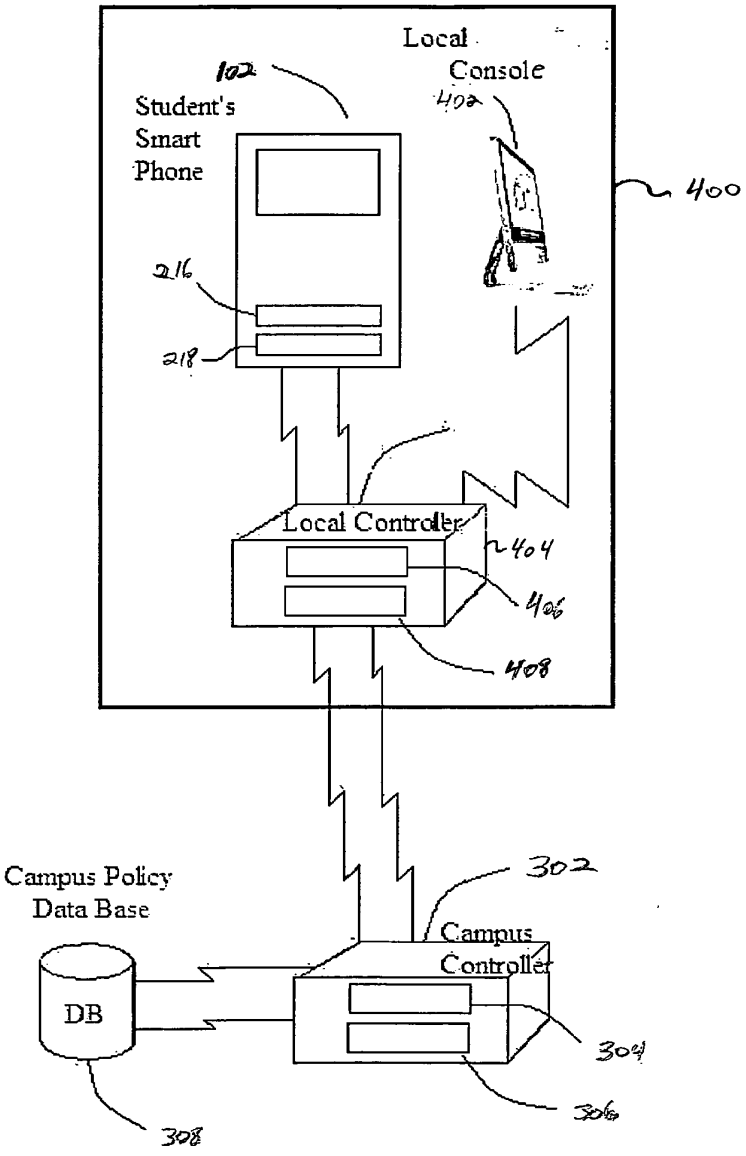
FIG. 2B

Fig 3



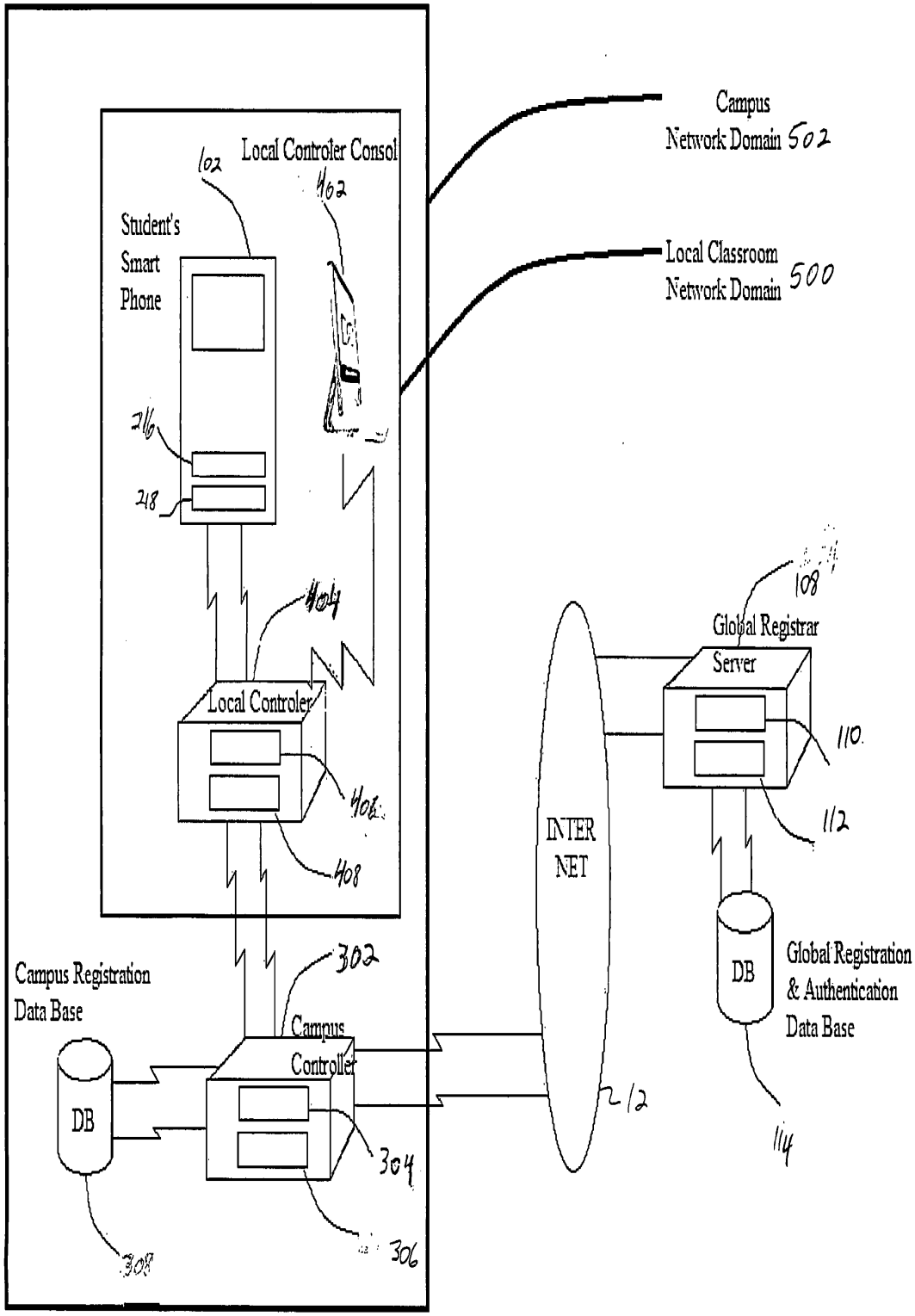
Petitioner Ex 1002, p. 143
Zimperium v. Taasera, IPR2024-00007

Fig 4



Petitioner Ex 1002, p. 144
Zimperium v. Taasera, IPR2024-00007

Fig 5


Campus
Network Domain 502
Local Classroom
Network Domain 500
Local Controler Consol
102
402
Student's
Smart
Phone
216
218
404
Local Controler
406
408
108
Global Registrar
Server
110
112
INTER
NET
212
DB
Global Registration
& Authentication
Data Base
114
Campus Registration
Data Base
302
Campus
Controller
DB
304
306
308

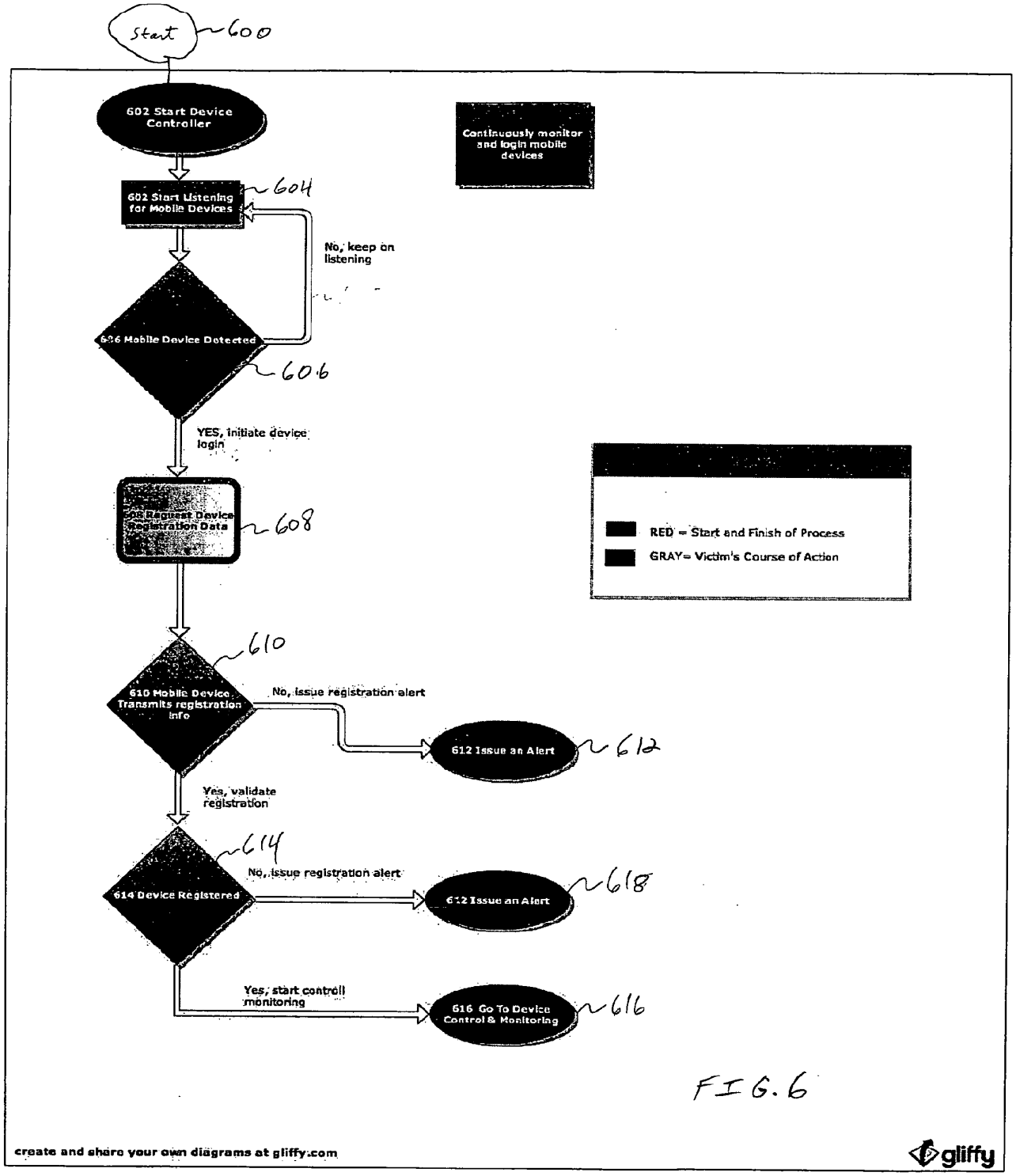


FIG. 6

Petitioner Ex 1002, p. 146
Zimperium v. Taasera, IPR2024-00007

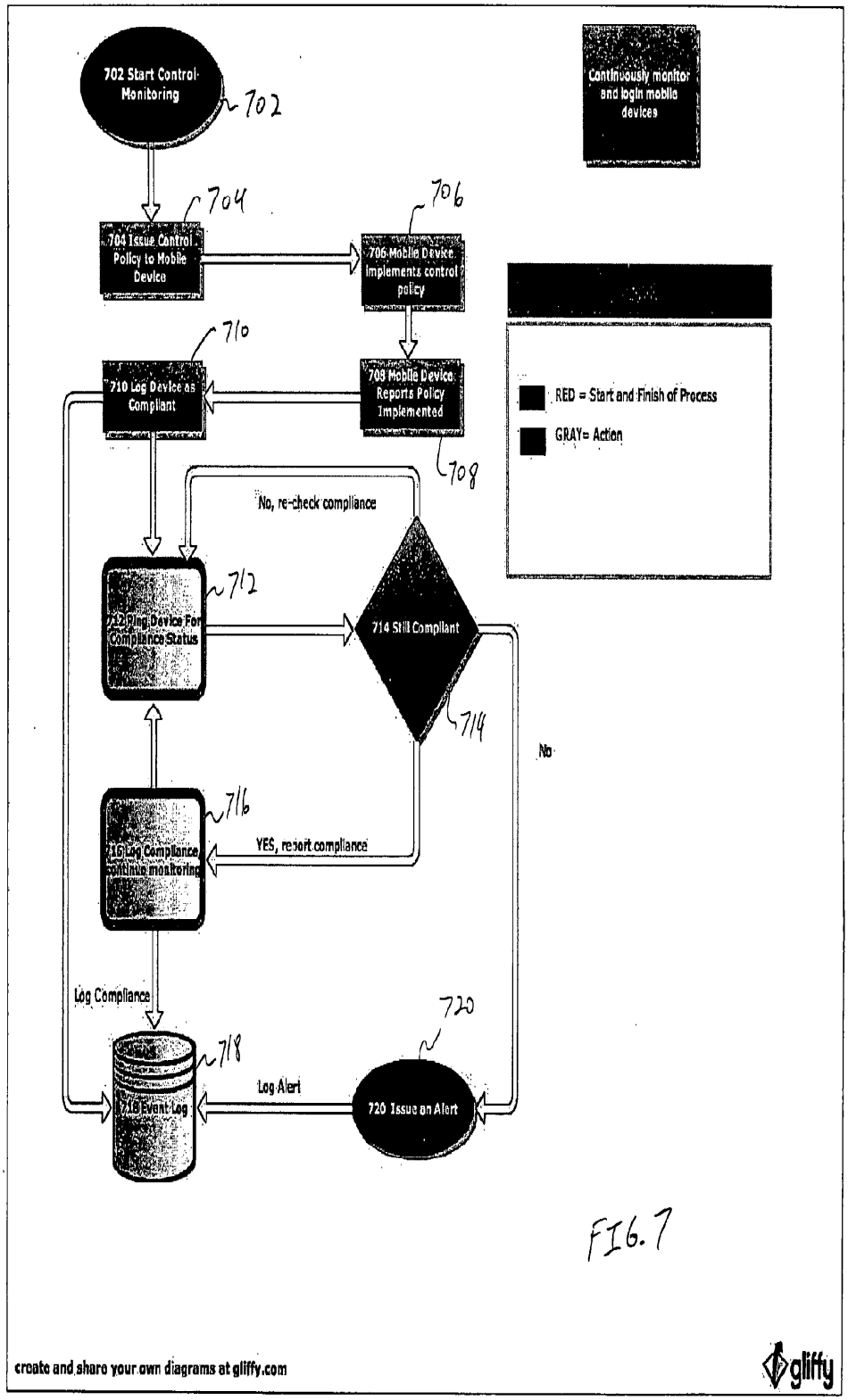

Continuously monitor and login mobile devices
702 Start Control Monitoring
702
704
704 Issue Control Policy to Mobile Device
706
706 Mobile Device implements control policy
708 Mobile Device Reports Policy Implemented
708
710
710 Log Device as Compliant
RED = Start and Finish of Process
GRAY= Action
No, re-check compliance
712
712 Ping Device For Compliance Status
714 Still Compliant
714
No
716
716 Log Compliance, continue monitoring
YES, report compliance
Log Compliance
718
718 Event Log
Log Alert
720
720 Issue an Alert
create and share your own diagrams at gliffy.com
gliffy

FIG. 7

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2010/002264

A. CLASSIFICATION OF SUBJECT MATTER
IPC(8) - G06F 21/22 (2010.01)
USPC - 455/420
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC(8) - G06F 9/445, 21/00, 06, 22; H04H 20/00, 12, 14 (2010.01)
USPC - 370/328, 338, 401; 455/3.01, 418-420, 425, 550.1

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
PatBase, Google Patents

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2008/0070495 A1 (STRICKLEN et al) 20 March 2008 (20.03.2008) entire document	10-18
Y	US 6,553,375 B1 (HUANG et al) 22 April 2003 (22.04.2003) entire document	1-9
Y	US 6,031,830 A (COWAN) 29 February 2000 (29.02.2000) entire document	1-9
Y	US 2008/0076400 A1 (MOOSAVI et al) 27 March 2008 (27.03.2008) entire document	3-4
Y	US 2006/0094412 A1 (NONOYAMA et al) 04 May 2006 (04.05.2006) entire document	5
Y	US 2008/0125079 A1 (O'NEIL et al) 29 May 2008 (29.05.2008) entire document	8-9

☐ Further documents are listed in the continuation of Box C. ☐

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
07 October 2010	14 OCT 2010
Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US, Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-3201	Authorized officer: Blaine R. Copenheaver PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774

Form PCT/ISA/210 (second sheet) (July 2009)

Electronic Acknowledgement Receipt

EFS ID:	15824239
Application Number:	13540142
International Application Number:	
Confirmation Number:	4198
Title of Invention:	RULES BASED ACTIONS FOR MOBILE DEVICE MANAGEMENT
First Named Inventor/Applicant Name:	Jatin MALIK
Customer Number:	86308
Filer:	Michael Kenneth Jones/Samantha Rizzo
Filer Authorized By:	Michael Kenneth Jones
Attorney Docket Number:	130839.02101
Receipt Date:	20-MAY-2013
Filing Date:	02-JUL-2012
Time Stamp:	18:58:23
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Form (SB08)	101IDS.pdf	65705 40307102a1edb401b920fd5f4f95a317e5f37af0	no	4

Warnings:	
Information:	

This is not an USPTO supplied IDS fillable form					
2	Foreign Reference	WO2011022053A1.pdf	1825899 74f27c830471dbcb8397dcb58c3ff3669359fffb	no	49
Warnings:					
Information:					
			Total Files Size (in bytes):	1891604	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99**)		
	Application Number	13540142
	Filing Date	2012-07-02
	First Named Inventor	Jatin Malik et al.
	Art Unit	2447
	Examiner Name	Joon H. Hwang
	Attorney Docket Number	130839.02101

U.S.PATENTS						
Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					
If you wish to add additional U.S. Patent citation information please click the Add button.						

U.S.PATENT APPLICATION PUBLICATIONS						
Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					
If you wish to add additional U.S. Published Application citation information please click the Add button.						

FOREIGN PATENT DOCUMENTS								
Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2]	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							☐
If you wish to add additional Foreign Patent Document citation information please click the Add button								

NON-PATENT LITERATURE DOCUMENTS			
Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**		
	Application Number	13540142
	Filing Date	2012-07-02
	First Named Inventor	Jatin Malik et al.
	Art Unit	2447
	Examiner Name	Joon H. Hwang
	Attorney Docket Number	130839.02101

	1	International Search Report and Written Opinion mailed 28 September 2012 for corresponding International Application No. PCT/US2012/045252	☐

If you wish to add additional non-patent literature document citation information please click the Add button

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99**)		
	Application Number	13540142
	Filing Date	2012-07-02
	First Named Inventor	Jatin Malik et al.
	Art Unit	2447
	Examiner Name	Joon H. Hwang
	Attorney Docket Number	130839.02101

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☐ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Michael K. Jones, Reg. #41100/	Date (YYYY-MM-DD)	2013-06-27
Name/Print	Michael K. Jones	Registration Number	41100

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

PATENT COOPERATION TREATY

From the INTERNATIONAL SEARCHING AUTHORITY

To: JAY MITCHELL
PEPPER HAMILTON LLP
400 BERWYN PARK
899 CASSATT ROAD
BERWYN, PA 19312

PCT

NOTIFICATION OF TRANSMITTAL OF THE INTERNATIONAL SEARCH REPORT AND THE WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY, OR THE DECLARATION

(PCT Rule 44.1)

Date of mailing *(day/month/year)*	28 SEP 2012
Applicant's or agent's file reference 130839.02102	**FOR FURTHER ACTION** See paragraphs 1 and 4 below
International application No. PCT/US2012/045252	International filing date *(day/month/year)* 02 July 2012
Applicant FIBERLINK COMMUNICATIONS CORPORATION	

1. ☒ The applicant is hereby notified that the international search report and the written opinion of the International Searching Authority have been established and are transmitted herewith.

   Filing of amendments and statement under Article 19:
   The applicant is entitled, if he so wishes, to amend the claims of the international application (see Rule 46):

   When? The time limit for filing such amendments is normally two months from the date of transmittal of the international search report.

   Where? Directly to the International Bureau of WIPO, 34 chemin des Colombettes 1211 Geneva 20, Switzerland, Facsimile No.: +41 22 338 82 70

   For more detailed instructions, see *PCT Applicant's Guide*, International Phase, paragraphs 9.004 – 9.011.

2. ☐ The applicant is hereby notified that no international search report will be established and that the declaration under Article 17(2)(a) to that effect and the written opinion of the International Searching Authority are transmitted herewith.

3. ☐ **With regard to any protest** against payment of (an) additional fee(s) under Rule 40.2, the applicant is notified that:

   ☐ the protest together with the decision thereon has been transmitted to the International Bureau together with any request to forward the texts of both the protest and the decision thereon to the designated Offices.

   ☐ no decision has been made yet on the protest; the applicant will be notified as soon as a decision is made.

4. **Reminders**

   The applicant may submit comments on an informal basis on the written opinion of the International Searching Authority to the International Bureau. The International Bureau will send a copy of such comments to all designated Offices unless an international preliminary examination report has been or is to be established. Following the expiration of 30 months from the priority date, these comments will also be made available to the public.

   Shortly after the expiration of **18 months** from the priority date, the international application will be published by the International Bureau. If the applicant wishes to avoid or postpone publication, a notice of withdrawal of the international application, or of the priority claim, must reach the International Bureau before the completion of the technical preparations for international publication (Rules 90*bis*.1 and 90*bis*.3).

   Within **19 months** from the priority date, but only in respect of some designated Offices, a demand for international preliminary examination must be filed if the applicant wishes to postpone the entry into the national phase **until 30 months** from the priority date (in some Offices even later); otherwise, the applicant must, **within 20 months** from the priority date, perform the prescribed acts for entry into the national phase before those designated Offices.

   In respect of other designated Offices, the time limit of **30 months** (or later) will apply even if no demand is filed within 19 months.

   For details about the applicable time limits, Office by Office, see www.wipo.int/pct/en/texts/time_limits.html and the *PCT Applicant's Guide*, National Chapters.

Name and mailing address of the ISA/ Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-3201	Authorized officer Blaine R. Copenheaver PCT Helpdesk: 571-272-4300 Telephone No. PCT OSP: 571-272-7774

Form PCT/ISA/220 (July 2010)

PATENT COOPERATION TREATY

PCT

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference 130839.02102	**FOR FURTHER ACTION**	see Form PCT/ISA/220 as well as, where applicable, item 5 below.
International application No. PCT/US2012/045252	International filing date *(day/month/year)* 02 July 2012	(Earliest) Priority Date *(day/month/year)* 01 July 2011
Applicant FIBERLINK COMMUNICATIONS CORPORATION		

This international search report has been prepared by this International Searching Authority and is transmitted to the applicant according to Article 18. A copy is being transmitted to the International Bureau.

This international search report consists of a total of 9 sheets.

☐ It is also accompanied by a copy of each prior art document cited in this report.

1. **Basis of the report**

a. With regard to the **language**, the international search was carried out on the basis of:

☒ the international application in the language in which it was filed.

☐ a translation of the international application into _____ which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b)).

b. ☐ This international search report has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43.6*bis*(a)).

c. ☐ With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, see Box No. I.

2. ☐ **Certain claims were found unsearchable** (see Box No. II).

3. ☐ **Unity of invention is lacking** (see Box No. III).

4. With regard to the **title**,

☒ the text is approved as submitted by the applicant.

☐ the text has been established by this Authority to read as follows:

5. With regard to the **abstract**,

☒ the text is approved as submitted by the applicant.

☐ the text has been established, according to Rule 38.2, by this Authority as it appears in Box No. IV. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority.

6. With regard to the **drawings**,

a. the figure of the **drawings** to be published with the abstract is Figure No. 1

☒ as suggested by the applicant.

☐ as selected by this Authority, because the applicant failed to suggest a figure.

☐ as selected by this Authority, because this figure better characterizes the invention.

b. ☐ none of the figures is to be published with the abstract.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2012/045252

A. CLASSIFICATION OF SUBJECT MATTER
IPC(8) - G06F 21/00 (2012.01)
USPC - 726/1
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC(8) - G06F 15/173, 17/00, 21/00 (2012.01)
USPC - 709/224, 225, 226; 726/1, 6, 25

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
PatBase, Orbit, Google Patent, Google, Google Scholar

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X --- Y	US 2010/0242088 A1 (THOMAS) 23 September 2010 (23.09.2010) entire document	1-2, 6, 9-10, 14, 16-18, 21, 23 --- 3-5, 7-8, 11-13, 15, 19-20, 22
Y	US 2008/0114862 A1 (MOGHADDAM et al) 15 May 2008 (15.05.2008) entire document	3
Y	WO 2011/022053 A1 (NAIMAN et al) 24 February 2011 (24.02.2011) entire document	4, 8, 15, 22
Y	US 2007/0266422 A1 (GERMANO et al) 15 November 2007 (15.11.2007) entire document	7, 12-13, 20
Y	US 2007/0206552 A1 (YAQUB et al) 06 September 2007 (06.09.2007) entire document	5, 11, 19

☐ Further documents are listed in the continuation of Box C. ☐

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
07 September 2012	28 SEP 2012
Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US, Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-3201	Authorized officer: Blaine R. Copenheaver PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774

Form PCT/ISA/210 (second sheet) (July 2009)

PATENT COOPERATION TREATY

From the
INTERNATIONAL SEARCHING AUTHORITY

To: JAY MITCHELL
PEPPER HAMILTON LLP
400 BERWYN PARK
899 CASSATT ROAD
BERWYN, PA 19312

PCT

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

(PCT Rule 43*bis*.1)

Date of mailing *(day/month/year)*	28 SEP 2012
Applicant's or agent's file reference 130839.02102	**FOR FURTHER ACTION** See paragraph 2 below

International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/US2012/045252	02 July 2012	01 July 2011

International Patent Classification (IPC) or both national classification and IPC
IPC(8) - G06F 21/00 (2012.01)
USPC - 726/1

Applicant FIBERLINK COMMUNICATIONS CORPORATION

1. This opinion contains indications relating to the following items:

- ☒ Box No. I Basis of the opinion
- ☐ Box No. II Priority
- ☐ Box No. III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- ☐ Box No. IV Lack of unity of invention
- ☒ Box No. V Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- ☐ Box No. VI Certain documents cited
- ☐ Box No. VII Certain defects in the international application
- ☐ Box No. VIII Certain observations on the international application

2. **FURTHER ACTION**

If a demand for international preliminary examination is made, this opinion will be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA") except that this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notified the International Bureau under Rule 66.1*bis*(b) that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.

For further options, see Form PCT/ISA/220.

Name and mailing address of the ISA/US	Date of completion of this opinion	Authorized officer:
Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-3201	07 September 2012	Blaine R. Copenheaver PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774

Form PCT/ISA/237 (cover sheet) (July 2011)

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US2012/045252

Box No. I Basis of this opinion

1. With regard to the **language**, this opinion has been established on the basis of:

   ☒ the international application in the language in which it was filed.

   ☐ a translation of the international application into _____ which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b)).

2. ☐ This opinion has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43*bis*.1(a))

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, this opinion has been established on the basis of a sequence listing filed or furnished:

   a. (means)

   ☐ on paper

   ☐ in electronic form

   b. (time)

   ☐ in the international application as filed

   ☐ together with the international application in electronic form

   ☐ subsequently to this Authority for the purposes of search

4. ☐ In addition, in the case that more than one version or copy of a sequence listing has been filed or furnished, the required statements that the information in the subsequent or additional copies is identical to that in the application as filed or does not go beyond the application as filed, as appropriate, were furnished.

5. Additional comments:

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US2012/045252

Box No. V **Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement**

1. Statement

Novelty (N)	Claims	3-5, 7-8, 11-13, 15, 19-20, 22	YES
	Claims	1-2, 6, 9-10, 14, 16-18, 21, 23	NO
Inventive step (IS)	Claims	None	YES
	Claims	1-23	NO
Industrial applicability (IA)	Claims	1-23	YES
	Claims	None	NO

2. Citations and explanations:

Claims 1-2, 6, 9-10, 14, 16-18, 21, 23 lack novelty under PCT Article 33(2) as being anticipated by Thomas.

Regarding claim 1, Thomas discloses a method for providing device management services (method for assessing the compliance state of a client facility, para. 0002-0003; corporate policy manager, para. 0023; see fig. 3) comprising steps of: gathering, from a network (over the Internet, fig. 1), status information related to each of a plurality of mobile devices (the security management facility scans the client facility's 144 files, clients are mobile, para. 0028, 0058; fig. 3, step 304), each mobile device utilizing one of a plurality of different mobile operating systems (security application may be loaded onto a plurality of computer platforms, para. 0050); storing the status information in an electronic database accessible to a server (detection techniques facility 130 monitors the enterprise facility 102 and stored data based on results of scanned files, para. 0047); evaluating a first compliance state of at least one of the mobile devices (mobile computing devices, para. 0047; see Fig. 3, step 308) from the status information (compliance is determined, para. 0017-0020, 0025, 0046) using a plurality of administrator-defined rules (threat management based on policies, para. 0025, 0043-0045); and initiating at least one action defined by the user-defined rules in response to the step of evaluating (remediation is effected based on enterprise rules, para. 0018-0020, 0036; see fig. 3, step 310), wherein the step of evaluation is performed by a server (server, para. 0093) automatically, in response to changes in the status information (remedial action facility 128 acts on policy violations, para. 0046).

Regarding claim 10, Thomas discloses a method for providing device management services (method for assessing the compliance state of a facility, para. 0002-0003; corporate policy manager, para. 0023; see fig. 3) comprising steps of: making a determination that an attribute of a mobile device has changed (threat management facility 100 monitors mobile computing devices for and detects threats and policy violations, para. 0046-0047); evaluating the attribute, by a processor at a server (server, para. 0093) in response to the determination, to determine if it triggers at least one of a plurality of administrator defined rules (threat management based on policies, para. 0025, 0043-0045), which indicates that the attribute is out of compliance (compliance is determined, para. 0017-0020, 0025, 0046); and automatically initiating, at the server, an action defined by the at least one of a plurality of administrator defined rules if the attribute is out of compliance (remedial action facility 128 acts on policy violations, para. 0046), wherein the attribute is stored in a data store accessible to the server (network access rules facility, para. 0044-0045), that includes substantially real-time data pertaining to a plurality of attributes of a plurality of mobile devices (threat management facility 100 performs frequent testing, para. 0025, 0048), comprising devices having different mobile operating systems (security application may be loaded onto a plurality of computer platforms, para. 0050).

Regarding claim 17, Thomas discloses a system for providing device management services (threat management facility 100, para. 0023, fig. 1) comprising: a data store (network access rules facility, para. 0044-0045) configured to be accessible by a server (server, para. 0093); computer readable instructions for execution on the server comprising instructions (instructions, para. 0090) configured to: make a determination that an attribute of a mobile device stored in the data store has changed (threat management facility 100 monitors mobile computing devices for and detects threats and policy violations, para. 0046-0047); evaluate the attribute, in response to the determination, to determine if it triggers at least one of a plurality of administrator defined rules (threat management based on policies, para. 0025, 0043-0045), which indicates that the attribute is out of compliance (compliance is determined, para. 0017-0020, 0025, 0046); and automatically initiate an action defined by the at least one of a plurality of administrator defined rules if the attribute is out of compliance (remedial action facility 128 acts on policy violations, para. 0046), wherein the data store is configured to include substantially real-time data pertaining to a plurality of attributes of a plurality of mobile devices (threat management facility 100 performs frequent testing, para. 0025, 0048), comprising devices having different mobile operating systems (security application may be loaded onto a plurality of computer platforms, para. 0050).

Regarding claim 2, Thomas discloses the method of claim 1, wherein the at least one action is selectable from a plurality of actions (remedial action may take a plurality of forms, para. 0046), comprising blocking access by the at least one of the mobile devices to a corporate resource (corporate facility restricts access to certain databases, para. 0026, 0043; see fig. 3, step 310, blocking communications).

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US2012/045252

Supplemental Box

In case the space in any of the preceding boxes is not sufficient.
Continuation of:

Regarding claims 6, 14, 21, Thomas discloses gathering information from that mobile device (the security management facility scans the client facility's 144 files, clients are mobile, para. 0028, 0058; fig. 3, step 304) and at least one other source on the network (security compliance information is derived from a security policy for comparison with scanned files, fig. 3 [step 304], para. 0074).

Regarding claims 9, 16, 23 Thomas discloses wherein the status information comprises location information about each mobile device (user's location is monitored, para. 0043, 0047).

Regarding claim 18, Thomas discloses the system of claim 17, wherein the computer readable instructions further comprise instructions configured to present a user interface to an administrator to allow selection of at least one attribute and one available action to define the at least one of the plurality of administrator defined rules (web portal accessible by administrator as user interface, para. 0053).

Claims 3 lacks an inventive step under PCT Article 33(3) as being obvious over Thomas in view of Moghaddam et al., hereinafter referred to as Moghaddam.

Regarding claim 3, Thomas teaches the method of claim 1, but lacks the teaching wherein the at least one action is selectable from a plurality of actions, comprising blocking e-mail access for the at least one of the mobile devices. Moghaddam is in the field of configurable mobile communication (title) and teaches wherein the at least one action is selectable from a plurality of actions, comprising blocking e-mail access for the at least one of the mobile devices (e-mail is restricted, para. 0045). It would have been obvious to one of ordinary skill in the art at the time of the invention to use the teachings of Moghaddam to incorporate the above teachings in the invention of Thomas. The motivation would have been to provide the ability to configure device usage restrictions for a mobile communications device (Moghaddam, para. 0012).

Claims 4, 8, 15, 22 lack an inventive step under PCT Article 33(3) as being obvious over Thomas in view of Naiman et al., hereinafter referred to as Naiman.

Regarding claim 4, Thomas teaches the method of claim 1, but lacks the teaching wherein the at least one action is selectable from a plurality of actions, comprising wiping information from the at least one of the mobile devices. Naiman is in the field of device management (title) and teaches wherein the at least one action is selectable from a plurality of actions, comprising wiping information from the at least one of the mobile devices (control policies invoke a function to wipe files, pg. 11, para 2). It would have been obvious to one of ordinary skill in the art at the time of the invention to use the teachings of Naiman to incorporate the above teachings in the invention of Thomas. The motivation would have been to prevent jail breaking, hacking and spoofing (Naiman, pg. 5, para 2).

Regarding claims 8, 15, 22 Thomas lacks the teaching wherein the plurality of different mobile operating systems comprise at least Android and iOS. Naiman is in the field of device management (title) and teaches wherein the plurality of different mobile operating systems comprise at least Android and iOS (iPhone and Android operating systems are used, pg. 10). It would have been obvious to one of ordinary skill in the art at the time of the invention to use the teachings of Naiman to incorporate the above teachings in the invention of Thomas. The motivation would have been to allow multiple different devices to use the system.

Claims 5, 11, 19 lack an inventive step under PCT Article 33(3) as being obvious over Thomas in view of Yaqub et al., hereinafter referred to as Yaqub.

Regarding claim 5, Thomas teaches the method of claim 1, wherein the at least one action is selectable from a plurality of actions (remedial action may take a plurality of forms, para. 0046), but lacks the teaching comprising warning a user of the at least one of the mobile devices that further action may be taken. Yaqub is in the field of network monitoring (abstract) and teaches comprising warning a user of the at least one of the mobile devices that further action may be taken (if a violation of QoS policy is found a warning will be sent, para. 0081). It would have been obvious to one of ordinary skill in the art at the time of the invention to use the teachings of Yaqub to incorporate the above teachings in the invention of Thomas. The motivation would have been to prevent unnecessary loss of access.

Regarding claims 11, 19 Thomas lacks the teaching warning a user of the mobile device that the device is out of compliance and subsequently causing the action to be performed if the attribute remains out of compliance after a period of time defined in the at least one rule. Yaqub is in the field of network monitoring (abstract) and teaches warning a user of the mobile device that the device is out of compliance and subsequently causing the action to be performed if the attribute remains out of compliance (if a violation of QoS policy is found a warning will be sent, if violation persists access is denied, para. 0081) but lacks the teaching after a period of time defined in the at least one rule. However, Yaqub teaches violation persisting after a warning is given. Furthermore defining a period of time before the causing the action would be a matter of design choice. Therefore it would have been obvious to incorporate the above features in the invention of Thomas. The motivation would have been to prevent access by stolen or otherwise unsecured devices.

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US2012/045252

Supplemental Box

In case the space in any of the preceding boxes is not sufficient.
Continuation of:

Claims 7, 12-13, 20 lack an inventive step under PCT Article 33(3) as being obvious over Thomas in view of Germano et al., hereinafter referred to as Germano.

Regarding claim 7, Thomas teaches the method of claim 1, but lacks the teaching further comprising the step of subsequently evaluating a second compliance state of at least one of the mobile devices to determine if the at least one action should be revoked. Germano is in the field of security control for mobile device networks (title, abstract) and teaches the step of subsequently evaluating a second compliance state of at least one of the mobile devices to determine if the at least one action should be revoked (once the mobile device is determined to be back in compliance [second compliance state] the limitations are removed [action is revoked], para. 0037). It would have been obvious to one of ordinary skill in the art at the time of the invention to use the teachings of Germano to incorporate the above teachings in the invention of Thomas. The motivation would have been to protect enterprise data from malicious access (Germano, para. 0016).

Regarding claims 12, 20 Thomas lacks teaching automatically revoking the action if the attribute is brought back into compliance. Germano teaches automatically revoking the action if the attribute is brought back into compliance (if user action brings mobile device back into compliance the limitations are removed, para. 0037). It would have been obvious to one of ordinary skill in the art at the time of the invention to use the teachings of Germano to incorporate the above teachings in the invention of Thomas. The motivation would have been to protect enterprise data from malicious access (Germano, para. 0016).

Regarding claim 13, modified Thomas teaches the method of claim 12, but lacks the teaching wherein the step of automatically revoking the action comprises determining if another of the plurality of rules is triggered. However, Thomas teaches monitoring for policy violations (para. 0047) and only providing access to resources if the device meets the policy requirements (para. 0024, 0043). Furthermore, Germano teaches automatically revoking the action comprises determining if another of the plurality of rules is triggered (access is limited until such a time as the security policies change, the mobile is synchronized and the enforcement agent is able to verify that device is in compliance [i.e. a new set of rules is triggered to remove the action of limiting access]). It would have been obvious to one of ordinary skill in the art at the time of the invention to use the teachings of Germano to incorporate the above teachings in the invention of Thomas. The motivation would have been to protect enterprise data from malicious access (Germano, para. 0016).

Claims 1-23 meet the criteria set out in PCT Article 33(4), and thus have industrial applicability because the subject matter claimed can be made or used in industry.

Electronic Acknowledgement Receipt

EFS ID:	16174941
Application Number:	13540142
International Application Number:	
Confirmation Number:	4198
Title of Invention:	RULES BASED ACTIONS FOR MOBILE DEVICE MANAGEMENT
First Named Inventor/Applicant Name:	Jatin MALIK
Customer Number:	86308
Filer:	Michael Kenneth Jones/Sara Harvell
Filer Authorized By:	Michael Kenneth Jones
Attorney Docket Number:	130839.02101
Receipt Date:	27-JUN-2013
Filing Date:	02-JUL-2012
Time Stamp:	16:40:06
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Form (SB08)	2101SIDS.pdf	65962 df1ad830a0707562811207ad7f71f8ad8cdd3a36	no	4
Warnings:					
Information:					

This is not an USPTO supplied IDS fillable form					
2	Other Reference-Patent/App/Search documents	2101ISR.pdf	456051 1cb8e4d4c9299b76b5c1e14a1650bb6524d4407e	no	8
Warnings:					
Information:					
			Total Files Size (in bytes):	522013	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/540,142	07/02/2012	Jatin MALIK	130839.02101	4198

86308 7590 12/19/2013

Pepper Hamilton LLP
400 Berywn Park
899 Cassatt Road
Berwyn, PA 19312-1183

EXAMINER	
KATSIKIS, KOSTAS J	
ART UNIT	PAPER NUMBER
2441	

MAIL DATE	DELIVERY MODE
12/19/2013	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No. 13/540,142	Applicant(s) MALIK ET AL.	
	Examiner KOSTAS KATSIKIS	Art Unit 2441	AIA (First Inventor to File) Status No

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTHS FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *2 July 2012*.

☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims*

5)☒ Claim(s) *1-23* is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6)☐ Claim(s) _____ is/are allowed.

7)☒ Claim(s) *1-23* is/are rejected.

8)☐ Claim(s) _____ is/are objected to.

9)☐ Claim(s) _____ are subject to restriction and/or election requirement.

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov.

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☒ The drawing(s) filed on *2 July, 2012* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

a)☐ All b)☐ Some** c)☐ None of the:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

** See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☒ Information Disclosure Statement(s) (PTO/SB/08a and/or PTO/SB/08b) Paper No(s)/Mail Date *05/20/2013, 06/27/2013*.

3) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

4) ☐ Other: _____.

DETAILED ACTION

1. This communication is in response to the Application filed on July 2, 2012, in which claims 1-23 have been presented for examination.

Status of Claims

2. Claims 1-23 are pending, of which Claims 1-2, 6, 9-10, 14, 16-18, 21 and 23 are rejected under 35 U.S.C. 102(b). Claims 3-5, 8, 11, 15, 19 and 22 are rejected under 35 U.S.C. 103. Claims 17-23 are also rejected under 35 U.S.C. 101.

Priority

3. Acknowledgement is made of Applicant's claim for the benefit of Provisional Application Serial No. 61/503,729, filed July 1, 2011.

Information Disclosure Statement

4. The information disclosure statements, filed May 20, 2013, and June 27, 2013, are in compliance with the provisions of 37 CFR 1.97, 1.98 and MPEP § 609. They have been placed in the application file, and the information referred to therein has been

considered as to the merits.

Claim Objections

5. Claims 8, 15 and 22 are objected to because of the following informalities: In each of claims 8, 15 and 22, use of the trademark ANDROID™ has been identified in the claims. Trademarks are not permissible in claim language. Appropriate correction is required.

Claim Rejections - 35 USC § 101

6. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

7. Claims 17-23 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

"A claim that covers both statutory and non-statutory embodiments (under the broadest reasonable interpretation of the claim when read in light of the specification and in view of one skilled in the art) embraces subject matter that is not eligible for patent protection and therefore is directed to non-statutory subject matter." See MPEP

2106(I) Ed. 8, Rev. 9, 2012

As per claim 17, it appears that claim 17 would reasonably be interpreted by one of ordinary skill in the art as a "system" of "software per se", failing to fall within a statutory category of invention. It is well known to those of ordinary skill in the art that data stores, can be implemented in software, (Oracle and SQL databases), and the computer readable instructions are clearly software instructions. Moreover, the server is not actually recited as being part of the claimed system. Thus, such a "system" alone (a claimed system comprising software units/applications alone) is not a machine, and it is clearly not a process, manufacture nor composition of matter. Therefore the claim is not limited to statutory subject matter and is therefore nonstatutory (Examiner respectfully suggests that the claim should be amended to avoid a rejection under 35 U.S.C. § 101 by adding the limitation "a CPU coupled to a memory" to the claim).

Dependent claims 18-23 fail to remedy the deficiencies of independent claim 17 and are therefore similarly rejected.

8. **Examiner's Note:** Examiner has cited particular paragraphs and/or columns and line numbers in the references applied to the claims above for the convenience of the applicant. Although the specified citations are representative of the teachings of the art and are applied to specific limitations within the individual claim, other passages and figures may apply as well. It is respectfully requested from the applicant in preparing responses, to fully consider the references in entirety as potentially teaching all or part

of the claimed invention, as well as the context of the passage as taught by the prior art or disclosed by the Examiner.

Claim Rejections - 35 USC § 102

9. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

10. Claims 1-2, 6, 9-10, 14, 16-18, 21 and 23 rejected under 35 U.S.C. 102(b) as being anticipated by Thomas et al. (United States Patent Application Publication No. US 2010/0242088 A1), hereinafter "Thomas".

Regarding claim 17, **Thomas** discloses a system for providing device management services comprising *(wherein **Thomas** discloses unified threat management facility 100)* **(Thomas, FIG. 1, paragraph [0023])**:

a data store configured to be accessible by a server *(wherein unified threat management facility 100 further includes network access rules facility 124, accessible via a server as discussed in paragraph [0084]-[0085])* **(Thomas, FIG. 1, paragraphs [0044]-[0045] and [0084]-[0085])**;

computer readable instructions for execution on the server comprising

instructions configured to *(wherein **Thomas** further discloses instructions)* **(Thomas, paragraph [0090])**:

make a determination that an attribute of a mobile device stored in the data store has changed *(wherein again, threat management facility executes a program or application to remediate against a threat or policy violation, and record interactions for subsequent evaluation)* **(Thomas, paragraphs [0046]-[0047])**;

evaluate the attribute, in response to the determination, to determine if it triggers at least one of a plurality of administrator defined rules *(wherein again, threat management is based on policy violation)* **(Thomas, paragraphs [0025] and [0043]-[0045])**, which indicates that the attribute is out of compliance *(wherein compliance is determined)* **(Thomas, paragraph [0017]-[0020], [0025] and [0046])**; and

automatically initiate an action defined by the at least one of a plurality of administrator defined rules if the attribute is out of compliance *(wherein again, remedial action facility 128 acts on policy violations)* **(Thomas, paragraph [0046])**, wherein the data store is configured to include substantially real-time data pertaining to a plurality of attributes of a plurality of mobile devices *(wherein threat management facility 100 performing increasingly automated and frequently testing)* **(Thomas, paragraphs [0025] and [0048])**, comprising devices having different mobile operating systems *(wherein security facility 152 may be an application loaded onto the computer platform or computer support component, where the application may accommodate the plurality of computer platforms)* **(Thomas, paragraph [0050])**.

Claim 10 includes a "method" claim that performs limitations substantially as described in "system" claim 17, and does not appear to contain any additional features with regard to novelty and/or inventive step; therefore, it is rejected under the same rationale.

Regarding claim 1, **Thomas** discloses a method for providing device management services comprising steps of:

gathering, from a network, status information related to each of a plurality of mobile devices, each mobile device utilizing one of a plurality of different mobile operating systems *(wherein **Thomas** discloses Internet correspondence (See FIG. 1), as well as security management facility 122 having the ability to scan the client facility 144 files for malicious code, remove or quarantine certain applications and files. See also FIG. 3, step 304, accessing security compliance info.)* **(Thomas, FIG. 1 and FIG. 3, paragraphs [0028] and [0058])**;

storing the status information in an electronic database accessible to a server *(wherein unified threat management facility 100 further includes network access rules facility 124, accessible via a server as discussed in paragraph [0084]-[0085])* **(Thomas, FIG. 1, paragraphs [0044]-[0045] and [0084]-[0085])**; evaluating a first compliance state of at least one of the mobile devices from the status information using a plurality of administrator-defined rules *(wherein again, threat management is based on policy violation)* **(Thomas, paragraphs [0025] and [0043]-[0045])**; and

initiating at least one action defined by the user-defined rules in response to the

step of evaluating, wherein the step of evaluation is performed by a server automatically, in response to changes in the status information *(wherein again, remedial action facility 128 acts on policy violations)* **(Thomas, paragraph [0046])**.

Regarding claim 2, **Thomas** discloses the method of claim 1, wherein the at least one action is selectable from a plurality of actions, comprising blocking access by the at least one of the mobile devices to a corporate resource *(wherein again, Thomas discloses blocking access)* **(Thomas, paragraphs [0046] and [0064])**.

Regarding claim 21, **Thomas** discloses the system of claim 17, wherein the computer readable instructions further comprise instructions configured to gather the plurality of attributes for at least one of the plurality of mobile device by gathering attribute information from that mobile device and at least one other source on a network *(wherein again, security management facility scans client's files 144, clients are mobile, and security compliance information is derived from security policy to compare scanned files (See FIG. 3, item 304))* **(Thomas, FIG. 3, paragraphs [0028], [0058] and [0074])**.

Claims 6 and 14 includes a “method” claims that perform limitations substantially as described in “system” claim 21, and do not appear to contain any additional features with regard to novelty and/or inventive step; therefore, they are rejected under the same rationale.

Regarding claim 23, **Thomas** discloses the system of claim 17, wherein the attribute comprises location information about the mobile device *(wherein user location is monitored)* **(Thomas, paragraphs [0043] and [0047])**.

Claims 9 and 16 include "method" claims that perform limitations substantially as described in "system" claim 21, and do not appear to contain any additional features with regard to novelty and/or inventive step; therefore, they are rejected under the same rationale.

Regarding claim 18, **Thomas** discloses the system of claim 17, wherein the computer readable instructions further comprise instructions configured to present a user interface to an administrator to allow selection of at least one attribute and one available action to define the at least one of the plurality of administrator defined rules *(wherein **Thomas** discloses a web portal accessible by an administrator as a user interface)* **(Thomas, paragraph [0053])**.

Claim Rejections - 35 USC § 103

11. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made

> to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

12. This application currently names joint inventors. In considering patentability of the claims under pre-AIA 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of pre-AIA 35 U.S.C. 103(c) and potential pre-AIA 35 U.S.C. 102(e), (f) or (g) prior art under pre-AIA 35 U.S.C. 103(a).

13. Claims 3 are rejected under 35 U.S.C. 103(a) as being unpatentable over Thomas in view of Moghaddam et al. (United States Patent Application Publication No. US 2008/0114862 A1), hereinafter "Moghaddam".

Regarding claim 3, **Thomas** discloses the method of claim 1, but does not expressly disclose wherein the at least one action is selectable from a plurality of actions, comprising blocking e-mail access for the at least one of the mobile devices.

However **Moghaddam** discloses at least one action is selectable from a plurality of actions, comprising blocking e-mail access for the at least one of the mobile devices *(wherein **Moghaddam** discloses restricting email)* **(Moghaddam, paragraph [0045])**.

Thomas and **Moghaddam** are analogous art because they are from the same

problem solving area, namely, systems and methods for configuring and using the mobile usage data and filtering and blocking access/content.

At the time of the invention, it would have been obvious to one of ordinary skill in the art, having the teachings of **Thomas** and **Moghaddam** before him or her, to modify the security system of **Thomas**, to include email restriction of **Moghaddam**, with reasonable expectation that this would result in a system that enabled users to customize their mobile devices such that usage restrictions were configurable **(Moghaddam, paragraph [0012])**. This approach to improving the computer security system of **Thomas** was well within the ordinary ability of one of ordinary skill in the art based on the teachings of **Moghaddam**.

Therefore, it would have been obvious to one of ordinary skill in the art to combine the teachings of **Thomas** with **Moghaddam** to obtain the invention as specified in claim 3.

14. Claims 4, 8, 15 and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Thomas in view of Naiman et al. (WIPO Patent Application Publication No. 2011022053), hereinafter "Naiman".

Regarding claim 4, **Thomas** discloses the method of claim 1, but does not expressly disclose wherein the at least one action is selectable from a plurality of actions, comprising wiping information from the at least one of the mobile devices.

However **Naiman** discloses that at least one action is selectable from a plurality

of actions, comprising wiping information from the at least one of the mobile devices *(wherein **Naiman** teaches a control policy to wipe files)* **(Naiman, page 11, paragraph 2)**.

Thomas and **Naiman** are analogous art because they are from the same problem solving area, namely, systems and methods of mobile device management.

At the time of the invention, it would have been obvious to one of ordinary skill in the art, having the teachings of **Thomas** and **Naiman** before him or her, to modify the security system of **Thomas**, to include the email restrictions of **Naiman**, with reasonable expectation that this would result in a system that prevented jail breaking and hacking and improved security **(Naiman, page 5, paragraph 2)**. This approach to improving the computer security system of **Thomas** was well within the ordinary ability of one of ordinary skill in the art based on the teachings of **Naiman**.

Therefore, it would have been obvious to one of ordinary skill in the art to combine the teachings of **Thomas** with **Naiman** to obtain the invention as specified in claim 4.

Regarding claim 22, **Thomas** discloses the system of claim 17, but does not expressly disclose wherein the plurality of different mobile operating systems comprise at least Android and iOS.

However **Naiman** discloses a plurality of different mobile operating systems comprise at least Android and iOS *(wherein Naiman discloses iPhone and ADROID™ operating systems)* **(Naiman, page 10)**.

Thomas and **Naiman** are analogous art because they are from the same problem solving area, namely, systems and methods of mobile device management.

At the time of the invention, it would have been obvious to one of ordinary skill in the art, having the teachings of **Thomas** and **Naiman** before him or her, to modify the security system of **Thomas**, to include the additional mobile operating systems of **Naiman**, with reasonable expectation that this would result in increased versatility and providing greater marketability to service providers that used various operating systems **(Naiman, page 5, paragraph 2)**. This approach to improving the computer security system of **Thomas** was well within the ordinary ability of one of ordinary skill in the art based on the teachings of **Naiman**.

Therefore, it would have been obvious to one of ordinary skill in the art to combine the teachings of **Thomas** with **Naiman** to obtain the invention as specified in claim 22.

Claims 8 and 15 include “method” claims that perform limitations substantially as described in “system” claim 21, and do not appear to contain any additional features with regard to novelty and/or inventive step; therefore, they are rejected under the same rationale.

15. Claims 5, 11 and 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Thomas in view of Yaqub et al. (United States Patent

Application Publication No. US 2007/0206552 A1), hereinafter "Yaqub".

Regarding claim 5, **Thomas** discloses the method of claim 1, wherein the at least one action is selectable from a plurality of actions *(wherein remedial action may take a plurality of forms)* **(Thomas, paragraph [0046])**, but does not explicitly disclose comprising warning a user of the at least one of the mobile devices that further action may be taken.

However **Yaqub** discloses that at least one action is selectable from a plurality of actions, comprising warning a user of the at least one of the mobile devices that further action may be taken *(wherein **Yaqub** teaches warning a user if QoS violations have occurred)* **(Yaqub, paragraph [0081])**.

Thomas and **Yaqub** are analogous art because they are from the same problem solving area, namely, systems and methods of mobile device management.

At the time of the invention, it would have been obvious to one of ordinary skill in the art, having the teachings of **Thomas** and **Yaqub** before him or her, to modify the security system of **Thomas**, to include the email restrictions of **Yaqub**, with reasonable expectation that this would result in improved quality of service. This approach to improving the computer security system of **Thomas** was well within the ordinary ability of one of ordinary skill in the art based on the teachings of **Yaqub**.

Therefore, it would have been obvious to one of ordinary skill in the art to combine the teachings of **Thomas** with **Yaqub** to obtain the invention as specified in

claim 5.

Regarding claim 19, **Thomas** discloses the system of claim 18, wherein at least one of the actions comprises warning a user of the mobile device that the device is out of compliance and causing subsequent action to be performed if the attribute remains out of compliance *(wherein again, the QoS warning. Furthermore, **Yaqub** discloses that if violation persists, access is denied)* **(Yaqub, paragraph [0081])**. **Yaqub** does not expressly disclose causing subsequent action to be performed if the attribute remains out of compliance after a period of time defined in the at least one rule.

However it would be an obvious matter of design choice to modify **Thomas-Yaqub** to include causing subsequent action to be performed if the attribute remains out of compliance after a period of time defined in the at least one rule, in order to prevent unauthorized access from unsecured devices (please note, in the instant Application, paragraphs [0066]-[0067] and [0080]-[0081], Applicants have not given any stated advantage for the claimed limitation).

Claim 11 includes a “method” claim that performs limitations substantially as described in “system” claim 19, and does not appear to contain any additional features with regard to novelty and/or inventive step; therefore, it is rejected under the same rationale.

16. Claims 7, 12-13 and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Thomas in view of Germano et al. (United States Patent Application Publication No. US 2007/0266422 A1), hereinafter "Germano".

Regarding claim 7, **Thomas** discloses the method of claim 1, but does not expressly disclose further comprising the step of subsequently evaluating a second compliance state of at least one of the mobile devices to determine if the at least one action should be revoked.

However **Germano** discloses a step of subsequently evaluating a second compliance state of at least one of the mobile devices to determine if the at least one action should be revoked *(wherein **Germano** discloses that mobile device enforcement agent will continue to limit access to network resources to those identified within the limited access security policy, until such a time as either: (a) the security policies change, the changed policies are synchronized with the mobile device, and the enforcement agent is able to verify that the mobile device is in compliance with the security policy set applicable to that mobile device; or (b) the mobile device comes into compliance via user action or via the implementation of self-corrective measures, such as automated restoration of deleted files or other configuration changes)* **(Germano, paragraph [0037])**.

Thomas and **Germano** are analogous art because they are from the same problem solving area, namely, systems and methods of mobile device security.

At the time of the invention, it would have been obvious to one of ordinary skill in

the art, having the teachings of **Thomas** and **Germano** before him or her, to modify the security system of **Thomas**, to continue to limit access until compliance is restored, such as disclosed in **Germano**, with reasonable expectation that this would result in protecting enterprise data from malicious attacks **(Germano, paragraph [0016])**. This approach to improving the computer security system of **Thomas** was well within the ordinary ability of one of ordinary skill in the art based on the teachings of **Germano**.

Therefore, it would have been obvious to one of ordinary skill in the art to combine the teachings of **Thomas** with **Germano** to obtain the invention as specified in claim 7.

Regarding claim 20, **Thomas-Germano** discloses the system of claim 17, wherein the computer readable instructions further comprise instructions configured to automatically revoke the action if the attribute is brought back into compliance *(wherein again, the mobile device enforcement agent will continue to limit access to network resources to those identified within the limited access security policy, until such a time as either: (a) the security policies change, the changed policies are synchronized with the mobile device, and the enforcement agent is able to verify that the mobile device is in compliance with the security policy set applicable to that mobile device; or (b) the mobile device comes into compliance via user action or via the implementation of self-corrective measures, such as automated restoration of deleted files or other configuration changes)* **(Germano, paragraph [0037])**. The motivation regarding the

obviousness of claim 7 is also applied to claim 20.

Claim 12 includes a "method" claim that performs limitations substantially as described in "system" claim 20, and does not appear to contain any additional features with regard to novelty and/or inventive step; therefore, it is rejected under the same rationale.

Regarding claim 13, **Thomas-Germano** discloses the method of claim 12, wherein the step of automatically revoking the action comprises determining if another of the plurality of rules is triggered *(wherein again, until such a time as the security policies change, the changed policies are synchronized with the mobile device, and the enforcement agent is able to verify that the mobile device is in compliance with the security policy set applicable to that mobile device)* **(Germano, paragraph [0037])**. The motivation regarding the obviousness of claim 7 is also applied to claim 13.

Conclusion

17. Further references of interest are cited on Form PTO-892, which is an attachment to this Office Action.

18. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kostas Katsikis whose telephone number is (571)270-

5434. The examiner can normally be reached on Monday - Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Wing Chan can be reached on (571)272-7493. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Kostas Katsikis/
Examiner
Art Unit 2441

December 16, 2013

Notice of References Cited	Application/Control No. 13/540,142	Applicant(s)/Patent Under Reexamination MALIK ET AL.	
	Examiner KOSTAS KATSIKIS	Art Unit 2441	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-2006/0217111 A1	09-2006	Marolia et al.	455/418
*	B	US-2009/0131020 A1	05-2009	van de Groenendaal, Joannes G.	455/411
*	C	US-2010/0048167 A1	02-2010	Chow et al.	455/410
*	D	US-2012/0151041 A1	06-2012	Gerber et al.	709/224
	E	US-			
	F	US-			
	G	US-			
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N	WO 2008110215 A1	09-2008	World Intellect	GYOERGY et al.	
	O	WO 2010129939 A1	11-2010	World Intellect	GUBA et al.	
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Petitioner Ex 1002, p. 185
Zimperium v. Taasera, IPR2024-00007

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
11 November 2010 (11.11.2010)

PCT

(10) International Publication Number
WO 2010/129939 A1

(51) International Patent Classification:
H04M 3/42 (2006.01)

(21) International Application Number:
PCT/US2010/034151

(22) International Filing Date:
8 May 2010 (08.05.2010)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

61/176,640	8 May 2009 (08.05.2009)	US
61/247,334	30 September 2009 (30.09.2009)	US
61/301,902	5 February 2010 (05.02.2010)	US

(71) Applicant *(for all designated States except US)*: **OBD-EDGE, LLC** [US/US]; 7117 Florida Boulevard, Baton Rouge, LA 70806 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **GUBA, Robert, William** [US/US]; 1231 South Columbine Street, Baton Rouge, LA 70808 (US). **POWERS, Donald, L.** [US/US]; 9565 Jefferson Highway, Baton Rouge, LA 70809 (US). **BROWN, Sean** [US/US]; 1020 Chestnut Haven Court, Curtis Bay, MD 21226 (US).

(74) Agent: **TODD, Jack, D.**; Seyfarth Shaw LLP, 1075 Peachtree Street, N.E., Suite 2500, Atlanta, GA 30309 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH,

[Continued on next page]

(54) Title: SYSTEMS, METHODS, AND DEVICES FOR POLICY-BASED CONTROL AND MONITORING OF USE OF MOBILE DEVICES BY VEHICLE OPERATORS

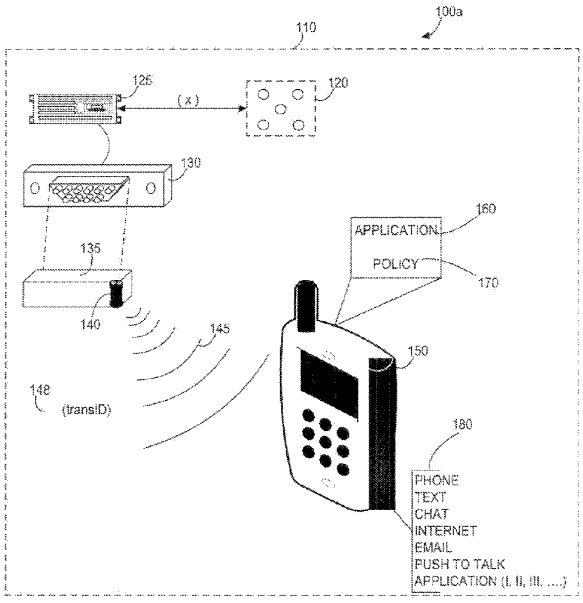


FIG. 1A

(57) Abstract: Systems, methods, and devices for controlling and limiting use of functions (180), such as calling, texting, chatting, emailing, Internet surfing, and similar applications, on a mobile device (150) when the mobile device (150) is in a moving vehicle (110), includes use of an on- board computer (125) installed within the vehicle (110), a transmitter (140) in electronic communication with the on-board computer (125) that periodically transmits speed data (148) of the vehicle to a receiver installed on the mobile device (150), wherein the mobile device includes suitable software (160) and a rules-based policy (170) that define and control when and which functions of the mobile device are disabled or interrupted by the software when the vehicle is in motion above a minimum threshold speed. Policies (170) are set by default but may be customized for particular individuals, devices, or circumstances. Policies may also be customized for particular groups or subgroups of employees or contractors for company or legal compliance to reduce distracted driving.

WO 2010/129939 A1

GM, KE, LR, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

— *of inventorship (Rule 4.17(iv))*

Published:

— *with international search report (Art. 21(3))*

SYSTEMS, METHODS, AND DEVICES FOR POLICY-BASED CONTROL AND MONITORING OF USE OF MOBILE DEVICES BY VEHICLE OPERATORS

Cross Reference to Related Applications

This application claims the benefit under 35 U.S.C. § 119(e) of U.S. Provisional Patent Application No. 61/176,640, entitled "System for Policy-Based Mobile Communications in Vehicles," filed May 8, 2009, and U.S. Provisional Patent Application No. 61/247,334, entitled "Improved System for Policy-Based Mobile Communications in Vehicles," filed October 13, 2009, and U.S. Provisional Patent Application No. 61/301,902, entitled "Further Improved System for Policy-Based Mobile Communications in Vehicles," filed February 22, 2010, all three of which are incorporated herein by reference, in their entirety. This application is also related to and incorporates herein by reference and in its entirety, U.S. Nonprovisional Patent Application No., which is filed contemporaneously herewith.

Field of the Present Inventions

The systems, methods, and devices described herein relate generally to use of mobile computing and communication devices in vehicles, and, more particularly, to systems, methods, and devices that use data provided by or obtained from the vehicle in conjunction with policy-based protocols or rules for selectively controlling, limiting, managing, monitoring, and auditing use and communications to and from such mobile devices while in the vehicle and for detecting, monitoring, and reporting on other vehicle usage using the mobile device.

Background of the Present Invention

Use of mobile computing and communication devices in vehicles is a hotly debated topic. While such use provides convenience and potentially enhances worker productivity, it has also been shown that such use has a detrimental effect and impact on the driver/operator's (hereinafter referred to, for convenience, as the "driver") ability to focus on driving or otherwise operating the vehicle - with some studies indicating that distracted driving may be even more dangerous than driving while intoxicated or under the influence of drugs. Numerous accidents by drivers of automobiles, trucks, motorcycles, buses, planes, helicopters, blimps, balloons,

Petitioner Ex 1002, p. 188
Zimperium v. Taasera, IPR2024-00007

gliders, boats, ferries, trains, trams, heavy equipment or machinery, and similar devices or machines (collectively and hereinafter referred to as "a vehicle" or "vehicles" for convenience) have been attributed to driver inattentiveness or distraction while talking, texting, surfing, browsing, or otherwise interacting with or using a mobile computing or communication device rather than focusing full attention on driving or operating the vehicle. The term "vehicle" is further intended to include any type of device or machine that is driven, operated, or controlled by a user (i.e., driver) and that is susceptible to accident or injury to self or others if the driver is careless or not paying full attention to operation of the vehicle.

Numerous cities, counties, states, and even the Federal government have imposed or are considering imposing legal restrictions on use of (or that imposed increased sanctions for accidents that occur due to use of) such mobile devices by a driver of a vehicle. As the functionality of such mobile computing and communication devices continues to increase and expand, the potential distractions posed by such mobile devices on vehicle drivers is likely to increase even more — leading to further accidents, higher risks to drivers, passengers, and any third parties near such vehicles, higher insurance rates, and more litigation.

As used herein, "mobile devices" are intended to include and encompass any type of hand-held or mobile device or other computing or communication device usable within a vehicle, such as but not limited to cell phones, smart phones, push-to-talk devices, PDAs, text or email dedicated devices, general computers, laptops, electronic reading devices, multimedia equipment, data tablets, and similar computing or communication device that would or could be used by or accessible to the driver of a vehicle while it is moving or otherwise in operation.

Although laws may be passed, company policies may be adopted, and insurance policies may be tailored to provide lower insurance rates for drivers who do not use their mobile device while operating a vehicle or to provide less or no coverage for drivers who are involved in accidents because of distraction from confirmed use of such a mobile device during an accident, the options and ability for physically or technologically controlling, managing, limiting, monitoring, and auditing use of and communications to and from such mobile devices, particularly in real time and based on other factors and variables (such as whether the vehicle is on and/or moving, how fast it is moving, what time of day it is, what day of the week it is, where the vehicle is located, and the like) has been limited, to date.

Petitioner Ex 1002, p. 189
Zimperium v. Taasera, IPR2024-00007

For all of these reasons, there are needs in the industry for systems, methods, and devices, that use computer-implemented, configurable policies to control, manage, limit, monitor, and/or audit use of and communications to and from mobile devices used in or by drivers of vehicles. Advantageously, data provided by or obtained from the vehicle, such as from a vehicle's on board computer or similar vehicle components or systems, alone or in conjunction with other available external data or information (such as GPS location data, time of day, day of week, type of activity or communication attempted on the mobile device, and the like) is usable to enable a default or configurable, policy-based software application, preferably installed on or interactive with such mobile devices, which defines rules and protocols selectively to control or limit use of the functionality of such mobile devices. Such systems can also be used advantageously to monitor, audit, and record use of mobile devices in vehicles, even if actual use is not limited, controlled, or prevented by the system or policy. In addition, such systems can be configured to capture relevant data and information about the vehicle when the mobile device is in or in close proximity to the vehicle – even if use of the mobile device is not limited, controlled, or prevented by the system or the policy. Further, such technology can be used advantageously to detect, monitor, and report on vehicle usage patterns, including period of excessive speeding or idle time.

There are needs for such controls and limits not only in consumer markets (e.g., for parents who want to limit or control use of a mobile device by their teen driver while the teen driver is driving the family car) but also in commercial or governmental applications (e.g., a company with a fleet of delivery trucks may need to ensure (for insurance, company policy, political, court settlement, or public relations reasons) that all of their designated employees are not engaged in personal calls, texting, surfing, or use of non-business software application while driving a company vehicle during work hours; or a municipality, county, state, or government agency may need to prevent their conductors or drivers from similar personal activities on mobile devices while operating a commuter train, tram, bus, or other public vehicle while they are on the job.

The above needs and features, as well as additional aspects and business applications, are disclosed herein and will become readily apparent to one of ordinary skill in the art after reading and studying the following summary of the present inventions, the detailed description of preferred embodiments, and the claims included hereinafter.

Petitioner Ex 1002, p. 190
Zimperium v. Taasera, IPR2024-00007

Summary of the Present Invention

The present invention relates generally to use of mobile computing and communication devices in vehicles, and, more particularly, to systems, methods, and devices that use data provided by or obtained from the vehicle in conjunction with policy-based protocols or rules for selectively controlling, limiting, managing, monitoring, and auditing use and communications to and from such mobile devices while in the vehicle and for detecting, monitoring, and reporting on other vehicle usage by means of the mobile device.

Briefly described, aspects of the present invention include the following.

In a first aspect, a system for controlling use of functions on a mobile device when the mobile device is in a vehicle, comprises a vehicular on-board computer installed within the vehicle and configured to obtain speed data from the vehicle, a transmitter in electronic communication with the on-board computer and configured to transmit an indication of the speed data on a periodic basis, a receiver installed on the mobile device adapted to receive the indication of speed data transmissions from the transmitter, a software application installed on the mobile device, wherein the software application runs in memory resident on the mobile device whenever the mobile device is powered on and wherein the software application receives the indication of speed data from the receiver, the software application including a policy associated therewith that defines when and which functions of the mobile device are disabled by the software application in response to the indication of speed data transmission, whereby, in response to receipt of the indication of speed transmission data, if the vehicle speed exceeds a minimum threshold speed level, the software application disables the functions of the mobile device in accordance with the policy associated therewith.

In a feature, the vehicular on-board computer obtains the speed data from the vehicle continuously or on a periodic or predefined basis.

In another feature, the functions of the mobile device remain disabled for a predetermined period of time after the indication of speed transmission data indicates that the vehicle speed exceeds the minimum threshold speed level. Preferably, this predetermined period of time in which the functions of the mobile device remain disabled is set by default or may be modified by a customized policy.

Petitioner Ex 1002, p. 191
Zimperium v. Taasera, IPR2024-00007

In yet a further feature, the functions of the mobile device are enabled after the indication of speed transmission data indicates that the vehicle speed has been below the minimum threshold speed level for a predetermined period of time. Again, the predetermined period of time in which the indication of speed transmission data indicates that the vehicle speed has been below the minimum threshold speed is set by default or may be modified by a customized policy.

In further features, the transmitter transmits the indication of the speed data continuously or on a periodic basis.

As used herein, a vehicle may include an automobile, truck, motorcycle, bus, aircraft, watercraft, plane, helicopter, blimp, hot air balloon, glider, boat, ferry, train, tram, heavy equipment or machinery, or any similar devices operated by a person.

As also used herein, a mobile device includes a cell phone, smart phone, push-to-talk device, PDA, text or email dedicated device, general computer, laptop, electronic reading device, multimedia equipment, data tablet, or any similar computing or communication device - each having a display or interface that is usable by or accessible to a driver of the vehicle.

Functions of a mobile device that may be blocked or interrupted include one or more of: making an outgoing call, receiving an incoming call, sending or receiving a text message, text chatting, push-to-talk, sending or receiving an email, Internet browsing, and launching of an application installed on the mobile device.

Preferably, speed includes relative speed of the vehicle whether the vehicle is moving in the forward or reverse direction.

In one embodiment, the transmitter is built into and integrated with the on-board computer. In another embodiment, the transmitter is included in an on-board diagnostic (OBD) device that plugs into the OBD port of the vehicle, wherein the OBD port is in electronic communication with the on-board computer. The OBD device preferably receives power from the vehicle through the OBD port, directly from a wired connection with the battery of the vehicle, and/or independently from the power supply of the vehicle.

Preferably, the OBD device transmits to the mobile device an indication that the OBD device has lost power whenever it has been unplugged from the OBD port or an indication that the OBD device has lost power whenever there has been a power interruption to the OBD device.

Petitioner Ex 1002, p. 192
Zimperium v. Taasera, IPR2024-00007

In another feature, the transmitter and receiver communicate through a wireless communication protocol. Such wireless communication protocol include an RF communication protocol, a WiFi or Zigby communication protocol, or a Bluetooth communication protocol. In one embodiment, the transmitter and receiver are paired using the Bluetooth protocol. In another embodiment, the transmitter broadcasts speed data without pairing with the receiver. In such embodiment, numerous mobile devices are able to receive the transmitter broadcast because there is no specific Bluetooth pairing.

In yet a further feature, the receiver searches for the electronic communication from the transmitter on a periodic basis.

In a further feature, the transmitter and receiver communicate through a wired connection between a data port of the vehicle and a data port of the mobile device.

In another feature, the indication of the speed data includes the actual speed of the vehicle. Preferably, the policy defines the speed of the threshold speed level

In another feature, the indication of the speed data includes a flag indicating that the speed of the vehicle is currently above the threshold speed level. Alternatively, the indication of the speed data includes the actual speed of the vehicle and the policy defines the threshold speed level.

In another feature, the transmitter only transmits the indication of the speed data when the vehicle is on.

In various features, the policy prevents outgoing calls from the mobile device, prevents the mobile device from accessing the phone functions on the mobile device, disables the display screen of the mobile device, causes the software application to display a system screen on the display screen of the mobile device when the vehicle speed exceeds the minimum threshold speed level, immediately interrupts and disables the functions of the mobile device when the vehicle speed exceeds the minimum threshold speed level, is associated with the vehicle, is associated with the mobile device, is only effective during predefined days of the week and hours of the day, has a plurality of rules that vary as a function of predefined days of the week and hours of the day, includes a plurality of rules that vary based upon the GPS-determined location of the mobile device, defines a PIN or password that can be entered into the mobile device to enable all functions of the mobile device even if the vehicle is in motion, defines a PIN or password that can be entered into the mobile device to enable predefined functions of the mobile

Petitioner Ex 1002, p. 193
Zimperium v. Taasera, IPR2024-00007

device even if the vehicle is in motion, prevents incoming calls from being received by the mobile device, allows incoming calls to be received by the mobile device, but prevents any indication of the incoming call from being detected by or notified to a user of the mobile device until a later period of time, routes incoming calls directly to voice mail, prevents incoming and outgoing text messages, disables the mobile device completely, identifies specific numbers or contacts from which the mobile device can receive communications on an incoming basis even when the vehicle is in motion, identifies specific numbers or contacts to which the mobile device is permitted to communicate on an outgoing basis even when the vehicle is in motion, and identifies specific applications that are usable and launchable by the mobile device even when the vehicle is in motion.

In another feature, the software application has a default policy that is associated with the software application when the software application is installed on the mobile device. Alternatively, the policy is customizable by an account administrator and may be distributed to a plurality of mobile devices, distributed to all employees of an organization, distributed to a subset of employees of an organization. Such organization may include a company or a governmental entity.

In one embodiment, the account administrator is an adult and the user of the mobile device is a dependent of the adult.

In another feature, insurance costs are reduced for an owner of the vehicle if the vehicle has the transmitter installed therein and if the software application is installed on the mobile device of one or more drivers of the vehicle.

In another feature, the mobile device first queries the transmitter to obtain a device name for the transmitter, after which the indication of speed data transmissions from the transmitter are receivable by the receiver of the mobile device.

In yet another feature, the transmitter is configured to transmit and the receiver is configured to receive additional data obtained from the on-board computer. Such additional data includes an indication of whether the vehicle is turned on or off, includes an indication of what gear the vehicle is in, includes a device name for the transmitter. In some embodiments, the indication of speed data is included as a variable in the device name transmitted by the transmitter.

Petitioner Ex 1002, p. 194
Zimperium v. Taasera, IPR2024-00007

In yet another feature, the policy is updated on the mobile device by means of a text message sent to the mobile device, or when the mobile device is connected to the Internet, or when the mobile device is synched with software installed on a computer of the user of the mobile device.

In another aspect, a computer program residing in computer-readable memory on a mobile device, wherein the mobile device includes a receiver, and further includes conventional firmware and hardware that enables the mobile device to engage in electronic communications and to perform other functions, the computer program comprises instructions that, when processed on a computer within the mobile device, causes the computer to (i) whenever the mobile device is powered on, launch the computer program and maintain the computer program as an application running in the background of the mobile device, (ii) periodically check, using the receiver, for a data signal transmission containing a transmitter identifier and an indication of speed data from a vehicle in proximity to the mobile device, (iii) store a policy within memory on the mobile device, wherein the policy defines when and which functions of the mobile device will be disabled based on the indication of speed data obtained from the data signal transmission, (iv) if an approved transmitter is identified by the transmitter identifier, extract and store the indication of speed data in memory on the mobile device, and (v) if the speed data indicates that the vehicle has exceeded a minimum threshold speed level, disabling selected functions of the mobile device according to the stored policy.

In a feature, the approved transmitter is in electronic communication with an on-board computer of the vehicle.

In another feature, the receiver checks for the data signal transmission on a first periodic basis until a first transmission is received and, thereafter, checks on a second, more frequent periodic basis thereafter. Preferably, the receiver resumes checking for the data signal transmission on the first periodic basis after a predetermined period of time in which no data signal transmissions are received from the vehicle.

In another feature, the functions of the mobile device remain disabled for a predetermined period of time after the indication of speed transmission data indicates that the vehicle speed exceeds the minimum threshold speed level. Preferably, the predetermined period of time in which the functions of the mobile device remain disabled is set according to the policy.

Petitioner Ex 1002, p. 195
Zimperium v. Taasera, IPR2024-00007

In yet a further feature, the functions of the mobile device are enabled after the indication of speed transmission data indicates that the vehicle speed has been below the minimum threshold speed level for a predetermined period of time. Preferably, the predetermined period of time in which the indication of speed transmission data indicates that the vehicle speed has been below the minimum threshold speed is set according to the policy.

In a feature, the functions of the mobile device are enabled after there are no data signal transmissions received by the receiver for a predetermined period of time.

In another feature, the mobile device includes one of a cell phone, smart phone, push-to-talk device, PDA, text or email dedicated device, general computer, laptop, electronic reading device, multimedia equipment, data tablet, and similar computing or communication device each having a display or interface that is usable by or accessible to a driver of the vehicle.

Preferably, functions on the mobile device include one or more of: making an outgoing call, receiving an incoming call, push-to-talk, sending or receiving a text message, text chatting, sending or receiving an email, Internet browsing, and launching of a specified application installed on the mobile device.

In another feature, the indication of speed data identifies relative speed of the vehicle whether the vehicle is moving in the forward or reverse direction.

Preferably, the data transmission signal is configured to include an indication that the transmitter has been disabled and/or an indication that the transmitter has experienced a power interruption.

In another feature, the transmitter and receiver communicate through a wireless communication protocol. Such wireless communication protocol include an RF communication protocol, a WiFi or Zigby communication protocol, or a Bluetooth communication protocol. In one embodiment, the transmitter and receiver are paired using the Bluetooth protocol. In another embodiment, the transmitter broadcasts speed data without pairing with the receiver. In such embodiment, numerous mobile devices are able to receive the transmitter broadcast because there is no specific Bluetooth pairing.

In another feature, the transmitter and receiver communicate through a wired connection between a data port of the vehicle and a data port of the mobile device.

In yet a further feature, the indication of the speed data includes the actual speed of the vehicle and, preferably, the policy defines the threshold speed level

Petitioner Ex 1002, p. 196
Zimperium v. Taasera, IPR2024-00007

In a feature, the indication of the speed data includes a flag indicating that the speed of the vehicle is currently above the threshold speed level. Alternatively, the indication of the speed data includes the actual speed of the vehicle and the policy defines the threshold speed level.

In various features, the policy prevents outgoing calls from the mobile device, prevents the mobile device from accessing the phone functions on the mobile device, disables the display screen of the mobile device, causes the software application to display a system screen on the display screen of the mobile device when the vehicle speed exceeds the minimum threshold speed level, immediately interrupts and disables the functions of the mobile device when the vehicle speed exceeds the minimum threshold speed level, is associated with the vehicle, is associated with the mobile device, is only effective during predefined days of the week and hours of the day, has a plurality of rules that vary as a function of predefined days of the week and hours of the day, includes a plurality of rules that vary based upon the GPS-determined location of the mobile device, defines a PIN or password that can be entered into the mobile device to enable all functions of the mobile device even if the vehicle is in motion, defines a PIN or password that can be entered into the mobile device to enable predefined functions of the mobile device even if the vehicle is in motion, prevents incoming calls from being received by the mobile device, allows incoming calls to be received by the mobile device, but prevents any indication of the incoming call from being detected by or notified to a user of the mobile device until a later period of time, routes incoming calls directly to voice mail, prevents incoming and outgoing text messages, disables the mobile device completely, identifies specific numbers or contacts from which the mobile device can receive communications on an incoming basis even when the vehicle is in motion, identifies specific numbers or contacts to which the mobile device is permitted to communicate on an outgoing basis even when the vehicle is in motion, and identifies specific applications that are usable and launchable by the mobile device even when the vehicle is in motion.

In another feature, the policy stored within memory on the mobile device is a default policy that is installed when the computer program is installed on the mobile device. Additionally or alternatively, the policy is customizable by an account administrator and may be distributed to a plurality of mobile devices, distributed to all employees of an organization,

Petitioner Ex 1002, p. 197
Zimperium v. Taasera, IPR2024-00007

distributed to a subset of employees of an organization. Preferably, the organization is a company or a governmental entity.

In yet a further feature, the account administrator is an adult and the user of the mobile device is a dependent of the adult.

Preferably, insurance costs are reduced for an owner of the vehicle if the vehicle has the transmitter installed therein and if the computer program is installed on the mobile device of one or more drivers of the vehicle.

In another feature, the computer program first queries the transmitter to obtain the transmitter identifier, after which the indication of speed data transmissions from the transmitter are receivable by the receiver of the mobile device.

In yet a further feature, the transmitter is configured to transmit and the receiver is configured to receive additional data obtained from the on-board computer. Such additional data may include an indication of whether the vehicle is turned on or off, an indication of what gear the vehicle is in, and/or a device name for the transmitter. Preferably, the indication of speed data is included as a variable in the device name transmitted by the transmitter.

In another feature, the policy is updated on the mobile device by means of a text message sent to the mobile device, when the mobile device is connected to the Internet, and/or when the mobile device is synched with software installed on a computer of the user of the mobile device.

The present invention also encompasses computer-readable medium having computer-executable instructions for performing methods of the present invention, and computer networks and other systems that implement the methods of the present invention. The present invention also may include one or more computer programs residing on computer-readable media or in computer-readable memory wherein the program(s) include computer-executable instructions that, when processed by the computer, cause the computer to performs selected steps and elements of methods described herein.

The above features as well as additional features and aspects of the present invention are disclosed herein and will become apparent from the following description of preferred embodiments of the present invention.

Petitioner Ex 1002, p. 198
Zimperium v. Taasera, IPR2024-00007

Brief Description of the Drawings

Further features and benefits of the present invention will be apparent from a detailed description of preferred embodiments thereof taken in conjunction with the following drawings, wherein similar elements are referred to with similar reference numbers, and wherein:

FIG. 1A is a system view of one embodiment of the present invention;

FIG. 1B is a system view of another embodiment of the present invention;

FIG. 2 is a high level overview of implementation of the system;

FIG. 3 is a flowchart of the processes for implementing policies of the present invention;

FIGS. 4-12 are flowcharts of various processes used by system software of the present invention; and

FIGS. 13-32 illustrate various screen shots from an Internet management console used within the systems described herein.

Detailed Description of Preferred Embodiments

Preferably, the exemplary systems, devices, and methods described herein are designed to improve upon the safe operation of a vehicle by a driver who has a mobile device, by limiting, controlling, managing, or preventing use of some or all functionality of the mobile device while the vehicle is in operation by the driver and/or in motion above a threshold speed, whether in reverse or forward direction. Preferably, a default or configurable policy, rule base, or set of protocols are installed on, uploaded to, or otherwise accessible by the mobile device to define what functionality of the mobile device is limited, controlled, managed, or prevented and under what circumstances. Advantageously, the systems, methods, and devices described herein are also capable of monitoring usage of a vehicle to detect, log, and report on dangerous or abusive operator behavior, such as excessive speeding or excessive idling of the vehicle.

As stated previously, the term "mobile device" is intended to include and encompass, but not be limited to, any type of hand-held, mobile, or other computing or communication device usable within a vehicle, such as but not limited to cell phones, smart phones, push-to-talk devices, PDAs, text or email dedicated devices, general computers, laptops, electronic reading devices, multimedia equipment, data tablets, and similar computing or communication device that would or could be used by or accessible to the driver of a vehicle while it is moving or otherwise in operation and that could contribute to driver inattentiveness or distraction because

Petitioner Ex 1002, p. 199
Zimperium v. Taasera, IPR2024-00007

of the talking, texting, surfing, or browsing functions of the mobile device, which can interfere with the driver's ability to focus full attention on driving or operating the vehicle. .

Also, as stated previously, the term "vehicle" is intended to include any type of device or machine that is driven, operated, or controlled by a user (i.e., driver) and that is susceptible to or capable of causing an accident or injury to self or others if the driver is careless or not paying full attention to operation of the vehicle, and includes and encompasses, but is not be limited to, automobiles, trucks, motorcycles, buses, planes, helicopters, blimps, balloons, gliders, boats, ferries, trains, trams, heavy equipment or machinery, and similar devices or machines (collectively and hereinafter referred to as "a vehicle" or "vehicles" for convenience).

Additional features, as described herein or as will be readily apparent to one of ordinary skill in the art, expand upon the capabilities of the core systems, methods, and devices described herein and are intended to improve the safe operation, manageability, portability, enforcement, and support of use of mobile devices by drivers of vehicles. Additional aspects and business applications, are disclosed herein and will also become readily apparent to one of ordinary skill in the art after reading and studying the summary of the present inventions, this detailed description of preferred embodiments, and the claims included hereinafter.

The systems, methods, and devices described herein enable mobile communication policy management and enforcement on mobile devices and in vehicles that are defined and enabled for use within the system. Such policies may be targeted to individual users, devices, and vehicles, or they may be targeted to fleets of vehicles and selectively to groups or subgroups of employees or other categories of people using a centralized policy distribution and management system. Preferably, there are one or more "default" or pre-defined policies usable and pre-configured for individual or corporate users and for different types of mobile devices - based on the capabilities and functionality of such mobile devices and based on the typical functions of the mobile device that are prevented, based on when such functionality needs to be prevented, and based on what functionality should not be prevented or is selectively permitted (such as the ability to make an emergency phone call, access a GPS map application, and the ability to text or call to or from specific numbers or people included on a "white" list or permitted list). In addition, some companies may want to allow some of their corporate software applications to be accessible to their employee drivers even while operating a vehicle, as part of their job. As will also be described in greater detail hereinafter, the system allows an administrator to define customized

Petitioner Ex 1002, p. 200
Zimperium v. Taasera, IPR2024-00007

policies for individuals or for larger groups of people (e.g. all family members, all kids in the family, employees of a division, specific types of employees, or all employees of the company, and the like). In a preferred embodiment, mobile devices and/or vehicles that are not integrated into the system or that do not have suitable system software application(s) installed on the mobile device will not be impacted or interfered with by the system.

Preferably, the system components, devices, and methods - from installation, to defining and implementation of policies, and to ongoing management and control of mobile devices used in vehicles is designed as a simple solution to self-install, setup, and run without the need for outside vendor assistance. Preferably, the system is usable by any mobile device users in the United States or internationally with vehicles that support the OBD standard, such as OBD-II (in the US from 1996 to current and as expected to continue, albeit in updated versions, in future automotive vehicles) or in any vehicle that has been configured (at the factory or in an after-market installation) to include suitable sensors, components, and communication devices/data transmitters to provide data similar to OBD data (such as current vehicle speed) without use of a conventional OBD port.

In one preferred embodiment, the system accesses an existing OBD port on a vehicle wherein the OBD port is connected to and obtains data from the vehicle's on-board computer and/or from mechanical systems and sensors within the vehicle. In alternative embodiments, such data may be obtained directly, such as through a wired data communication line or in a wireless communication, from such on-board computers or mechanical systems without the use of, benefit from, or need for an OBD port. Preferably, such data, whether obtained through the OBD port or otherwise, includes status information regarding the vehicle, such as but not limited to whether the vehicle is in motion, whether the vehicle is turned "on," what gear the vehicle is in, how fast the vehicle is currently going (in reverse or forward direction) at any point in time, or the maximum speed the vehicle has gone in the last x (e.g., 15 seconds) period of time.

It should also be understood that, although use of and description of OBD ports and data are described herein, the present system is also usable with other data interfaces that provide vehicle state or status information - now developed or adopted in the future. For example, the present system is also usable with other vehicle diagnostic protocols, such as OBD-I, OBD-1.5, EOBD (European On-Board Diagnostics), EOBD2 (enhanced version of EOBD), JOBD (Japanese On-Board Diagnostics), SAE J1939 (On-Board Diagnostic protocols used in the US

Petitioner Ex 1002, p. 201
Zimperium v. Taasera, IPR2024-00007

for heavy duty trucks, commercial vehicles, and similar equipment), and any other similar diagnostic or communication protocols now in use or developed hereinafter that provide vehicle state or status information in accessible data format.

The system is also preferably designed to be expandable to support complex environments with large numbers of mobile devices and large numbers of vehicles - in one to one, one to many, many to one, or many to many configurations between vehicles and mobile devices, as will be explained in greater detail hereinafter.

Turning now to FIG. 1A, a high level overview of one preferred embodiment of the system 100a is illustrated. The system 100a is designed to be used in a vehicle 110. As stated previously, vehicle 110 is intended to include any type of device or machine that is driven, operated, or controlled by a user (i.e., driver) and that is susceptible to accident or injury to self or others if the driver is careless or not paying full attention to operation of the vehicle. Although automobiles are the most typical type of vehicle with which the system will be used, the system is also usable and adaptable for use with many other types of vehicles including, but not limited to, trucks, motorcycles, buses, planes, helicopters, blimps, balloons, gliders, boats, ferries, trains, trams, heavy equipment or machinery, and similar devices or machines. For the present discussion, the vehicle 110 is shown only in the abstract by a dashed line. Most vehicles 110 include mechanical, electrical, and software sensors, shown in the abstract by box 120, that identify the state or status of the vehicle or of specific components or subsystems of the vehicle, such as fluid levels, tire pressure, whether the vehicle is on or off, what gear the vehicle is in, its current speed, mileage, pressure gauges, etc., as will be appreciated by those of ordinary skill in the art. Sensors 120 are preferably in electronic communication with a vehicular on-board computer 125. Data communication between the on-board computer 125 and sensors 120 may be either one way or two way (i.e., bidirectional); however, for most purposes disclosed herein, data (x) provided by the sensors 120 to the on-board computer 125 will be of most relevance. In this embodiment, on board computer 125 is also in electronic communication with an On-Board Diagnostics (OBD) interface or port 130 (typically accessible under or at the bottom of the dashboard of a typical automobile). In this first preferred embodiment, an OBD device 135 is adapted to plug into the OBD port 130. The OBD device 135 preferably includes a built-in transmitter 140. The location and configuration of the transmitter 140 on the OBD device 135 is typically not important, as long as the transmitter 140 is adapted to and capable of transmitting

Petitioner Ex 1002, p. 202
Zimperium v. Taasera, IPR2024-00007

data using wireless, RF, infrared, WiFi, Bluetooth, Zigby, or similar communication protocols to mobile devices 150 within the vehicle 110. The transmission signal 145 preferably includes a specific data transmission 148. The specific data transmission 148 preferably includes a transmitter identifier (transID) associated with or representative of the transmitter 140 and current speed data (v) associated with the vehicle 110, which was preferably obtained by the on-board computer 125 from the data (x) provided from the vehicle sensors 120. Additional data may also be transmitted and used to advantage within the system, as described hereinafter.

The system 100a also includes and is intended to be used with a mobile device 150 that is used by a driver (not shown) of the vehicle 110. As stated previously, a mobile device 150 is intended to include and encompass, but not be limited to, any type of hand-held or mobile computing or communication device usable within a vehicle, such as but not limited to cell phones, smart phones, push-to-talk devices, PDAs, text or email dedicated devices, general computers, laptops, electronic reading devices, multimedia equipment, data tablets, and similar computing or communication device that would or could be used by or accessible to the driver of a vehicle while it is moving or otherwise in operation. Preferably the mobile device 150 includes a receiver or antenna (not shown) that is typically built into, or in electronic communication with, the mobile device 150. The mobile device 150 also has suitable system software or firmware 160 installed thereon, as will be described herein. Additionally, the mobile device 150 also includes a system "policy" 170, that is either set by default or programmed/customized specifically for that mobile device or user of the mobile device. As will be explained hereinafter, the policy 170 is used to determine what functions 180 of the mobile device 150 will be permitted (and when) and which ones will be prohibited or interrupted, when the mobile device 150 is being used in a vehicle 150 that is moving above a threshold speed. The mobile device 150 typically has one or more of the following capabilities or functions 180, such as the ability to place or receive a call, the ability to send or receive a text message, the ability to engage in a real-time chat/textual communication, the ability to access the Internet or web browser, the ability to send or receive an email, the ability to engage in a "push-to-talk" communication, and the ability to launch, use, and access other software applications that are built into or installed thereon.

FIG. 1B illustrates a high level overview of an alternative preferred embodiment of the system 100b. The system 100b is similar to system 100a, except instead of using the OBD port

Petitioner Ex 1002, p. 203
Zimperium v. Taasera, IPR2024-00007

130 and OBD device 135, a suitable transmitter 140 is built onto the on-board computer 125 or otherwise is directly connected to the on-board computer 125. In this embodiment, the transmitter identifier (transID) may be used to identify the specific transmitter 140 or the vehicle 110 in which the transmitter 140 is installed. In yet a further embodiment (not shown), one or more of the sensors 120 (such as the speed or velocity sensor) may be adapted to include or communicate directly with its own transmitter without having to go through an on-board computer 125 (as may be desirable, for example, for use of this system with vehicles that do not have their own on board computer 125).

As stated previously, the system 100 described herein is capable of being used in alternate embodiments with any type of vehicle 110, even if it does not have an OBD interface or port 130 – as long as the vehicle 110 or the on-board computer 125 of the vehicle has a component or other transmitter 140 capable of transmitting data 145 about the vehicle, including its state or status, to the mobile device 150 (or at least to a suitable receiver on the mobile device that is in communication with the system or control software application 160). Such capability may already be built into some vehicles at the factory during manufacture or may be added or installed separately as an add-on or post-manufacture component. Such devices or components may include data transmitters 140 built into or in communication with the on-board computer 125 or they could include mechanical sensors 120, such as a transmission speed sensor, that is able to provide speed data (v) in digital or analog format and that can be transmitted or otherwise provided to the mobile device 150 through wired or wireless communication 145. Additionally, as will be described herein, the above components enable an individual or institution/company to define, manage, and enforce an individual or institution/company mobile communication policy 170 regarding permitted or restricted usage of functions or capabilities 180 of the mobile device 150 while operating the vehicle 110. Such functions or capabilities 180 include the sending or receiving of various communications (e.g. text, phone, push to talk, email, Internet, and chat) or the launching of non-critical, non-business, or non-essential applications that are potentially distracting to the driver/operator of the vehicle (e.g., games, camera, etc.). Preferably, the system 100 allows emergency communications, administrator permitted communications, GPS, or other necessary or administrator-permitted services or applications capable from the mobile device 150. Such allowed functions are capable of being initiated when the vehicle is in motion or they are able to continue even if the vehicle starts into motion. Advantageously, centralized

Petitioner Ex 1002, p. 204
Zimperium v. Taasera, IPR2024-00007

management of policies enables a company to define universal default policies that will be applied and enforced across the company with all employees so that policies do not have to be specified for each separate employee added to the system. Customized policies can then or can also be created for specific devices or vehicles, as desired.

As will be described hereinafter, the system 100 preferably includes a standard/default policy 170 configuration (for personal, government, or business applications) for ease of setup and immediate use. However, the system 100 also preferably enables the creation and implementation of customized policies to support more complex users and environments to meet the requirements of individuals, families, companies, or governments.

Basic Setup and Operation.

In preferred embodiments implemented in standard US automobiles built in or after 1996, having a standard OBD port 130 and conventional data available from on-board computers 125 accessible through the OBD port 130, the system 100 preferably uses standard OBDII Protocols, as will be appreciated and understood by those of ordinary skill in the art, to access specific operation information of the vehicle 110 in real time. Selected one or more of the standard OBD codes are advantageously usable herein, such as whether the vehicle is on or off, what gear the vehicle is in, what speed the vehicle is currently travelling, and the like; however, not all of the available or standard OBD codes are necessary for the primary functions of the system 100. However, as stated previously, the present system is also usable with other data interfaces that provide vehicle state or status information - now developed or adopted in the future. For example, the present system is also usable with other vehicle diagnostic protocols, such as OBD-I, OBD-1.5, EOBD (European On-Board Diagnostics), EOBD2 (enhanced version of EOBD), JOBD (Japanese On-Board Diagnostics), SAE J1939 (On-Board Diagnostic protocols used in the US for heavy duty trucks, commercial vehicles, and similar equipment), and any other similar diagnostic or communication protocols now in use or developed hereinafter that provide vehicle state or status information in accessible data format. But, for purposes of further discussion, use of OBD compliant data and devices will be referred to for convenience.

For standard use with the system 100a shown in FIG. 1A, the OBD device 135 is plugged into or otherwise connected into the standard OBD port 130 in a plug and socket configuration. Preferably, the OBD device 135 does not require an administrator or user to "turn on" or activate

Petitioner Ex 1002, p. 205
Zimperium v. Taasera, IPR2024-00007

the OBD device 135. The OBD device 135 is preferably set to power itself on. The primary source of power for the OBD device 135 is derived from the conventional battery of the vehicle 110, which power is accessible through one of the connections in the standard OBD port 130. An alternative power source (not shown) is optionally usable by the OBD wireless interface device 135, such as through a separate connection to the vehicle's battery other than through the standard ODB connection 130 or, as a backup, by connection to a dedicated, external battery (or similar power source), not tied to the vehicle's battery.

The control software application 160 of the present system is preferably installed on the relevant mobile device or devices 150 that are to be controlled or monitored by the system 100. The system software or control application software 160 can be acquired via CD, file transfer over wireless communication, or via the Internet in conventional manner. The specific installation instructions are dependent on the specific mobile device on which the application 160 will be running. Information on the application interaction is described in greater detail hereinafter.

The application preferably installs with a "standard" default setup, where the "default" policy 170 includes the following typical functionality:

- Preferably, emergency communication (911, etc…) are ALWAYS allowable. For safety and liability reasons, this preferably cannot be changed in any administrator-defined or configurable policy.
- If the vehicle is not on and not moving, all mobile phone communications and functionality is allowed.
- If the vehicle is on, but not moving (for at least a set period of time, such as 30 seconds), all mobile phone communications and functionality is allowed.
- If the vehicle is on and moving (forward or reverse, regardless of speed), all mobile phone communications and functionality are disallowed.
- If the vehicle is on, previously moving, but now stopped (but – stopped for less than 30 seconds), all mobile phone communications and functionality are disallowed.
- Once the vehicle stops and is turned off, all mobile phone communications and functionality is allowed.

Petitioner Ex 1002, p. 206
Zimperium v. Taasera, IPR2024-00007

The system 100 also allows an administrator (or employer or parent) to create a more specific or customized policy 170 for a specific device, user, or groups/subgroups or employees or devices, as will be described in greater detail hereinafter. Such customization allows, for example, for a modifiable time period during which a vehicle must be stopped before communications and functionality is allowed, how fast a vehicle must be moving (e.g., minimum threshold speed or velocity) before functionality is disallowed, what phone numbers, emails, and/or people are permitted to communicate in (initially or to continue an already existing communication) to the mobile device 150 even when the vehicle 110 is moving, what numbers, emails, and/or people the mobile device 150 is permitted to communicate with (whether initiating or continuing an already existing communication) even when the vehicle is moving, what applications are allowed or not allowed when the vehicle is moving, what days and what times of days communications and functionality may be allowed or disallowed, and the like. Customized policies may be programmed within the system 100 using an interface provided by the control software application 160 directly on the mobile device or by using a remote web-enabled or web-accessed interface (illustrated by some of the exemplary screen shots herein) that allows for the creation of the policy and dissemination of the policy directly to one or more mobile devices under management by the relevant administrator.

Preferably, whenever a mobile device 150 is initially powered on and at periodic interval thereafter (such as every hour), the system software 160 will query a central server (not shown) associated with the system (or with a company or other entity using the system) and determine if there are any updates to the system software that need to be downloaded and installed. Additionally, any updates or changes to the policy associated with that mobile device (or user of that mobile device) will also be downloaded and installed. In this manner, it is easy and quick for updates or changes to be propagated within the system generally or to be propagated to employees, groups, or selected groups of people within a company or organization.

Preferably, the mobile device has a receiver and suitable software installed thereon that enables wireless communications, such as Bluetooth. Such Bluetooth connection may be paired directly between a specific mobile device 150 and the corresponding transmitter 140 or, in alternate embodiments described hereinafter, Bluetooth communications are used by the transmitter 140 to broadcast data transmissions 148 to any mobile devices 150 in Bluetooth range - without a one-to-one pairing.

Petitioner Ex 1002, p. 207
Zimperium v. Taasera, IPR2024-00007

Turning now to FIG. 2, a high level overview 200 of the implementation of the system 100 based on use of a default policy 225 is disclosed. The first scenario 210 illustrates use of the default policy 225 when the vehicle 110 is parked or otherwise not moving, as shown by the vehicle gear 205 being in park or by the speed (v) of the vehicle being equal to zero (0) or less than the minimum threshold speed level set (for the minimum time requirement) by the policy 225. In this first scenario 210, the default policy 225 allows the mobile device 150 to make and receive phone calls, text messages, emails, Internet access, etc, as shown by check marks 220. The second scenario 260 illustrates use of the default policy 225 when the vehicle 110 is in gear and moving, as shown by the vehicle gear 205 being in a gear other than park and by the speed (v) of the vehicle is greater than the minimum threshold speed level set (or at least not below the minimum threshold speed for the minimum time requirement) by the policy 225. In this second scenario 260, the default policy 225 prevents the mobile device 150 from making or receiving phone calls, text messages, emails, Internet access, etc, as shown by blocked marks 270. As described above, emergency communications/phone numbers, permitted applications, or other "white listed" functions would still be permitted in this second scenario 260 - for logical (e.g., business or safety) reasons.

Preferably, the system application 160 installed on the mobile device 150 is always running in the background and is transparent to the end user (i.e., the user of the mobile device). When the end user approaches a vehicle with an OBD wireless device 135 installed therein or with a suitable transmitter 140 built into or otherwise directly accessible to the on-board computer 125, a one-time authorized/initialization connection is made between the system application software 160 and the OBD wireless device 135 or suitable transmitter 140 - now the system is ready to monitor and implement the default or customized policy 170 and to perform the actions defined for allowing or disallowing mobile communication or running of specified applications based upon data received from the vehicle on-board computer 125 and/or other sources of data regarding the status (on/off, in gear, in motion, etc.) of the vehicle 110. There is no required or additional action on the part of the end user, after initial installation of the system software 160 on the mobile device 150 to enable the system 100 and to initiate the protection and blocking or interference functions of the system software 160. As stated previously, whenever a mobile device 150 is initially powered on and at periodic interval thereafter (such as every hour), the system software 160 will query a central server (not shown) associated with the system (or

Petitioner Ex 1002, p. 208
Zimperium v. Taasera, IPR2024-00007

with a company or other entity using the system) and determine if there are any updates to the system software 160 that need to be downloaded and installed. Additionally, any updates or changes to the policy 170 associated with that mobile device 150 (or user of that mobile device) will also be downloaded and installed. In this manner, it is easy and quick for updates or changes to the software 160 or policy 170 to be propagated within the system 100 generally or to be propagated to specific employees, groups, or selected groups of people within a company or organization.

In an alternate embodiment, the one-time initiation described above is not required by the firmware 160 installed on the mobile device 150. In this alternate embodiment, the firmware 160 allows for "one to many" connections between mobile devices 150 and Bluetooth enabled transmitters 140 - whether installed as part of a OBD wireless device 135 or built into or otherwise directly accessible to the on-board computer 125. As will be appreciated by one of skill in the art, with conventional Bluetooth communication protocols, once a single mobile device 150 has "paired" and connected with a particular Bluetooth transmitter 140, other mobile devices are not able to connect with the Bluetooth transmitter 140 until the original mobile device disconnects and the pairing is dropped. Thus, with conventional Bluetooth connectivity, only one mobile device can be used in a vehicle at a time. That may be fine for some or many applications and uses, but not for all.

To address this challenge, in one embodiment, multiple mobile devices 150 can connect simultaneously to a single Bluetooth enabled transmitter 140 of the present system through the use of piconets. The Bluetooth enabled transmitter 140 acts as the "server" and is designated as the "master" device and each associated mobile device is designated as a "slave." However, to initiate the connection, the mobile device initiates the connection initially as the "master" device. Conventional Bluetooth protocols support a procedure called the master slave switch, which allows the mobile device to become the slave after initiating this initial connection. However, not all mobile devices, at least currently, are configured to enable master slave switching.

For this reason, in another preferred embodiment, the present system 100 does not use the "normal" or "orthodox" connection or paired oriented protocol for Bluetooth connections. Instead of initiating a connection in the normal Bluetooth sense using the mobile device 150, the transmitter 140 communicates its "state" information in a broadcast manner to any listening mobile devices 150 in Bluetooth range. It does this by changing its "friendly name" to represent

Petitioner Ex 1002, p. 209
Zimperium v. Taasera, IPR2024-00007

the current state of the vehicle 110. This unorthodox use of Bluetooth enables the system 100 to support a much wider array of mobile devices 150 while also retaining the ability to block or control multiple mobile devices 150 in the same vehicle 110 using a single transmitter 140.

For example, in one simple embodiment, (1) on a predetermined or set interval (such as every second, or other predetermined period of time), the current speed, as well as other metrics of interest of the vehicle, are queried from the on-board computer 125; (2) once the speed data is obtained from the on-board computer 125, firmware installed on the on-board computer 125 or on the OBD device 135 receives the speed from the vehicle and causes the Bluetooth enabled transmitter 140 to change and transmit its device name to incorporate the current speed (or similar) information obtained from the onboard computer. For example, the device name may be initially defined as obdedge|-1| when the car is off; may be set as obdedge|0| when the car is on but not moving; or may be set as obdedge|55| if the car is traveling 55 MPH. The use of "obdedge" as the actual device name is arbitrary, and would typically be unique for each transmitter - the importance is the additional field information that is inserted into the transmitter name or ID (transID). This data is updated in real time on whatever predetermined period of time is desired and configured in the system 100, but preferably at intervals of no less than 3-5 seconds apart - at least while the vehicle is "on." As will be described hereinafter, it may be desirable, for battery and energy saving modes, to reduce transmission frequency (i.e., increase data transmission intervals) once a vehicle is off and confirmed off; (3) once the mobile device 150 identifies a Bluetooth enabled transmitter 140 of interest and in range (for example, determining that the Bluetooth enabled transmitter 140 belongs to the user of the mobile device 150 based on matching the device's Bluetooth Address or confirming that the transmitter ID is in an expected system configuration), the mobile device 150 then begins to request the current name of the Bluetooth enabled transmitter 140 at set intervals. After performing simple parsing techniques, the vehicle's real time speed can be extracted by the application 160 installed on the mobile device 150 from the current name information for the Bluetooth enabled transmitter 140, and then applied against the policy 170 on the mobile device 150 to make blocking and/or allowance decisions for features and functionality of the mobile device 150 based on the default or user's customized policy 170.

In another preferred and more sophisticated embodiment, if the vehicle 110 is "on" (i.e., its RPM > 0), the Bluetooth friendly name of the transmitter 140 is updated on a periodic basis

Petitioner Ex 1002, p. 210
Zimperium v. Taasera, IPR2024-00007

(e.g., every 3 seconds) to provide multiple pieces of data, such as vehicle state (on/off), current speed, max speed of the vehicle in the last predefined period of time (e.g., past 15 seconds), idle time information, VIN information, an incremental counter (used for detecting when a user has removed or disconnected an OBD device 135 or otherwise disabled the transmitter 140 or to identify when power has been lost to the OBD device 135 or transmitter 140 - noted by a reset of the incremental counter). The amount of data and information that can be sent as part of the transmitter's Bluetooth "friendly name" depends upon the software and hardware used. For example, some transmitters 140 have a 16 character limitation in regards to how long the "friendly name" or transmitter ID (transID) can be. Therefore, in such a case, it is not possible to send all potentially relevant vehicle state or status data in a single friendly name data transmission. In such a case, the information transmitted can be divided into frames. Obviously, the more characters that the transmitter is capable of using as its Bluetooth friendly name, the fewer frames and fewer cycles of name transmissions required to pass on all relevant data to the listening mobile device. For purposes of the following discussion, we assume a 16 character limitation.

FRAMES:

Every frame starts with a predefined set of character used within the system and which enables the system to identify compliant transmitters. For discussion purposes for this embodiment, we will use the characters "ceicon" to designate a transmitter 140 compliant with the system 100. Once the software 160 on the mobile device 150 determines that the transmitter 140 is compliant with the system 100, the software 160 on the mobile device 150 then compares the transmitter's Mac address with the policy 170 on the mobile device 150 to determine if the system is permitted to make blocking or interruption decisions based on data transmissions received from the transmitter 140. If so, the software 160 on the mobile device enters into a loop to constantly refresh the transmitter's "friendly name."

In this example, the 7th character in the device name is used as a "frame identifier."

- If the frame character is an "I": this means that the communication is in "initialization mode." The vehicle is currently off and ECU (engine control unit) or on-board computer

Petitioner Ex 1002, p. 211
Zimperium v. Taasera, IPR2024-00007

is not responding to requests. During this frame the next 4 characters are ignored so should be set to 0's.

- If the frame character is an "0": this means that this frame contains the first 4 characters of the VIN number of the vehicle. These four VIN numbers will be the following 4 characters of the name.
- If the frame character is an "1": this means that this frame contains the second or next 4 characters of the VIN number of the vehicle. These four VIN numbers will be the following 4 characters of the name.
- If the frame character is an "2": this means that this frame contains the third or next 4 characters of the VIN number of the vehicle. These four VIN numbers will be the following 4 characters of the name.
- If the frame character is an "3": this means that this frame contains the fourth or next 4 characters of the VIN number of the vehicle. These four VIN numbers will be the following 4 characters of the name.
- If the frame character is an "4": this means that this frame contains the last digit of the VIN number of the vehicle. The next character is an S and the final two characters will contain the maximum speed encountered in the previous 15 seconds - with speed represented in hexadecimal format.
- If the frame character is a "V": this means that the vehicle does not support VIN information. The next character will be 0 and is ignored. The next character is an S and the final two characters will contain the maximum speed encountered in the previous 15 seconds - with speed represented in hexadecimal format.
- If the frame character is an "L": this is the "Idle Time Frame". The next 4 characters will contain a base 62 digit (0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ) representing 10 minute accumulations of idle time. For instance, if the first digit was a 3, that would mean in the last 24 hours recorded, the vehicle had 30 minutes of idle time. If the second digit is a 5, that would mean the 24 hour period before the last one had 50 minutes of idle time, etc. This 62 digit number would represent a total of the past 4 days worth of idle time the vehicle saw. Idle time is calculated based on when speed =0, but rpm >0.

Petitioner Ex 1002, p. 212
Zimperium v. Taasera, IPR2024-00007

The remaining characters (12-16) of the name are standardized and every frame displays it. Characters 12 and 13 represent the vehicles current speed in hexadecimal format. Characters 14-16 contain an incremental counter. If the device can not be removed, then the incremental counter does not need to be used and these characters can be set to 0's. Otherwise, the incremental counter can be used to determine if there has been a disconnect or power interruption, which would apparent if the counter reset to zero after having been incrementing previously.

Depending on the vehicle's state, not all frames need to be cycled through.

VEHICLE STATES:

The OBD device or associated transmitter has 3 primary states that it can be in:

State 1: The car is off and ECU is not responding. In this state, only 2 frames are shown. Frame "I" and Frame "L". The device should cycle between these 2 frames every time the transmitter name is updated. In this state, the device name is only updated once every 15 seconds unless the state changes.

State 2: The car is off but the ECU is responding. In this state, the device is able to determine VIN information so the following frames are cycled through Frames "0" through "4" - if the vehicle has a VIN; otherwise, Frame "V" is transmitted. The "L" frame is also cycled through. Because of the extra frames shown, the device name (transID) is updated every 3 seconds. Because the car is off, the speed should be set to "FF" in every frame, which alerts the system software installed on the mobile device that the vehicle is still off.

State 3: The car is on. Here the device name is updated every 3 seconds and the following frames are cycled through: Frame "0" through "4" if the vehicle has a VIN, otherwise Frame "V". The "L" frame is also cycled through.

Petitioner Ex 1002, p. 213
Zimperium v. Taasera, IPR2024-00007

GETTING INFORMATION FROM VEHICLE:

When the vehicle is in State 1, the OBD device attempts to initialize the ECU every 10 seconds to see if the vehicle has come on. If the battery voltage of the vehicle drops below 12.4, the OBD device should stop querying the ECU until voltage rises above 12.4 again. Once the ECU responds, the OBD device should move into State 2 or State 3.

In State 2 and State 3, the OBD device should query the ECU every second for RPM and Speed information. RPM = 0 means that the vehicle is "off" and RPM > 0 means that the vehicle is "on."

Policy [Definition - Parameters]

The system 100 allows for the centralized management and enforcement of a mobile communications policy 170 for one or more of a plurality of users or selectable groups or subgroups of users. The policy 170 addresses the various methods of communication (phone call, text message, email message, Internet, computer usage, push-to-talk, etc.) that a mobile device 150 can provide and, in some embodiments, which applications and functions on the device 150 are permitted to be initiated or continued when the vehicle is in motion. Preferably, the system 100 has a pre-defined (default) set of policies (rules) that are applied to the mobile device 150 during installation, that are included in the software 160 installed on the mobile device, or that are uploaded (or uploadable upon request) from the vehicle's on-board computer 125. A system administrator has the ability to re-define or apply a different customized policy that controls inbound or outbound communication and other functionality when the vehicle 110 is in motion or not for the driver or additional vehicle occupants.

As shown in FIG. 3, a system administrator 310 (such as a parent or a company or division administrator, etc.) selects (step 320) whether a default policy or customized policy 340 will be applied to a specific user or mobile device. Preferably, a standard default policy is installed on or uploaded to each mobile device during initial software installation, so no "affirmative" action need to be taken by the system administrator to have the default policy in place and in effect once the software on the mobile device is installed and operational. If the policy is going to be customized, the system administrator has the option (step 322) of defining and configuring the customized policy using an Internet management console or interface 350

Petitioner Ex 1002, p. 214
Zimperium v. Taasera, IPR2024-00007

(described in greater detail hereinafter) or provided through the system software interface 360 built into and accessible directly on the mobile device (also described in greater detail hereinafter). As shown, the customized policy 340 is configured to have sub-policies or components defined for each of the major functions and capabilities of the mobile device, such as incoming and outgoing phone calls 341, Internet access 342, incoming and outgoing emails 343, incoming and outgoing text messages 344, push to talk capabilities 345, and other software applications 346 (such as maps, games, business software, address book, video or audio entertainment, etc.). Very precise customization is possible and desirable. Once the default policy is chosen or the customized policy is configured, it is made available to and accessible by the system application 370, by being installed or uploaded, typically, into memory on the mobile device itself. The system software 370 is then able to receive vehicular information from the vehicle transmitter 380 (once paired or otherwise in communication/broadcast mode) and the rules and exceptions 390 from the policy are consulted and used by the system software 370 to make real time decisions on whether to allow or block specific functionality based on the policy and the data received from the vehicular transmitter.

When using the remote Internet management console 350, the ability to define and provide multiple policies to multiple individuals can be implemented in real time, as long as the mobile device is accessible to the Internet or mobile data network. As stated previously, whenever a mobile device 150 is initially powered on and at periodic interval thereafter (such as every hour), the system software 160 will query a central server associated with the system (or with a company or other entity using the system) and determine if there are any updates to the system software that need to be downloaded and installed. Additionally, any updates or changes to the policy associated with that mobile device (or user of that mobile device) will also be downloaded and installed. In this manner, it is easy and quick for updates or changes to be propagated within the system generally or to be propagated to employees, groups, or selected groups of people within a company or organization.

Primary Application:

The system software application 160 may be written in a wide variety of programming languages now known or hereinafter developed, depending upon the mobile device platform. Currently, Java and C are two such exemplary programming languages. The application 160 has

Petitioner Ex 1002, p. 215
Zimperium v. Taasera, IPR2024-00007

the ability to be configured and have the administrator-customized communication policy 170 either defined via the mobile device user interface or via the remote Internet management console, as shown in the exemplary screen shots attached hereto. The administrator-defined policy 170 determines how the mobile device 150 will handle incoming and outgoing communications (phone, text, push-to-talk, email, Internet, chat, etc…) and, in some embodiments, what applications installed or native to the mobile device 150 will be allowed to operate or run (whether initiated or, if already in progress, whether to remain operational). The application, installed and running actively in the background of the mobile device, checks for a connection between the mobile device and the wireless OBD interface installed on the vehicle, which is configured to access the OBD vehicle computer on a regular and consistent basis. If a legitimate and authorized connection is detected, the system application on the mobile device monitors and enforces communication policy, which may be based on the speed of the vehicle, the location of the vehicle, whether the vehicle is "on," what gear the vehicle is in, what day of the week, what time of the day, and the like. A conventional wireless OBDII interface may be used in the system; however, some of the system features and functions may not work or work as well as the customized ODB interface described herein.

Turning now to FIGS. 4-12, various processes of the system software application 160 are described in association with the embodiment in which the mobile device pairs with the relevant transmitter. FIG. 4 illustrates application initialization process 400. When the application initially starts (step 405), permissions are then checked (step 410). Such permissions include phone permissions, input simulation permissions, and Bluetooth permissions, if applicable to the particular mobile device. If any of the permissions fail, then any such missing permissions are requested (step 415), which preferably displays a prompt on the user's mobile device to approve any permission changes. If the permissions are successful (or once they are successful), the register phone listener (thread) is initiated (step 420). Phone listener thread 1200 is described in greater detail in association with FIG. 12. Main thread process is also initiated (step 425). Main thread process 500 is described in greater detail in association with FIG. 5.

FIG. 5 illustrates main thread process 500. Main thread process initiates (step 505) and blocking mode is set to "off." Bluetooth listening thread is then created (step 510). Bluetooth listener thread 700 is described in greater detail in association with FIG. 7. Loop (step 515) then runs continuously while the application is running. The process checks (step 520) to see if the

Petitioner Ex 1002, p. 216
Zimperium v. Taasera, IPR2024-00007

mobile device is connected to an OBD device. If yes, then the application "sleeps" (step 525) for a predetermined period of time (x). The application communicates (step 540) with the system server if a connection can be made and if there is sufficient time. Such connection enables data from the device to be transmitted to the administrator, if desired, and also enables updates to the software application to be uploaded, if necessary. If the mobile device is not connected to an OBD device, as determined at step 520, then the application checks (step 530) to see if a connection thread is already trying. If yes, then the application "sleeps" (step 525) for a predetermined period of time (x). If no, then a connection thread is launched (step). Connection thread 600 is described in greater detail in association with FIG. 6.

FIG. 6 illustrates connection thread process 600. Connection thread process 600 first checks (step 605) to see if the connection thread is already running. If so, then the connection thread process is exited (step 610). If not, then connection thread process starts a loop (step 615) and checks connected variables (step 620). A value of "1" indicates that a connection is made and the connection thread process is exited (step 610). A value of "-1" indicates that a connection is still trying to be made and the connection thread process continues to loop (step 615). A value of 0 indicates no connection, and a run connect function (step 625) is launched to attempt to establish a connection to the OBD device.

FIG. 7 illustrates Bluetooth listener thread process 700. Bluetooth listener thread process 700 first processes a new event (step 705). If data is being received, that data is processed (step 710). If the Bluetooth connection is disconnected, blocking mode is reset (step 715) to allow all communications and mobile device functionality. The connected value is set back to "0" (step 720), and connection thread is launched (step 725), then the Bluetooth listener thread process is exited (step 750). If there is a connection event associated with the processing of a new event (at step 705), then the application checks for a return value (step 730). If the return value fails, the blocking mode is reset to allow all communications and mobile device functionality and connected value is set back to "0" (step 745), connection thread is launched (step 725), then the Bluetooth listener thread process is exited (step 750). If the return value succeeds, the connected value is set to "1" (step 735) and the initialize device thread is launched (step 740). The initialize device thread 900 is described in greater detail in association with FIG. 9.

FIG. 8 illustrates Process Received Data from OBD Device thread 800. Process Received Data from OBD Device thread 800 first checks the command type (step 805). If

Petitioner Ex 1002, p. 217
Zimperium v. Taasera, IPR2024-00007

initialization is OK, then the process initializes (step 810) and then exits (step 890). If mileage data is provided, the mileage data is processed (step 820) and then the process exits (step 890). If current speed data is provided, the process analyzes the speed (step 825) to determine if the speed of the vehicle is above or below a set threshold (shown as 0 in this example). If the speed is below the threshold, a counter is incremented (step 830), the application is set into non-blocking mode (step 890), and the process exits (step 890). If the speed is above the threshold, the process determines (step 840) what mobile device functions are currently "in process." The policy is checked (step 845) All functions that are not allowed by the policy are terminated, paused, or interrupted (step 850). Next, the policy is applied (step 860) and blocking mode is implemented for all functions not allowed while the vehicle is in motion above the threshold value (step 865). The process then exits (step 890).

FIG. 9 illustrates the Initialize Device Thread process 900. The Initialize Device Thread process 900 starts (step 905) and the connected variable is first checked (step 910). If the connected variable value is "1" the OBD Device Initialization command is then sent (step 920), the process "sleeps" for a predetermined period of time (step 925), then the get speed thread process 1000 is launched (step 930). The get speed thread 1000 is described in greater detail in FIG. 10. The process then exits (step 950). If the connected variable value is "-1" or "0", then the process merely exits (step 950).

FIG. 10 illustrates the get speed thread process 1000. The get speed thread process 1000 first check for the connected variable (step 1005). If the connected variable value is "-1" or "0", then the process merely exits (step 1090). If the connected variable value is "1", then the process sends (step 1010) a get speed command. The process then determines (step 1020) if the vehicle is on or off. If the vehicle is "on", the process sleeps for a predetermined period of time X (step 1030). If the vehicle is "off", the process sleeps for a predetermined period of time Y (step 1040), which is longer than predetermined period of time X. The process then loops (step 1050) repeatedly.

FIG. 11 illustrates message listener thread process 1100. Message listener thread process 1100 first processes a new event (step 1105). If there is an incoming text (sms/mms) or email, the policy is checked (step 1110). The process determines if the system is in blocking mode and if the message sender or recipient is on the white list (step 1120). If the system is in blocking

Petitioner Ex 1002, p. 218
Zimperium v. Taasera, IPR2024-00007

mode and if the message sender or recipient is not on the white list, the message or email is blocked (step 1130). Otherwise, the process ends (step 1150).

FIG. 12 illustrates phone listener thread process 1200. Phone listener thread process 1200 first processes a new event (step 1205). If there is an outgoing call, the process determines if the system is in blocking mode (step 1210) and then checks the policy (step 1220). The system determines (step 1230) if the call recipient is on the white list or otherwise approved. If so, then the outgoing call is permitted to continue without interruption (step 1240). If not, then the outgoing call is blocked (step 1250). If there is an incoming call, the process determines if the system is in blocking mode (step 1260) and then checks the policy (step 1270). The system determines (step 1275) if the call originator is on the white list or otherwise approved. If so, then the incoming call is permitted to continue without interruption (step 1280). If not, then the incoming call is blocked, terminated, routed to an automated response, routed to voicemail or similar handling (step 1290).

FIGS. 13-32 illustrate exemplary screen shots of the Internet management console or interface 350 as may be used in the present system. FIG. 13 illustrates a customer activation screen shot. FIG. 14 illustrates a typical login page for access to the Internet management console. FIG. 15 illustrates a main dashboard page, from which an administrator is able to access other key functions and pages within the management console, including creating, accessing, and editing: (a) site information, (b) user information, (c) group information, (d) devices information, (e) policies, and (f) support. FIG. 16 illustrates a manage my numbers interface that enables an administrator to add or delete specific phone numbers for a specific user from the allowed or white list of numbers that would not be blocked even when the user's vehicle is in motion. FIG. 17 illustrates a main policy configuration interface for configuring a single policy and includes check boxes for selecting or deselecting: (i) block phone calls; (ii) block text messages; (iii) block emails; (iv) allowed overrides per day; (v) allowed personal numbers; (vi) email address for receipt of notices of policy overrides or breaches; (vii) approval for sending of text messages associated with notices of policy overrides or breaches; (viii) defining of text to display on the screen of the mobile device during blocking of functionality; and similar customization. FIG. 18 illustrates a standard user information settings interface. FIG. 19 illustrates a groups management page that allows an administrator to define a group and set the policy or policies that will apply to that group. FIG. 20 illustrates an edit page that

Petitioner Ex 1002, p. 219
Zimperium v. Taasera, IPR2024-00007

enables an administrator to modify, add, or delete policies that apply to a particular group. FIG. 21 illustrates a main groups management and search page that allows an administrator to review the list of groups under management and to select one or more for review or access. FIG. 22 illustrates a centralized phone management interface. FIG. 23 illustrates a policy management page that enables an administrator to define and create a new, customized policy. FIG. 24 illustrates a policy edit and further configuration interface. FIG. 25 illustrates a main policies management and search page that allows an administrator to review the list of policies created and used by the administrator and to select one or more for review or access. FIG. 26 illustrates an allowed phone numbers list for inclusion on a group policy. FIG. 27 illustrates a site management interface page that enables an administrator to manage sites under current management. FIG. 28 illustrates a site creation interface page that enables an administrator to create and identify sites under current management. FIG. 29 illustrates a user management interface that enables an administrator to view and edit information about specific users. FIG. 30 illustrates a user creation interface that enables an administrator to create and define a new user in the system. FIG. 31 illustrates an edit page that enables an administrator to configure the policy for a specific user. FIG. 32 illustrates an edit page that enables an administrator to configure the allowed phone numbers associated with a specific user.

Policy Implementation for Mobile Devices that Have Texting Capabilities But No Data Plan

For mobile devices that do not have Internet access and only have texting capability (as opposed to a data plan), once the system application or firmware is installed on the mobile device, policy parameters and status or reporting information can be communicated between the main system or central server and the mobile device using traditional texting - with header information that is picked up by the firmware. Policy variables and parameters are passed in known order or in determinable format so that the firmware can implement the policy or any changes in policy that are made at any point in time. Likewise, the firmware makes use of the texting function built onto the mobile device to enable information and data to be passed back to the system or central server as needed.

Petitioner Ex 1002, p. 220
Zimperium v. Taasera, IPR2024-00007

For those few mobile devices that have neither texting or data plans, policies need to be installed at time of install of the system software or upgrade or update of such system software.

OBD Interface:

The wireless OBD interface of the system is the preferred method of communication between the vehicle on-board computer and the system application or firmware installed on the mobile device if a suitable transmitter is not installed directly on the vehicle's on board computer. The OBD interface includes conventional and currently available functions and features of ODBII compliant interfaces, but preferably includes the following additional functions and features:

-Engineered board and chipset with custom micro code to communicate with OBD compliant vehicle on-board computer protocols (i.e.: ISO, CAN, etc…) and mobile device application;

-On-board data storage for analysis, policy enforcement, troubleshooting, reliability and recovery;

-Self-contained backup battery power supply for situations when vehicle provided power is absent, thus ensuring continued analysis, policy enforcement, troubleshooting, reliability and recovery; and

-Unique identification assigned to each system wireless OBD interface in addition to the unique identification generated by Bluetooth. This is to facilitate:

--unique tracking capabilities related to the operation of the system (e.g., proprietary wireless OBD interface assigned to a specific VIN number or series of VIN numbers);

--portability between multiple OBD vehicles;

--audit capability by capturing and storing information with a unique identifier(s) and time stamp; and

--support

As stated previously, however, the system described herein is capable of being used in alternate embodiments with any type of vehicle, even if such vehicle does not have an OBD interface or port (or if the system does not need to use the OBD port) – as long as the vehicle or

Petitioner Ex 1002, p. 221
Zimperium v. Taasera, IPR2024-00007

the on-board computer of the vehicle has a component or other device capable of transmitting data about the vehicle or status of the vehicle to the mobile device. Such capability may already be built into some vehicles or may need to be added or installed separately. Such capabilities may be implemented entirely by hardware or they may include a combination of hardware and software. Such devices or components may also include data transmitters built into or in communication with the on-board computer or they could include mechanical sensors, such as a transmission speed sensor, that is able to provide speed data in digital or analog format and that provide data that can be transmitted or otherwise provided to the mobile device through wired or wireless communication.

Application Uses:

A first practical or business use of the system described herein is the ability to provide, implement, and enforce a rules-based mobile communications policy for the driver/operator of the vehicle or even additional passengers. The application rules are pre-defined (default) – or set by the administrator(s) associated with the end users. The system accurately detects the forward /reverse movement of a vehicle, based preferably on data provided by the on board computer of the vehicle, and refers to policy (end user/vehicle) as to allow or disallow various methods of communication (e.g., phone, text, push-to-talk, email, Internet, chat) or operation of particular applications or other functionality of the mobile device. For example, if vehicle is running but not moving, policy default may be to allow all forms of communication and any applications. However, once forward /reverse movement (of any speed) is detected, the policy default is to prevent any "non-emergency" or "non-pre-approved" communications or applications. Movement includes situations in which a vehicle is actually moving in forward or reverse direction or in which the vehicle has stopped temporarily due to traffic congestion, stop sign, or red light. In a preferred embodiment, the default policy is to allow for communication or use of an application after 30 seconds of vehicle non-movement. Should the vehicle move at a detectable rate, the communication and application will be disallowed or disconnected. Once the vehicle stops again, a new 30 second timer starts to run. If the vehicle is turned off and ceases to run, the default policy is to allow immediate communications, both outbound and inbound, and use of all applications. Movement detection based on data provided by conventional on board computers is highly accurate. Preferably, a "default" detectable or actionable speed is set to 1

Petitioner Ex 1002, p. 222
Zimperium v. Taasera, IPR2024-00007

mph; however, this value or level may be changed or set to a different default level or a different customized level by the administrator. Default policy is to allow emergency communications; administrator permitted communication, GPS, and any other necessary mobile device services or applications.

Preferably, if the mobile device user is engaged in active communication or use of a non-permitted application and enters a system-enabled vehicle and starts the engine, the default policy permits such communication or application to continue until forward or reverse movement, above the threshold level, is detected. . Once the vehicle is detected to be moving above the threshold level, the communication or application will be disallowed, discontinued, or stopped, per the "default" policy. Again, the policy or rules may be customized by the administrator for specific business or personal needs.

Additional Applications and Uses of System

1. Parent – Teen (New Driver) Network: The web enabled management console also allows for a individual end user to notify and distribute the application to other interested parties so that they may add their mobile device to the protection of the system. An example of this is presented in appendix 6. Example - A parent has enabled the system on their child's vehicle. They access the management console and begin the process of additional participant notification. They simply add in the email addresses and names of their child's friend's parents and send them a message explaining the program and inviting them to participate. They are provided a link to download the application for their child's phone or other mobile device if the wish. Upon doing so, they can apply the default installation policy along with their added emergency number. Now the system (once keyed) will recognize the mobile device when in proximity and will begin to monitor and enforce communications inbound and outbound if the vehicle is moving. Stated differently, an administrator (parent, individual, group, etc…) has the ability to craft, distribute, and manage invitations to download the mobile device firmware application to allow for policy enforcement when riding in a proprietary wireless OBDII Interface vehicle. The web-enabled management console provides the administrator with a utility to produce an email from a template, send the email to a defined list of recipients, see who has opened and agreed or declined to participate, and allow continued management.

Petitioner Ex 1002, p. 223
Zimperium v. Taasera, IPR2024-00007

The limited web-enabled management console for those that agree to participate provides limited functionality. After agreeing to a license agreement and remote policy agreement, the participant is able to define some basic policies related to emergency contact numbers. Participants can easily migrate this account to a fully protected account with the acquisition of a proprietary wireless OBDII Interface.

2. Fleet with non-assigned vehicles and many drivers: The system allows for the support of multiple drivers for multiple vehicles. The drivers and vehicles are activated and managed in the system. When a driver approaches and enters the vehicle the system connects via the unique Bluetooth connection and checks the database to see what policy is applicable.

3. Speed alerting: There are two methods of communicating the speed of the vehicle to the system and multiple methods for reporting and alerting the speed to the administrator and/or parent. The preferred method of communication of the speed from the vehicle to the device and solution is by using the unique Bluetooth connection method whereas the firmware delivers the speed embedded in the transmitter ID (transID) or "friendly name" of the broadcast. The second method of communication is via the standard Bluetooth connection and OBD communication. The reporting and alerting can be logged in the system. In addition the administrator and/or parent can set limits in the management console that will alert them via text, email or phone of the violation.

4. After hours alerting: Another instance that can be monitored is the use of a vehicle after hours or after a predefined time by the administrator and/or parent. When the vehicle is determined to be moving, the time is cross referenced with the policy to determine if a violation has occurred. If so, the administrator and/or parent can define policy protocols in the management console that will alert them via text, email or phone of the violation.

5. Vehicle optimization and performance reporting: The system enables and allow the real time or near real time reporting of vehicle diagnostic information back to the system server. Because the mobile device is in communication with the on-board computer of

Petitioner Ex 1002, p. 224
Zimperium v. Taasera, IPR2024-00007

the vehicle and because any associated mobile devices have communications set up with the system server, the present system enables the real time or near real time reporting of vehicle diagnostic information to identify problems or potential problems with the vehicle or engine of the vehicle before a "check engine" light or alarm is triggered and before or without having to take the vehicle into a service center for routine connection of the on-board computer to a service computer through the OBD interface.

6. Integration with Fleet management solutions: Since much relevant data about the vehicle and about usage of mobile devices by the driver/operator of the vehicle are available within the system, the system enables companies to monitor and control behavior by its employees who use company-owned vehicles or mobile devices. Speed, driving patterns, and mobile device usage can be monitored to ensure that employees adhere to required or permitted driving patterns. Such monitoring enables companies to reduce their risk and liabilities and encourages/rewards good driving behaviors – particularly for companies and organizations that require or use employees that spend much or all of their time for the employer as a driver/operator of a vehicle.

7. Monitoring of Idle Time of a Vehicle: As stated previously, much relevant data about a vehicle is available to the system and can be captured and communicated through one or more mobile devices associated with the respective vehicle back to a central management system. For example, since the system detects and monitors both when a vehicle is "on" and when the vehicle is in motion beyond the threshold minimum – in order to implement the communication blocking policy on the mobile device, it follows that the system is also able to identify when the vehicle is "on" but not moving – in other words, when a vehicle is in "idle" status. Since this analysis of vehicle motion is taken on a frequent and periodic basis, the amount of idle time associated with a particular vehicle can be determined. Such "idle status" data can be collected by the mobile device and forwarded back to the central control on a predetermined frequency. For example, such data may be transmitted every hour, every day, or when a threshold idle time has been exceeded within a set period of time.

Petitioner Ex 1002, p. 225
Zimperium v. Taasera, IPR2024-00007

In addition, since the speed data is collected in real time and on a continuous basis, it is possible to distinguish a vehicle that is moving slowly or periodically in traffic or one that is merely sitting in a parked or stopped position for non-traffic reasons.

Depending upon the space available for data transmission and other factors, such as communication bandwidth and battery life, etc., the idle time may be transmitted by the mobile device as the exact number of minutes of idle time in the predefined period of time. Alternatively, to reduce bandwidth, the data transmitted for idle time may represent a larger chunk of time. For example, each unit of data transmitted could equal 1 minute of idle time or each unit of data could represent a larger chunk of idle time, such as a ten minute increment.

Why is this important? With unleaded gasoline running between $2.00 and $4.00 per gallon in the United States and much more in other countries, and idle running of the motor of a vehicle costing anywhere from 1/3 to 2 gallons or more per hour of idling, excessive idling can be a difficult to detect loss of gas mileage for the vehicle and extra fuel cost for running the vehicle. Although idle time and cost of operation for a single vehicle may not be significant in and of itself, it is easy to see how a company with a large fleet of vehicles, in which just 10-20% of such vehicles are engaged in unnecessary or abusive idling, can greatly increase the operating costs for the entire fleet.

With such data captured and forwarded to the central management control, reports can be generated to show the company which vehicles in its fleet are left running, in idle position, excessively, abusively, or unnecessarily. Having this data enables a company with a large fleet to identify and change behavior of specific drivers and also gives the company greater control in reducing fuel charges for its fleet of vehicles. Reports can be generated on any desired basis or frequency (daily, weekly, monthly, etc.

In a preferred embodiment, anytime a vehicle is "on" but not moving, the system starts incrementing the minutes. Every 24 hours, the system adds up all the idle time minutes that occurred in the last 24 hour period (24 hours is just used for exemplary purposes; any other time frame can be specified or chosen). The system then sets a data field in the mobile device communication packet to that value associated with the amount of idle time. To compress data usage, the idle time value can be divided by some divisor, such as a 10 or 15 minute block, so that each idle time unit actually represents a

Petitioner Ex 1002, p. 226
Zimperium v. Taasera, IPR2024-00007

10 or 15 minute block. Preferably, the prior 3 to 5 (preferably 4) days worth of idle time is sent in one or more communications from the mobile device back to the central control for recordation and synchronization purposes with the database servers at central control. This enables data to be collected (without interruption) even for vehicles that are not used for several days at a time. Once the system tallies all the idle time from the past 24 hours, it is then added to the frame of data being sent. Preferably, the idle time from a current 24 hour segment is not sent until the end of the relevant 24 hour period. Once that data is "finalized," then its added to the 3-5 (preferably 4) days of idle time data that are being sent.

To illustrate further, a frame of data (described earlier) sent to the mobile device could look like the following: celconL3781ff031. In this frame, L is merely and arbitrarily used to represent that this is an idle time frame, then the following characters: 3,7, 8, and 1 represent the past 4 groups of idle time data. So, if the system were using 24 hour blocks for a "group," and if each unit of idle time value equaled 10 minutes of idle time, then that would mean that yesterday, the respective vehicle had 30 minutes of idle time; the day before, it had 70 minutes of idle time, the day before that had 80 minutes, and four days ago the idle time was 10 minutes.

Idle time is calculated based on when speed =0, but rpm >0.

8. Reporting to Insurance companies: Since much relevant data about the vehicle and about usage of mobile devices by the driver/operator of the vehicle are available within the system, the system enables insurance policies to be developed and customized to encourage particular behaviors and to discourage or punish, by means of higher premiums or exclusions for coverage, other behaviors.

Safety Assurance:

The system is preferably configured to allow immediate and direct communication with a emergency contact/number (e.g., 911, 411, 991, 112, ICE, etc...) or any administrator pre-approved number(s) (e.g., main office, supervisor, dispatch, etc. for business applications; parent, home, etc. for personal or family applications) if an emergency or trouble situation arises. The solution will not deny inbound or outbound communications that are considered to be an

Petitioner Ex 1002, p. 227
Zimperium v. Taasera, IPR2024-00007

emergency regardless of the status of the vehicle. The administrator pre-defined or pre-approved number(s) are dependent upon the administrator's policies and settings.

Policy Enforcement:

The administrator-defined policy is enforced by the application installed on the mobile device. The application allows for emergency communications (e.g., to or from 911, 411, 991, 112, ICE, etc…) and other administrator-approved numbers and applications. The administrator-approved numbers may be defined as (i) allow in / allow out; (ii) allow in / disallow out; (iii) disallow in/allow out; and (iv) disallow in/ disallow out. The communication is either allowed or disallowed by the application, which delivers a disconnect/no connect command for communications (or a close/pause command for applications) in the mobile device. The administrator is also able to specify operational hours and operational days for the policy that are independent of vehicle motion. For example, the system policy may be configured to block communications or applications only during weekday business hours or only during night-time driving, and the like. Similarly, GPS functionality may be incorporated into the system to disallow communications or applications based on the location of the vehicle in a geographic location.

Policy Breaking Protection:

Policy enforcement is also performed by collecting and analyzing logging information for predefined triggers and/or anomalies detected against regular usage information. For example, the administrator may be notified in real time (using the communication capabilities of the mobile device itself) when detection of a break/breach in policy is detected/discovered. Alternatively, vehicle data and mobile device usage may be examined periodically by the administrator by accessing logged data stored on the mobile device and/or on the ODB interface device.

Disabling Protection:

To ensure policy protection and enforcement and to protect against disabling the mobile device application and/or the wireless OBD interface, internal controls have been engineered to detect and log the history and alert when a disabling incident takes place.

Petitioner Ex 1002, p. 228
Zimperium v. Taasera, IPR2024-00007

For example, the wireless OBD interface has memory added and constant power provided by the vehicle and/or an onboard/built-in battery power supply. When a user approaches an enabled vehicle, a connection is made and logged both on the mobile device and in memory on the wireless ODB interface. During normal operation, the system application on the mobile device is configured to communicate periodically with a remote Internet management console to provide user history and usage statistics. The secure remote Internet management console regularly analyzes this information for anomalies. If a user disables the wireless OBD interface, the log will reflect this action, and discovered by the ongoing analysis and make notification to the administrator. Also, as discussed above, the system application can also be configured to send a text message or otherwise send an "alert" to the administrator using the communication capabilities of the mobile device if an anomaly, error, or potential policy violation is detected by disabling the system application or OBD interface, or by attempting to circumvent the policy (e.g., by reprogramming or renaming an application or contact on the mobile device to try to make an unauthorized contact or application appear to be one of the approved ones).

In one embodiment, disabling protection is built in to detect when the user removes the wireless OBD interface from the connection to the vehicle on-board diagnostics connection. The preferred wireless OBD interface has memory added and backup battery power to log any disconnection event. The backup battery power enables the wireless OBD interface to establish or maintain communication with the mobile device even when power from the vehicle is unavailable or lost. Functionality has been built into the wireless OBD interface to detect the disconnection and then send a request to the mobile device to send an alert to the administrator. If the mobile device is unable to make an immediate notification, the alert is stored until a connection and delivery is possible and such alert is logged on the OBD interface until accessed by the administrator.

In another embodiment, disabling protection has been built in when the user attempts and successfully disables the mobile device application permissions (e.g., disabling Bluetooth, stop connecting, etc.). The system application monitors and checks for this activity. An alert can be sent to the administrator to notify when a permission/parameter has been changed or violated. Alternatively, the incremental counter information can be sent back to the administrator or

Petitioner Ex 1002, p. 229
Zimperium v. Taasera, IPR2024-00007

centralized server, which would enable the administrator or server to identify a disconnection or power outage.

In another embodiment, to help with detecting the removal of an OBD device, in lieu of or in combination with an on-board power supply and memory on the OBD device which can store and report disconnection of the OBD device, firmware installed on the OBD device may be configured to include a variable, on a timer that increments that variable by 1 every minute or other predetermined period of time after the OBD device has been installed and plugged into the vehicle's OBD port. So, when the OBD device is first plugged in, the timer variable is set to zero (0), then after 10 minutes, for example, the variable has incremented to 10, and after 1 hour, the variable has incremented to 60, etc. After 1 month, the variable is around 40,300. Each time the mobile device connects with the OBD device, the timer variable is obtained by the mobile device and sent to the main system server. The server will store that timer variable and if that variable every starts over or is a lower value than a prior saved value, the system will know that the OBD device has been disconnected. Preferably, the variable is maintained in volatile memory on the OBD device and will maintain and increment its value as long as the OBD device remains connected to the OBD port of the vehicle and as long as the battery of the vehicle does not lose power. If the OBD device is disconnected or if the vehicle battery loses all power, the timer variable will reset back to zero. At some point the timer variable may get too big and will naturally roll back over to zero. However, the server knows what the maximum value is for the timer variable and can determine when the variable resets back to zero on a normal rollover event.

Permission enabled use on device with application running:

Policy can be enabled by the administrator to enable permission-based use/communication with a PIN provided by the administrator. In this embodiment, a vehicle operator can allow a passenger of the vehicle full use of a mobile device that has the application installed and enabled to be used upon entry of the authorized PIN. The PIN logs but allows a temporary override of administrator-defined policy enforcement and permits immediate device communication and use of applications. To prevent abuse of this feature, the administrator can apply a policy to restrict the number of permission-enabled uses within a defined time frame.

Petitioner Ex 1002, p. 230
Zimperium v. Taasera, IPR2024-00007

Other Functionality:

The system is configurable to support multiple users and multiple wireless OBD interfaces. This supports a business application for managing a fleet of vehicles assigned to one or many individuals. The Bluetooth master slave designation described above allows and enables this multiple mobile devices with one or more OBD devices – where there are multiple drivers and mobile devices associated with one or more vehicles and corresponding OBD devices.

Battery Savings Protocols

Battery saving modes may be used to reduce battery consumption required by firmware installed on the relevant mobile device. The below programming illustrates the values that may be used to control battery consumption in a basic manner.

Connection Attempt Delay is the amount of time in milliseconds between searching for nearby Bluetooth devices (i.e., OBD devices).

ConnectionAttemptDelaySmall is number of milliseconds between trying to connect to OBD devices found on the search.

SpeedAttemptDelay is the number of milliseconds between speed readings.

SpeedAttemptDelayOff is the number of milliseconds between trying to read speed when connected to a vehicle that is OFF.

obscureDelay is the number of milliseconds between writing the system screen on top of other applications when the mobile device is in "blocking" mode.

Low is the preferred, default setting, which uses the battery the fastest.

Max is the most conservative mode to preserve battery life.

Petitioner Ex 1002, p. 231
Zimperium v. Taasera, IPR2024-00007

Low battery mode: (default):

connectionAttemptDelay=20000;
connectionAttemptDelaySmall=3000;
speedAttemptDelay=1000;
speedAttemptDelayOff=15000;
obscureDelay=500;

Medium battery mode:

connectionAttemptDelay=25000;
connectionAttemptDelaySmall=5000;
speedAttemptDelay=2000;
speedAttemptDelay2=2000;
speedAttemptDelayOff=20000;
obscureDelay=1000;

High battery mode:

connectionAttemptDelay=35000;
connectionAttemptDelaySmall=7000;
speedAttemptDelay=3000;
speedAttemptDelay2=2000;
speedAttemptDelayOff=30000;
obscureDelay=1500;

Max battery mode:

connectionAttemptDelay=40000;
connectionAttemptDelaySmall=9000;
speedAttemptDelay=5000;
speedAttemptDelay2=2000;
speedAttemptDelayOff=40000;
obscureDelay=2000;

Petitioner Ex 1002, p. 232
Zimperium v. Taasera, IPR2024-00007

In view of the foregoing detailed description of preferred embodiments of the present invention, it readily will be understood by those persons skilled in the art that the present invention is susceptible to broad utility and application. While various aspects have been described in the context of screen shots, additional aspects, features, and methodologies of the present invention will be readily discernable therefrom. Many embodiments and adaptations of the present invention other than those herein described, as well as many variations, modifications, and equivalent arrangements and methodologies, will be apparent from or reasonably suggested by the present invention and the foregoing description thereof, without departing from the substance or scope of the present invention. Furthermore, any sequence(s) and/or temporal order of steps of various processes described and claimed herein are those considered to be the best mode contemplated for carrying out the present invention. It should also be understood that, although steps of various processes may be shown and described as being in a preferred sequence or temporal order, the steps of any such processes are not limited to being carried out in any particular sequence or order, absent a specific indication of such to achieve a particular intended result. In most cases, the steps of such processes may be carried out in various different sequences and orders, while still falling within the scope of the present inventions. In addition, some steps may be carried out simultaneously. Accordingly, while the present invention has been described herein in detail in relation to preferred embodiments, it is to be understood that this disclosure is only illustrative and exemplary of the present invention and is made merely for purposes of providing a full and enabling disclosure of the invention. The foregoing disclosure is not intended nor is to be construed to limit the present invention or otherwise to exclude any such other embodiments, adaptations, variations, modifications and equivalent arrangements, the present invention being limited only by the claims appended hereto and the equivalents thereof. It should also be understood that the present invention also encompasses computer-readable medium having computer-executable instructions for performing methods of the present inventions, and computer networks and other systems that implement the methods of the present inventions.

Petitioner Ex 1002, p. 233
Zimperium v. Taasera, IPR2024-00007

We claim:

Claim 1. A system for controlling use of functions on a mobile device when the mobile device is in a vehicle, comprising

a vehicular on-board computer installed within the vehicle and configured to obtain speed data from the vehicle;

a transmitter in electronic communication with the on-board computer and configured to transmit an indication of the speed data on a periodic basis;

a receiver installed on the mobile device adapted to receive the indication of speed data transmissions from the transmitter;

a software application installed on the mobile device, wherein the software application runs in memory resident on the mobile device whenever the mobile device is powered on and wherein the software application receives the indication of speed data from the receiver, the software application including a policy associated therewith that defines when and which functions of the mobile device are disabled by the software application in response to the indication of speed data transmission;

whereby, in response to receipt of the indication of speed transmission data, if the vehicle speed exceeds a minimum threshold speed level, the software application disables the functions of the mobile device in accordance with the policy associated therewith.

Claim 2. The system of claim 1 wherein the vehicular on-board computer obtains the speed data from the vehicle continuously.

Petitioner Ex 1002, p. 234
Zimperium v. Taasera, IPR2024-00007

Claim 3. The system of claim 1 wherein the vehicular on-board computer obtains the speed data from the vehicle on a periodic basis.

Claim 4. The system of claim 1 wherein the functions of the mobile device remain disabled for a predetermined period of time after the indication of speed transmission data indicates that the vehicle speed exceeds the minimum threshold speed level.

Claim 5. The system of claim 4 wherein the predetermined period of time in which the functions of the mobile device remain disabled is set according to the policy.

Claim 6. The system of claim 1 wherein the functions of the mobile device are enabled after the indication of speed transmission data indicates that the vehicle speed has been below the minimum threshold speed level for a predetermined period of time.

Claim 7. The system of claim 6 wherein the predetermined period of time in which the indication of speed transmission data indicates that the vehicle speed has been below the minimum threshold speed is set according to the policy.

Claim 8. The system of claim 1 wherein the transmitter transmits the indication of the speed data continuously.

Claim 9. The system of claim 1 wherein the transmitter transmits the indication of the speed data on a periodic basis.

Claim 10. The system of claim 1 wherein the vehicle includes one of an automobile, truck, motorcycle, bus, aircraft, watercraft, plane, helicopter, blimp, hot air balloon, glider, boat, ferry, train, tram, heavy equipment or machinery, and similar devices operated by a person.

Claim 11. The system of claim 1 wherein the mobile device includes one of a cell phone, smart phone, push-to-talk device, PDA, text or email dedicated device, general computer, laptop, electronic reading device, multimedia equipment, data tablet, and similar computing or

Petitioner Ex 1002, p. 235
Zimperium v. Taasera, IPR2024-00007

communication device each having a display or interface that is usable by or accessible to a driver of the vehicle.

Claim 12. The system of claim 1 wherein functions on the mobile device include one or more of: making an outgoing call, receiving an incoming call, sending or receiving a text message, text chatting, sending or receiving an email, Internet browsing, and launching of a specified application installed on the mobile device.

Claim 13. The system of claim 1 wherein speed includes relative speed of the vehicle whether the vehicle is moving in the forward or reverse direction.

Claim 14. The system of claim 1 wherein the transmitter is built into and integrated with the on-board computer.

Claim 15. The system of claim 1 wherein the transmitter is included in an on-board diagnostic (OBD) device that plugs into the OBD port of the vehicle, wherein the OBD port is in electronic communication with the on-board computer.

Claim 16. The system of claim 15 wherein the OBD device receives power from the vehicle through the OBD port.

Claim 17. The system of claim 15 wherein the OBD device receives power directly from a wired connection with the battery of the vehicle.

Claim 18. The system of claim 15 wherein the OBD device receives power independently from the power supply of the vehicle.

Claim 19. The system of claim 15 wherein the OBD device transmits to the mobile device an indication that the OBD device has lost power whenever it has been unplugged from the OBD port.

Petitioner Ex 1002, p. 236
Zimperium v. Taasera, IPR2024-00007

Claim 20. The system of claim 15 wherein the OBD device transmits to the mobile device an indication that the OBD device has lost power whenever there has been a power interruption to the OBD device.

Claim 21. The system of claim 1 wherein the transmitter and receiver communicate through a wireless communication protocol.

Claim 22. The system of claim 21 wherein the wireless communication protocol is an RF communication protocol.

Claim 23. The system of claim 21 wherein the wireless communication protocol is a WiFi or Zigby communication protocol.

Claim 24. The system of claim 21 wherein the wireless communication protocol is a Bluetooth communication protocol.

Claim 25. The system of claim 24 wherein the transmitter and receiver are paired using the Bluetooth protocol.

Claim 26. The system of claim 24 wherein the transmitter broadcasts speed data without pairing with the receiver.

Claim 27. The system of claim 26 wherein one or more mobile devices are able to receive and act upon the transmitter broadcast simultaneously because there is no specific Bluetooth pairing.

Claim 28. The system of claim 26 wherein the transmitter broadcasts speed data by embedding the speed data in its device name.

Claim 29. The system of claim 26 wherein the transmitter broadcasts additional data by embedding the additional data in its device name.

Petitioner Ex 1002, p. 237
Zimperium v. Taasera, IPR2024-00007

Claim 30. The system of claim 1 wherein the receiver searches for the electronic communication from the transmitter on a periodic basis

Claim 31. The system of claim 1 wherein the transmitter and receiver communicate through a wired connection between a data port of the vehicle and a data port of the mobile device.

Claim 32. The system of claim 1 wherein the indication of the speed data includes the actual speed of the vehicle.

Claim 33. The system of claim 32 wherein the policy defines the threshold speed level

Claim 34. The system of claim 1 wherein the indication of the speed data includes a flag indicating that the speed of the vehicle is currently above the threshold speed level.

Claim 35. The system of claim 1 wherein the indication of the speed data includes the actual speed of the vehicle and the policy defines the threshold speed level.

Claim 36. The system of claim 1 wherein the transmitter only transmits the indication of the speed data when the vehicle is on.

Claim 37. The system of claim 1 wherein the policy prevents outgoing calls from the mobile device.

Claim 38. The system of claim 1 wherein the policy prevents the mobile device from accessing the phone functions on the mobile device.

Claim 39. The system of claim 1 wherein the policy disables the display screen of the mobile device.

Petitioner Ex 1002, p. 238
Zimperium v. Taasera, IPR2024-00007

Claim 40. The system of claim 1 wherein the policy causes the software application to display a system screen on the display screen of the mobile device when the vehicle speed exceeds the minimum threshold speed level.

Claim 41. The system of claim 1 wherein the policy immediately interrupts and disables the functions of the mobile device when the vehicle speed exceeds the minimum threshold speed level.

Claim 42. The system of claim 1 wherein the policy is associated with the vehicle.

Claim 43. The system of claim 1 wherein the policy is associated with the mobile device.

Claim 44. The system of claim 1 wherein the policy is only effective during predefined days of the week and hours of the day.

Claim 45. The system of claim 1 wherein the policy has a plurality of rules that vary as a function of predefined days of the week and hours of the day.

Claim 46. The system of claim 1 wherein the policy includes a plurality of rules that vary based upon the GPS-determined location of the mobile device.

Claim 47. The system of claim 1 wherein the policy defines a PIN or password that can be entered into the mobile device to enable all functions of the mobile device even if the vehicle is in motion.

Claim 48. The system of claim 1 wherein the policy defines a PIN or password that can be entered into the mobile device to enable predefined functions of the mobile device even if the vehicle is in motion.

Claim 49. The system of claim 1 wherein the policy prevents incoming calls from being received by the mobile device.

Petitioner Ex 1002, p. 239
Zimperium v. Taasera, IPR2024-00007

Claim 50. The system of claim 1 wherein the policy allows incoming calls to be received by the mobile device, but prevents any indication of the incoming call from being detected by or notified to a user of the mobile device until a later period of time.

Claim 51. The system of claim 1 wherein the policy routes incoming calls directly to voice mail.

Claim 52. The system of claim 1 wherein the policy prevents incoming and outgoing text messages.

Claim 53. The system of claim 1 wherein the policy disables the mobile device completely.

Claim 54. The system of claim 1 wherein the policy identifies specific numbers or contacts from which the mobile device can receive communications on an incoming basis even when the vehicle is in motion.

Claim 55. The system of claim 1 wherein the policy identifies specific numbers or contacts to which the mobile device is permitted to communicate on an outgoing basis even when the vehicle is in motion.

Claim 56. The system of claim 1 wherein the policy identifies specific applications that are usable or launchable by the mobile device even when the vehicle is in motion.

Claim 57. The system of claim 1 wherein the software application has a default policy that is associated with the software application when the software application is installed on the mobile device.

Claim 58. The system of claim 1 wherein the policy is customizable by an account administrator.

Petitioner Ex 1002, p. 240
Zimperium v. Taasera, IPR2024-00007

Claim 59. The system of claim 58 wherein the customized policy is distributed to a plurality of mobile devices.

Claim 60. The system of claim 58 wherein the customized policy is distributed to all employees of an organization.

Claim 61. The system of claim 58 wherein the customized policy is distributed to a subset of employees of an organization.

Claim 62. The system of claim 61 wherein the organization is a company.

Claim 63. The system of claim 61 wherein the organization is a governmental entity.

Claim 64. The system of claim 58 wherein the account administrator is an adult and the user of the mobile device is a dependent of the adult.

Claim 65. The system of claim 1 wherein insurance costs are reduced for an owner of the vehicle if the vehicle has the transmitter installed therein and if the software application is installed on the mobile device of one or more drivers of the vehicle.

Claim 66. The system of claim 1 wherein the mobile device first queries the transmitter to obtain a device name for the transmitter, after which the indication of speed data transmissions from the transmitter are receivable by the receiver of the mobile device.

Claim 67. The system of claim 1 wherein the transmitter is configured to transmit and the receiver is configured to receive additional data obtained from the on-board computer.

Claim 68. The system of claim 67 wherein the additional data includes an indication of whether the vehicle is turned on or off.

Petitioner Ex 1002, p. 241
Zimperium v. Taasera, IPR2024-00007

Claim 69. The system of claim 67 wherein the additional data includes an indication of what gear the vehicle is in.

Claim 70. The system of claim 67 wherein the additional data includes a device name for the transmitter.

Claim 71. The system of claim 70 wherein the indication of speed data is included as a variable in the device name transmitted by the transmitter.

Claim 72. The system of claim 1 wherein the policy is updated on the mobile device by means of a text message sent to the mobile device.

Claim 73. The system of claim 1 wherein the policy is updated on the mobile device when the mobile device is connected to the Internet.

Claim 74. The system of claim 1 wherein the policy is updated on the mobile device when the mobile device is synched with software installed on a computer of the user of the mobile device.

Petitioner Ex 1002, p. 242
Zimperium v. Taasera, IPR2024-00007

Claim 75. A computer program residing in computer-readable memory on a mobile device, wherein the mobile device includes a receiver, and further includes conventional firmware and hardware that enables the mobile device to engage in electronic communications and to perform other functions, the computer program comprising instructions that, when processed on a computer within the mobile device, causes the computer to:

whenever the mobile device is powered on, launch the computer program and maintain the computer program as an application running in the background of the mobile device;

periodically check, using the receiver, for a data signal transmission containing a transmitter identifier and an indication of speed data from a vehicle in proximity to the mobile device;

store a policy within memory on the mobile device, wherein the policy defines when and which functions of the mobile device will be disabled based on the indication of speed data obtained from the data signal transmission;

if an approved transmitter is identified by the transmitter identifier, extract and store the indication of speed data in memory on the mobile device; and

if the speed data indicates that the vehicle has exceeded a minimum threshold speed level, disabling selected functions of the mobile device according to the stored policy.

Claim 76. The computer program of claim 75 wherein the approved transmitter is in electronic communication with an on-board computer of the vehicle.

Claim 77. The computer program of claim 75 wherein the receiver checks for the data signal transmission on a first periodic basis until a first transmission is received and, thereafter, checks on a second, more frequent periodic basis thereafter.

Petitioner Ex 1002, p. 243
Zimperium v. Taasera, IPR2024-00007

Claim 78. The computer program of claim 77 wherein the receiver resumes checking for the data signal transmission on the first periodic basis after a predetermined period of time in which no data signal transmissions are received from the vehicle.

Claim 79. The computer program of claim 75 wherein the functions of the mobile device remain disabled for a predetermined period of time after the indication of speed transmission data indicates that the vehicle speed exceeds the minimum threshold speed level.

Claim 80. The computer program of claim 79 wherein the predetermined period of time in which the functions of the mobile device remain disabled is set according to the policy.

Claim 81. The computer program of claim 75 wherein the functions of the mobile device are enabled after the indication of speed transmission data indicates that the vehicle speed has been below the minimum threshold speed level for a predetermined period of time.

Claim 82. The computer program of claim 81 wherein the predetermined period of time in which the indication of speed transmission data indicates that the vehicle speed has been below the minimum threshold speed is set according to the policy.

Claim 83. The computer program of claim 77 wherein the functions of the mobile device are enabled after there are no data signal transmissions received by the receiver for a predetermined period of time.

Claim 84. The computer program of claim 75 wherein the mobile device includes one of a cell phone, smart phone, push-to-talk device, PDA, text or email dedicated device, general computer, laptop, electronic reading device, multimedia equipment, data tablet, and similar computing or communication device each having a display or interface that is usable by or accessible to a driver of the vehicle.

Petitioner Ex 1002, p. 244
Zimperium v. Taasera, IPR2024-00007

Claim 85. The computer program of claim 75 wherein functions on the mobile device include one or more of: making an outgoing call, receiving an incoming call, sending or receiving a text message, text chatting, sending or receiving an email, Internet browsing, and launching of a specified application installed on the mobile device.

Claim 86. The computer program of claim 75 wherein the indication of speed data identifies relative speed of the vehicle whether the vehicle is moving in the forward or reverse direction.

Claim 87. The computer program of claim 75 wherein the data transmission signal is configured to include an indication that the transmitter has been disabled.

Claim 88. The computer program of claim 75 wherein the data transmission signal is configured to include an indication that the transmitter has experienced a power interruption.

Claim 89. The computer program of claim 75 wherein the receiver receives the data transmission signal communicate through a wireless communication protocol.

Claim 90. The computer program of claim 89 wherein the wireless communication protocol is an RF communication protocol.

Claim 91. The computer program of claim 89 wherein the wireless communication protocol is a WiFi or Zigby communication protocol.

Claim 92. The computer program of claim 89 wherein the wireless communication protocol is a Bluetooth communication protocol.

Claim 93. The computer program of claim 92 wherein the transmitter and receiver are paired using the Bluetooth protocol.

Claim 94. The computer program of claim 92 wherein the transmitter broadcasts an indication of speed data without pairing with the receiver.

Petitioner Ex 1002, p. 245
Zimperium v. Taasera, IPR2024-00007

Claim 95. The computer program of claim 94 wherein numerous mobile devices are able to receive the transmitter broadcast because there is no specific Bluetooth pairing.

Claim 96. The system of claim 94 wherein the transmitter broadcasts speed data by embedding the speed data in its device name.

Claim 97. The system of claim 94 wherein the transmitter broadcasts additional data by embedding the additional data in its device name.

Claim 98. The computer program of claim 75 wherein the transmitter and receiver communicate through a wired connection between a data port of the vehicle and a data port of the mobile device.

Claim 99. The computer program of claim 75 wherein the indication of the speed data includes the actual speed of the vehicle.

Claim 100. The computer program of claim 99 wherein the policy defines the threshold speed level.

Claim 101. The computer program of claim 75 wherein the indication of the speed data includes a flag indicating that the speed of the vehicle is currently above the threshold speed level.

Claim 102. The computer program of claim 75 wherein the indication of the speed data includes the actual speed of the vehicle and the policy defines the threshold speed level.

Claim 103. The computer program of claim 75 wherein the policy prevents outgoing calls from the mobile device.

Claim 104. The computer program of claim 75 wherein the policy prevents the mobile device from accessing the phone functions on the mobile device.

Petitioner Ex 1002, p. 246
Zimperium v. Taasera, IPR2024-00007

Claim 105. The computer program of claim 75 wherein the policy disables the display screen of the mobile device.

Claim 106. The computer program of claim 75 wherein the policy causes the computer program to display a system screen on the display screen of the mobile device when the vehicle speed exceeds the minimum threshold speed level.

Claim 107. The computer program of claim 75 wherein the policy immediately interrupts and disables the functions of the mobile device when the vehicle speed exceeds the minimum threshold speed level.

Claim 108. The computer program of claim 75 wherein the policy is associated with the vehicle.

Claim 109. The computer program of claim 75 wherein the policy is associated with the mobile device.

Claim 110. The computer program of claim 75 wherein the policy is only effective during predefined days of the week and hours of the day.

Claim 111. The computer program of claim 75 wherein the policy has a plurality of rules that vary as a function of predefined days of the week and hours of the day.

Claim 112. The computer program of claim 75 wherein the policy includes a plurality of rules that vary based upon the GPS-determined location of the mobile device.

Claim 113. The computer program of claim 75 wherein the policy defines a PIN or password that can be entered into the mobile device to enable all functions of the mobile device even if the vehicle is in motion.

Petitioner Ex 1002, p. 247
Zimperium v. Taasera, IPR2024-00007

Claim 114. The computer program of claim 75 wherein the policy defines a PIN or password that can be entered into the mobile device to enable predefined functions of the mobile device even if the vehicle is in motion.

Claim 115. The computer program of claim 75 wherein the policy prevents incoming calls from being received by the mobile device.

Claim 116. The computer program of claim 75 wherein the policy allows incoming calls to be received by the mobile device, but prevents any indication of the incoming call from being detected by or notified to a user of the mobile device until a later period of time.

Claim 117. The computer program of claim 75 wherein the policy routes incoming calls directly to voice mail.

Claim 118. The computer program of claim 75 wherein the policy prevents incoming and outgoing text messages.

Claim 119. The computer program of claim 75 wherein the policy disables the mobile device completely.

Claim 120. The computer program of claim 75 wherein the policy identifies specific numbers or contacts from which the mobile device can receive communications on an incoming basis even when the vehicle is in motion.

Claim 121. The computer program of claim 75 wherein the policy identifies specific numbers or contacts to which the mobile device is permitted to communicate on an outgoing basis even when the vehicle is in motion.

Claim 122. The computer program of claim 75 wherein the policy identifies specific applications that are usable and launchable by the mobile device even when the vehicle is in motion.

Petitioner Ex 1002, p. 248
Zimperium v. Taasera, IPR2024-00007

Claim 123. The computer program of claim 75 wherein the policy stored within memory on the mobile device is a default policy that is installed when the computer program is installed on the mobile device.

Claim 124. The computer program of claim 75 wherein the policy is customizable by an account administrator.

Claim 125. The computer program of claim 124 wherein the customized policy is distributed to a plurality of mobile devices.

Claim 126. The computer program of claim 124 wherein the customized policy is distributed to all employees of an organization.

Claim 127. The computer program of claim 124 wherein the customized policy is distributed to a subset of employees of an organization.

Claim 128. The computer program of claim 127 wherein the organization is a company.

Claim 129. The computer program of claim 127 wherein the organization is a governmental entity.

Claim 130. The computer program of claim 124 wherein the account administrator is an adult and the user of the mobile device is a dependent of the adult.

Claim 131. The computer program of claim 75 wherein insurance costs are reduced for an owner of the vehicle if the vehicle has the transmitter installed therein and if the computer program is installed on the mobile device of one or more drivers of the vehicle.

Claim 132. The computer program of claim 75 wherein the computer program first queries the transmitter to obtain the transmitter identifier, after which the indication of speed data transmissions from the transmitter are receivable by the receiver of the mobile device.

Petitioner Ex 1002, p. 249
Zimperium v. Taasera, IPR2024-00007

Claim 133. The computer program of claim 75 wherein the transmitter is configured to transmit and the receiver is configured to receive additional data obtained from the on-board computer.

Claim 134. The computer program of claim 133 wherein the additional data includes an indication of whether the vehicle is turned on or off.

Claim 135. The computer program of claim 133 wherein the additional data includes an indication of what gear the vehicle is in.

Claim 136. The computer program of claim 133 wherein the additional data includes a device name for the transmitter.

Claim 137. The computer program of claim 136 wherein the indication of speed data is included as a variable in the device name transmitted by the transmitter.

Claim 138. The computer program of claim 75 wherein the policy is updated on the mobile device by means of a text message sent to the mobile device.

Claim 139. The computer program of claim 75 wherein the policy is updated on the mobile device when the mobile device is connected to the Internet.

Claim 140. The computer program of claim 75 wherein the policy is updated on the mobile device when the mobile device is synched with software installed on a computer of the user of the mobile device.

Petitioner Ex 1002, p. 250
Zimperium v. Taasera, IPR2024-00007

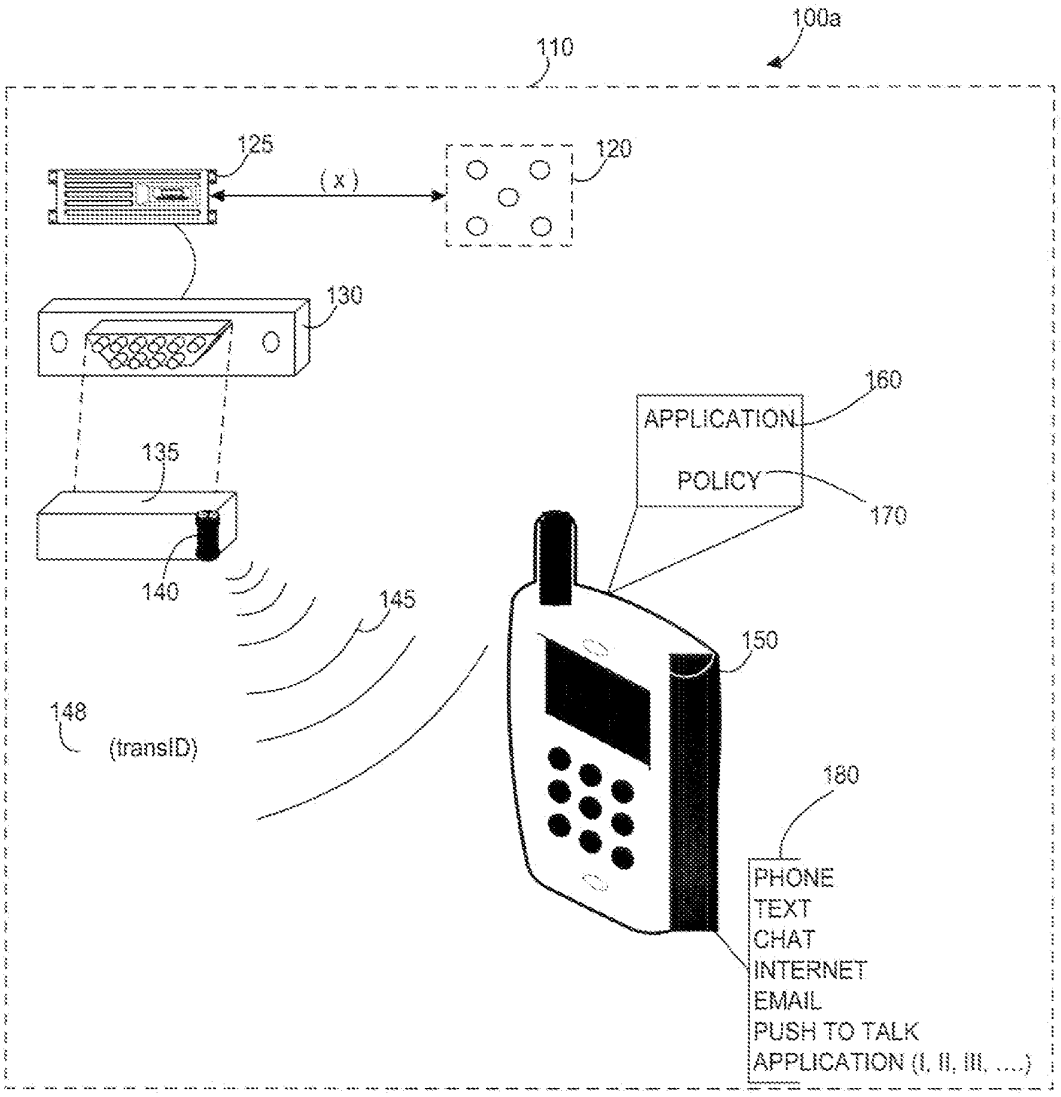

100a
110
125
(x)
120
130
135
140
145
148
(transID)
160
APPLICATION
POLICY
170
150
180
PHONE
TEXT
CHAT
INTERNET
EMAIL
PUSH TO TALK
APPLICATION (I, II, III, ...)

FIG. 1A

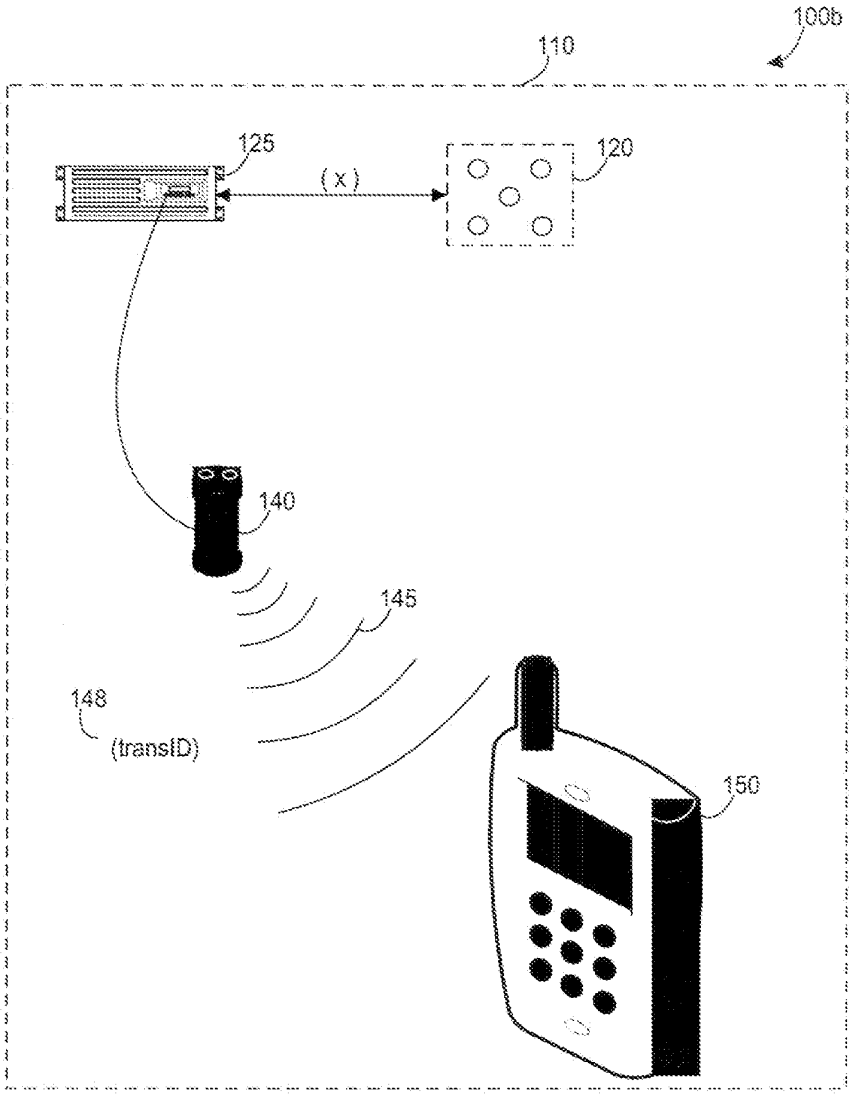


FIG. 1B

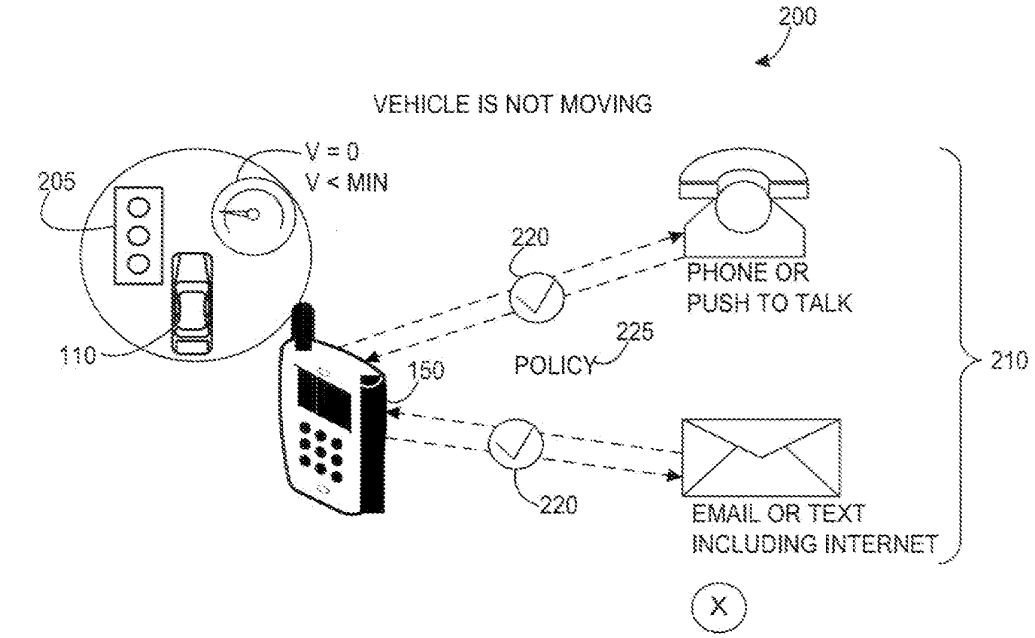

200
VEHICLE IS NOT MOVING
V = 0
V < MIN
205
110
220
PHONE OR
PUSH TO TALK
225
POLICY
150
210
220
EMAIL OR TEXT
INCLUDING INTERNET
X
VEHICLE IS MOVING
V > MIN
205
ONLY EMERGENCY
OR PREDEFINED
NUMBER
220
X
PHONE OR
PUSH TO TALK
110
225
POLICY
150
260
X
220
SENT TO VOICEMAIL
AIR MAILBOX
EMAIL OR TEXT
INCLUDING INTERNET

FIG. 2

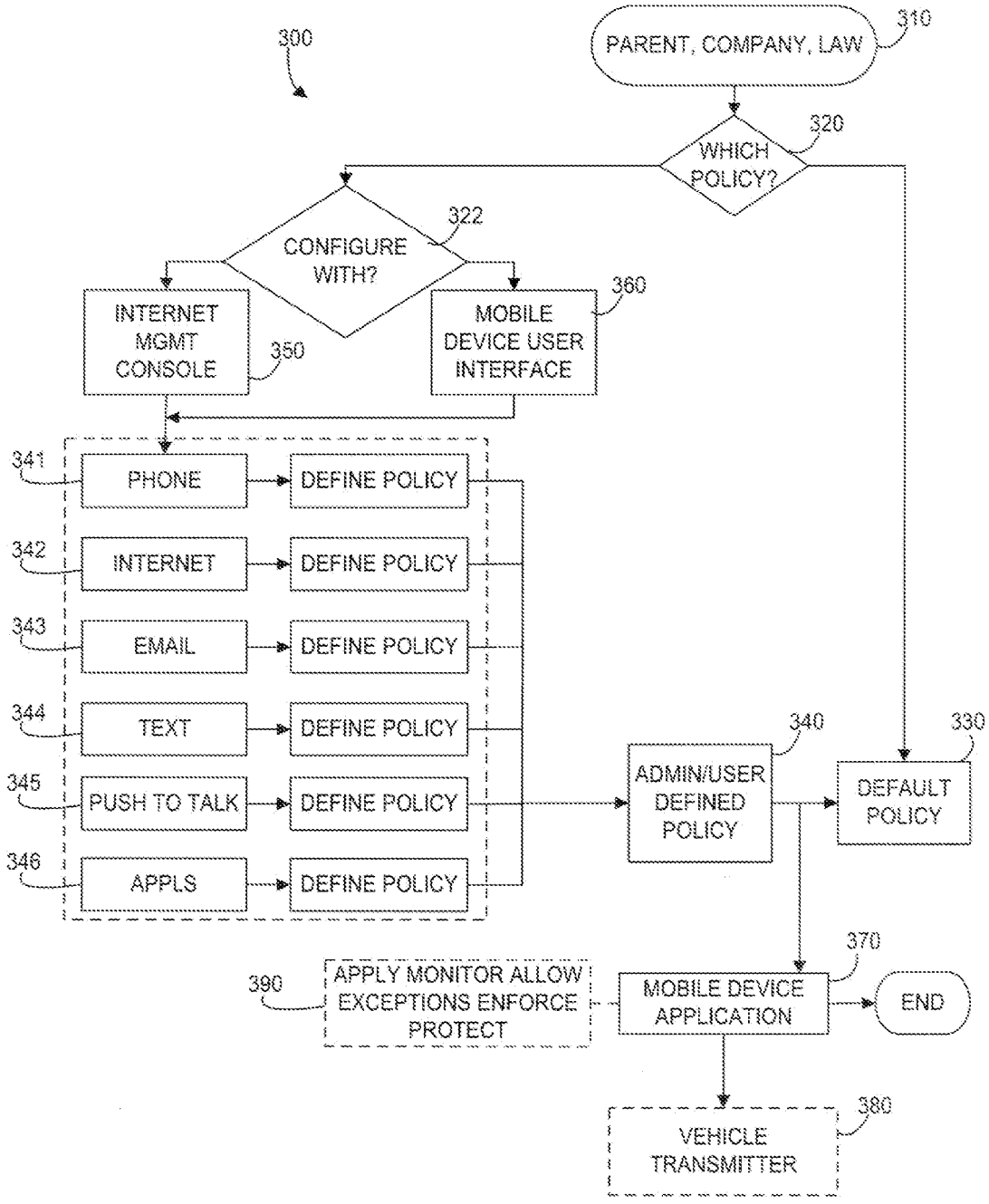

300
PARENT, COMPANY, LAW
310
WHICH POLICY?
320
CONFIGURE WITH?
322
INTERNET MGMT CONSOLE
350
MOBILE DEVICE USER INTERFACE
360
341
PHONE
DEFINE POLICY
342
INTERNET
DEFINE POLICY
343
EMAIL
DEFINE POLICY
344
TEXT
DEFINE POLICY
345
PUSH TO TALK
DEFINE POLICY
346
APPLS
DEFINE POLICY
340
ADMIN/USER DEFINED POLICY
330
DEFAULT POLICY
370
390
APPLY MONITOR ALLOW EXCEPTIONS ENFORCE PROTECT
MOBILE DEVICE APPLICATION
END
380
VEHICLE TRANSMITTER

FIG. 3

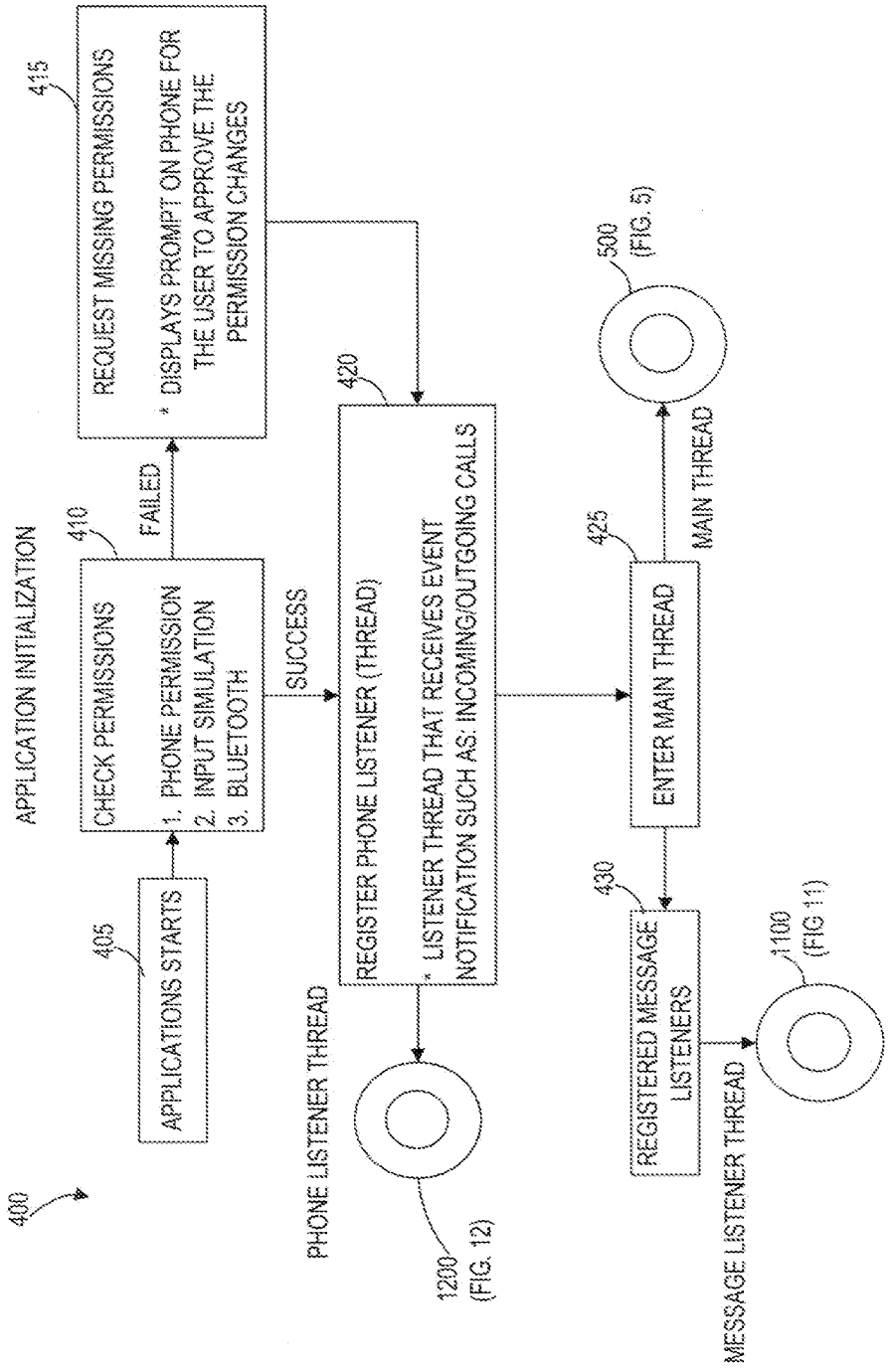

400
APPLICATION INITIALIZATION
405
APPLICATIONS STARTS
410
CHECK PERMISSIONS
1. PHONE PERMISSION
2. INPUT SIMULATION
3. BLUETOOTH
FAILED
SUCCESS
415
REQUEST MISSING PERMISSIONS
* DISPLAYS PROMPT ON PHONE FOR THE USER TO APPROVE THE PERMISSION CHANGES
420
REGISTER PHONE LISTENER (THREAD)
* LISTENER THREAD THAT RECEIVES EVENT NOTIFICATION SUCH AS: INCOMING/OUTGOING CALLS
PHONE LISTENER THREAD
1200
(FIG. 12)
425
ENTER MAIN THREAD
MAIN THREAD
500
(FIG. 5)
430
REGISTERED MESSAGE LISTENERS
MESSAGE LISTENER THREAD
1100
(FIG 11)

FIG. 4

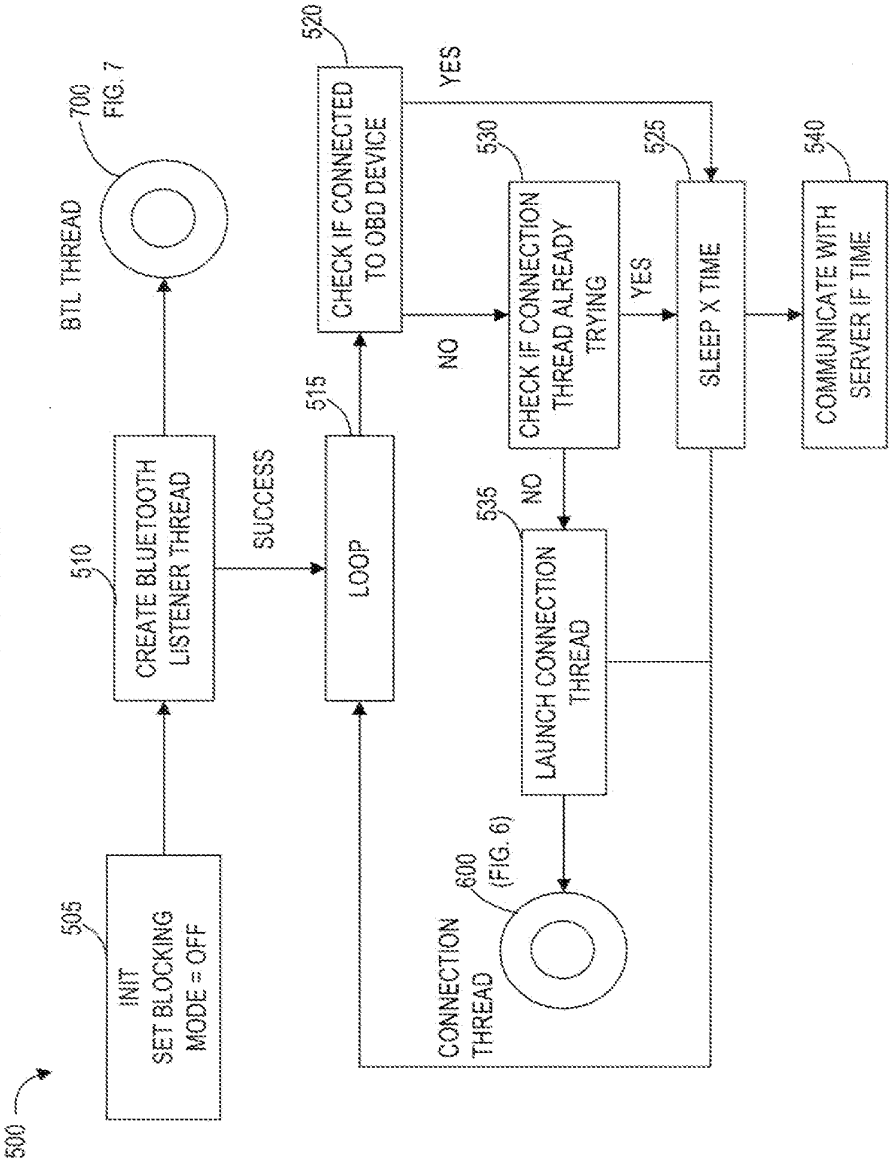

500
MAIN THREAD
505
INIT
SET BLOCKING
MODE = OFF
510
CREATE BLUETOOTH
LISTENER THREAD
700
FIG. 7
BTL THREAD
SUCCESS
515
LOOP
520
CHECK IF CONNECTED
TO OBD DEVICE
YES
NO
530
CHECK IF CONNECTION
THREAD ALREADY
TRYING
YES
525
SLEEP X TIME
540
COMMUNICATE WITH
SERVER IF TIME
NO
535
LAUNCH CONNECTION
THREAD
600
(FIG. 6)
CONNECTION
THREAD

FIG. 5

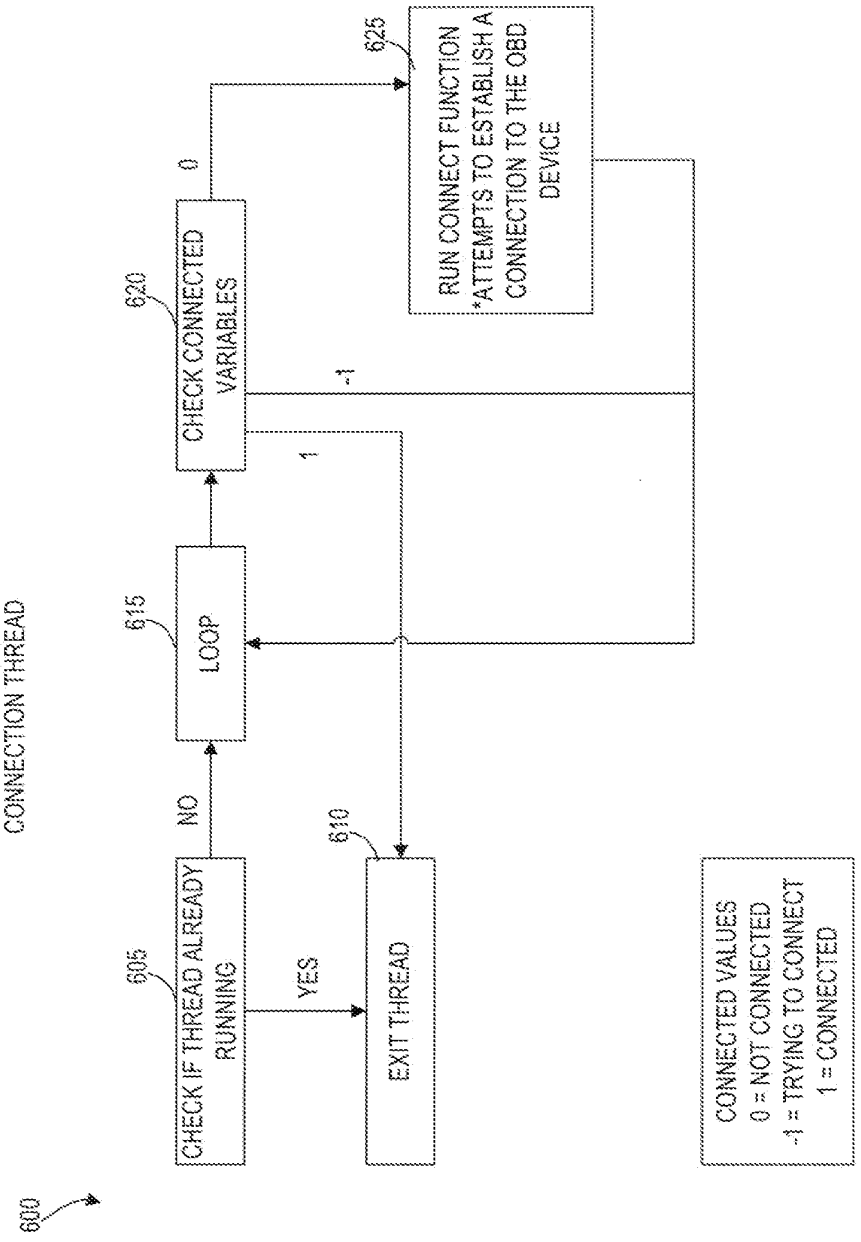

CONNECTION THREAD
600
CHECK IF THREAD ALREADY RUNNING
605
YES
EXIT THREAD
610
NO
LOOP
615
CHECK CONNECTED VARIABLES
620
0
-1
1
RUN CONNECT FUNCTION *ATTEMPTS TO ESTABLISH A CONNECTION TO THE OBD DEVICE
625
CONNECTED VALUES
0 = NOT CONNECTED
-1 = TRYING TO CONNECT
1 = CONNECTED

FIG. 6

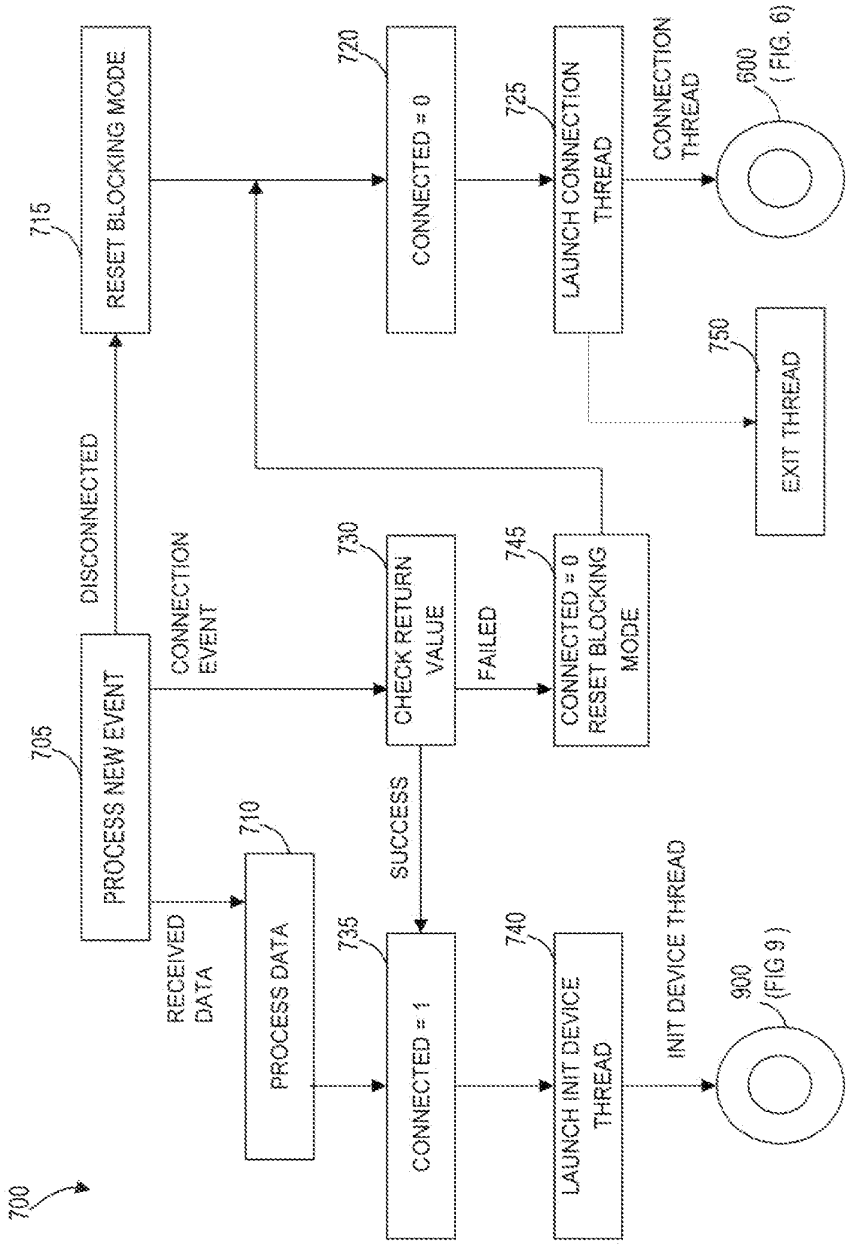

BLUETOOTH LISTENER THREAD
700
705
PROCESS NEW EVENT
DISCONNECTED
715
RESET BLOCKING MODE
720
CONNECTED = 0
725
LAUNCH CONNECTION THREAD
CONNECTION THREAD
600 (FIG. 6)
750
EXIT THREAD
CONNECTION EVENT
730
CHECK RETURN VALUE
FAILED
745
CONNECTED = 0 RESET BLOCKING MODE
RECEIVED DATA
710
PROCESS DATA
SUCCESS
735
CONNECTED = 1
740
LAUNCH INIT DEVICE THREAD
INIT DEVICE THREAD
900 (FIG 9)

FIG. 7

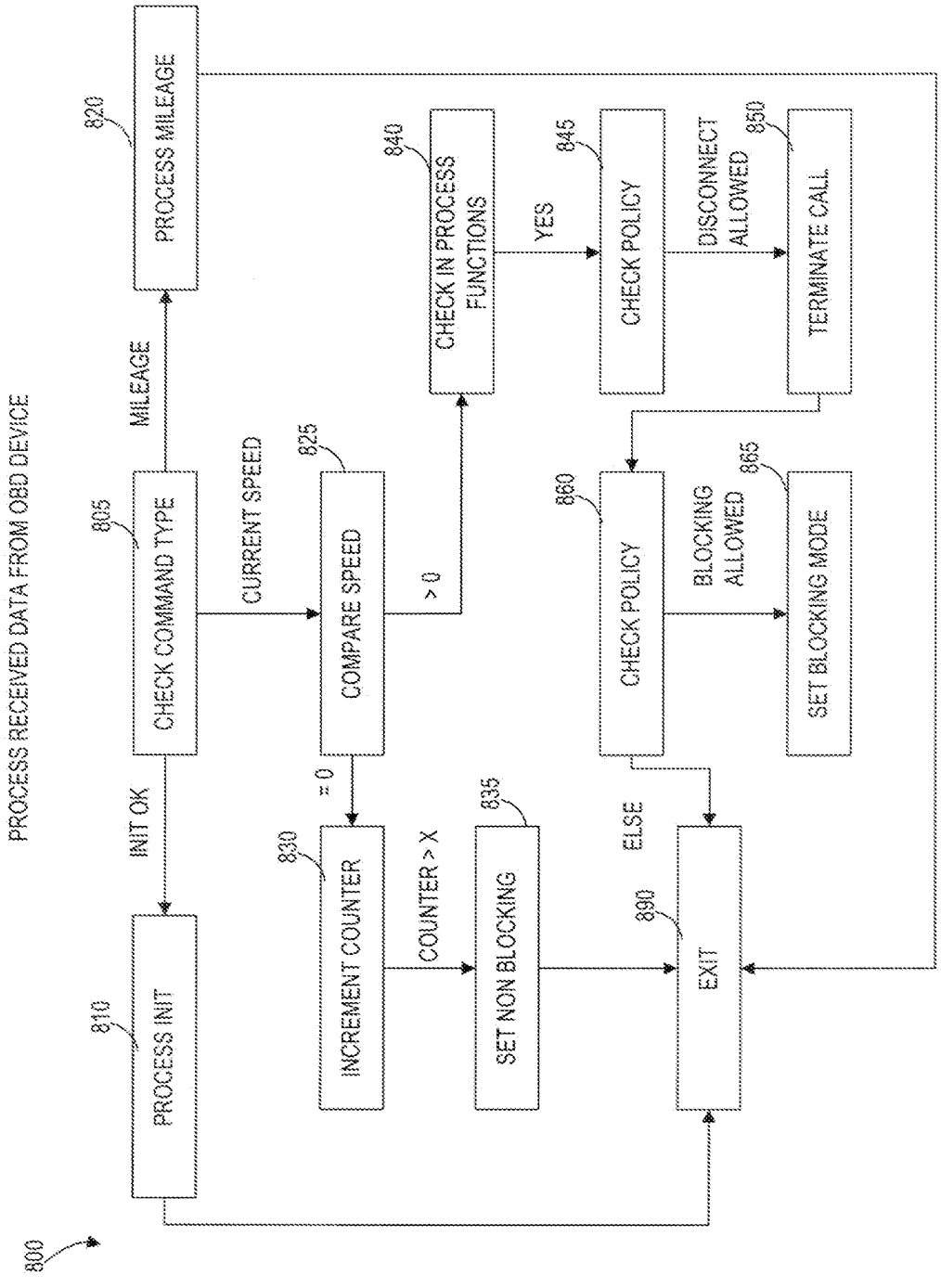

PROCESS RECEIVED DATA FROM OBD DEVICE
800
PROCESS INIT
810
INIT OK
CHECK COMMAND TYPE
805
MILEAGE
PROCESS MILEAGE
820
CURRENT SPEED
COMPARE SPEED
825
= 0
INCREMENT COUNTER
830
COUNTER > X
SET NON BLOCKING
835
> 0
CHECK IN PROCESS FUNCTIONS
840
YES
CHECK POLICY
845
DISCONNECT ALLOWED
TERMINATE CALL
850
CHECK POLICY
860
BLOCKING ALLOWED
SET BLOCKING MODE
865
ELSE
EXIT
890

FIG. 8

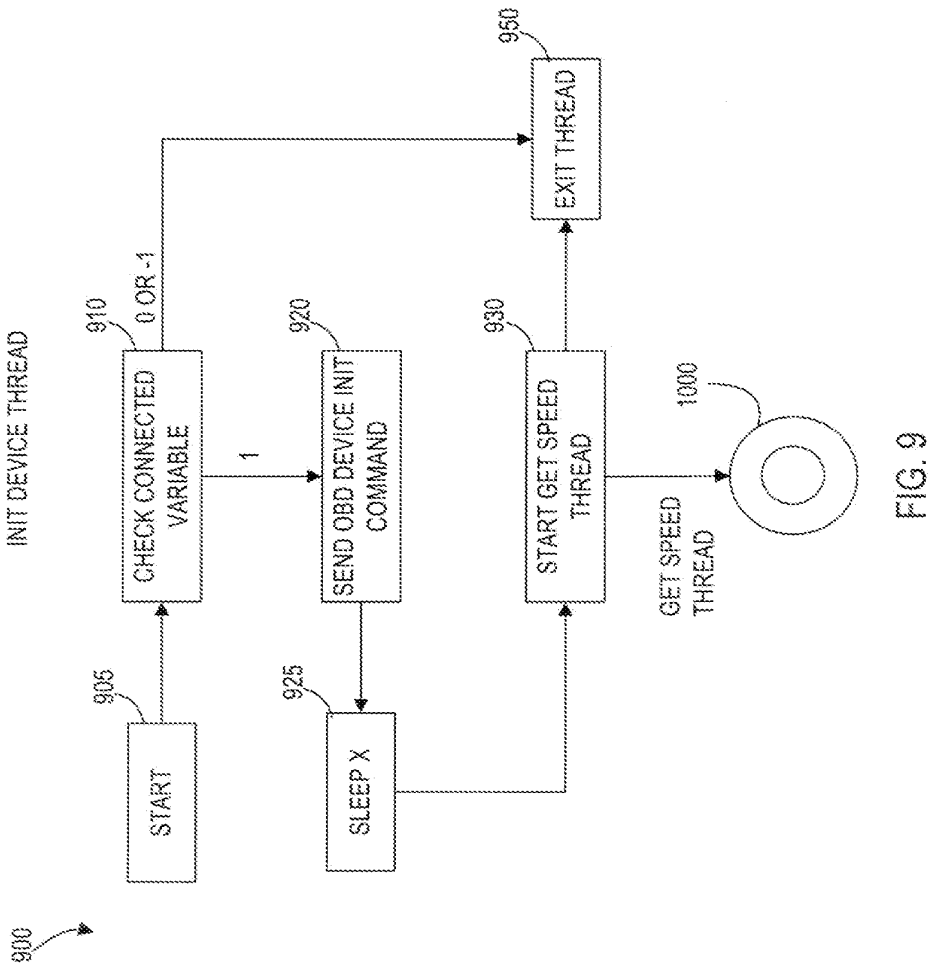

INIT DEVICE THREAD
900
START
905
CHECK CONNECTED VARIABLE
910
0 OR -1
1
SEND OBD DEVICE INIT COMMAND
920
SLEEP X
925
START GET SPEED THREAD
930
EXIT THREAD
950
GET SPEED THREAD
1000

FIG. 9

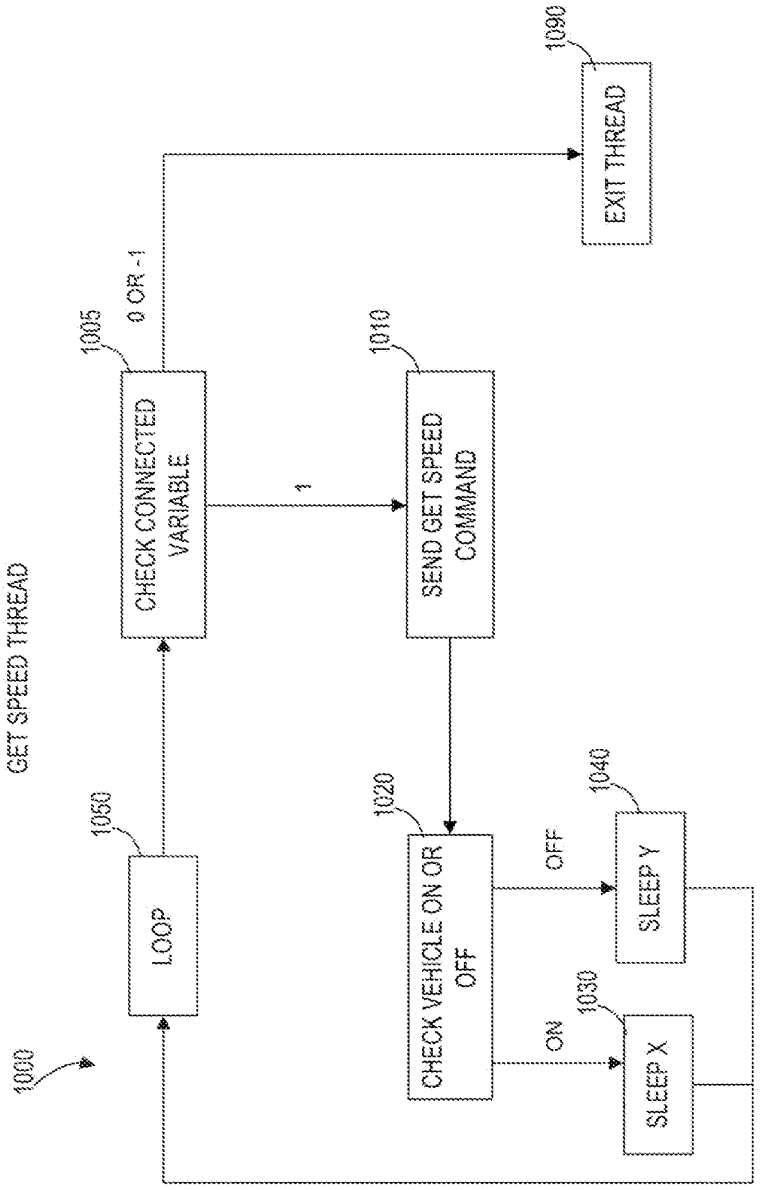

GET SPEED THREAD
1000
1050
LOOP
1005
CHECK CONNECTED VARIABLE
0 OR -1
1
1010
SEND GET SPEED COMMAND
1020
CHECK VEHICLE ON OR OFF
OFF
ON
1040
SLEEP Y
1030
SLEEP X
1090
EXIT THREAD

FIG. 10

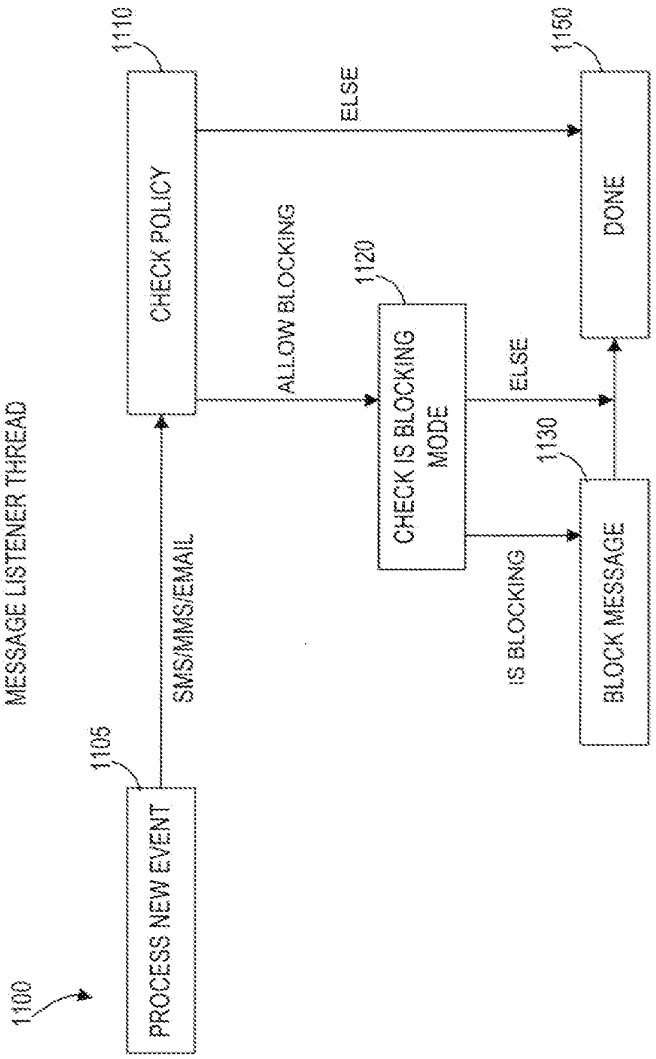

MESSAGE LISTENER THREAD
1100
PROCESS NEW EVENT
1105
SMS/MMS/EMAIL
CHECK POLICY
1110
ELSE
ALLOW BLOCKING
CHECK IS BLOCKING MODE
1120
ELSE
IS BLOCKING
BLOCK MESSAGE
1130
DONE
1150

FIG. 11

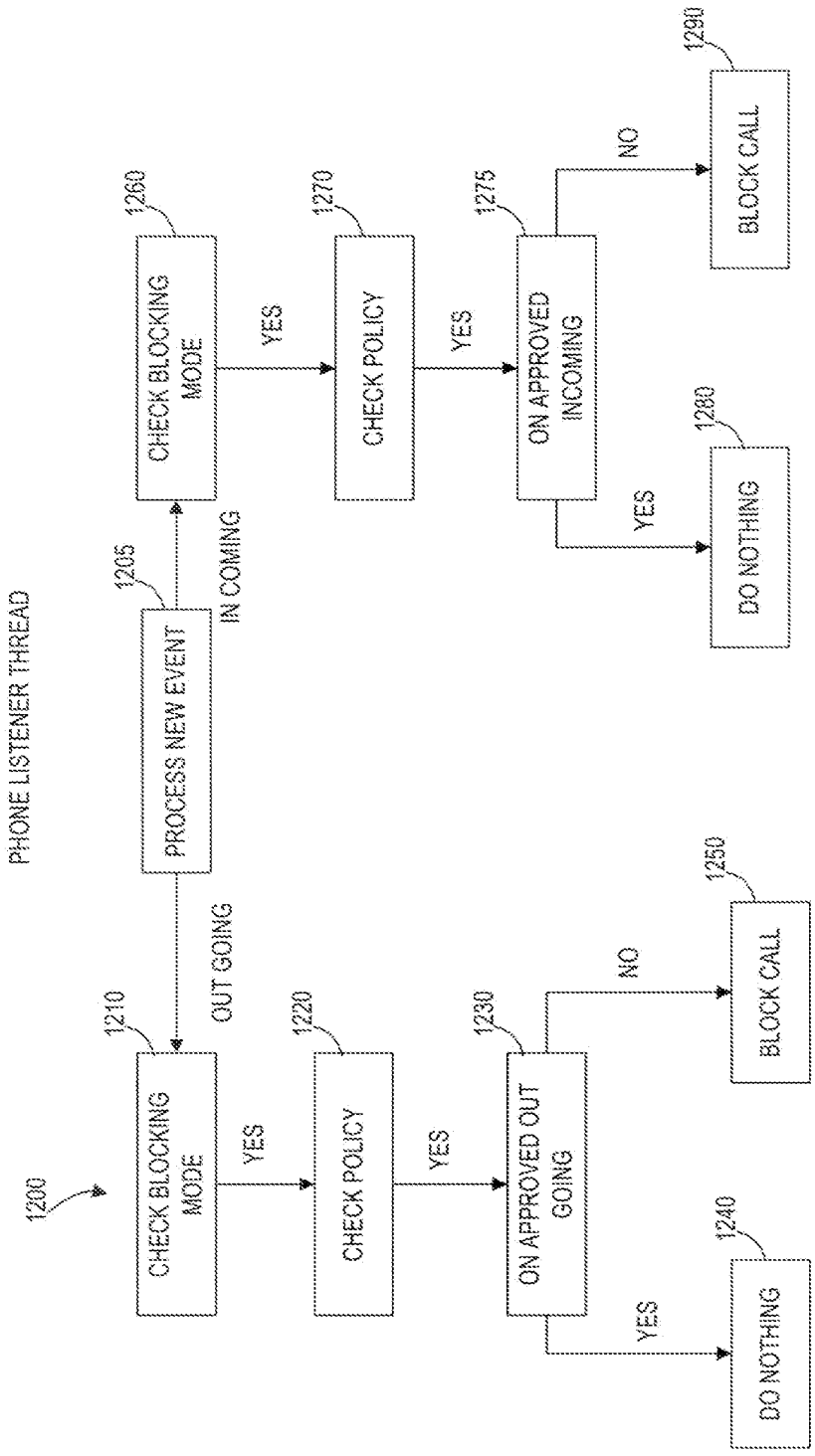

PHONE LISTENER THREAD
1200
CHECK BLOCKING MODE
1210
YES
CHECK POLICY
1220
YES
ON APPROVED OUT GOING
1230
NO
BLOCK CALL
1250
YES
DO NOTHING
1240
OUT GOING
PROCESS NEW EVENT
1205
IN COMING
CHECK BLOCKING MODE
1260
YES
CHECK POLICY
1270
YES
ON APPROVED INCOMING
1275
NO
BLOCK CALL
1290
YES
DO NOTHING
1280

FIG. 12

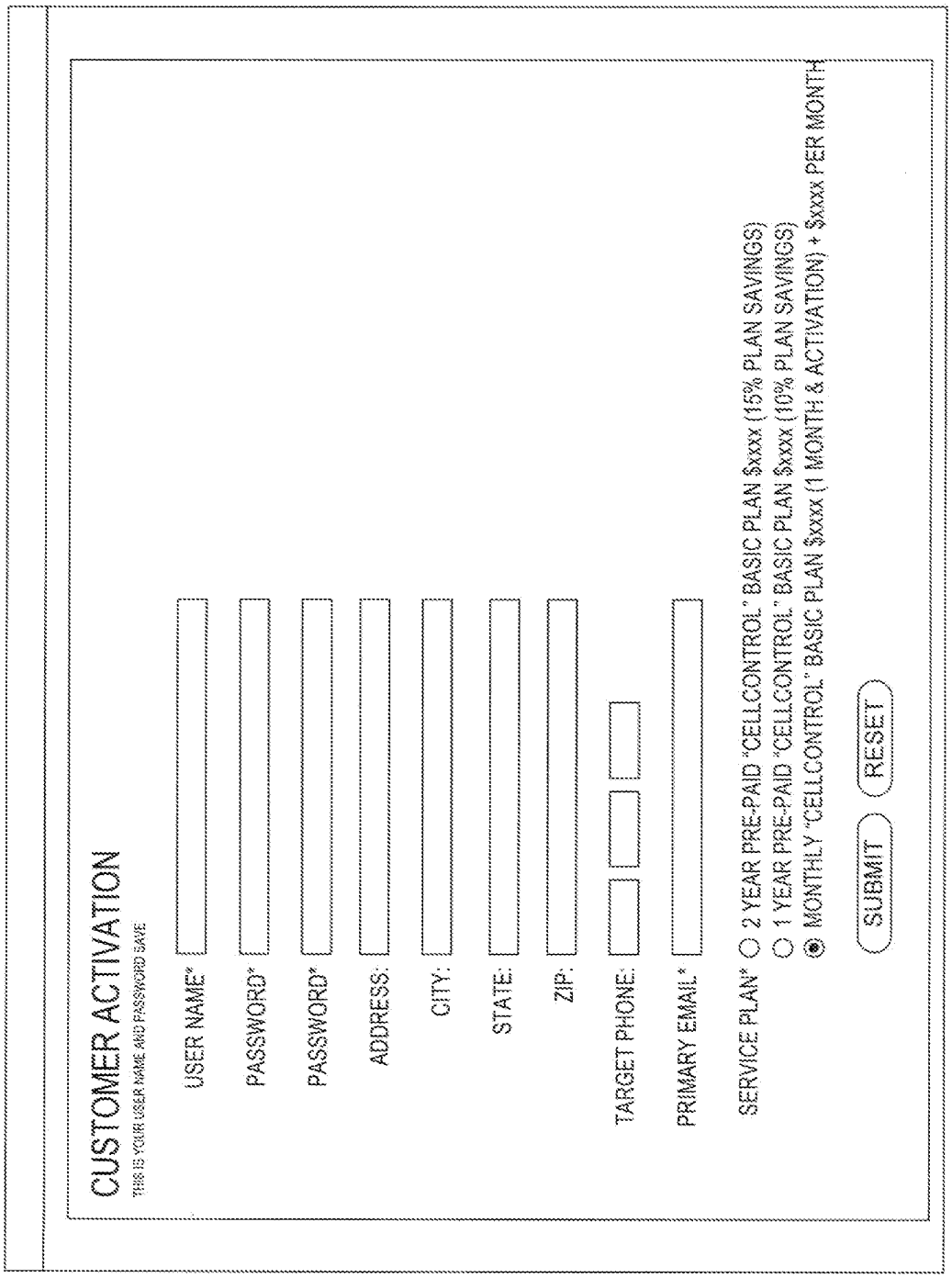

CUSTOMER ACTIVATION
THIS IS YOUR USER NAME AND PASSWORD SAVE
USER NAME*
PASSWORD*
PASSWORD*
ADDRESS:
CITY:
STATE:
ZIP:
TARGET PHONE:
PRIMARY EMAIL*
SERVICE PLAN*
2 YEAR PRE-PAID "CELLCONTROL" BASIC PLAN $xxxx (15% PLAN SAVINGS)
1 YEAR PRE-PAID "CELLCONTROL" BASIC PLAN $xxxx (10% PLAN SAVINGS)
MONTHLY "CELLCONTROL" BASIC PLAN $xxxx (1 MONTH & ACTIVATION) + $xxxx PER MONTH
SUBMIT
RESET

FIG. 13

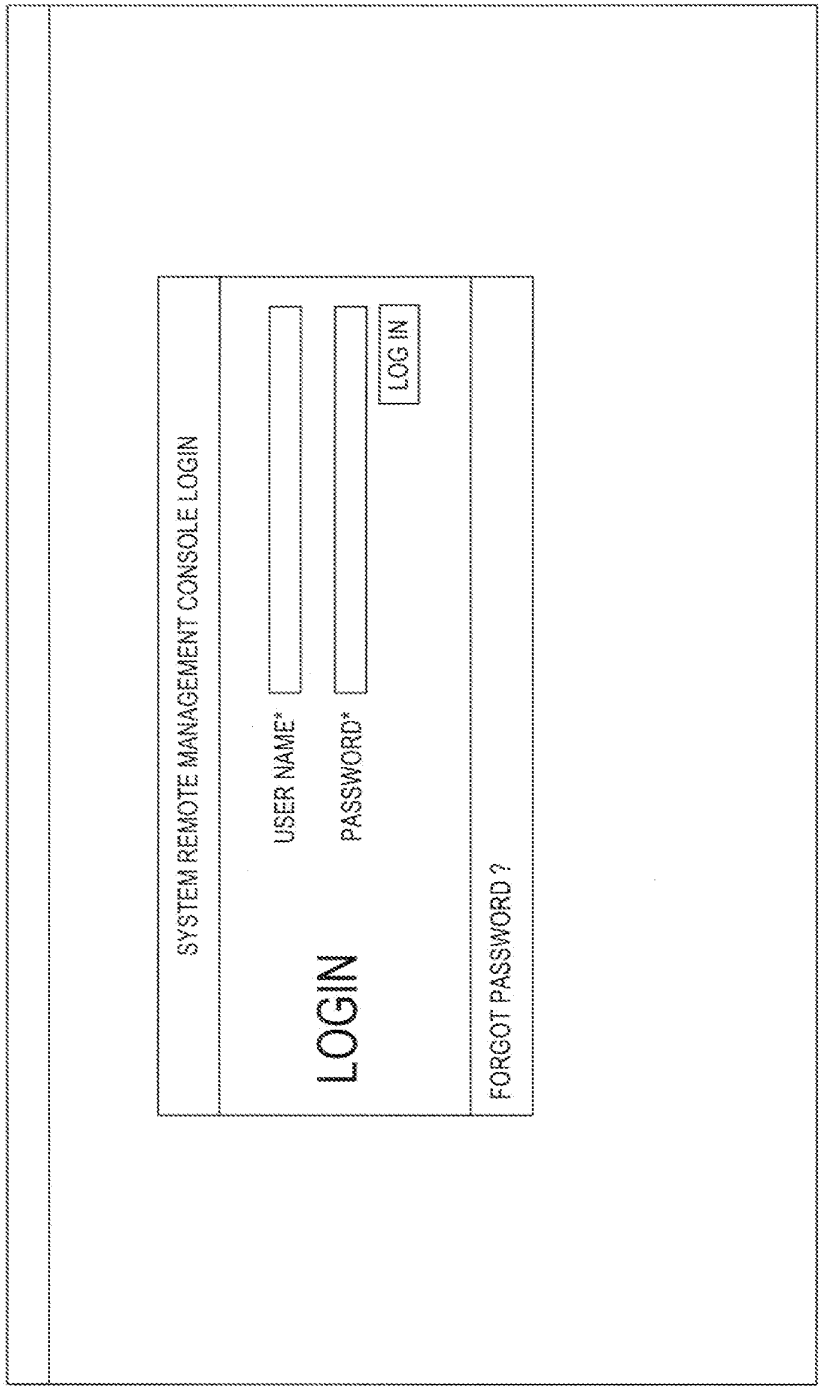

SYSTEM REMOTE MANAGEMENT CONSOLE LOGIN
LOGIN
USER NAME*
PASSWORD*
LOG IN
FORGOT PASSWORD ?

FIG. 14

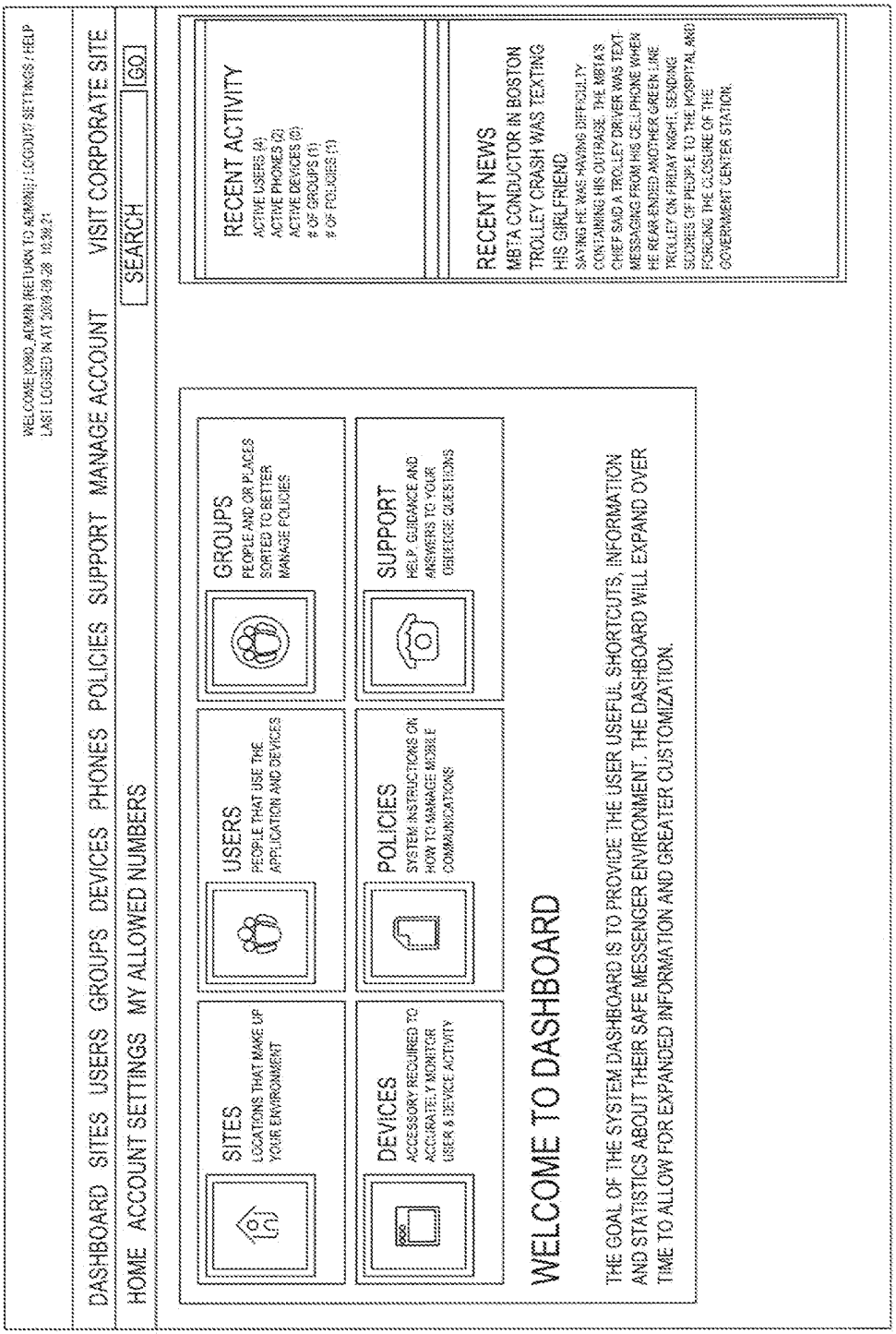

WELCOME [ID#0] ADMIN [RETURN TO ADMIN] | LOGOUT SETTINGS / HELP
LAST LOGGED IN AT 2009-09-08 10:38:21
DASHBOARD SITES USERS GROUPS DEVICES PHONES POLICIES SUPPORT MANAGE ACCOUNT VISIT CORPORATE SITE
HOME ACCOUNT SETTINGS MY ALLOWED NUMBERS
SEARCH
GO
SITES
LOCATIONS THAT MAKE UP YOUR ENVIRONMENT
USERS
PEOPLE THAT USE THE APPLICATION AND DEVICES
GROUPS
PEOPLE AND OR PLACES SORTED TO BETTER MANAGE POLICIES
DEVICES
ACCESSORY REQUIRED TO ACCURATELY MONITOR USER & DEVICE ACTIVITY
POLICIES
SYSTEM INSTRUCTIONS ON HOW TO MANAGE MOBILE COMMUNICATIONS
SUPPORT
HELP, GUIDANCE AND ANSWERS TO YOUR OBSERVE QUESTIONS
WELCOME TO DASHBOARD
THE GOAL OF THE SYSTEM DASHBOARD IS TO PROVIDE THE USER USEFUL SHORTCUTS, INFORMATION AND STATISTICS ABOUT THEIR SAFE MESSENGER ENVIRONMENT. THE DASHBOARD WILL EXPAND OVER TIME TO ALLOW FOR EXPANDED INFORMATION AND GREATER CUSTOMIZATION.
RECENT ACTIVITY
ACTIVE USERS (8)
ACTIVE PHONES (2)
ACTIVE DEVICES (6)
OF GROUPS (1)
OF POLICIES (1)
RECENT NEWS
MBTA CONDUCTOR IN BOSTON TROLLEY CRASH WAS TEXTING HIS GIRLFRIEND
SAYING HE WAS HAVING DIFFICULTY CONTAINING HIS OUTRAGE. THE MBTA'S CHIEF SAID A TROLLEY DRIVER WAS TEXT MESSAGING FROM HIS CELLPHONE WHEN HE REAR-ENDED ANOTHER GREEN LINE TROLLEY ON FRIDAY NIGHT, SENDING SCORES OF PEOPLE TO THE HOSPITAL AND FORCING THE CLOSURE OF THE GOVERNMENT CENTER STATION.

FIG. 15

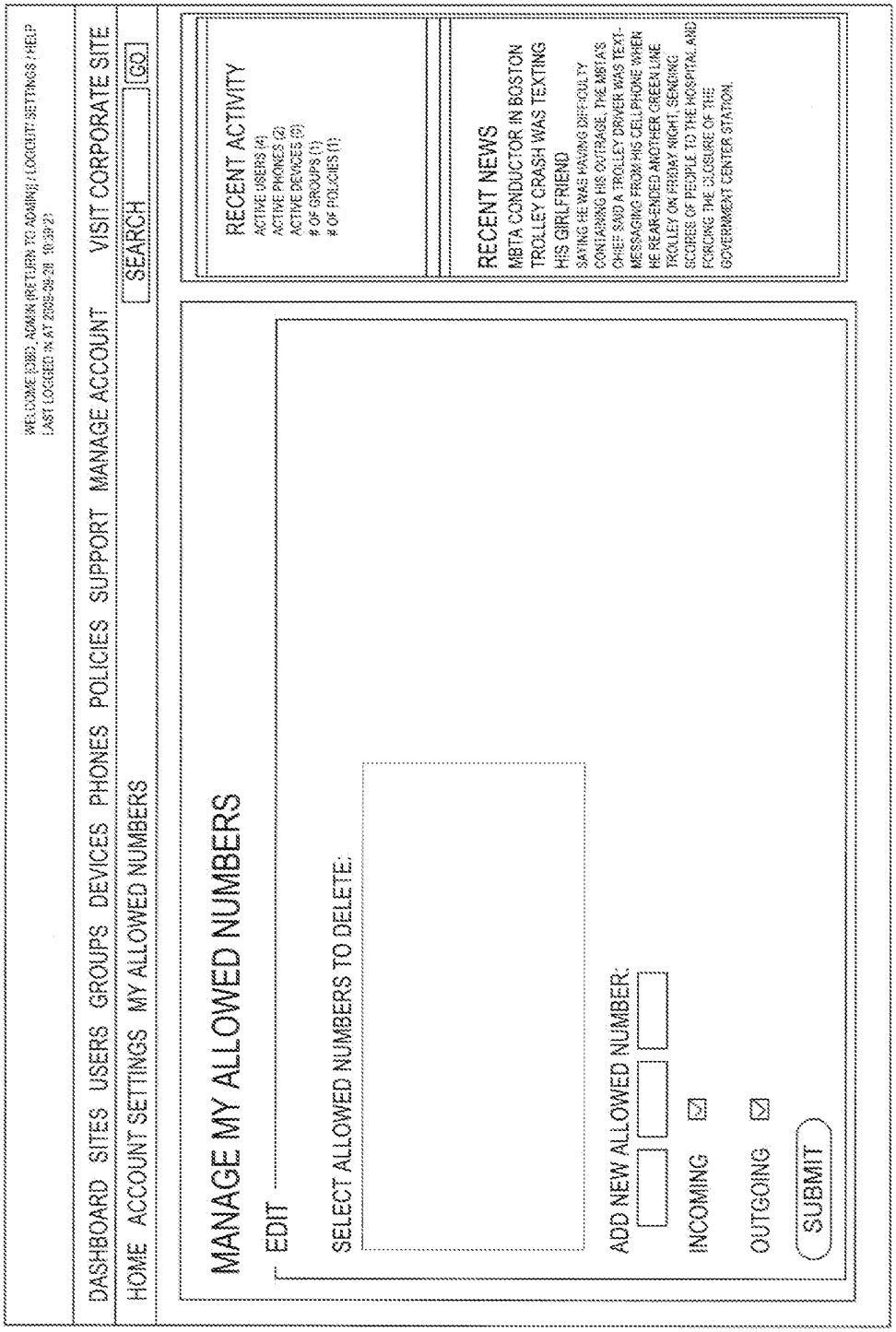

WELCOME [USER], ADMIN (RETURN TO ADMIN) | LOGOUT/ SETTINGS / HELP
LAST LOGGED IN AT 2009-06-28 10:39:27
DASHBOARD SITES USERS GROUPS DEVICES PHONES POLICIES SUPPORT MANAGE ACCOUNT VISIT CORPORATE SITE
HOME ACCOUNT SETTINGS MY ALLOWED NUMBERS
SEARCH
GO
MANAGE MY ALLOWED NUMBERS
EDIT
SELECT ALLOWED NUMBERS TO DELETE:
ADD NEW ALLOWED NUMBER:
INCOMING
OUTGOING
SUBMIT
RECENT ACTIVITY
ACTIVE USERS (4)
ACTIVE PHONES (2)
ACTIVE DEVICES (5)
OF GROUPS (1)
OF POLICIES (1)
RECENT NEWS
MBTA CONDUCTOR IN BOSTON TROLLEY CRASH WAS TEXTING HIS GIRLFRIEND
SAYING HE WAS HAVING DIFFICULTY CONTACTING HIS OUTBACK, THE MBTA'S CHIEF SAID A TROLLEY DRIVER WAS TEXT-MESSAGING FROM HIS CELLPHONE WHEN HE REAR-ENDED ANOTHER GREEN LINE TROLLEY ON FRIDAY NIGHT, SENDING SCORES OF PEOPLE TO THE HOSPITAL AND FORCING THE CLOSURE OF THE GOVERNMENT CENTER STATION.

FIG. 16

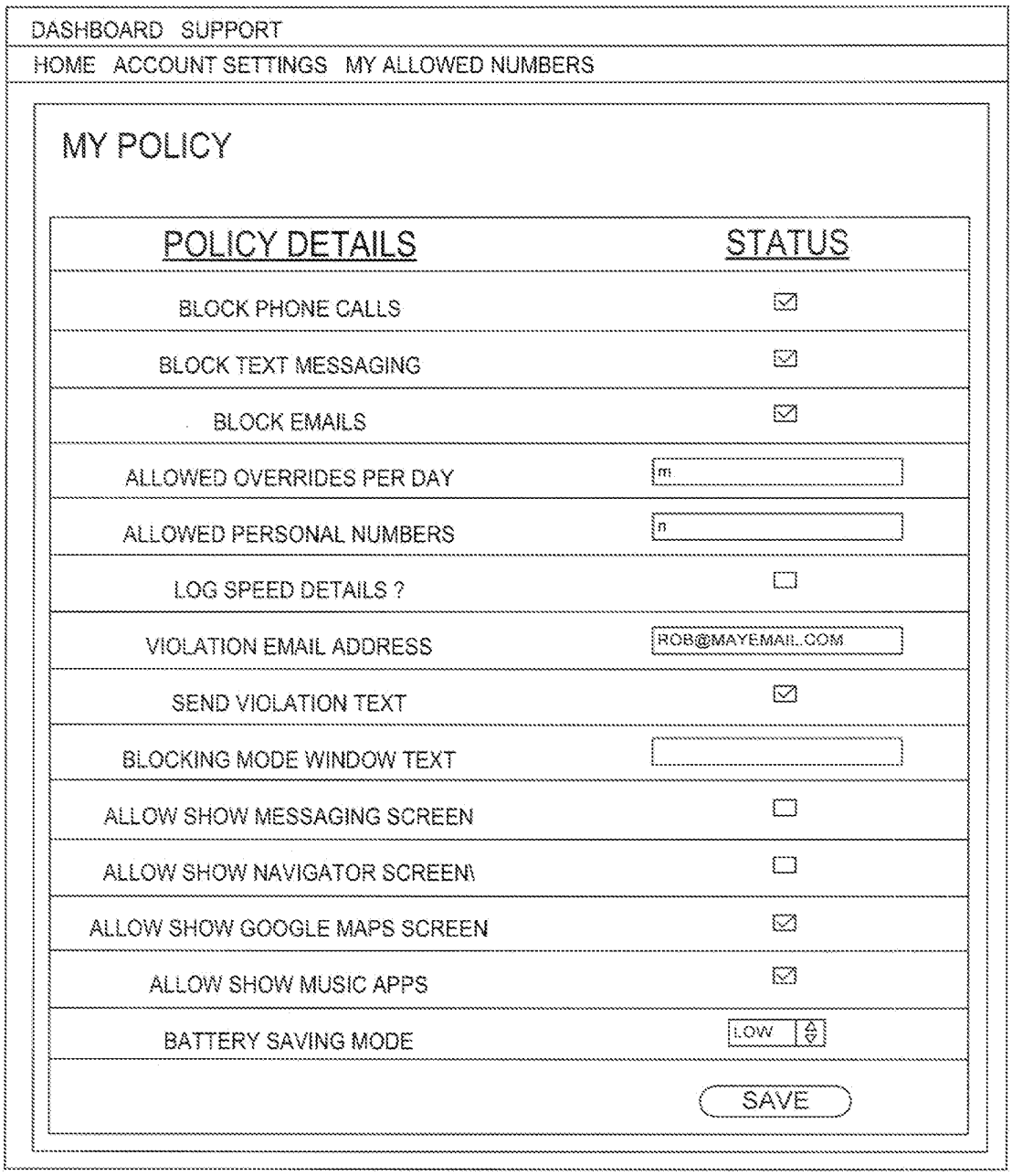

DASHBOARD SUPPORT
HOME ACCOUNT SETTINGS MY ALLOWED NUMBERS
MY POLICY
POLICY DETAILS
STATUS
BLOCK PHONE CALLS
BLOCK TEXT MESSAGING
BLOCK EMAILS
ALLOWED OVERRIDES PER DAY
m
ALLOWED PERSONAL NUMBERS
n
LOG SPEED DETAILS ?
VIOLATION EMAIL ADDRESS
ROB@MAYEMAIL.COM
SEND VIOLATION TEXT
BLOCKING MODE WINDOW TEXT
ALLOW SHOW MESSAGING SCREEN
ALLOW SHOW NAVIGATOR SCREEN\
ALLOW SHOW GOOGLE MAPS SCREEN
ALLOW SHOW MUSIC APPS
BATTERY SAVING MODE
LOW
SAVE

FIG. 17

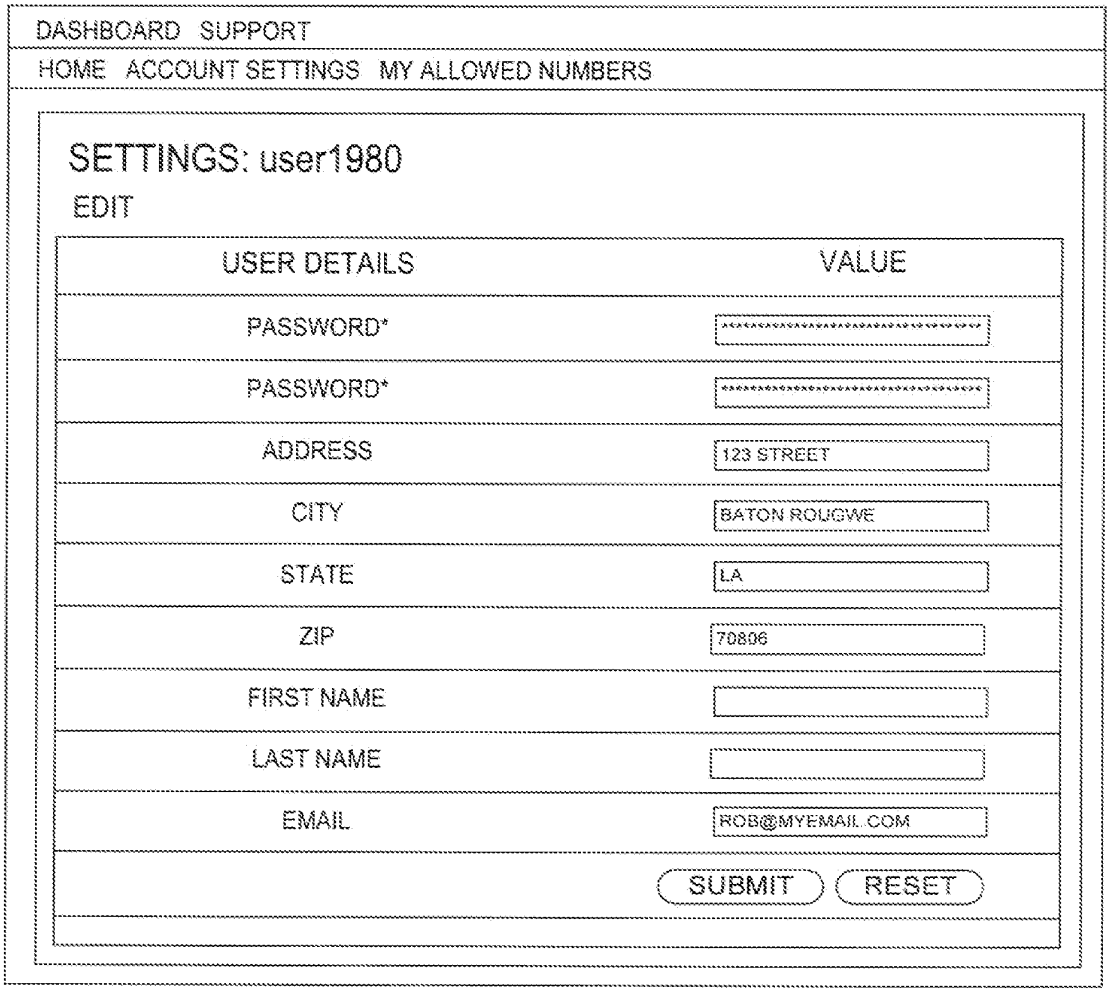

DASHBOARD SUPPORT
HOME ACCOUNT SETTINGS MY ALLOWED NUMBERS
SETTINGS: user1980
EDIT
USER DETAILS
VALUE
PASSWORD*
PASSWORD*
ADDRESS
123 STREET
CITY
BATON ROUGWE
STATE
LA
ZIP
70806
FIRST NAME
LAST NAME
EMAIL
ROB@MYEMAIL.COM
SUBMIT
RESET

FIG. 18

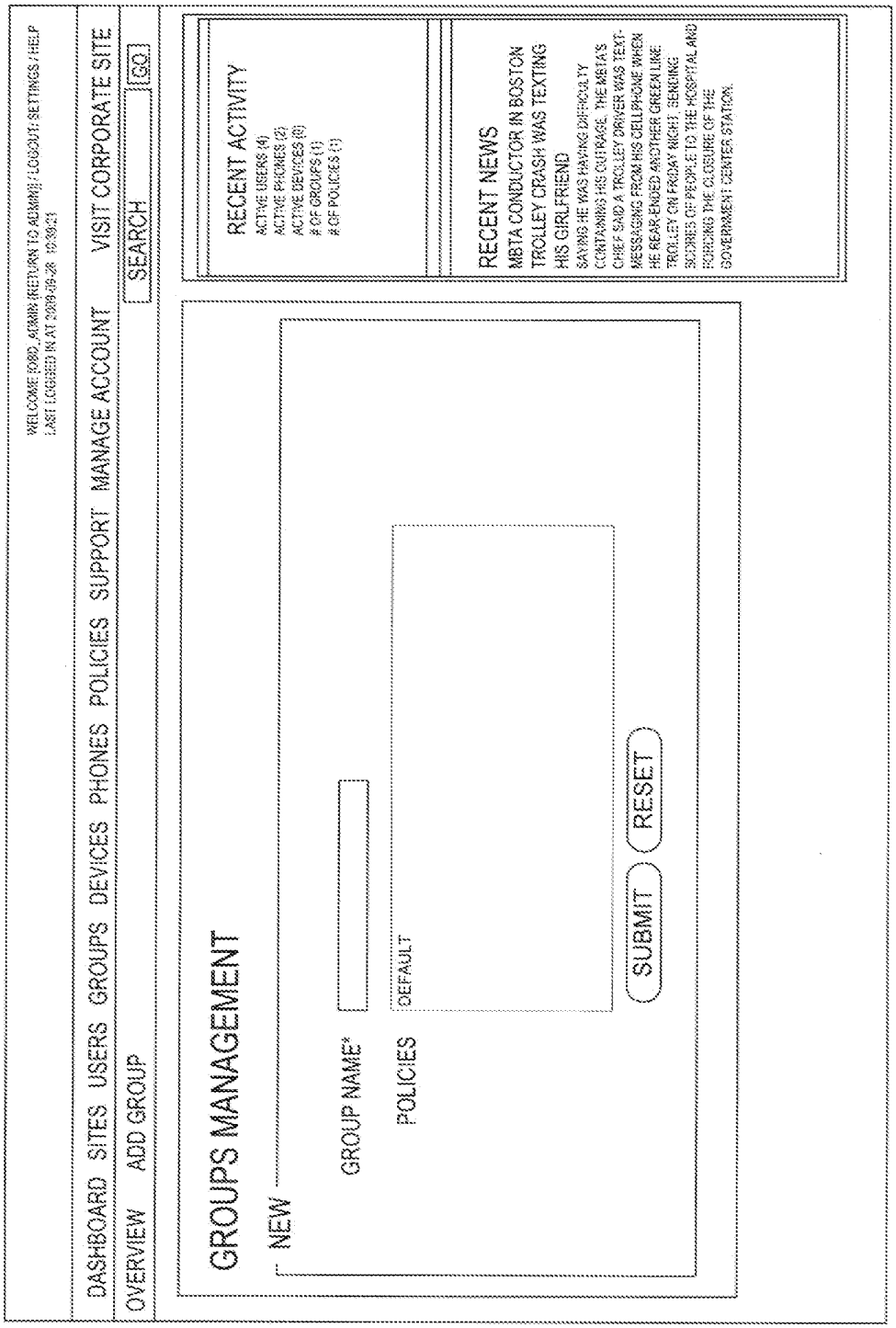

WELCOME [USER_ADMIN] (RETURN TO ADMIN) | LOGOUT/SETTINGS / HELP
LAST LOGGED IN AT 2009-05-28 10:39:21
DASHBOARD SITES USERS GROUPS DEVICES PHONES POLICIES SUPPORT MANAGE ACCOUNT VISIT CORPORATE SITE
OVERVIEW ADD GROUP
SEARCH GO
GROUPS MANAGEMENT
NEW
GROUP NAME*
POLICIES
DEFAULT
SUBMIT
RESET
RECENT ACTIVITY
ACTIVE USERS (4)
ACTIVE PHONES (2)
ACTIVE DEVICES (6)
OF GROUPS (1)
OF POLICIES (1)
RECENT NEWS
MBTA CONDUCTOR IN BOSTON TROLLEY CRASH WAS TEXTING HIS GIRLFRIEND
SAYING HE WAS HAVING DIFFICULTY CONTAINING HIS OUTRAGE, THE MBTA'S CHIEF SAID A TROLLEY DRIVER WAS TEXT-MESSAGING FROM HIS CELLPHONE WHEN HE REAR-ENDED ANOTHER GREEN LINE TROLLEY ON FRIDAY NIGHT, SENDING SCORES OF PEOPLE TO THE HOSPITAL AND FORCING THE CLOSURE OF THE GOVERNMENT CENTER STATION.

FIG. 19

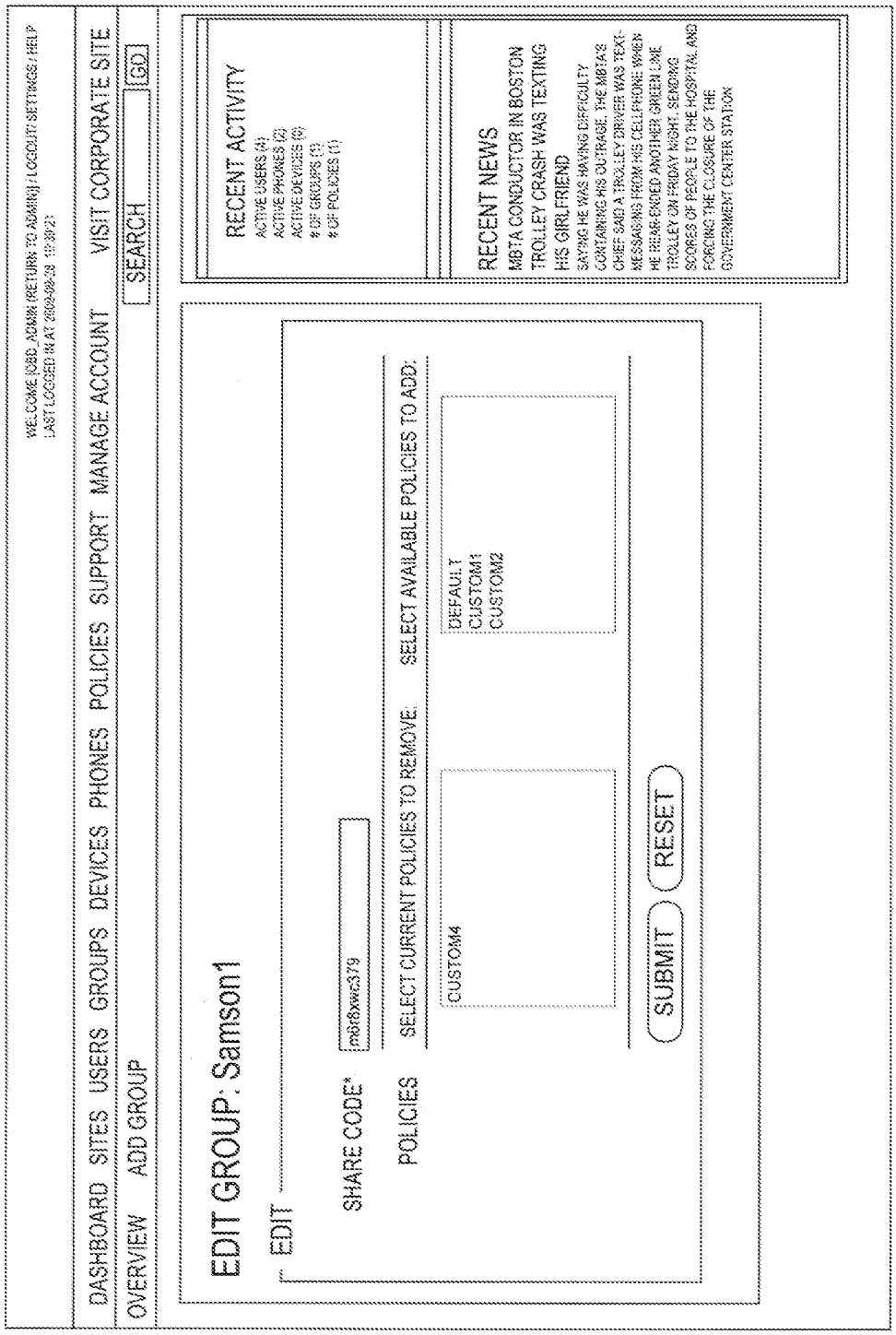

WELCOME [OBD_ADMIN (RETURN TO ADMIN)] / LOGOUT/ SETTINGS / HELP
LAST LOGGED IN AT 2009-08-28 19:39:21
DASHBOARD SITES USERS GROUPS DEVICES PHONES POLICIES SUPPORT MANAGE ACCOUNT VISIT CORPORATE SITE
OVERVIEW ADD GROUP
SEARCH
GO
EDIT GROUP: Samson1
EDIT
SHARE CODE*
m6r8xwc379
POLICIES
SELECT CURRENT POLICIES TO REMOVE:
CUSTOM4
SELECT AVAILABLE POLICIES TO ADD:
DEFAULT
CUSTOM1
CUSTOM2
SUBMIT
RESET
RECENT ACTIVITY
ACTIVE USERS (4)
ACTIVE PHONES (2)
ACTIVE DEVICES (6)
OF GROUPS (1)
OF POLICIES (1)
RECENT NEWS
MBTA CONDUCTOR IN BOSTON TROLLEY CRASH WAS TEXTING HIS GIRLFRIEND
SAYING HE WAS HAVING DIFFICULTY CONTAINING HIS OUTRAGE, THE MBTA'S CHIEF SAID A TROLLEY DRIVER WAS TEXT-MESSAGING FROM HIS CELLPHONE WHEN HE REAR-ENDED ANOTHER GREEN LINE TROLLEY ON FRIDAY NIGHT, SENDING SCORES OF PEOPLE TO THE HOSPITAL AND FORCING THE CLOSURE OF THE GOVERNMENT CENTER STATION

FIG. 20

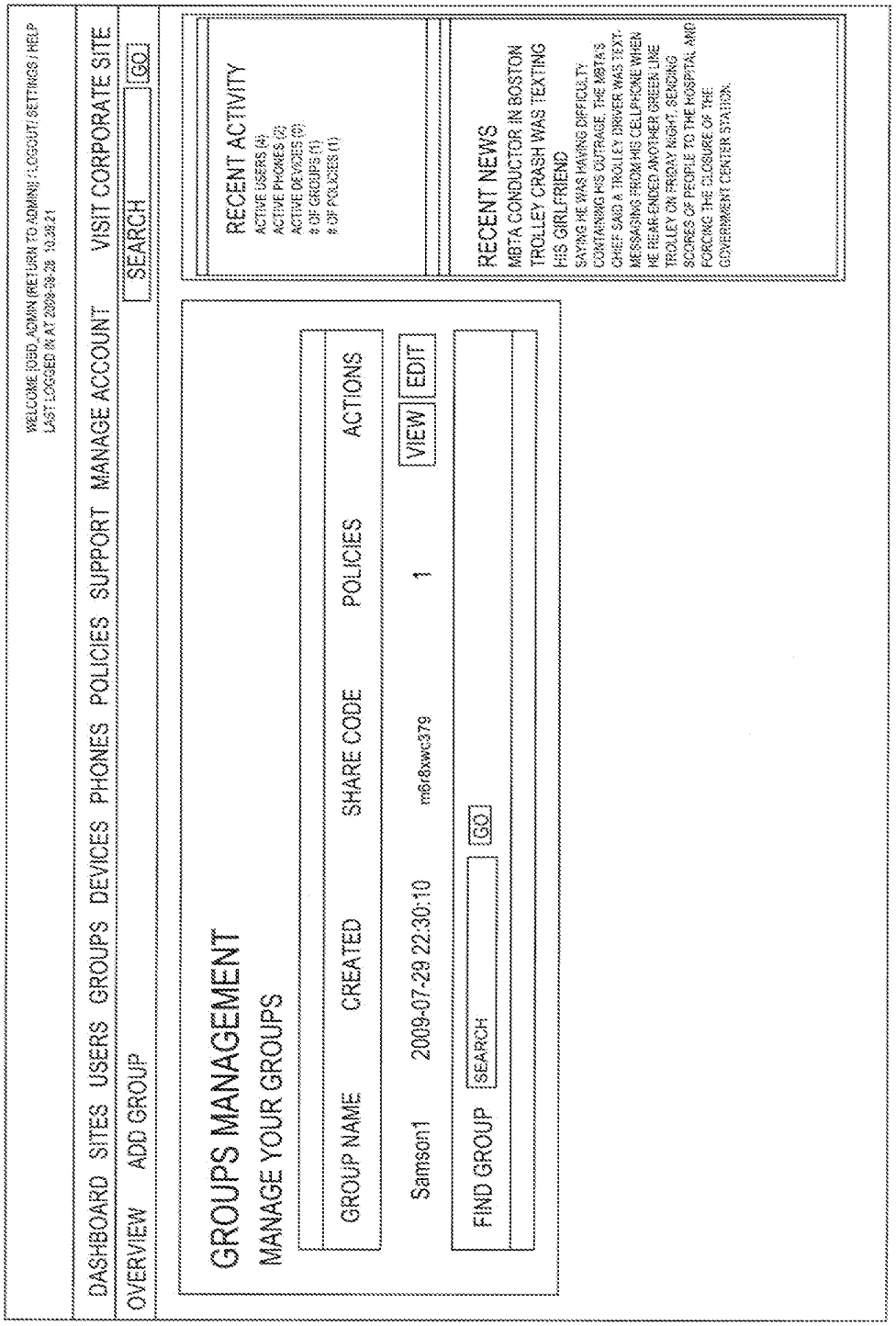

WELCOME (GBD_ADMIN (RETURN TO ADMIN) | LOGOUT/ SETTINGS / HELP
LAST LOGGED IN AT 2009-09-28 10:38:21
DASHBOARD SITES USERS GROUPS DEVICES PHONES POLICIES SUPPORT MANAGE ACCOUNT VISIT CORPORATE SITE
OVERVIEW ADD GROUP
SEARCH
GO
GROUPS MANAGEMENT
MANAGE YOUR GROUPS
GROUP NAME
CREATED
SHARE CODE
POLICIES
ACTIONS
Samson1
2009-07-29 22:30:10
m6r8xwc379
1
VIEW
EDIT
FIND GROUP
SEARCH
GO
RECENT ACTIVITY
ACTIVE USERS (4)
ACTIVE PHONES (2)
ACTIVE DEVICES (0)
OF GROUPS (1)
OF POLICIES (1)
RECENT NEWS
MBTA CONDUCTOR IN BOSTON TROLLEY CRASH WAS TEXTING HIS GIRLFRIEND
SAYING HE WAS HAVING DIFFICULTY CONTAINING HIS OUTRAGE THE MBTA'S CHIEF SAID A TROLLEY DRIVER WAS TEXT-MESSAGING FROM HIS CELLPHONE WHEN HE REAR-ENDED ANOTHER GREEN LINE TROLLEY ON FRIDAY NIGHT, SENDING SCORES OF PEOPLE TO THE HOSPITAL AND FORCING THE CLOSURE OF THE GOVERNMENT CENTER STATION.

FIG. 21

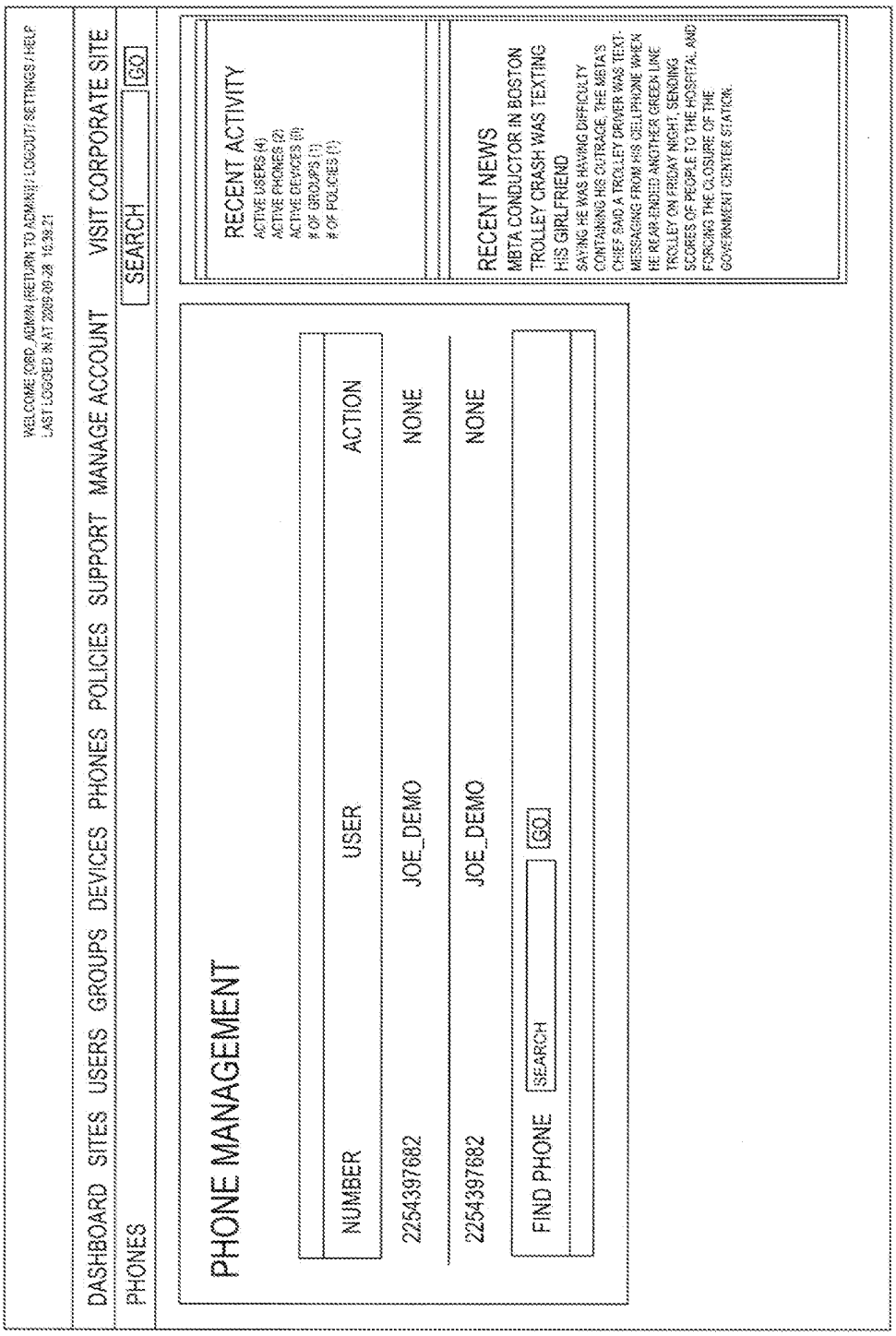

WELCOME ROBO_ADMIN (RETURN TO ADMIN) | LOGOUT | SETTINGS | HELP
LAST LOGGED IN AT 2009-09-28 16:39:21
DASHBOARD SITES USERS GROUPS DEVICES PHONES POLICIES SUPPORT MANAGE ACCOUNT VISIT CORPORATE SITE
PHONES
SEARCH
GO
PHONE MANAGEMENT
NUMBER
USER
ACTION
2254397682
JOE_DEMO
NONE
2254397682
JOE_DEMO
NONE
FIND PHONE
SEARCH
GO
RECENT ACTIVITY
ACTIVE USERS (4)
ACTIVE PHONES (2)
ACTIVE DEVICES (6)
OF GROUPS (1)
OF POLICIES (1)
RECENT NEWS
MBTA CONDUCTOR IN BOSTON TROLLEY CRASH WAS TEXTING HIS GIRLFRIEND
SAYING HE WAS HAVING DIFFICULTY CONTAINING HIS OUTRAGE, THE MBTA'S CHIEF SAID A TROLLEY DRIVER WAS TEXT-MESSAGING FROM HIS CELLPHONE WHEN HE REAR-ENDED ANOTHER GREEN LINE TROLLEY ON FRIDAY NIGHT, SENDING SCORES OF PEOPLE TO THE HOSPITAL AND FORCING THE CLOSURE OF THE GOVERNMENT CENTER STATION.

FIG. 22

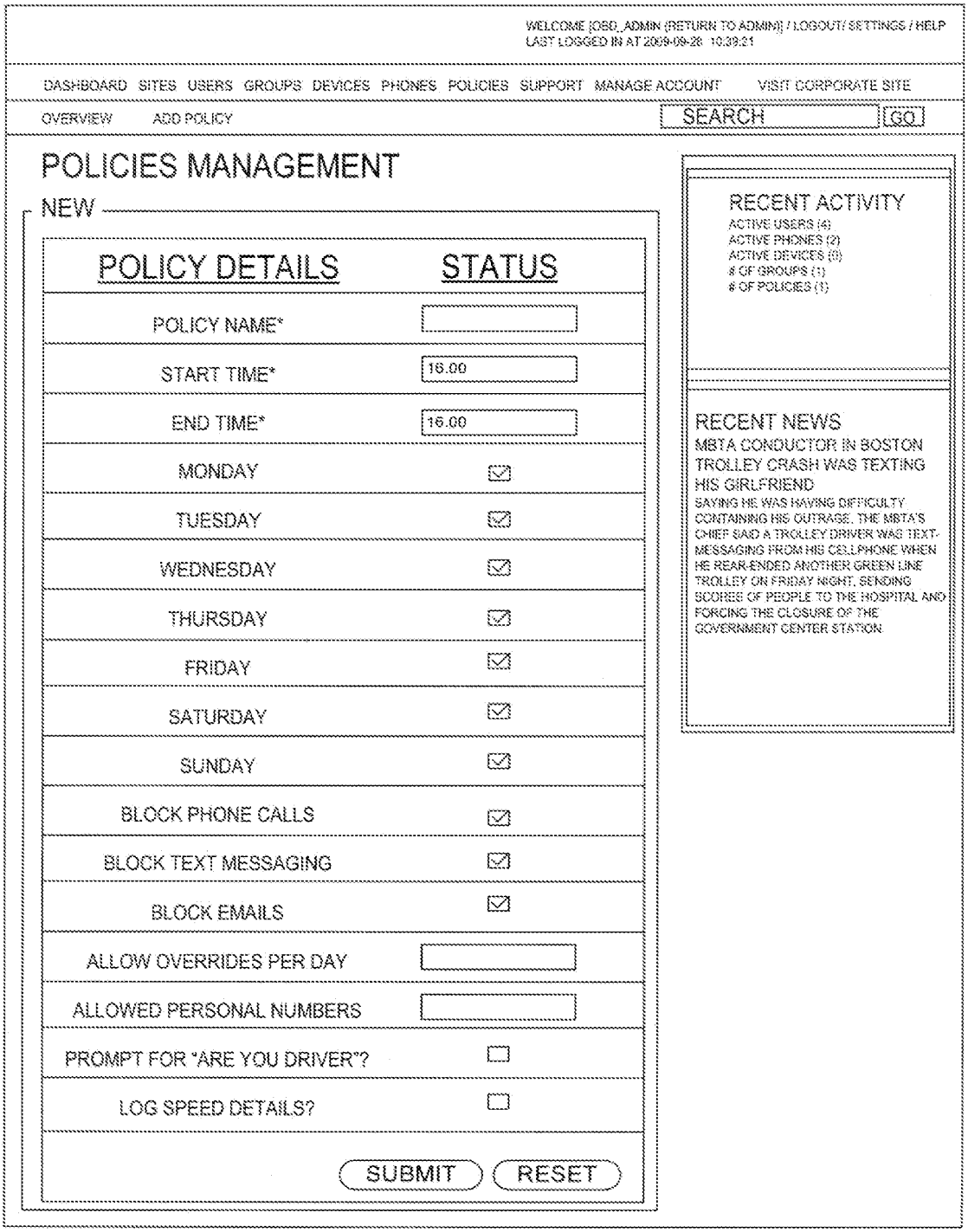

WELCOME [OSD_ADMIN (RETURN TO ADMIN)] / LOGOUT/ SETTINGS / HELP
LAST LOGGED IN AT 2009-09-28 10:39:21
DASHBOARD SITES USERS GROUPS DEVICES PHONES POLICIES SUPPORT MANAGE ACCOUNT VISIT CORPORATE SITE
OVERVIEW ADD POLICY
SEARCH
GO
POLICIES MANAGEMENT
NEW
POLICY DETAILS
STATUS
POLICY NAME*
START TIME*
16.00
END TIME*
16.00
MONDAY
TUESDAY
WEDNESDAY
THURSDAY
FRIDAY
SATURDAY
SUNDAY
BLOCK PHONE CALLS
BLOCK TEXT MESSAGING
BLOCK EMAILS
ALLOW OVERRIDES PER DAY
ALLOWED PERSONAL NUMBERS
PROMPT FOR "ARE YOU DRIVER"?
LOG SPEED DETAILS?
SUBMIT
RESET
RECENT ACTIVITY
ACTIVE USERS (4)
ACTIVE PHONES (2)
ACTIVE DEVICES (0)
OF GROUPS (1)
OF POLICIES (1)
RECENT NEWS
MBTA CONDUCTOR IN BOSTON TROLLEY CRASH WAS TEXTING HIS GIRLFRIEND
SAYING HE WAS HAVING DIFFICULTY CONTAINING HIS OUTRAGE, THE MBTA'S CHIEF SAID A TROLLEY DRIVER WAS TEXT-MESSAGING FROM HIS CELLPHONE WHEN HE REAR-ENDED ANOTHER GREEN LINE TROLLEY ON FRIDAY NIGHT, SENDING SCORES OF PEOPLE TO THE HOSPITAL AND FORCING THE CLOSURE OF THE GOVERNMENT CENTER STATION

FIG. 23

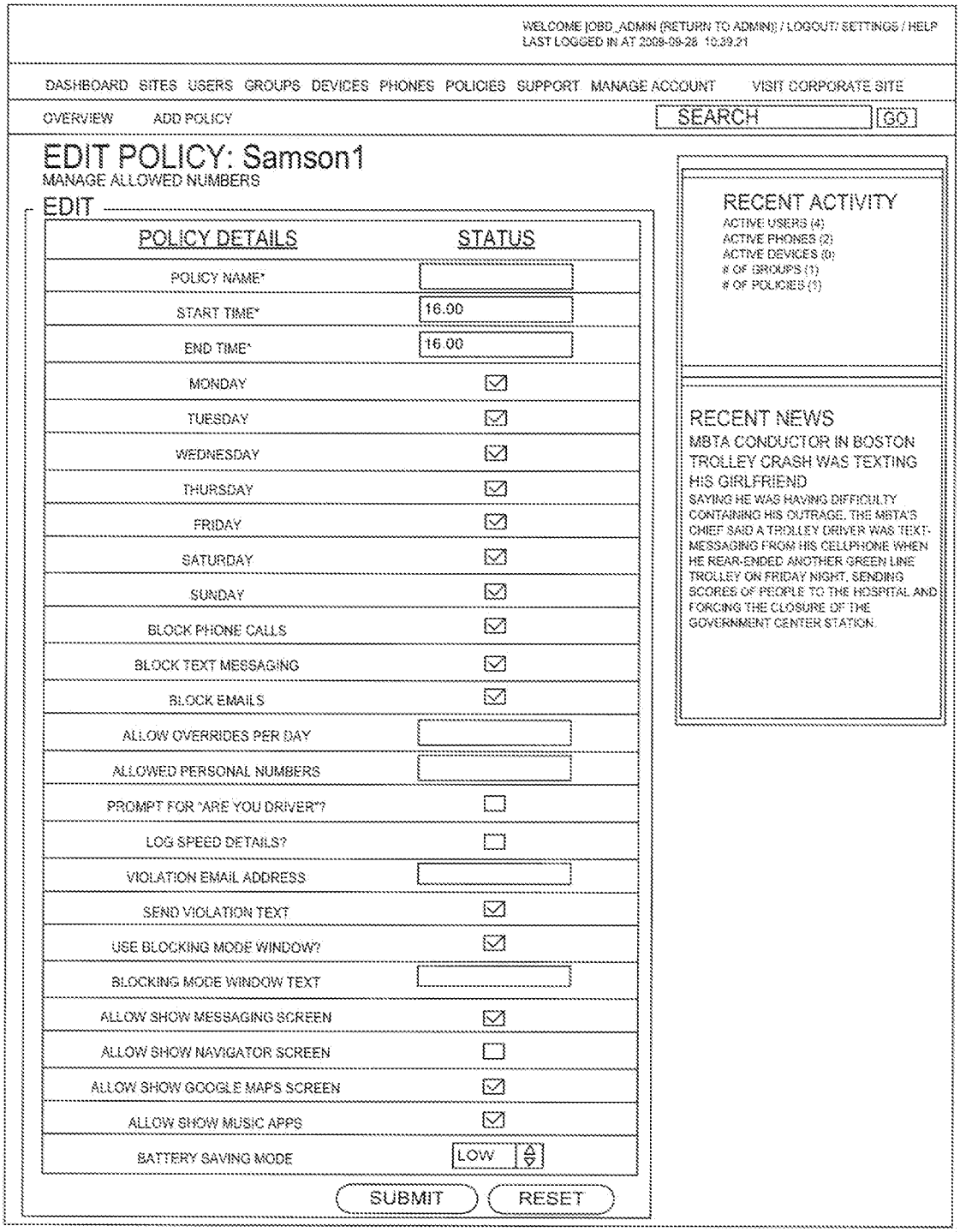

WELCOME JOBD_ADMIN (RETURN TO ADMIN) / LOGOUT/ SETTINGS / HELP
LAST LOGGED IN AT 2009-09-28 10.39.21
DASHBOARD SITES USERS GROUPS DEVICES PHONES POLICIES SUPPORT MANAGE ACCOUNT VISIT CORPORATE SITE
OVERVIEW ADD POLICY
SEARCH
GO
EDIT POLICY: Samson1
MANAGE ALLOWED NUMBERS
EDIT
POLICY DETAILS
STATUS
POLICY NAME*
START TIME*
16.00
END TIME*
16.00
MONDAY
TUESDAY
WEDNESDAY
THURSDAY
FRIDAY
SATURDAY
SUNDAY
BLOCK PHONE CALLS
BLOCK TEXT MESSAGING
BLOCK EMAILS
ALLOW OVERRIDES PER DAY
ALLOWED PERSONAL NUMBERS
PROMPT FOR "ARE YOU DRIVER"?
LOG SPEED DETAILS?
VIOLATION EMAIL ADDRESS
SEND VIOLATION TEXT
USE BLOCKING MODE WINDOW?
BLOCKING MODE WINDOW TEXT
ALLOW SHOW MESSAGING SCREEN
ALLOW SHOW NAVIGATOR SCREEN
ALLOW SHOW GOOGLE MAPS SCREEN
ALLOW SHOW MUSIC APPS
BATTERY SAVING MODE
LOW
SUBMIT
RESET
RECENT ACTIVITY
ACTIVE USERS (4)
ACTIVE PHONES (2)
ACTIVE DEVICES (0)
OF GROUPS (1)
OF POLICIES (1)
RECENT NEWS
MBTA CONDUCTOR IN BOSTON TROLLEY CRASH WAS TEXTING HIS GIRLFRIEND
SAYING HE WAS HAVING DIFFICULTY CONTAINING HIS OUTRAGE, THE MBTA'S CHIEF SAID A TROLLEY DRIVER WAS TEXT-MESSAGING FROM HIS CELLPHONE WHEN HE REAR-ENDED ANOTHER GREEN LINE TROLLEY ON FRIDAY NIGHT, SENDING SCORES OF PEOPLE TO THE HOSPITAL AND FORCING THE CLOSURE OF THE GOVERNMENT CENTER STATION.

FIG. 24

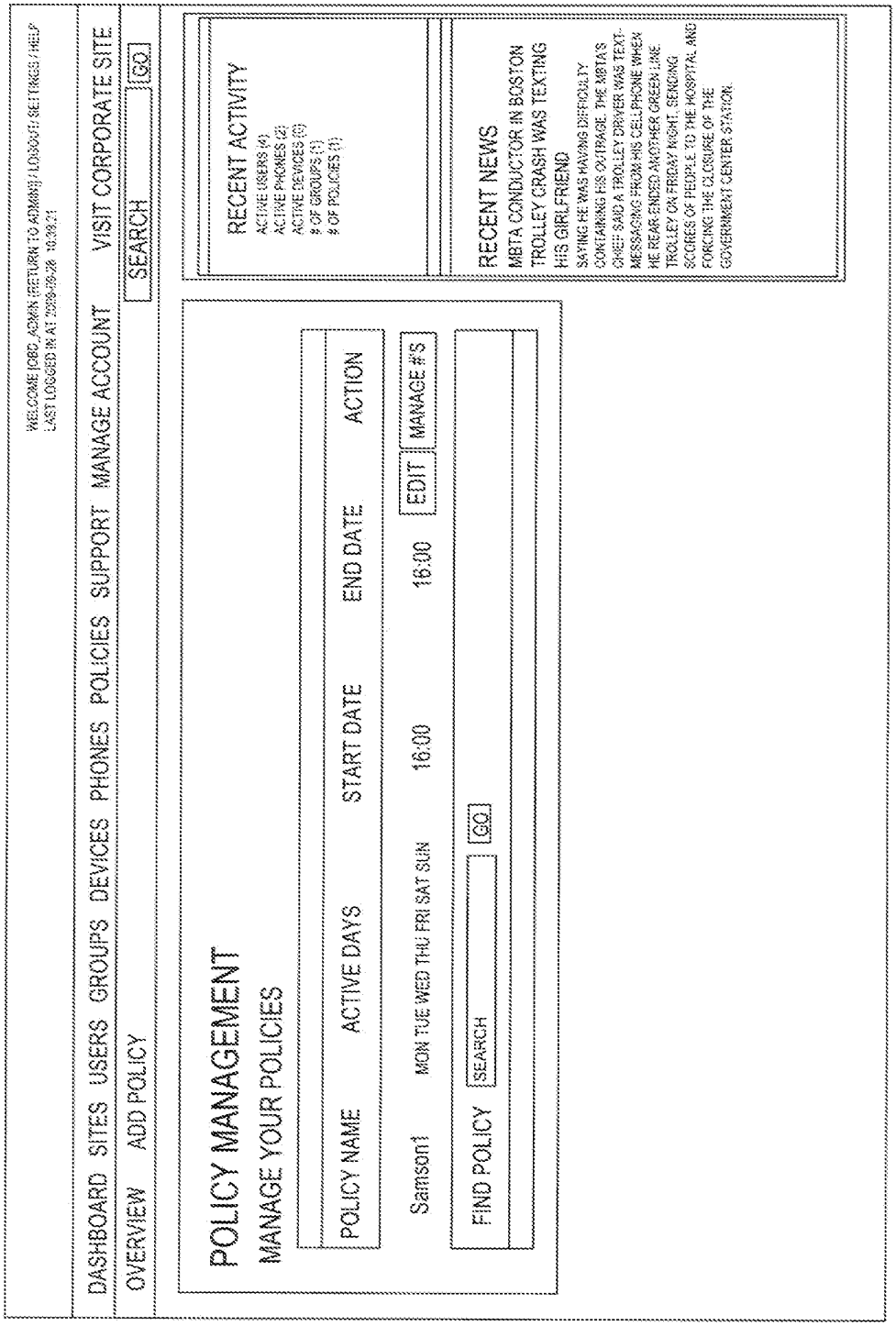

WELCOME JOBO_ADMIN (RETURN TO ADMIN) | LOGOUT | SETTINGS | HELP
LAST LOGGED IN AT 2009-05-28 10:38:21
DASHBOARD SITES USERS GROUPS DEVICES PHONES POLICIES SUPPORT MANAGE ACCOUNT VISIT CORPORATE SITE
OVERVIEW ADD POLICY
SEARCH GO
POLICY MANAGEMENT
MANAGE YOUR POLICIES
POLICY NAME ACTIVE DAYS START DATE END DATE ACTION
Samson1 MON TUE WED THU FRI SAT SUN 16:00 16:00 EDIT MANAGE #'S
FIND POLICY SEARCH GO
RECENT ACTIVITY
ACTIVE USERS (4)
ACTIVE PHONES (2)
ACTIVE DEVICES (5)
OF GROUPS (1)
OF POLICIES (1)
RECENT NEWS
MBTA CONDUCTOR IN BOSTON TROLLEY CRASH WAS TEXTING HIS GIRLFRIEND
SAYING HE WAS HAVING DIFFICULTY CONTAINING HIS OUTRAGE, THE MBTA'S CHIEF SAID A TROLLEY DRIVER WAS TEXT-MESSAGING FROM HIS CELLPHONE WHEN HE REAR-ENDED ANOTHER GREEN LINE TROLLEY ON FRIDAY NIGHT, SENDING SCORES OF PEOPLE TO THE HOSPITAL AND FORCING THE CLOSURE OF THE GOVERNMENT CENTER STATION.

FIG. 25

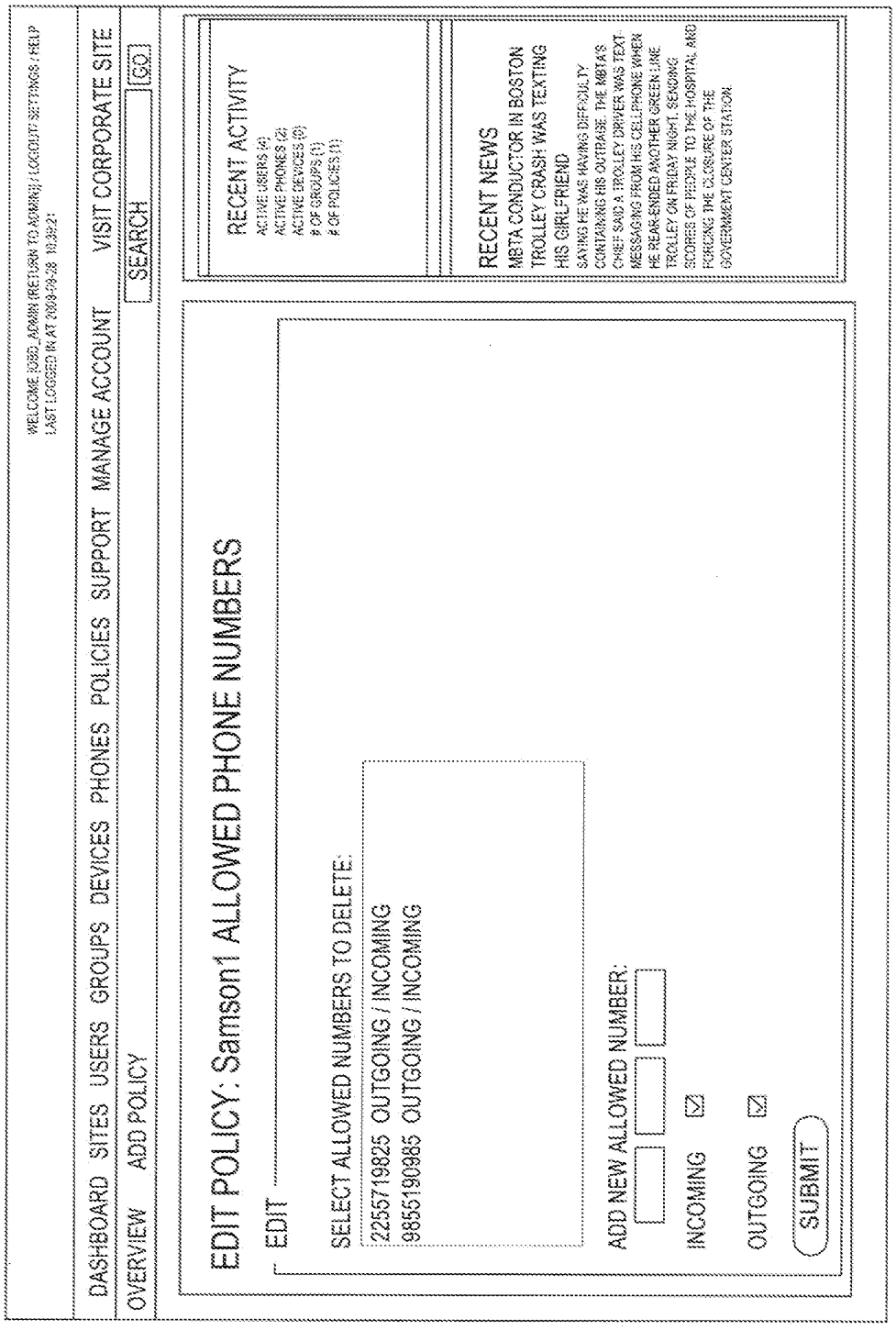

WELCOME (USER_ADMIN (RETURN TO ADMIN)) LOGOUT SETTINGS / HELP
LAST LOGGED IN AT 2009-09-08 10:39:27
DASHBOARD SITES USERS GROUPS DEVICES PHONES POLICIES SUPPORT MANAGE ACCOUNT VISIT CORPORATE SITE
OVERVIEW ADD POLICY
SEARCH GO
EDIT POLICY: Samson1 ALLOWED PHONE NUMBERS
EDIT
SELECT ALLOWED NUMBERS TO DELETE:
2255719825 OUTGOING / INCOMING
9855190985 OUTGOING / INCOMING
ADD NEW ALLOWED NUMBER:
INCOMING
OUTGOING
SUBMIT
RECENT ACTIVITY
ACTIVE USERS (4)
ACTIVE PHONES (2)
ACTIVE DEVICES (0)
OF GROUPS (1)
OF POLICIES (1)
RECENT NEWS
MBTA CONDUCTOR IN BOSTON TROLLEY CRASH WAS TEXTING HIS GIRLFRIEND
SAYING HE WAS HAVING DIFFICULTY CONTAINING HIS OUTBREAK. THE MBTA'S CHIEF SAID A TROLLEY DRIVER WAS TEXT-MESSAGING FROM HIS CELLPHONE WHEN HE REAR-ENDED ANOTHER GREEN LINE TROLLEY ON FRIDAY NIGHT, SENDING SCORES OF PEOPLE TO THE HOSPITAL AND FORCING THE CLOSURE OF THE GOVERNMENT CENTER STATION.

FIG. 26

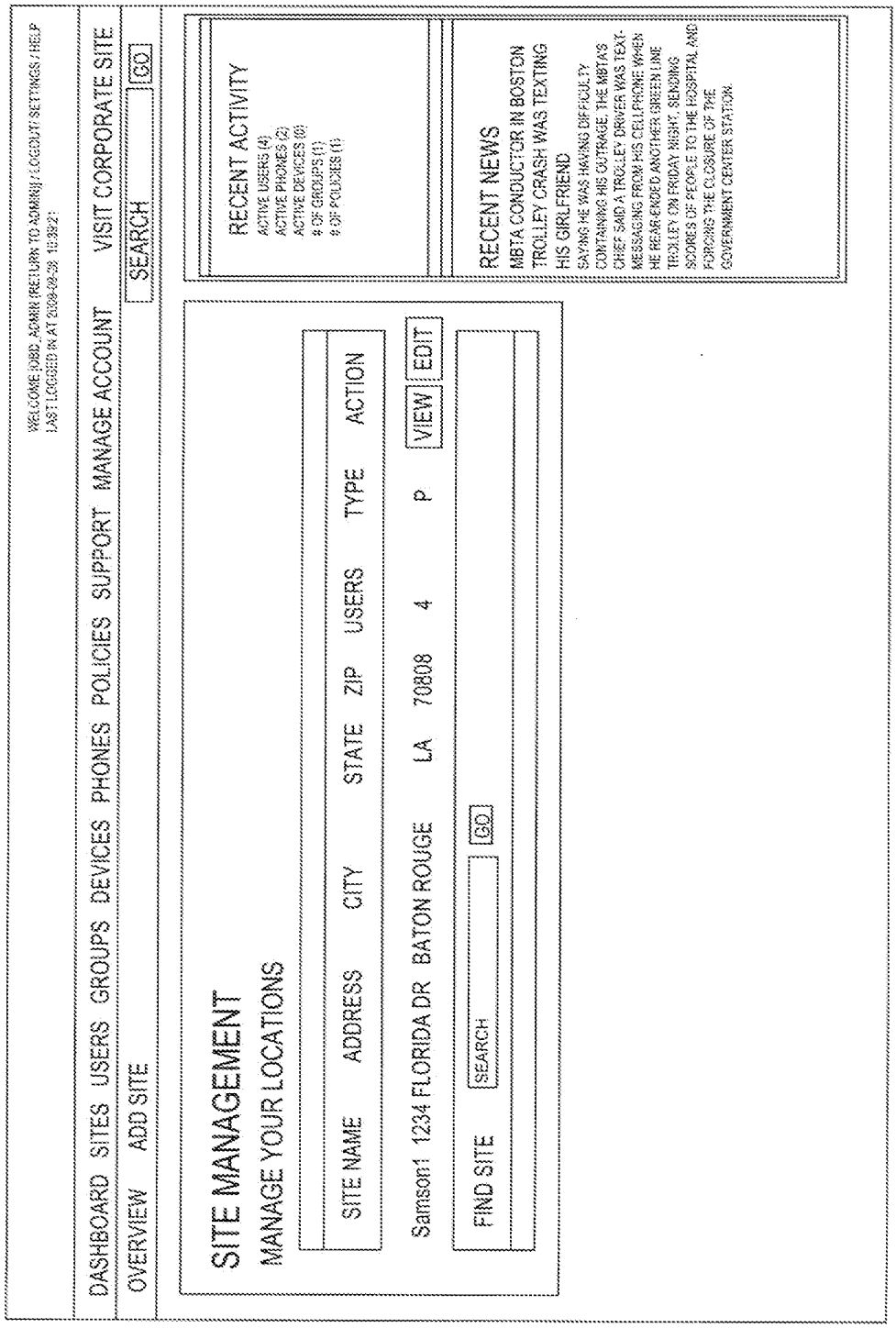

WELCOME (OBD_ADMIN (RETURN TO ADMIN) / LOGOUT/ SETTINGS / HELP
LAST LOGGED IN AT 2009-09-28 15:39:21
DASHBOARD SITES USERS GROUPS DEVICES PHONES POLICIES SUPPORT MANAGE ACCOUNT VISIT CORPORATE SITE
OVERVIEW ADD SITE
SEARCH GO
SITE MANAGEMENT
MANAGE YOUR LOCATIONS
SITE NAME ADDRESS CITY STATE ZIP USERS TYPE ACTION
Samson1 1234 FLORIDA DR BATON ROUGE LA 70808 4 P VIEW EDIT
FIND SITE SEARCH GO
RECENT ACTIVITY
ACTIVE USERS (4)
ACTIVE PHONES (2)
ACTIVE DEVICES (6)
OF GROUPS (1)
OF POLICIES (1)
RECENT NEWS
MBTA CONDUCTOR IN BOSTON TROLLEY CRASH WAS TEXTING HIS GIRLFRIEND
SAYING HE WAS HAVING DIFFICULTY CONTAINING HIS OUTRAGE, THE MBTA'S CHIEF SAID A TROLLEY DRIVER WAS TEXT-MESSAGING FROM HIS CELLPHONE WHEN HE REAR-ENDED ANOTHER GREEN LINE TROLLEY ON FRIDAY NIGHT, SENDING SCORES OF PEOPLE TO THE HOSPITAL AND FORCING THE CLOSURE OF THE GOVERNMENT CENTER STATION.

FIG. 27

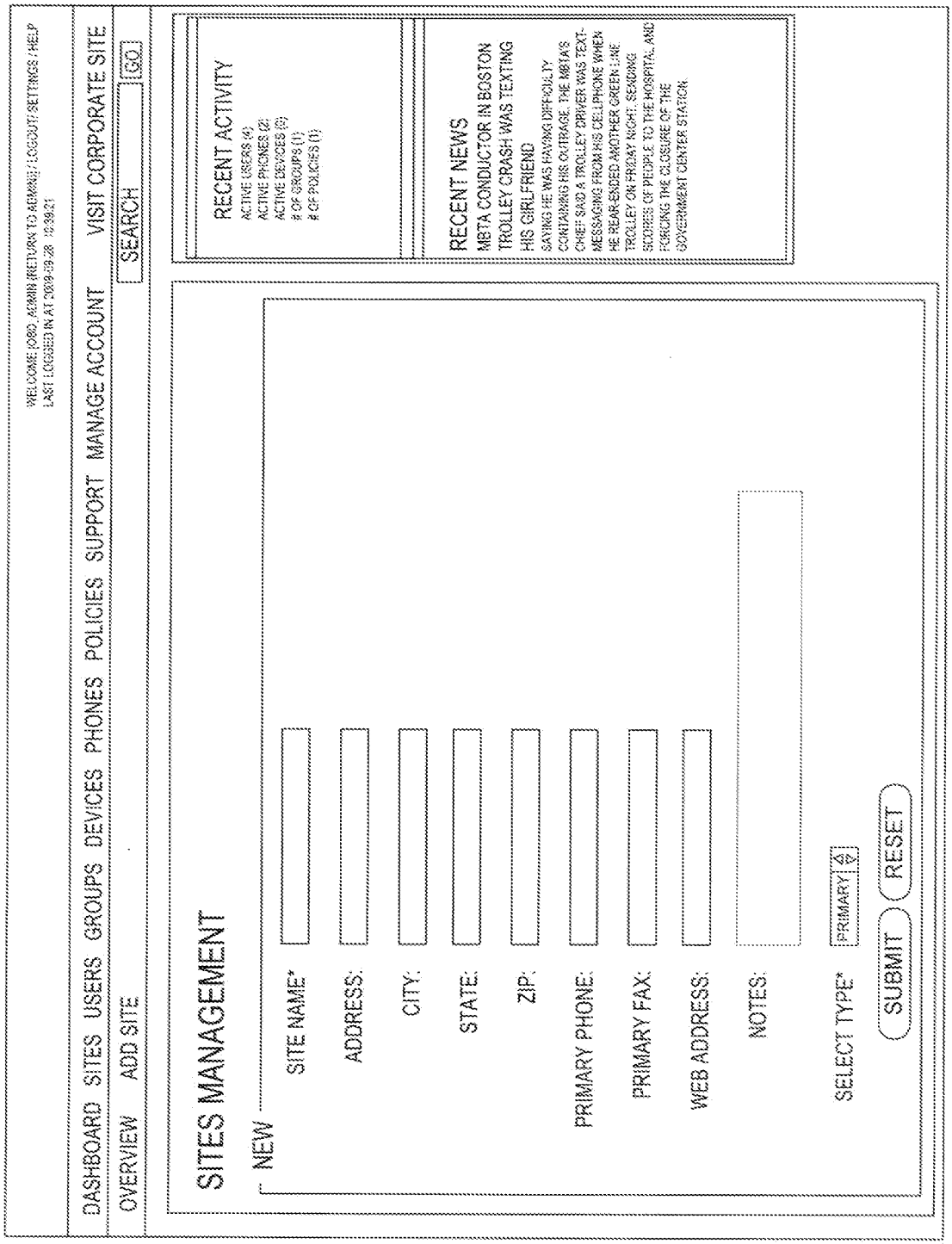

WELCOME JOBO_ADMIN (RETURN TO ADMIN) | LOGOUT SETTINGS / HELP
LAST LOGGED IN AT 2009-09-28 10:39:21
DASHBOARD SITES USERS GROUPS DEVICES PHONES POLICIES SUPPORT MANAGE ACCOUNT VISIT CORPORATE SITE
OVERVIEW ADD SITE
SEARCH
GO
SITES MANAGEMENT
NEW
SITE NAME*
ADDRESS:
CITY:
STATE:
ZIP:
PRIMARY PHONE:
PRIMARY FAX:
WEB ADDRESS:
NOTES:
SELECT TYPE*
PRIMARY
SUBMIT
RESET
RECENT ACTIVITY
ACTIVE USERS (4)
ACTIVE PHONES (2)
ACTIVE DEVICES (5)
OF GROUPS (1)
OF POLICIES (1)
RECENT NEWS
MBTA CONDUCTOR IN BOSTON TROLLEY CRASH WAS TEXTING HIS GIRLFRIEND
SAYING HE WAS HAVING DIFFICULTY CONTAINING HIS OUTRAGE, THE MBTA'S CHIEF SAID A TROLLEY DRIVER WAS TEXT-MESSAGING FROM HIS CELLPHONE WHEN HE REAR-ENDED ANOTHER GREEN LINE TROLLEY ON FRIDAY NIGHT, SEVERING SCORES OF PEOPLE TO THE HOSPITAL AND FORCING THE CLOSURE OF THE GOVERNMENT CENTER STATION.

FIG. 28

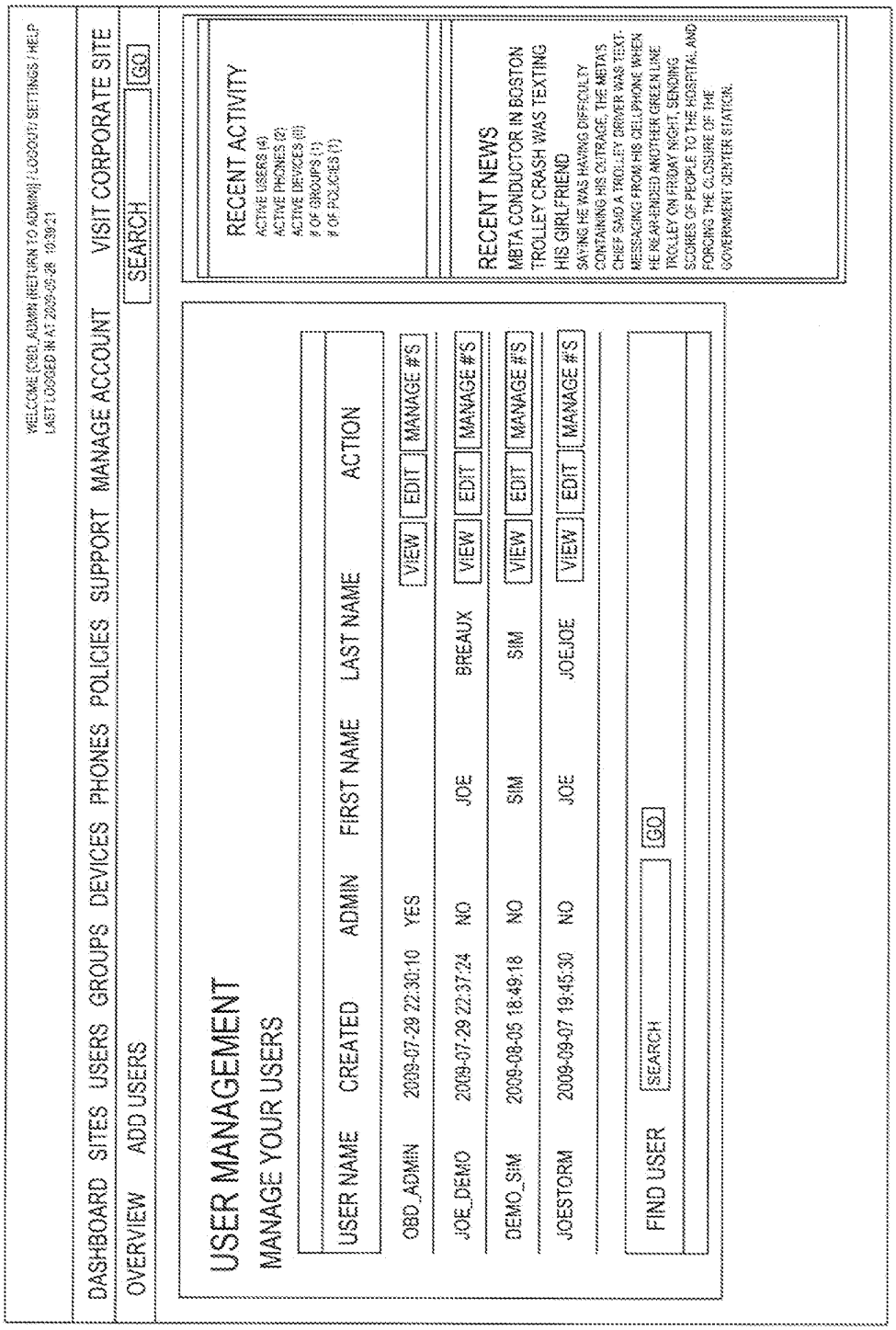

WELCOME [OBD_ADMIN (RETURN TO ADMIN)] / LOGOUT/ SETTINGS / HELP
LAST LOGGED IN AT 2009-09-08 10:39:21
DASHBOARD SITES USERS GROUPS DEVICES PHONES POLICIES SUPPORT MANAGE ACCOUNT VISIT CORPORATE SITE
OVERVIEW ADD USERS
SEARCH GO
USER MANAGEMENT
MANAGE YOUR USERS
USER NAME CREATED ADMIN FIRST NAME LAST NAME ACTION
OBD_ADMIN 2009-07-29 22:36:10 YES VIEW EDIT MANAGE #'S
JOE_DEMO 2009-07-29 22:37:24 NO JOE BREAUX VIEW EDIT MANAGE #'S
DEMO_SIM 2009-08-05 18:49:18 NO SIM SIM VIEW EDIT MANAGE #'S
JOESTORM 2009-09-07 19:45:30 NO JOE JOEJOE VIEW EDIT MANAGE #'S
FIND USER SEARCH GO
RECENT ACTIVITY
ACTIVE USERS (4)
ACTIVE PHONES (2)
ACTIVE DEVICES (8)
OF GROUPS (1)
OF POLICIES (7)
RECENT NEWS
MBTA CONDUCTOR IN BOSTON TROLLEY CRASH WAS TEXTING HIS GIRLFRIEND
SAYING HE WAS HAVING DIFFICULTY CONTAINING HIS OUTRAGE, THE MBTA'S CHIEF SAID A TROLLEY DRIVER WAS TEXT-MESSAGING FROM HIS CELLPHONE WHEN HE REAR-ENDED ANOTHER GREEN LINE TROLLEY ON FRIDAY NIGHT, SENDING SCORES OF PEOPLE TO THE HOSPITAL AND FORCING THE CLOSURE OF THE GOVERNMENT CENTER STATION.

FIG. 29

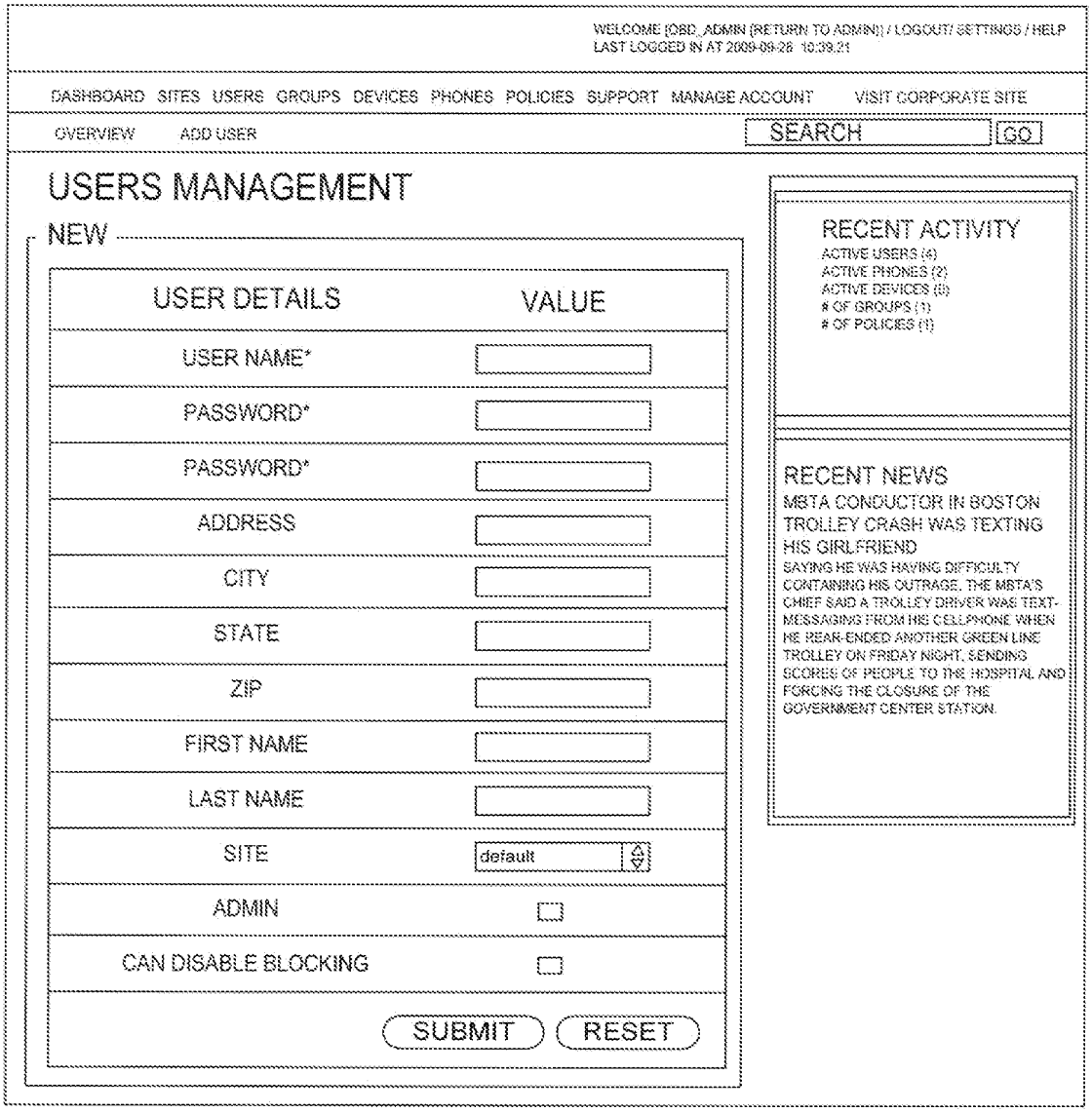

WELCOME [OBD_ADMIN (RETURN TO ADMIN)] / LOGOUT/ SETTINGS / HELP
LAST LOGGED IN AT 2009-09-28 10:39:21
DASHBOARD SITES USERS GROUPS DEVICES PHONES POLICIES SUPPORT MANAGE ACCOUNT VISIT CORPORATE SITE
OVERVIEW ADD USER
SEARCH
GO
USERS MANAGEMENT
NEW
USER DETAILS
VALUE
USER NAME*
PASSWORD*
PASSWORD*
ADDRESS
CITY
STATE
ZIP
FIRST NAME
LAST NAME
SITE
default
ADMIN
CAN DISABLE BLOCKING
SUBMIT
RESET
RECENT ACTIVITY
ACTIVE USERS (4)
ACTIVE PHONES (2)
ACTIVE DEVICES (0)
OF GROUPS (1)
OF POLICIES (1)
RECENT NEWS
MBTA CONDUCTOR IN BOSTON TROLLEY CRASH WAS TEXTING HIS GIRLFRIEND
SAYING HE WAS HAVING DIFFICULTY CONTAINING HIS OUTRAGE, THE MBTA'S CHIEF SAID A TROLLEY DRIVER WAS TEXT-MESSAGING FROM HIS CELLPHONE WHEN HE REAR-ENDED ANOTHER GREEN LINE TROLLEY ON FRIDAY NIGHT, SENDING SCORES OF PEOPLE TO THE HOSPITAL AND FORCING THE CLOSURE OF THE GOVERNMENT CENTER STATION.

FIG. 23

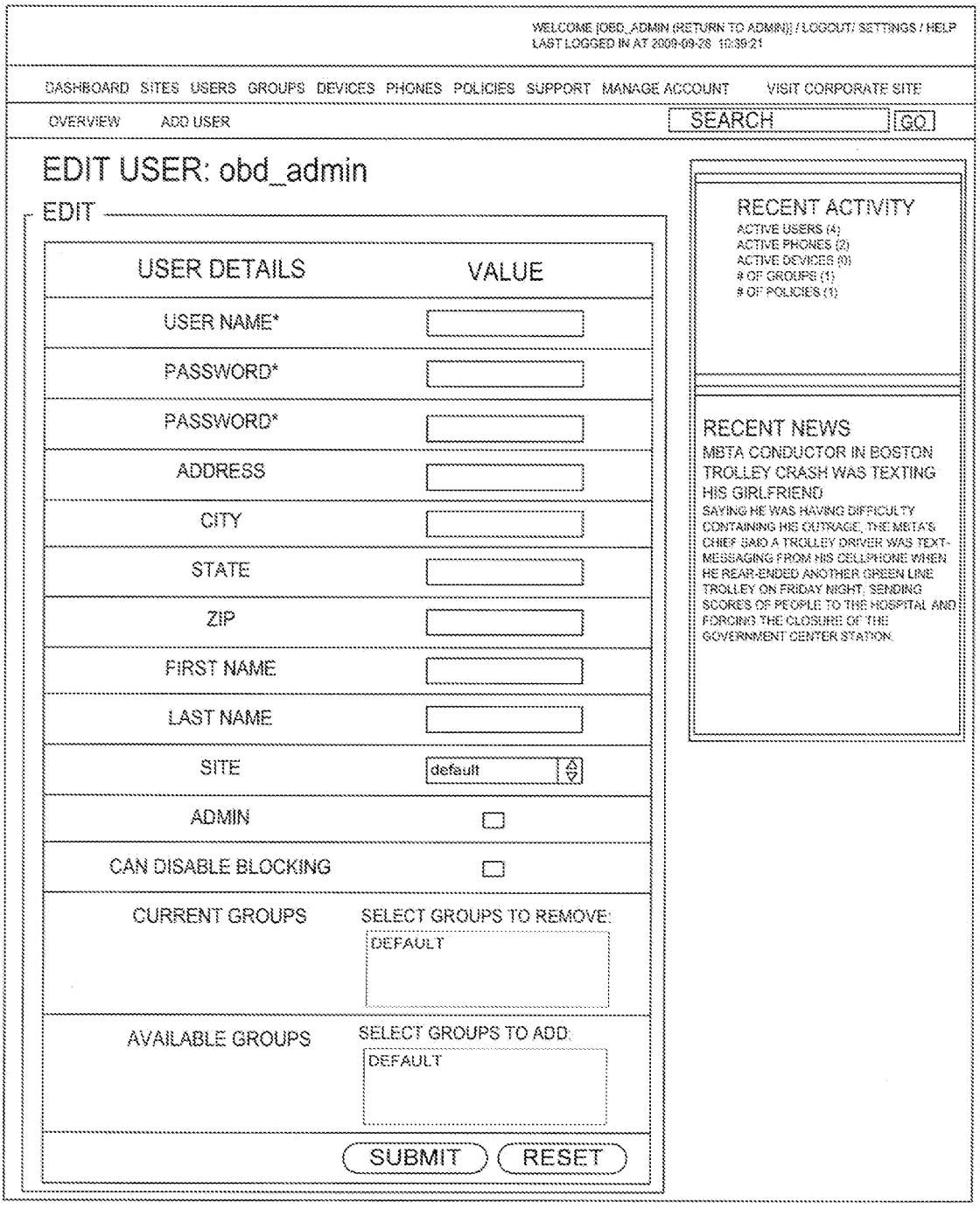

WELCOME [OBD_ADMIN (RETURN TO ADMIN)] / LOGOUT/ SETTINGS / HELP
LAST LOGGED IN AT 2009-09-28 10:39:21
DASHBOARD SITES USERS GROUPS DEVICES PHONES POLICIES SUPPORT MANAGE ACCOUNT VISIT CORPORATE SITE
OVERVIEW ADD USER
SEARCH
GO
EDIT USER: obd_admin
EDIT
USER DETAILS
VALUE
USER NAME*
PASSWORD*
PASSWORD*
ADDRESS
CITY
STATE
ZIP
FIRST NAME
LAST NAME
SITE
default
ADMIN
CAN DISABLE BLOCKING
CURRENT GROUPS
SELECT GROUPS TO REMOVE:
DEFAULT
AVAILABLE GROUPS
SELECT GROUPS TO ADD:
DEFAULT
SUBMIT
RESET
RECENT ACTIVITY
ACTIVE USERS (4)
ACTIVE PHONES (2)
ACTIVE DEVICES (0)
OF GROUPS (1)
OF POLICIES (1)
RECENT NEWS
MBTA CONDUCTOR IN BOSTON TROLLEY CRASH WAS TEXTING HIS GIRLFRIEND
SAYING HE WAS HAVING DIFFICULTY CONTAINING HIS OUTRAGE, THE MBTA'S CHIEF SAID A TROLLEY DRIVER WAS TEXT-MESSAGING FROM HIS CELLPHONE WHEN HE REAR-ENDED ANOTHER GREEN LINE TROLLEY ON FRIDAY NIGHT, SENDING SCORES OF PEOPLE TO THE HOSPITAL AND FORCING THE CLOSURE OF THE GOVERNMENT CENTER STATION.

FIG. 31

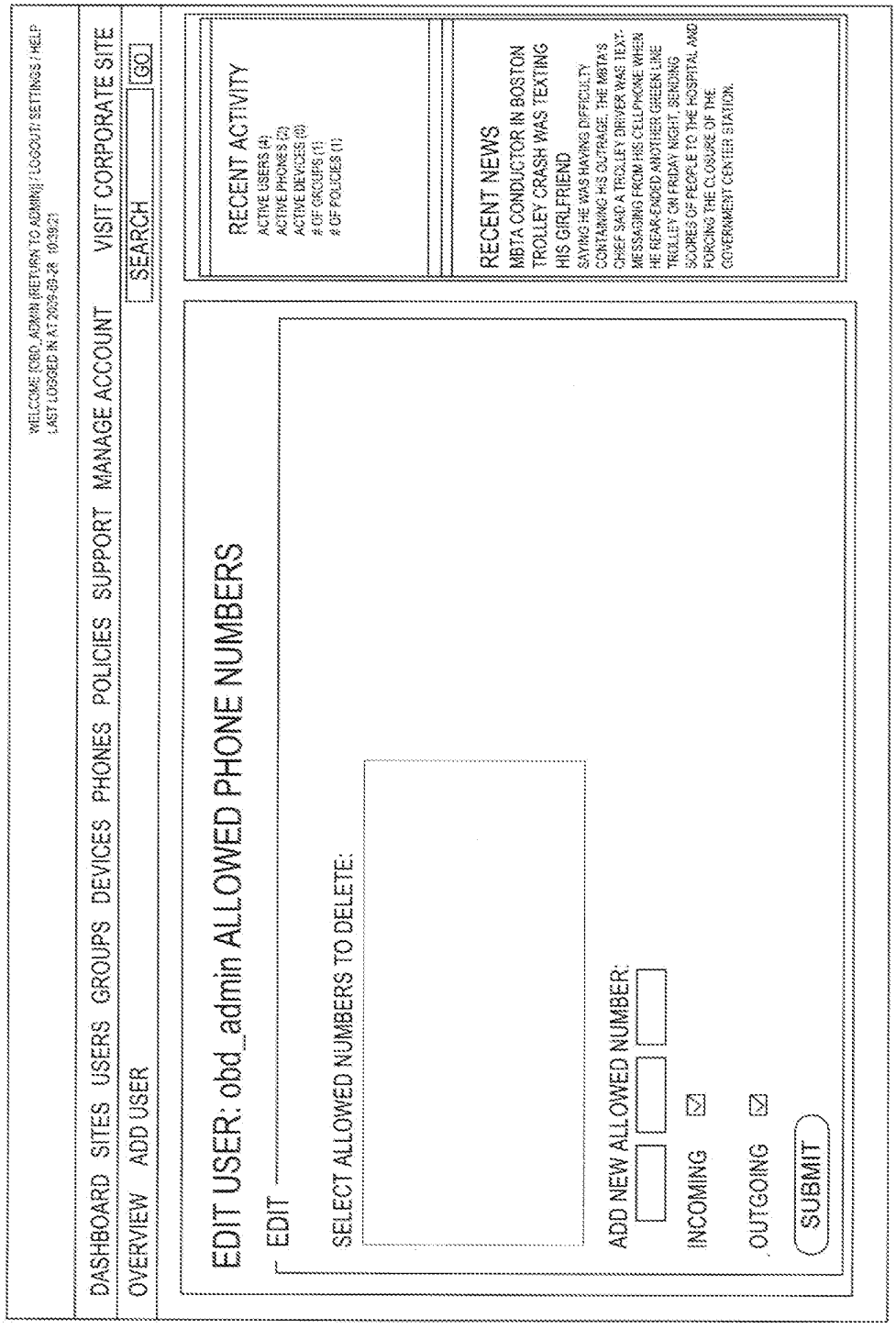

WELCOME [OBD_ADMIN (RETURN TO ADMIN)] LOGOUT SETTINGS / HELP
LAST LOGGED IN AT 2009-09-28 10:39:21
DASHBOARD SITES USERS GROUPS DEVICES PHONES POLICIES SUPPORT MANAGE ACCOUNT VISIT CORPORATE SITE
OVERVIEW ADD USER
SEARCH
GO
EDIT USER: obd_admin ALLOWED PHONE NUMBERS
EDIT
SELECT ALLOWED NUMBERS TO DELETE:
ADD NEW ALLOWED NUMBER:
INCOMING
OUTGOING
SUBMIT
RECENT ACTIVITY
ACTIVE USERS (4)
ACTIVE PHONES (2)
ACTIVE DEVICES (0)
OF GROUPS (1)
OF POLICIES (1)
RECENT NEWS
MBTA CONDUCTOR IN BOSTON TROLLEY CRASH WAS TEXTING HIS GIRLFRIEND
SAYING HE WAS HAVING DIFFICULTY CONTAINING HIS OUTRAGE. THE MBTA'S CHIEF SAID A TROLLEY DRIVER WAS TEXT-MESSAGING FROM HIS CELLPHONE WHEN HE REAR-ENDED ANOTHER GREEN LINE TROLLEY ON FRIDAY NIGHT, SENDING SCORES OF PEOPLE TO THE HOSPITAL AND FORCING THE CLOSURE OF THE GOVERNMENT CENTER STATION.

FIG. 32

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2010/034151

A. CLASSIFICATION OF SUBJECT MATTER
IPC(8) - H04M 3/42 (2010.01)
USPC - 455/412.2
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC(8) - H04M 3/42, H04W 4/12 (2010.01)
USPC - 455/412.2, 414.1

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
PatBase, Micropat

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2002/0128000 A1 (DO NASCIMENTO, JR) 12 September 2002 (12.09.2002) entire document	1-140
Y	US 7,187,953 B2 (BAUCHOT et al) 06 March 2007 (06.03.2007) entire document	1-140
Y	US 2007/0271234 A1 (RAVIKIRAN) 22 November 2007 (22.11.2007) entire document	75-140
Y	US 6,925,105 B1 (PARTYKA) 02 August 2005 (02.08.2005) entire document	75-140
Y	US 7,437,752 B2 (HEARD et al) 14 October 2008 (14.10.2008) entire document	59-63, 72-74, 125-129, 138-140
Y	US 2007/0088823 A1 (FOWLER et al) 19 April 2007 (19.04.2007) entire document	19-20, 88
Y	US 2007/0287420 A1 (KIRKE) 13 December 2007 (13.12.2007) entire document	26-29, 94-97
Y	US 7,505,784 B2 (BARBERA) 17 March 2009 (17.03.2009) entire document	40, 56, 106, 122
Y	US 7,319,696 B2 (INOUE et al) 15 January 2008 (15.01.2008) entire document	45, 111
Y	US 7,035,828 B2 (KETONEN et al) 25 April 2006 (25.04.2006) entire document	28-29, 96-97, 137
Y	US 2008/0294302 A1 (BASIR) 27 November 2008 (27.11.2008) entire document	68, 134

☐ Further documents are listed in the continuation of Box C. ☐

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
02 July 2010	13 JUL 2010
Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US, Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-3201	Authorized officer: Blaine R. Copenheaver PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774

Form PCT/ISA/210 (second sheet) (July 2009)

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
18 September 2008 (18.09.2008)

PCT

(10) International Publication Number
WO 2008/110215 A1

(51) International Patent Classification:
H04L 29/06 (2006.01)

(21) International Application Number:
PCT/EP2007/052465

(22) International Filing Date: 15 March 2007 (15.03.2007)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant *(for all designated States except US)*: **Telefonaktiebolaget LM Ericsson (publ)** [SE/SE]; S-16483 Stockholm (SE).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: **GYÖRGY, Miklos** [HU/HU]; Karokatona u. 3/H., H-2096 Üröm (HU). **HALL, Göran** [SE/SE]; Ejdergatan 14, S-43164 Mölndal (SE). **BACKMAN, Jan** [SE/SE]; Snäckliden 24, S-44271 Kärna (SE).

(74) Agents: **MOHSLER, Gabriele** et al.; Ericsson Allee 1, 52134 Herzogenrath (DE).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declaration under Rule 4.17:
— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*

Published:
— *with international search report*

(54) Title: A METHOD AND APPARATUS FOR PROVIDING LOCAL BREAKOUT IN A MOBILE NETWORK

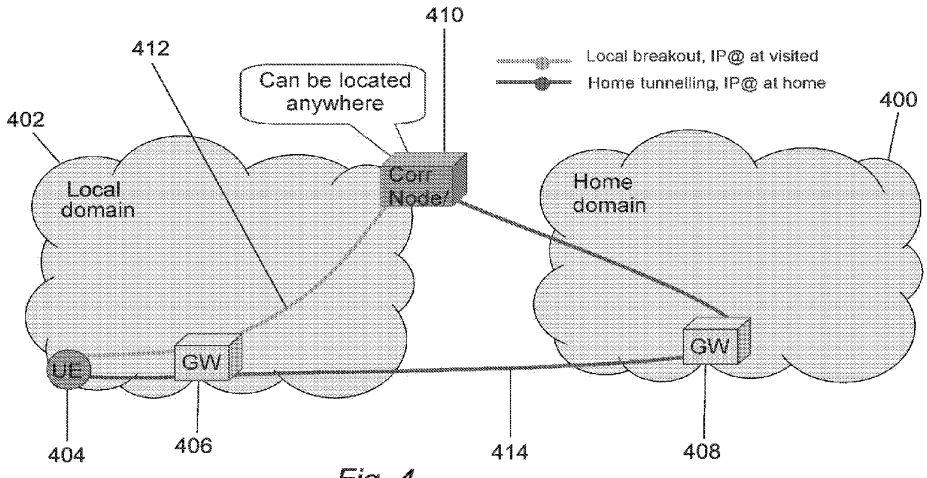


Fig. 4

(57) Abstract: A method of providing local breakout from a local network for a user equipment associated with a home network, which is located at the local network; wherein communication between the home and local networks includes information signalling between the home and local networks characterised in that the method comprises the steps of: • identifying a possibility of carrying out a first local breakout in relation to the communication of a specific type; • communicating the rules for the local breakout at the local network from the home network by means of an extension of the information signalling; • effecting local breakout from the local network for the user equipment based on the rules defined by the home network.

WO 2008/110215 A1

Title: A method and apparatus for providing local breakout in a mobile network.

Description

Field of the invention

This invention relates to a method and apparatus for providing local breakout in a mobile network, particularly but not exclusively a network which also includes an IP multimedia system (IMS).

Background of the invention

In a mobile network it is not uncommon for a user to wish to operate at a home location and maybe one or more other locations. That is to say a user may be roaming to another operator's network. Generally in this situation the media routing occurs as is shown in figure 1. Figure 1 shows a home domain 100 and a visited domain 102. If the user equipment 104 is located in a visited domain any media is routed through the visited domain gateway 106 to the home domain gateway 108 before it is passed to the network node 110 for onward transmission or as the ultimate destination.

The provision of local breakout is not typically deployed in most mobile networks, although a number of proposals of how this may be carried out, have been made with respect to the 3GPP standards. Figure 2 shows a proposal of approaching local breakout using the network address translator (NAT) function 200 in the visited network gateway 106. This NAT would be applied to any local breakout traffic and map the home address of the user to and/or from a local address in the visited public land mobile network (VPLMN). The NAT would be placed at an anchor node in the visited network and be under the control of the home operator such that the home public land mobile network (HPLMN) remains in control of which traffic flows are allowed to go locally or otherwise. The result of this is the requirement to have a control interface between the HPLMN and VPLMN which can specify the traffic which should go through the home gateway 108 and that which should not go through the home network gateway 108.

The type of control interface for controlling the decision in the VPLMN is not specified, however the 3GPP standards suggest one possible solution: the use of a policy and charging rules function (PCRF) by specifying a PCRF to PCRF roaming interface. This type of implementation is not yet specified and would require complex development to achieve a workable system, although a proposed example of such a system is shown schematically in figure 3.

One object of the present invention is to provide a means of local breakout , which overcomes at least some of the problems associated with the prior art.

Summary of the invention

According to one aspect of the present invention there is provided a method of providing local breakout from a local network for a user equipment associated with a home network, which is located at the local network; wherein communication between the home and local networks includes information signalling between the home and local networks characterised in that the method comprises the steps of: identifying a possibility of carrying out a first local breakout in relation to the communication of a specific type; communicating the rules for the local breakout at the local network from the home network by means of an extension of the information signalling; and effecting local breakout from the local network for the user equipment based on the rules defined by the home network.

According to a second aspect of the present invention, there is provided a local gateway for allowing local break out for a user equipment associated with home network, the local gateway comprising a control module for recognising the possibility of carrying out a local breakout in relation to a communication of a specific type; and communicating this possibility to the home network; a receiver for receiving rules for local breakout form the home network in the form of information signalling and a switch for switching traffic to local breakout in accordance with the rules.

According to a third aspect of the present invention, there is provided a home gateway for generating rules by which a local network can effect local break out or a user equipment associated with a home network, the home gateway comprising:

a control module for receiving a communication indicating the ability to effect local breakout from the local network in information signalling between the home and local gateway, wherein the control module generates a set of rules for local breakout and communicates the same with the local network, so as to permit local breakout at the local network.

This invention has the advantage that it is possible to adopt a system and network which permits local breakout and that overcomes many of the problems of the prior art. The invention requires very little changes to currently existing systems, which ensures that the invention can be adopted with minimal expense.

Brief description of the drawings

Reference will now be made by way of example, to the accompanying drawings, in which:

Figure 1 is a schematic diagram of the basic concept of roaming associated with the prior art;

Figure 2 is a schematic diagram of a prior art NAT-based local breakout;

Figure 3 is a schematic diagram of NAT controlled system using a PCRF to PCRF interface;

Figure 4 is a schematic diagram of the basic concept of local breakout according to the present invention;

Figure 5 is a more detailed diagram of NAT control as an extension of the PDP context signalling in accordance with the present invention;

Figure 6 is the signalling diagram of a primary PDP context activation in accordance with the present invention;

Figure 7 is the signalling diagram of a terminal initiated secondary PDP context activation in accordance with the present invention;

Figure 8 is a signalling diagram of a network initiated secondary PDP first context activation in accordance with the present invention;

Figure 9 is a signalling diagram of a network initiated secondary PDP second context activation in accordance with the present invention;

Figure 10 is a signalling diagram of a VPLMN initiated secondary first alternative PDP context set up in accordance with the present invention;

Figure 11 is a signalling diagram of a VPLMN initiated secondary second alternative PDP context to set up in accordance with the present invention.

Detailed description of the preferred embodiments

Referring to figure 4 the basic concept of local breakout in in accordance with the present invention is demonstrated. Figure 4 shows a home network 400, a visited (or local) network 402 at which a user equipment (UE) 404 is located. The home network and the local network include gateways 408 and 406 respectively. The UE 404 communicates with node 410, which can be located anywhere. In accordance with the present invention any media to or from the user 404 may be routed to the node 410 directly as shown by line 412 (local breakout, IP@local), rather than the home tunnelling route shown by line 414 (home tunnelling, IP@home). The user is said to be roaming when not located at the home network of the user. IP@local and IP@home are abbreviations for indicating that an IP address would be allocated at the local or home gateway, respectively.

It should be noted that the invention is described with respect to uplink traffic, but the invention may equally apply to downlink traffic as will be clear to the person skilled in the art.

The invention relates to a mobile network, for example a GPRS core network or any other type of network where roaming and/or local breakout are envisaged. Local breakout is used in this specification to refer to traffic which is not routed through the home network, but instead is routed in a different way. The control and management of this different routing will remain with the home network.

The manner in which the invention is achieved is explained in greater detail with respect to figure 5. This shows a home network 500 and visited (or local) network 502. The home network includes a gateway 504 connected to the packet data network 506. The local network includes a gateway 508 connected to a packet data network 510. A user terminal 512 is shown located at the current time at the local network. Depending on the nature of the terminal media from the terminal, data is passed to the local gateway 508 via any appropriate means. For

example this may be via a GSM/EDGE radio access network (GERAN) 514 or a UMTS terrestrial radio access network (UTRAN) 516. For either of these radio access networks traffic is passed through a serving GPRS support node (SGSN) 518. In an alternative e.g., an Evolved UTRAN 520 may be connected to the local gateway 508 without passing through an SGSN. The local core gateway 508 includes NAT control 522 for facilitating local breakout using an extension of a PDP context signalling without requiring a PCRF to PCRF interface. This has the effect of reducing the complexity of realising local breakout as will be described below.

There are a number of considerations that need to be made in order to implement the present invention and implement local breakout. The considerations include the following:

- Indication of the local breakout capability between gateways, terminals and networks;
- Determination of which traffic should go locally and which should not;
- Determining whether mixed traffic is allowed or not in a single PDP context
- Determining whether the VPLMN or the HPLMN select the local address required;
- Determination of the PDP context activation procedures;
- Determination of the PDP context setup by VPLMN request;
- The provision of a policy and charging rules function to the VPLMN gateway depending on the type of control previously determined.

For ease of understanding each of the above considerations will be considered in turn.

Indication of the local breakout capability between gateways, terminals and networks.

When a user is located within a local network (also known as the visited public land mobile network (VPLMN)), determination is necessary to indicate whether the local network is capable of providing local breakout to the home

network (also known as the home public land mobile network (HPLMN)). This determination can be made in a number of different ways. The local breakout capability can be agreed as part of roaming agreement between the local and home operators or networks. In this circumstance, the identification of the operator of the user will be used to determine whether there is an agreement for the provision of local breakout. The identification may be made by means of a list of home operators with which the local operator has an agreement, for example.

The local breakout capability can be signalled as part of the attachment or authentication procedure from the local network to the home network when the user terminal attaches to the local network. The local breakout capability will be signalled, possibly along with other capabilities, as a bit or bits in a predetermined part of the attachment signalling. For example, in the existing GPRS attachment procedure, the Update Location signal may be used to signal local breakout capability.

The local breakout capability can be signalled in the packet data protocol (PDP) context request message that is sent from the VPLMN to the HPLMN by adding a new field to a possibly evolved/extended Create PDP Context Request message. The packet data protocol context will depend on the format of the data packet in question. If any other interfaces exist between the local and home networks the local breakout capability can be indicated in any of these types of communication. For example once PCRF-PCRF roaming interface is implemented the local breakout capability may be indicated therein although this is not necessary for realisation of the invention.

The indication of local breakout capability need not be merely yes or no, but could be dependent on other criteria, for example, on the subscriptions of the user or users packet data type or whatever. In other words, for certain types of packets local breakout may be permitted but for others it may not. In the event that the HPLMN does not receive any indication of local breakout capability from the VPLMN the HPLMN can assume that there is no such capability at the VPLMN and operate in an appropriate manner.

The examples of determination of local breakout capability are just examples and other means of communicating the capability from the VPLMN to the HPLMN are equally as relevant to the present invention as those described above.

Determination of which traffic should go locally and which should not

As indicated above not all traffic should always be part of local breakout traffic. This decision should come from the home network, taking into account e.g. whether policy and charging control is preferred in the home network or not.

A local breakout selection criterion is used by the VPLMN gateway for a given PDP context. If there is no local breakout selection criteria available then all traffic would be transported as defined by existing GPRS (General Packet Radio Service) protocols, e.g., all the traffic will be processed via the home network in accordance with currently accepted techniques.

The PDP context may contain a single bit which may be read at the gateway to determine whether the gateway should break out the traffic locally or should transmit the traffic to the home network. This single bit may be referred to as the home/local breakout selector bit and will be part of the PDP context in the local gateway.

In a further embodiment a set of packet filters (not shown) may be provided to determine which media should be broken out locally and which should be transmitted via the home network. The TFT (Traffic Flow Template) format used for PDP context can be reused for specifying local breakout filters. The home network will construct the filtering rules for determining which packets are broken out locally and which are not. It should be noted that the home network may not know the local address used by the NAT at this stage. If this is the case the home network can use e.g., a predetermined character in the filtering rules which gives the local networks a possibility to replace this predetermined character with the correct local IP address which can be generated by the local network.

In this situation where a secondary PDP context activation occurs with the same user, i.e. another call or communication using the same IP address by the same user in the local network, the local network may use the rules already

defined for the first PDP context activation. That is to say the IP address of the same user has been activated for a local breakout under a specific PDP context.

The local gateway can use any combination of the various different selection rules indicated above, either individually or by using more than one of the rules. This provides a very flexible means of determining the type of traffic, which can be enabled for local breakout for individual users. It is possible to specify local breakout filters for each primary PDP context activation and then use the same filters, without needing to specify them again at any subsequent secondary PDP context activation. It is possible to specify at a primary PDP context activation that all traffic should be transmitted via the home network. This can be updated at a later time by specifying a different local breakout filter for each secondary PDP context activation. A further possibility is to specify the local breakout filters at primary PDP context activation and to activate a secondary PDP context for all traffic which is local, overriding the filter for the primary PDP context.

Determining whether mixed traffic is allowed or not in a single PDP context

Another consideration that must be taken into account is whether or not both home tunnelling and local breakout traffic can occur in a single PDP context. The idea of allowing both home tunnelling and local breakout traffic is referred to as "mixed traffic". Basically there are two possibilities in respect of mixed traffic: allowing it or not allowing it.

One embodiment of the present invention provides that mixed traffic is disallowed. Traffic in a single PDP context can be either tunnelled to the home network or be subject to local breakout, but cannot be subject to both. If no mixed traffic is to be allowed a single bit is sufficient to indicate to the gateway how the specific PDP context should be handled. In this case it is not necessary to use local breakout filters as described above. The single bit indicates to the gateway that the traffic must be either tunnelled to the home network or broken out locally. The bit could be part of the PDP context, stored in the gateway. In the case of uplink traffic, home traffic is tunnelled to the home gateway, and in the case of local traffic this may be for example „NAT-ed". There are a number of advantages in disallowing mixed traffic in a single PDP context, including the fact that there is

a requirement for less additional parameters (i.e. no local breakout filters are required) and less modification to the existing PDP context signalling is required. On the other hand, this may lead to a greater number of PDP contexts being required, which may impact resources in the terminal and network nodes.

If a terminal is not adapted to handle secondary PDP context activations it would not be possible for these terminals to take advantage, in this embodiment, of local breakout. In this embodiment there is no mixed traffic in one PDP context, but there is traffic into different secondary PDP context depending on whether it is local or home traffic. So it is important that the terminal supports secondary PDP context activation.

In another embodiment of the invention mixed traffic may be allowed. In this situation, both tunnelling to the home network and local breakout is possible for a single PDP context. This is a more general approach than disallowing mixed traffic but requires additional functionality. In the first instance it is necessary to specify the local breakout filters mentioned above. In addition, separate quality of service (QoS) parameters may be applied to tunnelling to the home network than would be the case for the local breakout traffic. The individual quality of service parameters for each may not be completely independent, as generally the media has to be transmitted by the wireless operator irrespective of which route is chosen. However, the bit rate parameters of each may be different.

From a Quality of Service point of view, the sum of the tunnelling to the home network and local breakout traffic is what is relevant to both the terminal and the gateway in the local network. As a consequence of this if a network initiated PDP context setup is started, the home network gateway should not only specify the overall quality of service parameters for the PDP context but also the bit rate parameters that apply to the local breakout traffic or the tunnelling to the home network. This is due to the fact that the total bit rate is equal to the sum of the home tunnelling bit rate and the local breakout bit rate. Accordingly it is only necessary for the home gateway to specify one of the individual bit rates, either home tunnelling or local breakout. As the total bit rate is known, the other one of the two individual bit rates can be calculated.

In the case of a terminal initiated PDP context setup it is the terminal which will specify the quality of service parameters. The home gateway determines the bit rate for the local breakout traffic and supplies it to the local gateway.

Determining whether the VPLMN or HPLMN select the local address required

In order for a local breakout to occur a local address has to be selected so that the NAT in the local network can map the PDP address of the terminal (or terminals) to and from the local address (or addresses). This local address can be selected either by the local network or by the home network. In each case a different functionality is required. It is expected that the typical way in which the local address will be selected is by local network rather than the home network although the invention is not limited to this.

In the case where the home network selects the local address, additional configuration parameters are required to indicate the available local addresses which may be used. This could form part of a roaming agreement or may be implemented in other ways. Address selection by the home network could be based on an alignment with fixed network architectures, where master slave relationship exists between the SIP server and the media server. In fixed networks, a SIP server node assigns the address and notifies the media gateway about the selection. This may result in address allocation in the home network. In one embodiment of the invention the home network selects the local address by means of signalling in the PDP context signalling from the home to local network.

If the local network selects the local address, this will be determined based on local rules. The local network may notify the home network of the chosen address, although this is optional.

In a further embodiment of the present invention, there are circumstances where the NAT carries out port translation functions (NAPT). If this is the case port translation parameters need to be provided as part of the PDP context activation procedures.

PDP context activation procedures

A number of different scenarios for PDP context activation procedure are described with respect to the signal diagrams in figures 6, 7, 8 and 9. In these diagrams the text in italics indicates the additional PDP context signalling provided by the present invention. It should be noted that not all the signalling between the user equipment, the local gateway and the home gateway are shown in the signalling diagrams, instead only those relevant to the explanations at that time are shown. Where an action is activated from the user equipment, the user equipment is making a call or trying to send something to a third party. Where the action is activated by a network (generally the home network) a third party is making a call or trying to send something to the user equipment.

Figure 6 shows the primary PDP context activation initiated by the user equipment (UE) 600 via the local and home networks 602 and 604 respectively. Primary PDP context activation is generally terminal initiated, although the network initiated primary PDP context activation may occur. The user equipment generates and activates a PDP context request, which is transmitted to the local gateway 606. It will be appreciated that at other means of local breakout indication may alternatively be used, as discussed above. The local gateway generates a create PDP context request that includes an indication that local breakout capability is permitted (illustrated by signal 608) in the local network. The indication may include details relating to the type of traffic which can become local breakout traffic, details of address selection, information relating to mixed traffic, packet filters, NAT configuration data or any other appropriate or relevant information. The home gateway responds to the create PDP contexts with a local breakout request 610. The local gateway can then activate the PDP context accept signal which is transmitted to the user equipment 612. If either network is unable to respond to any message an error message or failure message may be sent between the gateways by means of the local breakout error handling box 614. An error may result in a resend of the request or reply, or any other type of request depending on the error type that is recognized by the appropriate gateway.

If a network initiated primary PDP context activation occurs, the signalling diagram of figures 6 would be modified as follows. The activate PDP context

request would e.g., be preceded by a network initiated signal to the terminal requesting the transmission of the activate PDP context request. The primary PDP context activation signal may be combined with attachment signalling. Attachment is a separate procedure that is performed before primary PDP context activation, however attachment and primary PDP context activation may be combined.

Figure 7 shows the signal diagram for a terminal initiated secondary PDP context activation. In figure 7, like elements are given the same reference numerals as in figure 6. The secondary PDP context activation is very similar to the primary PDP context activation with the exception that the request 608 and the response 610 may not include local breakout capability requests or responses, as these may have already been provided in the primary PDP context activation. Thus in this case the user equipment activates a secondary PDP context request 616, which causes the local network to generate a create PDP context request without necessarily indicating local breakout capability. The home gateway similarly responds by it providing a permission to create a PDP context response either with or without the local breakout permission as the case may be. The local gateway then activates the user equipment by means of a secondary PDP context response 618.

Figures 8 and 9 show two possible alternatives for the network initiated secondary PDP context activation.

The first alternative, as shown in figure 8, and is in accordance with the network initiated secondary PDP context activation in GPRS release 7. This is similar to the terminal initiated secondary PDP context activation and differs there from by the inclusion of an initiation of a PDP context activation 800 from the home gateway to the local gateway, which generates a request for PDP context activation 802 from the local gateway to the user equipment. In figure 8, like elements are shown by the same reference numerals as figure 6 and 7. As in figure 7, since this is a secondary activation, local breakout requests and responses may not be included if that is the chosen setup by the home and local networks.

The second alternative, shown in figure 9 is in accordance with the network initiated set up in the system architecture evolution (SAE) as disclosed in the 3GPP technical report 23.882. The signalling is started by the home gateway sending a create bearer request 900. It is transmitted to the local gateway and may include a local breakout request. The home gateway relies on the fact that an earlier primary PDP context activation message has indicated local breakout capability in the local network. The local gateway sends an activate bearer request 902 to the user equipment and the users equipment generates and activate bearer response 904 which is sent back the local gateway. The local gateway can then communicate a create bearer response 906 to the home gateway. The PDP context modification and the deactivation procedures may also be defined based on the activation procedures.

Determination of the PDP context set up by VPLMN request

It is generally the case, for a home IP address, the home gateway or the user terminal sets up a new PDP context. However for local breakout, the local gateway may wish to setup new local breakout traffic that would require a new PDP context set up or modification. This may be the case in a situation where the local network takes part of the service provisioning for example service specific nodes, such as P-CSCF, media gateway, etc. In order to achieve the network requested PDP context setup the local network may send a request to the home gateway asking for a secondary PDP context activation. In this way it is possible to start a new local breakout initiated by the local network but about which the home network is fully informed and in full control.

Signalling diagrams 10 and 11 show two alternatives of network initiated PDP context activations in this scenario. Referring to figure 10, the local gateway 602 generates a VPLMN requested PDP context activation 1000 to the home gateway. The home gateway initiates a PDP context activation 1002 which is sent back to the local network 602. The local network then requests PDP context activation 1004 from the user equipment. The user equipment can then activate a secondary PDP control request 1006 which causes the local gateway to generate a create PDP context request which may indicate local breakout capability 1008. The home gateway replies with a create PDP context response including a local

breakout request 1010. This causes the local gateway to send an activate secondary PDP context response 1012 to the user equipment. In this way the control of local breakout remains at the home network as the home network is not required to accept the initial request of the local gateway. If this is the case and the home network does not wish local breakout to occur a negative response may also be sent to the local gateway.

Referring to figure 11 a second alternative of how the local network may initiate secondary PDP context setup is shown. Again the local gateway generates a VPLMN requested PDP context activation 1000 this causes the home gateway to generate a create bearer request including the local breakout request 1002. The local gateway then generates an activate bearer request 1100 to the user equipment which then responds with an activate bearer response 1102. The local gateway then generates a create bearer response 1104 which is sent back to the home gateway. Once again the home gateway is in control of any determination as to whether or not a local breakout should be allowed.

The provision of policy and charging rules to the VPLMN gateway depending on the type of control previously determined.

In the case of home tunnelling traffic it is clear that the home operator or network via the home gateway is in a position to apply policy and charging functions e.g., according to 3GPP TS 23.203. However local breakout traffic may bypass the policy and charging enforcement point in the home gateway. For this reason the home network may require that policy and/or charging rules are applied to the local breakout traffic as would be the case for the home tunnelling traffic. To achieve this policy and charging rules could be provided as further optional extensions to the PDP context setup signalling from their home network to the local network. In other words, policy and charging rules could be communicated alongside local breakout filters that specify which traffic is permitted to go locally. One example of a simple policy rule would be to perform bandwidth policing of the traffic in the local gateway. Alternatively marking or remarking packets based on packet filtering and bandwidth parameters may also be used. The policy and charging rules can be based on a subset of those specified over the Gx interface and could be attached to the PDP context messages.

PDP is a term which indicates the type of packet data protocol which applies for a specific type of communication that may be instigated by a terminal or gateway. In other words this is an indication of the various protocols supported by the terminal, the network or both. PDP context signalling refers to the control signalling that is present between the two gateways.

The example shown in this invention is in relation to IMS, although it will be appreciated that this invention may apply also to I-WLAN. In this case a TTG node is used to achieve the dynamic configuration of a NAT function to achieve local breakout. In this case the PDP context signalling is extended such that the signalling goes between the TTG and a gateway in the network of the operator.

It should be noted that the invention described above may be utilised in a number of environments, for example for a large operator in the country for example or between national companies of the same operator that have a close relationship. Although, these are merely examples and many other possibilities may arise. It should also be noted that while this invention has been described with respect to 3GPP, it may also apply to other wireless communications standards. The present invention allows local breakout to be realised without the extra complexity of standardisation, implementation or the deployment of special interfaces. The PCRF-PCRF type of interface is not required for the present invention. This will have a great advantage in providing local breakout in a simple, cost-effective and instantly available manner.

Claims

1. A method of providing local breakout from a local network for a user equipment associated with a home network, which is located at the local network; wherein communication between the home and local networks includes information signalling between the home and local networks characterised in that the method comprises the steps of:

   - identifying a possibility of carrying out a first local breakout in relation to the communication of a specific type;

   - communicating the rules for the local breakout at the local network from the home network by means of an extension of the information signalling;

   - effecting local breakout from the local network for the user equipment based on the rules defined by the home network.

2. The method as claimed in claim 1, further comprising communicating packet data protocol (PDP) context signalling as the information signalling.

3. A method as claimed in claim 1 or 2, further comprising using the previously established rules associated with the local breakout in relation to a subsequent local break out of the same specific type.

4. A method as claimed in any preceding claim, wherein the step of identifying further comprises identifying a possibility of carrying out a first local breakout in relation to the communication of a specific PDP context.

5. A method as claimed in any preceding claim, further comprising processing at least some of the information by means of a network address translator (NAT) at the local gateway.

6. A method as claimed in any preceding claim, further comprising assigning a local breakout address at the local network for any local breakout traffic.

7. A method as claimed in any preceding claim, further comprising defining the rules for any local breakout at the local network.

8. A method as claimed in claim 7, wherein the step of defining the rules comprises indicating the local breakout capability at the local network.

9. A method as claimed in claim 7 or claim 8, wherein the step of defining the rules comprises determining which traffic should be subjected to local breakout and which should not.

10. A method as claimed in any of claims 7 to 9, wherein the step of defining the rules comprises determining which type of traffic can be subjected to both local breakout and home network tunnelling.

11. A method as claimed in any one of claims 7 to 10, wherein the step of defining the rules comprises determining the local address for the user equipment during local breakout.

12. A method as claimed in any one of claims 7 to 11, wherein the step of defining the rules comprises determining policy and charging rules for the local gateway.

13. A local gateway for allowing local break out for a user equipment associated with home network, the local gateway comprising

- a control module for recognising the possibility of carrying out a local breakout in relation to a communication of a specific type; and communicating this possibility to the home network;

- a receiver for receiving rules for local breakout form the home network in the form of information signalling

- a switch for switching traffic to local breakout in accordance with the rules

14. A home gateway for generating rules by which a local network can effect local break out or a user equipment associated with a home network, the home gateway comprising: a control module for receiving a communication indicating

the ability to effect local breakout from the local network in information signalling between the home and local gateway, wherein the control module generates a set of rules for local breakout and communicates the same with the local network, so as to permit local breakout at the local network.

15. The gateway of claim 13 or claim 14, wherein the information signalling comprises PDP context signalling

16. A network including a gateway as claimed in any one of claims 13 to 15.

17. A system including one or more networks as claimed in claim 16.

18. A computer program comprising instructions for carrying out the steps of the method according to any one of claims 1 to 12 when said computer program is executed on a computer.

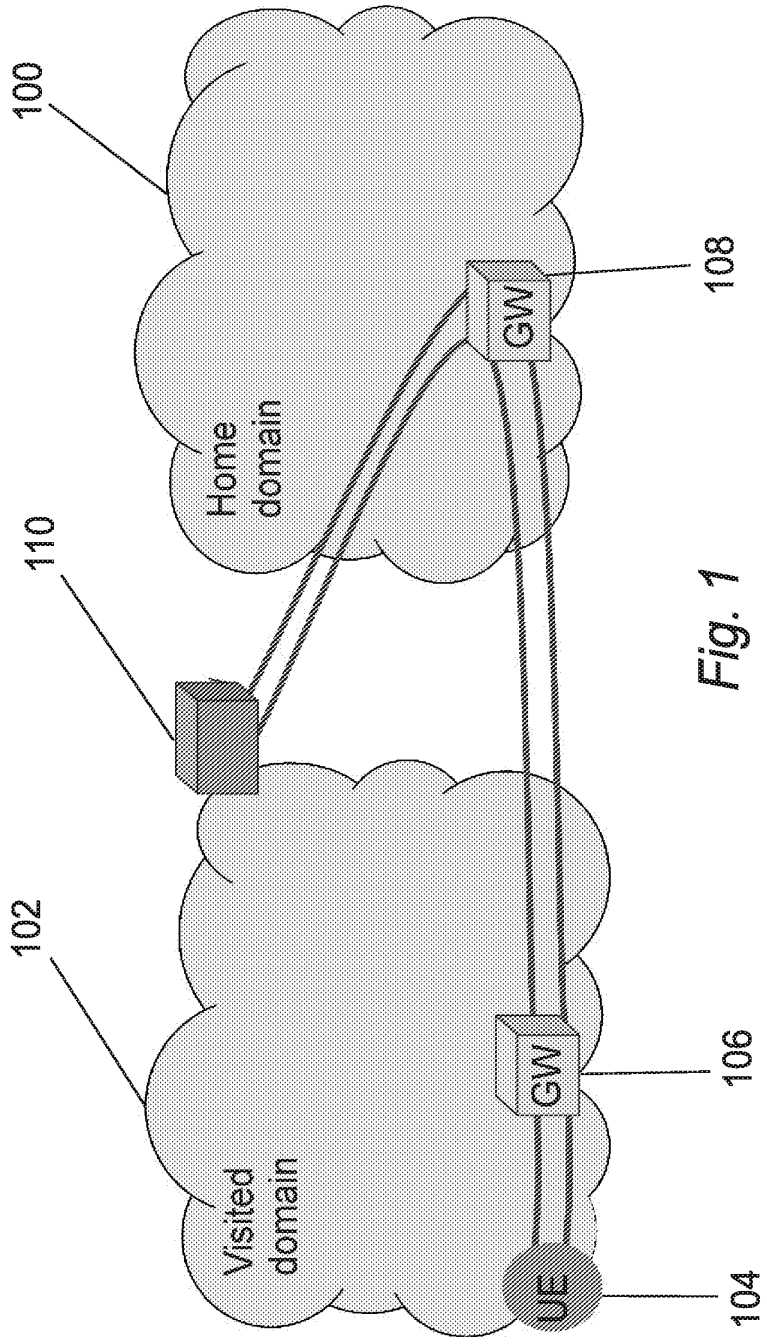


Fig. 1

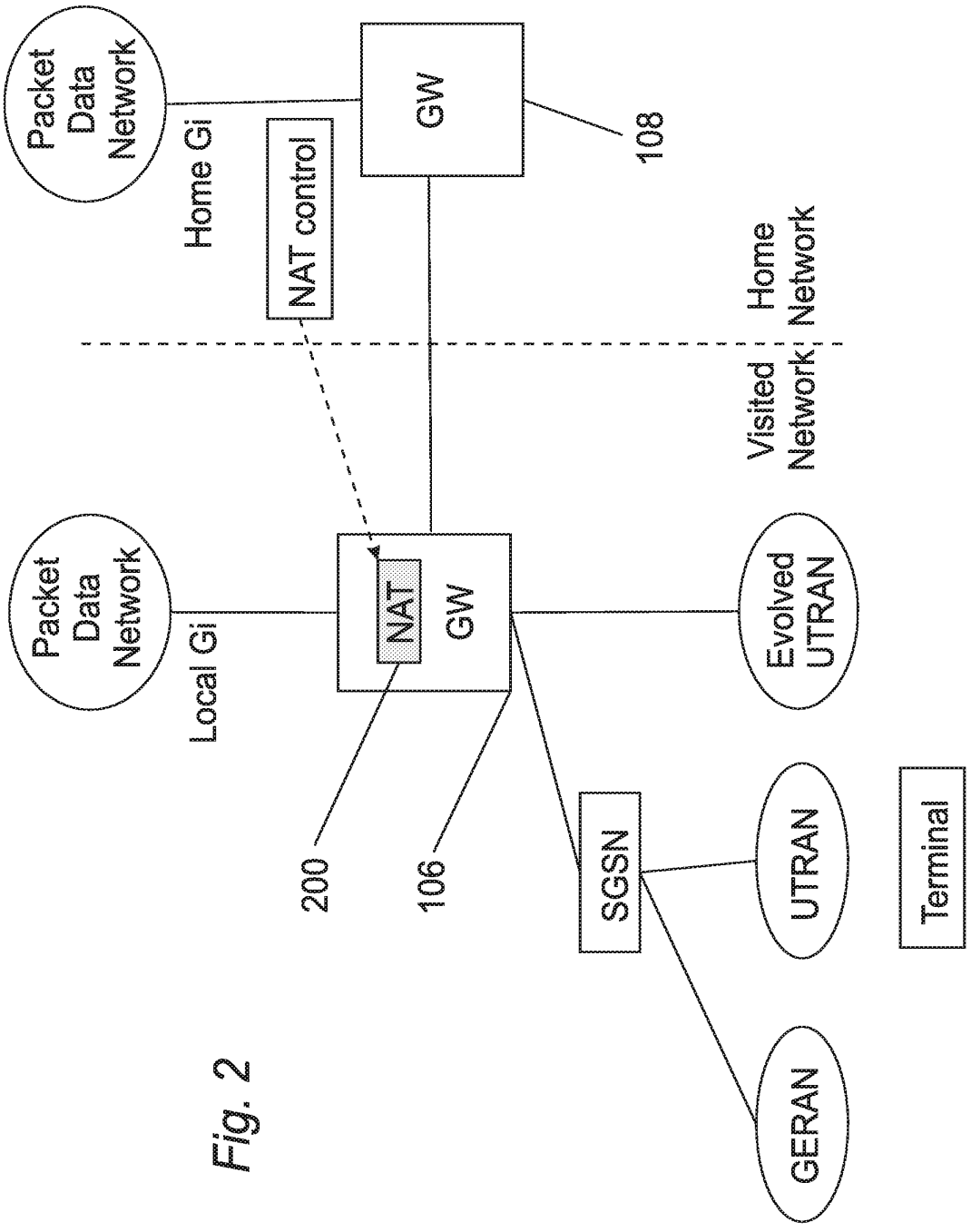

Packet Data Network
Home Gi
NAT control
GW
108
Home Network
Visited Network
Packet Data Network
Local Gi
NAT
GW
Evolved UTRAN
200
106
SGSN
UTRAN
Terminal
GERAN

Fig. 2

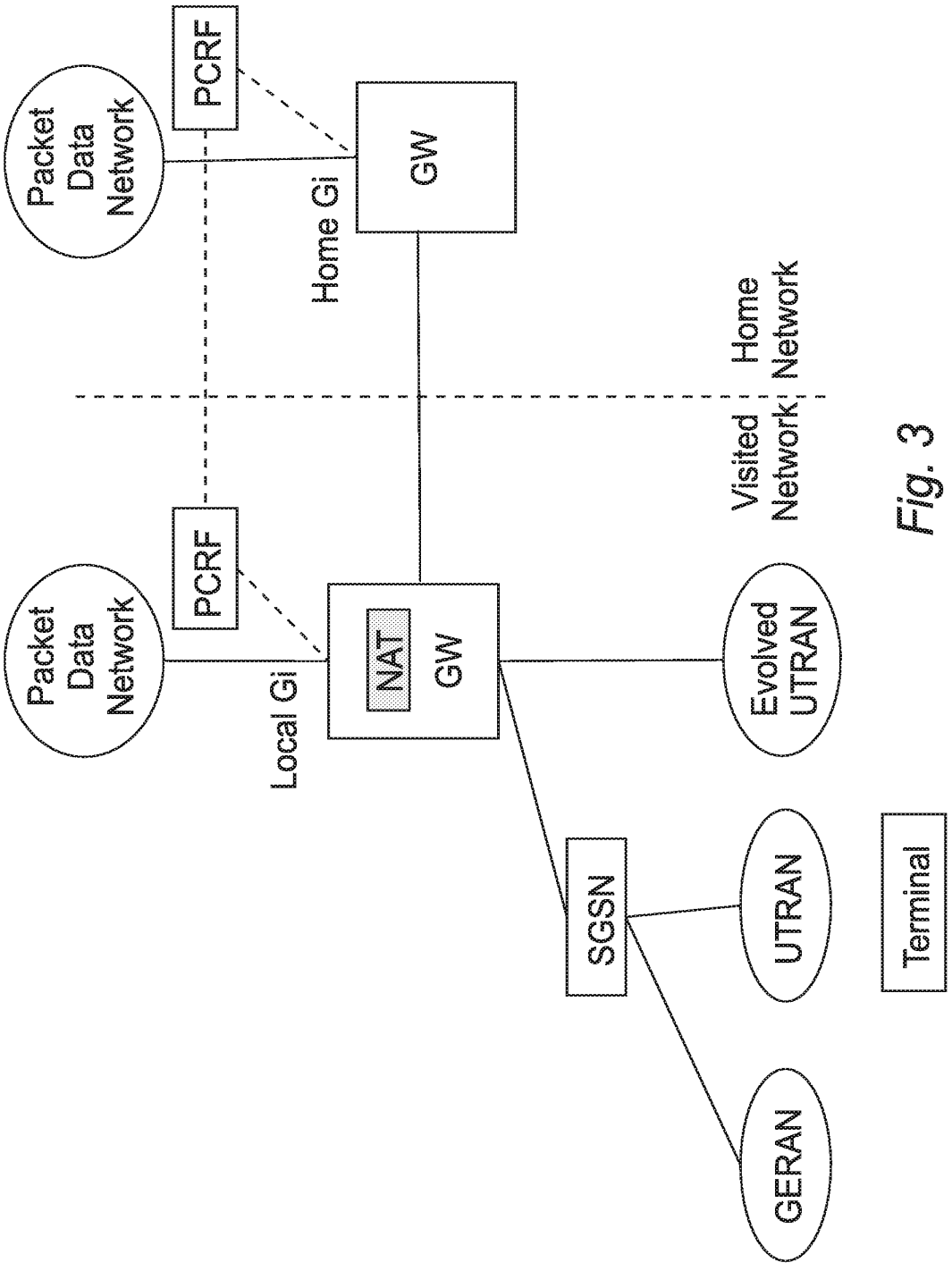

Packet Data Network
PCRF
GW
Home Gi
Home Network
Visited Network
Packet Data Network
PCRF
NAT
GW
Local Gi
Evolved UTRAN
SGSN
UTRAN
Terminal
GERAN

Fig. 3

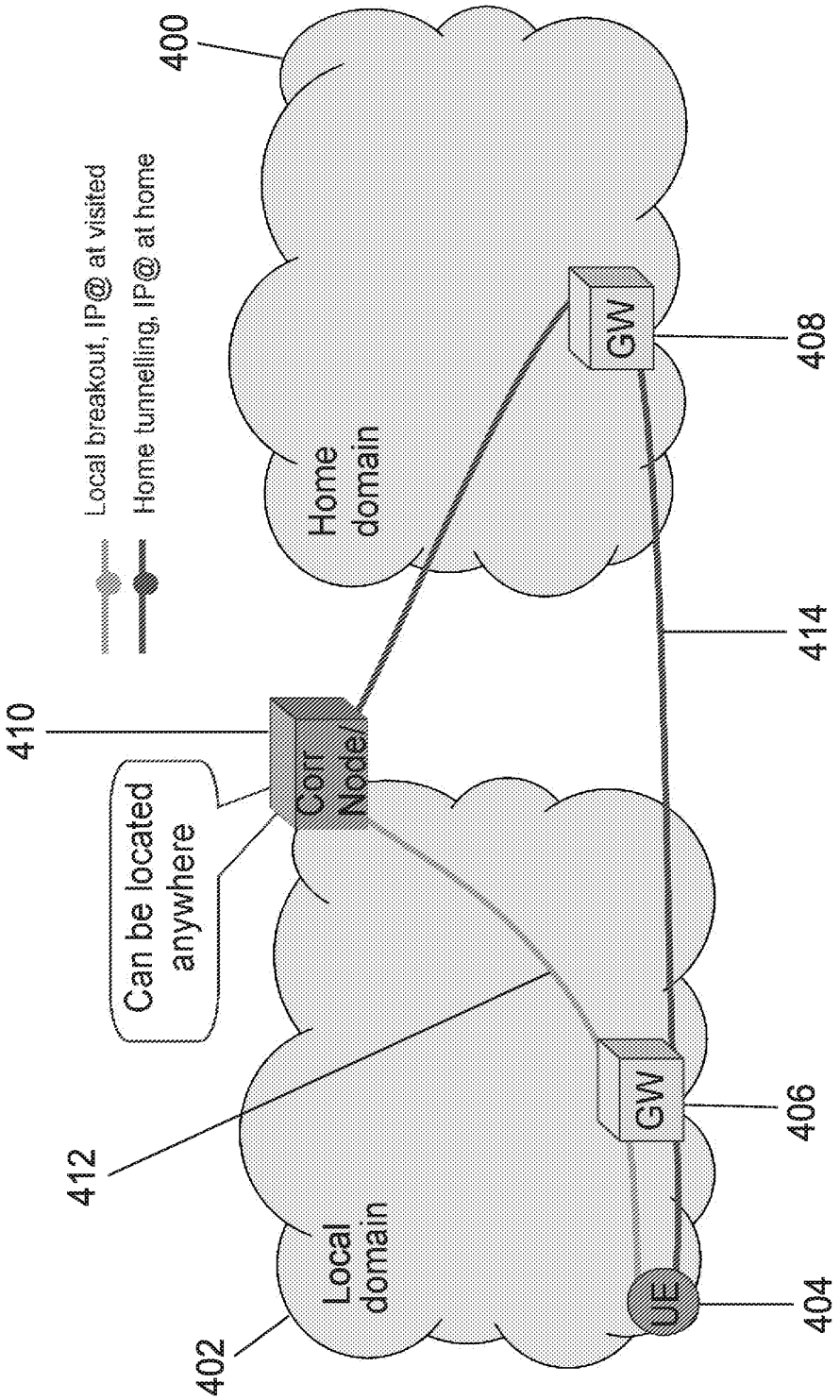

400
Local breakout, IP@ at visited
Home tunnelling, IP@ at home
Home domain
GW
408
414
410
Corr Node
Can be located anywhere
412
GW
406
Local domain
UE
404
402

Fig. 4

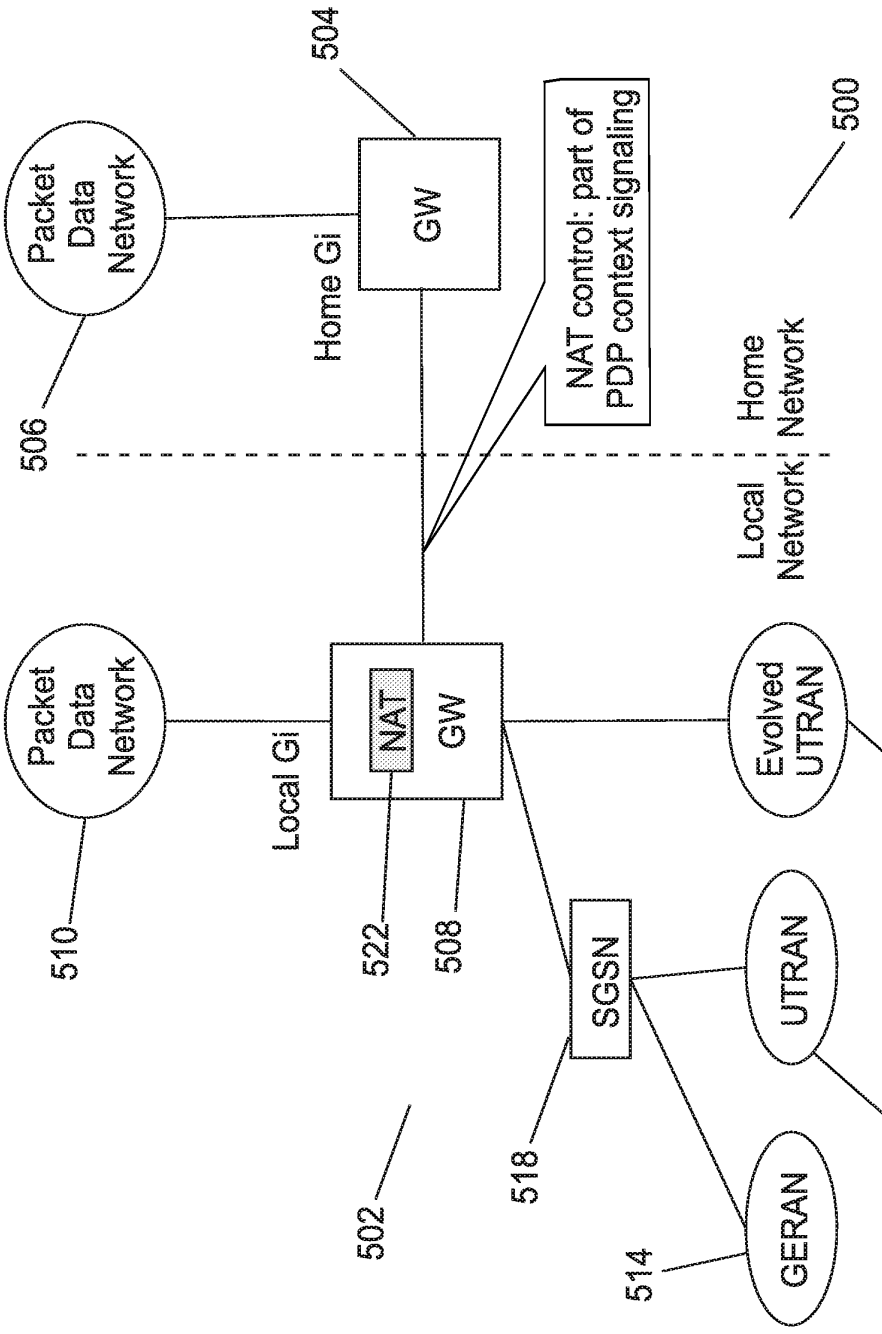

Packet Data Network
506
Home Gi
GW
504
NAT control: part of PDP context signaling
500
Home Network
Local Network
Packet Data Network
510
Local Gi
NAT
GW
522
508
Evolved UTRAN
520
SGSN
UTRAN
Terminal
502
518
516
512
GERAN
514

Fig. 5

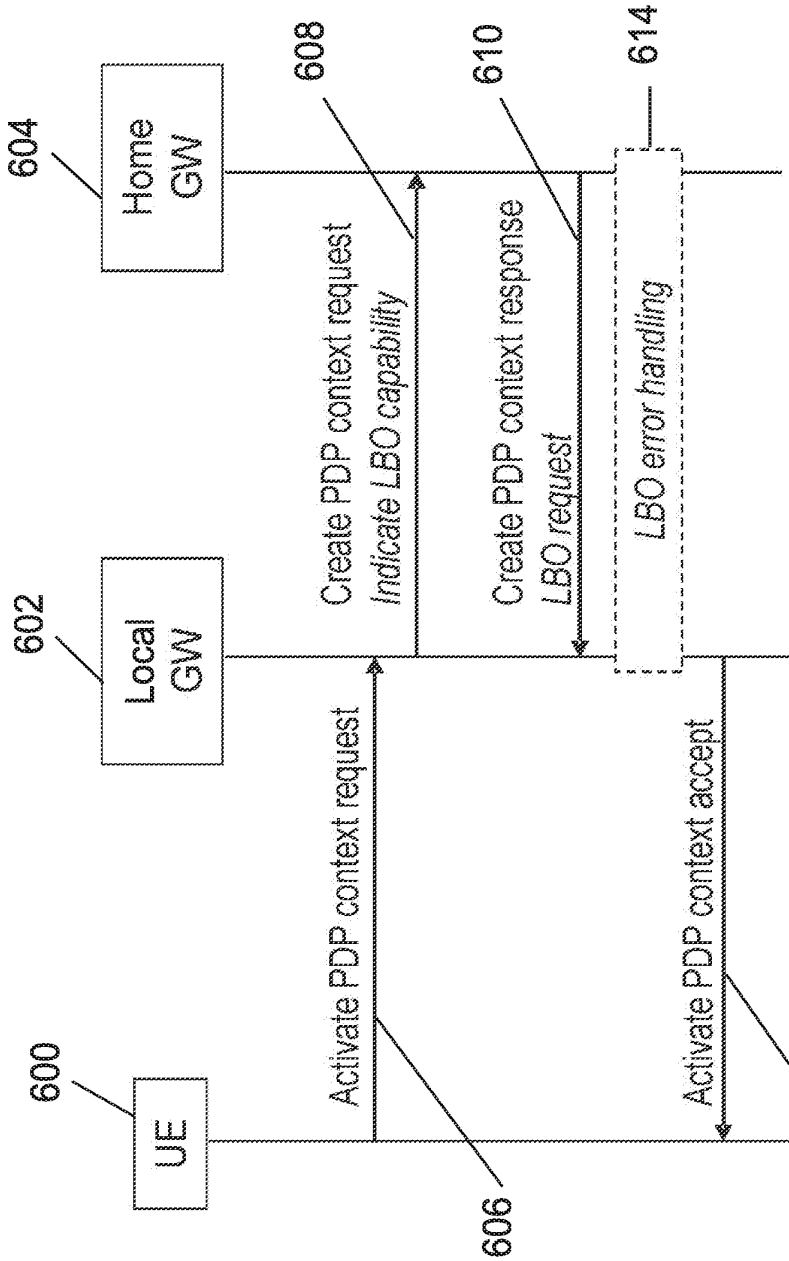

600
UE
602
Local GW
604
Home GW
606
Activate PDP context request
608
Create PDP context request
Indicate LBO capability
610
Create PDP context response
LBO request
612
Activate PDP context accept
614
LBO error handling

Fig. 6

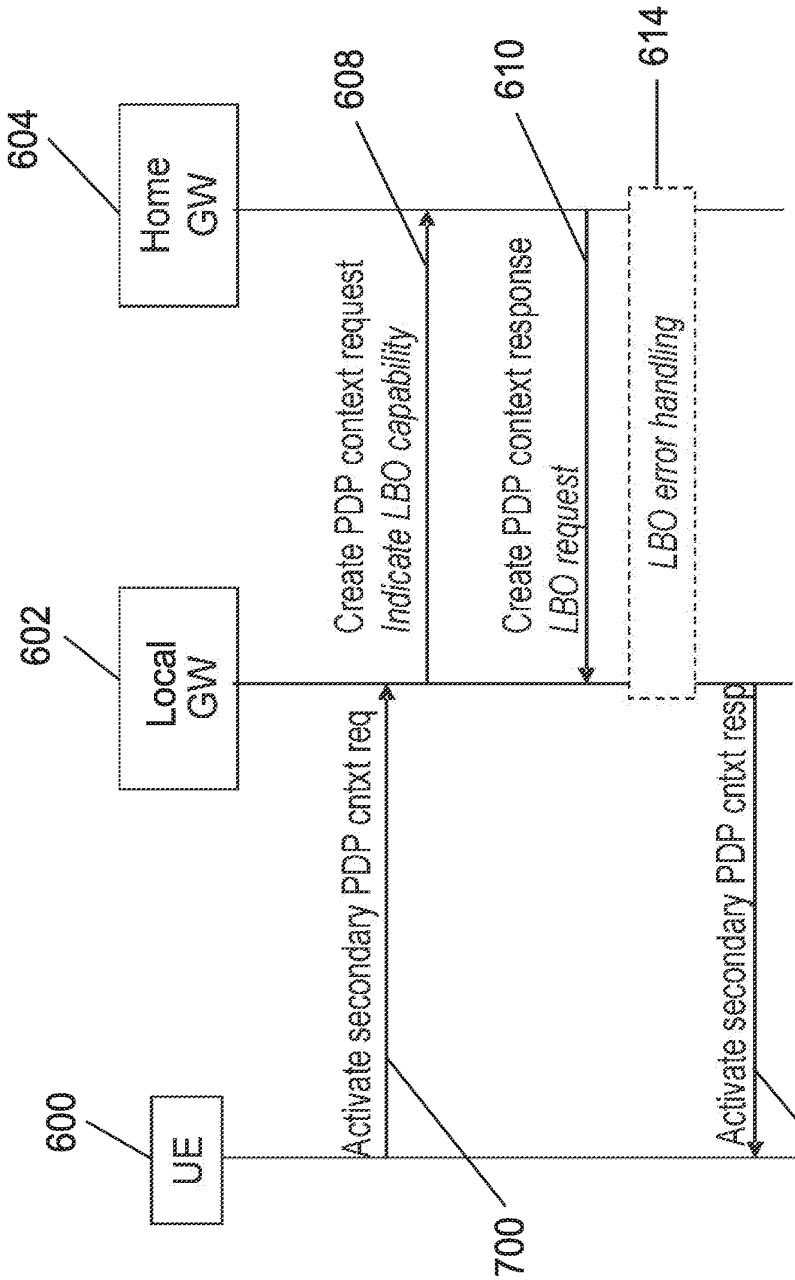

604
Home GW
608
610
614
602
Local GW
Create PDP context request
Indicate LBO capability
Create PDP context response
LBO request
LBO error handling
600
UE
Activate secondary PDP cntxt req
Activate secondary PDP cntxt resp
700
702

Fig. 7

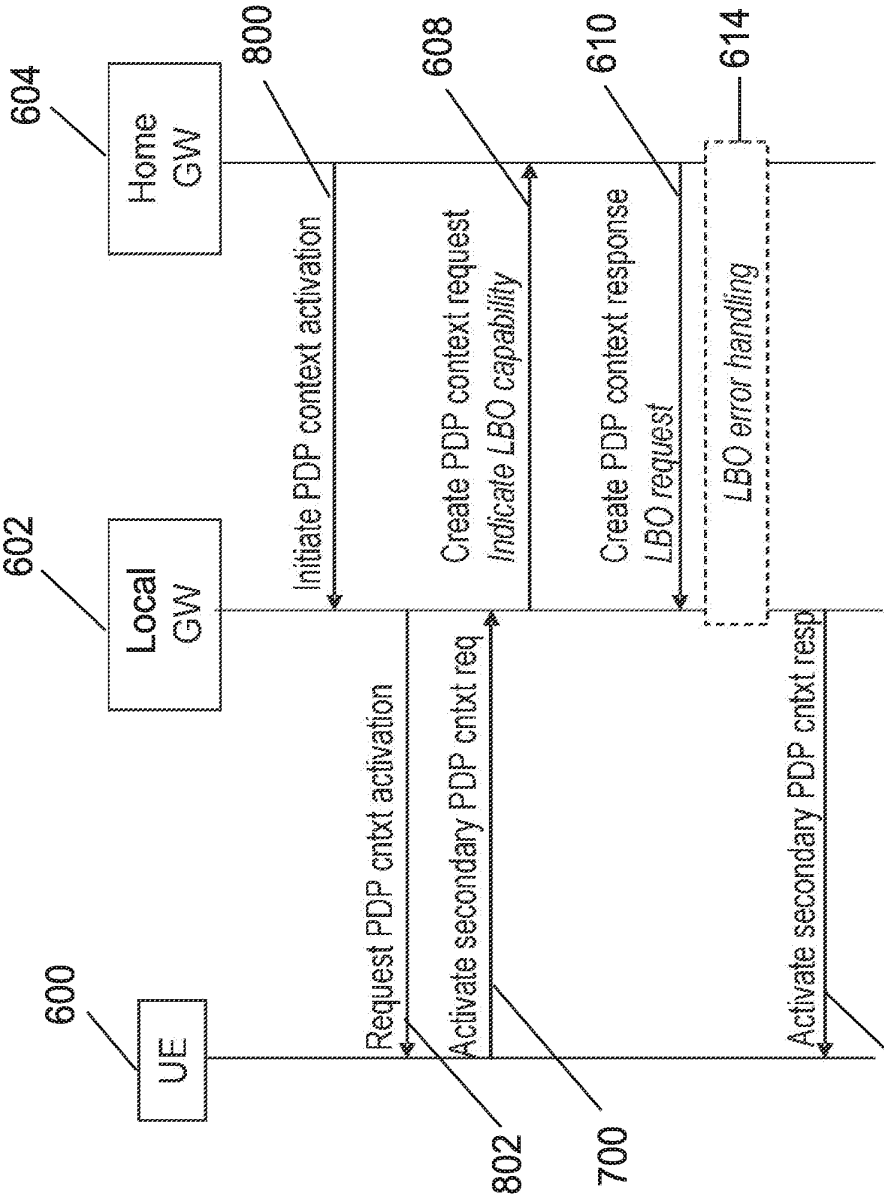

604
Home GW
800
608
610
614
602
Local GW
Initiate PDP context activation
Create PDP context request
Indicate LBO capability
Create PDP context response
LBO request
LBO error handling
600
UE
Request PDP cntxt activation
Activate secondary PDP cntxt req
Activate secondary PDP cntxt resp
802
700
702

Fig. 8

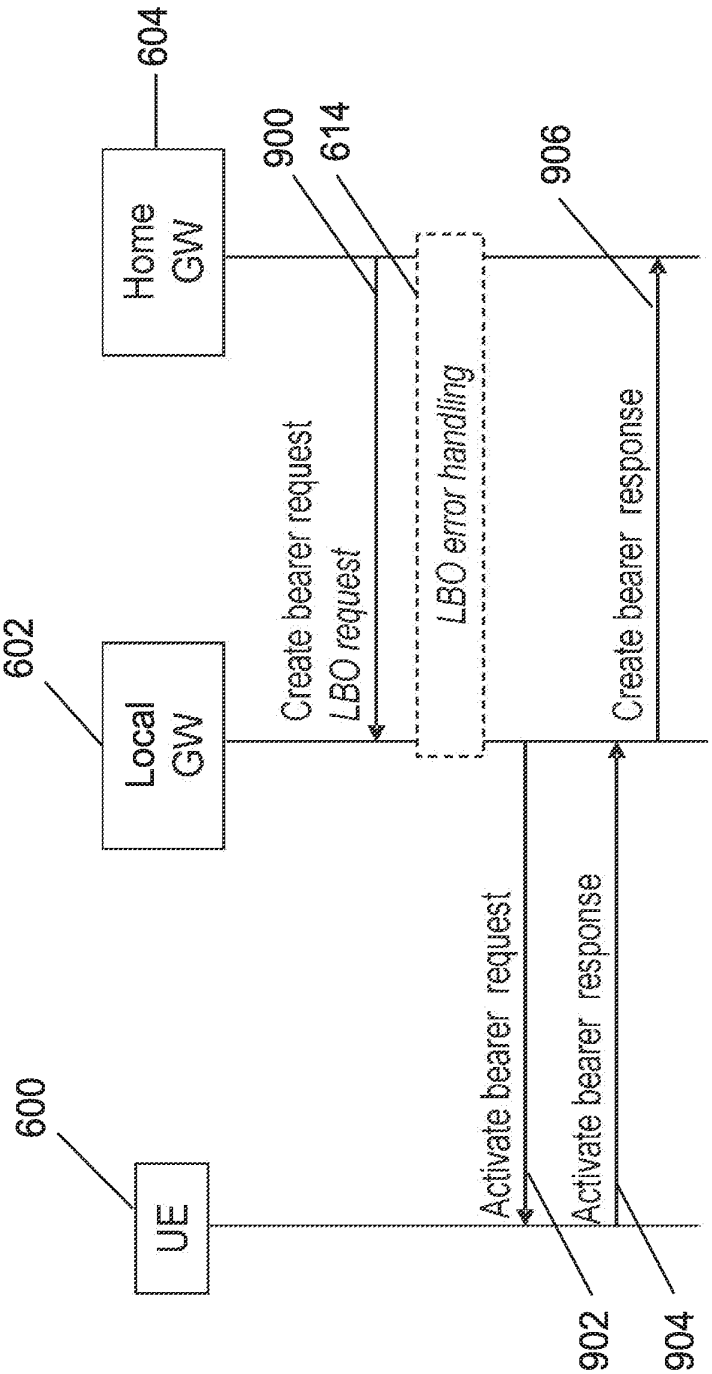

604
Home GW
900
614
906
602
Local GW
Create bearer request
LBO request
LBO error handling
Create bearer response
600
UE
Activate bearer request
Activate bearer response
902
904

Fig. 9

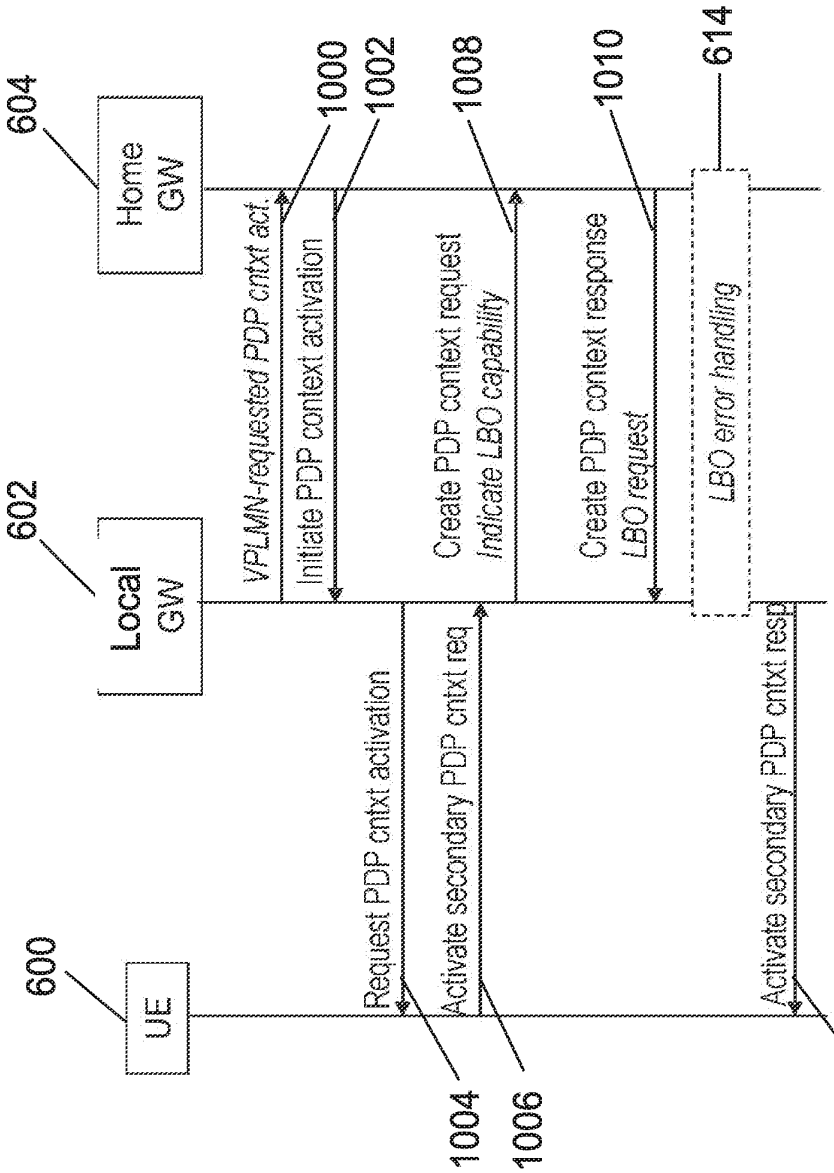

600
UE
602
Local GW
604
Home GW
Request PDP cntxt activation
VPLMN-requested PDP cntxt act.
Initiate PDP context activation
Activate secondary PDP cntxt req
Create PDP context request
Indicate LBO capability
Create PDP context response
LBO request
LBO error handling
Activate secondary PDP cntxt resp
1000
1002
1004
1006
1008
1010
1012
614

Fig. 10

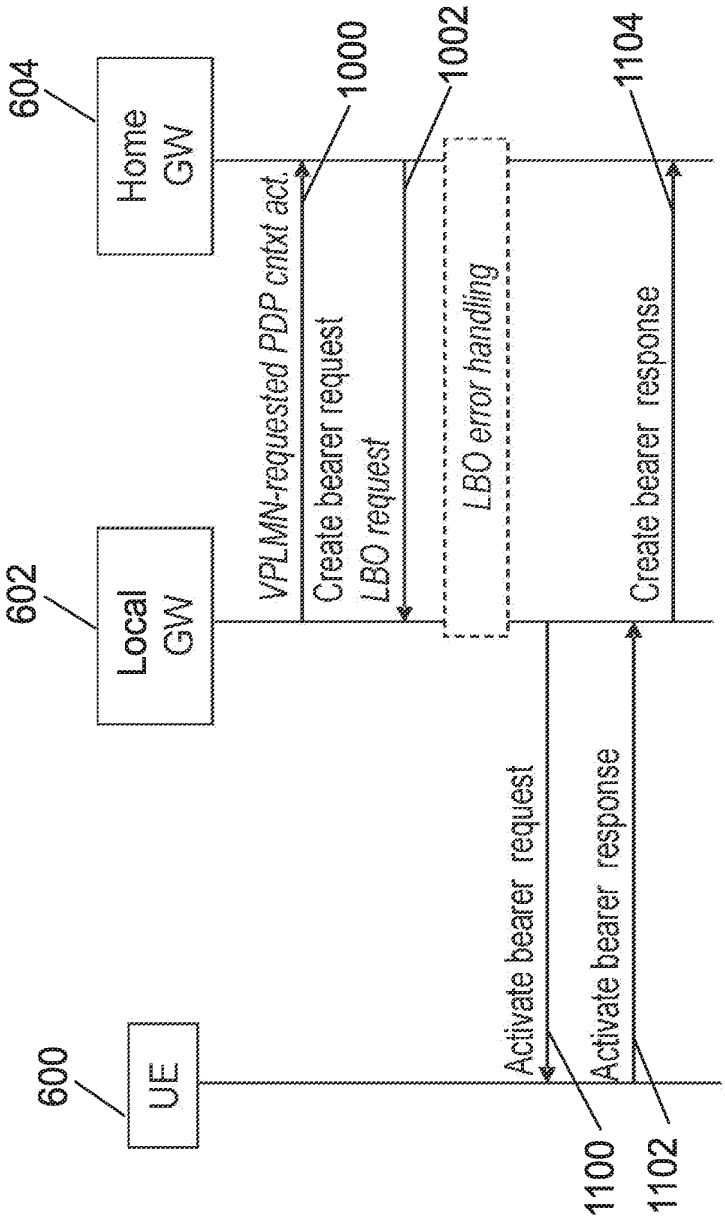

604
Home GW
602
Local GW
600
UE
VPLMN-requested PDP cntxt act.
Create bearer request
LBO request
LBO error handling
Create bearer response
Activate bearer request
Activate bearer response
1000
1002
1104
1100
1102

Fig. 11

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2007/052465

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L29/06

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2004/208153 A1 (MIZELL JERRY [US] ET AL) 21 October 2004 (2004-10-21) paragraph [0009] paragraph [0037] figures 2-5	1,5,6, 13,14, 16-18
A	WO 2004/010669 A (NOKIA CORP [FI]; GREIS MARC [US]; FACCIN STEFANO M [US]) 29 January 2004 (2004-01-29) claim 13; figure 1	1,5-9, 11-14, 16-18

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
20 December 2007	03/01/2008

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Farese, Luca

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/EP2007/052465

Box No. II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

see additional sheet

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers allsearchable claims.

2. ☒ As all searchable claims could be searched without effort justifying an additional fees, this Authority did not invite payment of additional fees.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search reportcovers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest and, where applicable, the payment of a protest fee.

☐ The additional search fees were accompanied by the applicant's protest but the applicable protest fee was not paid within the time limit specified in the invitation.

☐ No protest accompanied the payment of additional search fees.

Petitioner Ex 1002, p. 316
Zimperium v. Taasera, IPR2024-00007

FURTHER INFORMATION CONTINUED FROM PCT/ISA/ 210

This International Searching Authority found multiple (groups of) inventions in this international application, as follows:

1. claims: 1-18

1.1. claims: 1,2,5-9,11-18

PDP extension

1.2. claim: 3

use of previous rules

1.3. claim: 4

PDP triggering

1.4. claim: 10

mixed traffic

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2007/052465

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2004208153 A1	21-10-2004	NONE	
WO 2004010669 A	29-01-2004	AU 2003249479 A1	09-02-2004
		EP 1523840 A2	20-04-2005
		US 2004013116 A1	22-01-2004

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S1	1	"13540142"	US-PGPUB; USPAT	ADJ	ON	2013/12/13 15:50
S2	1	"20130007245"	DERWENT	ADJ	ON	2013/12/13 15:50
S3	41873	709/223$	US-PGPUB; USPAT	ADJ	ON	2013/12/13 15:51
S4	43047	709/224$	US-PGPUB; USPAT	ADJ	ON	2013/12/13 15:51
S5	1	"20100242088"	US-PGPUB; USPAT	ADJ	ON	2013/12/13 15:57
S6	960	H04L41/0816.cpc.	US-PGPUB; USPAT	ADJ	ON	2013/12/13 16:01
S7	3684	H04L43/0817.cpc.	US-PGPUB; USPAT	ADJ	ON	2013/12/13 16:01
S8	2594	H04L41/0893.cpc.	US-PGPUB; USPAT	ADJ	ON	2013/12/13 16:02
S9	31	H04L41/0618.cpc.	US-PGPUB; USPAT	ADJ	ON	2013/12/13 16:21
S10	577	455/26.1$	US-PGPUB; USPAT	ADJ	ON	2013/12/13 16:26
S11	3571	455/425$	US-PGPUB; USPAT	ADJ	ON	2013/12/13 16:28
S12	3995	455/456.5$	US-PGPUB; USPAT	ADJ	ON	2013/12/13 16:31
S13	22104	(gather$3 or collect$3 or assembl$3 or aggregat$3) near4 (status)	US-PGPUB; USPAT	ADJ	ON	2013/12/13 16:38
S14	358	(evaluat$3 or assess$3 or determin$3) near20 (compl$5 or conform$4) near20 (polic$3 or rule$1) near20 (violat$3 or break$3 or infract$3)	US-PGPUB; USPAT	ADJ	ON	2013/12/13 16:42
S15	0	S13 same3 S14	US-PGPUB; USPAT	ADJ	ON	2013/12/13 16:43
S16	24731	(polic$3 or rule$1) near20 (violat$3 or break$3 or infract$3)	US-PGPUB;	ADJ	ON	2013/12/13 16:43

Petitioner Ex 1002, p. 319
Zimperium v. Taasera, IPR2024-00007

			USPAT			
S17	92	S13 same3 S16	US-PGPUB; USPAT	ADJ	ON	2013/12/13 16:44
S18	1883	(compl$5 or conform$4) near20 (polic$3 or rule$1) near20 (violat$3 or break$3 or infract$3)	US-PGPUB; USPAT	ADJ	ON	2013/12/13 16:47
S19	2	S13 same3 S18	US-PGPUB; USPAT	ADJ	ON	2013/12/13 16:47
S20	110055	(polic$3 or rule$1) near20 (violat$3 or break$3 or infract$3 or compl$5 or conform$3)	US-PGPUB; USPAT	ADJ	ON	2013/12/13 16:50
S21	1750	(gather$3 or collect$3) near20 (status or state) near20 (((subscriber or mobile or wireless) adj1 (station or device)) or ((user or subscriber) adj1 equipment) or "MS" or "UE" or "MA")	US-PGPUB; USPAT	ADJ	ON	2013/12/13 16:54
S22	31	S20 same3 S21	US-PGPUB; USPAT	ADJ	ON	2013/12/13 16:55
S23	2	S3 and S22	US-PGPUB; USPAT	ADJ	ON	2013/12/13 16:55
S24	2	"20120151041"	US-PGPUB; USPAT	ADJ	ON	2013/12/13 16:57
S25	2	S4 and S22	US-PGPUB; USPAT	ADJ	ON	2013/12/13 16:57
S26	1	S6 and S22	US-PGPUB; USPAT	ADJ	ON	2013/12/13 16:58
S27	1	S7 and S22	US-PGPUB; USPAT	ADJ	ON	2013/12/13 16:58
S28	1	S8 and S22	US-PGPUB; USPAT	ADJ	ON	2013/12/13 16:59
S29	0	S9 and S22	US-PGPUB; USPAT	ADJ	ON	2013/12/13 16:59
S30	0	S10 and S22	US-PGPUB; USPAT	ADJ	ON	2013/12/13 16:59
S31	0	S11 and S22	US-PGPUB; USPAT	ADJ	ON	2013/12/13 16:59
S32	0	S12 and S22	US-PGPUB; USPAT	ADJ	ON	2013/12/13 16:59
S33	3	((JATIN) near2 (MALIK)).INV.	US-PGPUB; USPAT	ADJ	ON	2013/12/13 18:01
S34	3	((RATNESH) near2 (SINGH)).INV.	US-PGPUB; USPAT	ADJ	ON	2013/12/13 18:01

Petitioner Ex 1002, p. 320
Zimperium v. Taasera, IPR2024-00007

S35	1	((RAJAKUMAR) near2 (BOPALLI)).INV.	US-PGPUB; USPAT	ADJ	ON	2013/12/13 18:01
S36	1	S33 and S34 and S35	US-PGPUB; USPAT	ADJ	ON	2013/12/13 18:01
S37	1	S33 and ((status adj1 information) and gathering and initiating).clm.	US-PGPUB; USPAT	ADJ	ON	2013/12/13 18:02
S38	1	S34 and ((status adj1 information) and gathering and initiating).clm.	US-PGPUB; USPAT	ADJ	ON	2013/12/13 18:02
S39	1	S33 and (status and information and gathering and initiating).clm.	US-PGPUB; USPAT	ADJ	ON	2013/12/13 18:03
S40	1	S34 and (status and information and gathering and initiating).clm.	US-PGPUB; USPAT	ADJ	ON	2013/12/13 18:03
S41	2204	(polic$3 or rule$1) near20 (violat$3 or break$3 or infract$3 or compl$5 or conform$3)	FPRS; EPO; JPO	ADJ	ON	2013/12/13 18:05
S42	238	(gather$3 or collect$3) near20 (status or state) near20 (((subscriber or mobile or wireless) adj1 (station or device)) or ((user or subscriber) adj1 equipment) or "MS" or "UE" or "MA")	FPRS; EPO; JPO	ADJ	ON	2013/12/13 18:05
S43	0	S41 same3 S42	FPRS; EPO; JPO	ADJ	ON	2013/12/13 18:05
S44	0	S41 and S42	FPRS; EPO; JPO	ADJ	ON	2013/12/13 18:05
S45	33818	(status or state) near20 (((subscriber or mobile or wireless) adj1 (station or device)) or ((user or subscriber) adj1 equipment) or "MS" or "UE" or "MA")	FPRS; EPO; JPO	ADJ	ON	2013/12/13 18:05
S46	8	S41 same3 S45	FPRS; EPO; JPO	ADJ	ON	2013/12/13 18:05
S47	1	"20100242088"	US-PGPUB; USPAT	ADJ	ON	2013/12/16 12:39
S48	2	"20080114862"	US-PGPUB; USPAT	ADJ	ON	2013/12/16 13:17
S49	1	"20070206552"	US-PGPUB; USPAT	ADJ	ON	2013/12/16 13:53
S50	0	((alert$3 or warning) near4 compliance near20 qos) same3 ((time or grace) adj1 period)	US-PGPUB; USPAT	ADJ	ON	2013/12/16 14:14
S51	0	((alert$3 or warning) near20 compliance near20 qos) same3 ((time or grace) adj1 period)	US-PGPUB; USPAT	ADJ	ON	2013/12/16 14:14
S52	3	((alert$3 or warning) near20 qos) same3 ((time or grace) adj1 period)	US-PGPUB; USPAT	ADJ	ON	2013/12/16 14:14
S53	1	"20070266422"	US-PGPUB; USPAT	ADJ	ON	2013/12/16 14:20

Petitioner Ex 1002, p. 321
Zimperium v. Taasera, IPR2024-00007

12/16/2013 2:45:04 PM
C:\Users\kkatsikis1\Documents\EAST\Workspaces\13540142.wsp

Petitioner Ex 1002, p. 322
Zimperium v. Taasera, IPR2024-00007

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13540142	MALIK ET AL.
	Examiner	Art Unit
	KOSTAS KATSIKIS	2441

CPC- SEARCHED		
Symbol	Date	Examiner
H04L41/0816	12/13/2013	KK
H04L43/0817	12/13/2013	KK
H04L41/0893	12/13/2013	KK
H04L41/0618	12/13/2013	KK

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner
709	223, 224	12/13/2013	KK
455	26.1, 425, 456.5	12/13/2013	KK

SEARCH NOTES		
Search Notes	Date	Examiner
Examiner conducted thorough EAST search.	12/13/2013 and 12/16/2013	KK
EAST (USPAT, US-PGPUB) - see search history printout.	12/13/2013 and 12/16/2013	KK
EAST (EPO, JPO, FPRS) - see search history printout.	12/13/2013	KK
709/223 (text search - see search history printout).	12/13/2013	KK
709/224 (text search - see search history printout).	12/13/2013	KK
H04L41/0816 (text search - see search history printout).	12/13/2013	KK
H04L43/0817 (text search - see search history printout).	12/13/2013	KK
H04L41/0893 (text search - see search history printout).	12/13/2013	KK
H04L41/0618 (text search - see search history printout).	12/13/2013	KK
Examiner conducted Inventor Name search in EAST.	12/13/2013	KK
455/26.1 (text search - see search history printout).	12/13/2013	KK
455/425 (text search - see search history printout).	12/13/2013	KK
455/456.5 (text search - see search history printout).	12/13/2013	KK

/KOSTAS KATSIKIS/ Examiner.Art Unit 2441	

INTERFERENCE SEARCH			
US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner

/KOSTAS KATSIKIS/ Examiner.Art Unit 2441	

Petitioner Ex 1002, p. 324
Zimperium v. Taasera, IPR2024-00007

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	13540142
Filing Date	2012-07-02
First Named Inventor	Malik, Jatin
Art Unit	~~2447~~
Examiner Name	~~Hwang, Joon H.~~
Attorney Docket Number	130839.02101

U.S.PATENTS

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button.

U.S.PATENT APPLICATION PUBLICATIONS

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
/K.K./	1	20100242088		2010-09-23	THOMAS	
/K.K./	2	20080114862		2008-05-15	MOGHADDAM ET AL.	
/K.K./	3	20070266422		2007-11-15	GERMANO ET AL.	
/K.K./	4	20070206552		2007-09-06	YAQUB ET AL.	

If you wish to add additional U.S. Published Application citation information please click the Add button.

FOREIGN PATENT DOCUMENTS

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]

Receipt date: 05/20/2013	Application Number	13540142 13540142 - GAU: 2441
INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99**)	Filing Date	2012-07-02
	First Named Inventor	Malik, Jatin
	Art Unit	~~2447~~
	Examiner Name	~~Hwang, Joon H.~~
	Attorney Docket Number	130839.02101

/K.K./	1	2011022053	WO	A1	2011-02-24	NAIMAN ET AL.		☐

If you wish to add additional Foreign Patent Document citation information please click the Add button

NON-PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1		☐

If you wish to add additional non-patent literature document citation information please click the Add button

EXAMINER SIGNATURE

Examiner Signature	/Kostas Katsikis/	Date Considered	12/13/2013

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

Receipt date: 06/27/2013

Doc code: IDS

Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99**)		
	Application Number	13540142
	Filing Date	2012-07-02
	First Named Inventor	Jatin Malik et al.
	Art Unit	~~2447~~ 13540142 - GAU: 2441
	Examiner Name	~~Joon H. Hwang~~
	Attorney Docket Number	130839.02101

U.S.PATENTS						
Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					
If you wish to add additional U.S. Patent citation information please click the Add button.						

U.S.PATENT APPLICATION PUBLICATIONS						
Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					
If you wish to add additional U.S. Published Application citation information please click the Add button.						

FOREIGN PATENT DOCUMENTS								
Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2]	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							☐
If you wish to add additional Foreign Patent Document citation information please click the Add button								

NON-PATENT LITERATURE DOCUMENTS			
Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]

Receipt date: 06/27/2013	Application Number	13540142
INFORMATION DISCLOSURE STATEMENT BY APPLICANT	Filing Date	2012-07-02
	First Named Inventor	Jatin Malik et al.
(Not for submission under 37 CFR 1.99)	Art Unit	~~2447~~ 13540142 - GAU: 2441
	Examiner Name	~~Joon H. Hwang~~
	Attorney Docket Number	130839.02101

/K.K./	1	International Search Report and Written Opinion mailed 28 September 2012 for corresponding International Application No. PCT/US2012/045252	☐

If you wish to add additional non-patent literature document citation information please click the Add button

EXAMINER SIGNATURE

Examiner Signature	/Kostas Katsikis/	Date Considered	12/13/2013

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13540142	MALIK ET AL.
	Examiner	Art Unit
	KOSTAS KATSIKIS	2441

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	12/16/2013								
	1	✓								
	2	✓								
	3	✓								
	4	✓								
	5	✓								
	6	✓								
	7	✓								
	8	✓								
	9	✓								
	10	✓								
	11	✓								
	12	✓								
	13	✓								
	14	✓								
	15	✓								
	16	✓								
	17	✓								
	18	✓								
	19	✓								
	20	✓								
	21	✓								
	22	✓								
	23	✓								

Petitioner Ex 1002, p. 329
Zimperium v. Taasera, IPR2024-00007

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: **Jatin MALIK et al.**

Title: **RULES BASED ACTIONS FOR MOBILE DEVICE MANAGEMENT**

Application No.: **13/540,142** Group Art Unit: **2441**

Filed: **July 2, 2012** Examiner: **Kostas J. Katsikis**

Confirmation: **4198** Filed by EFS on: **May 19, 2014**

Mail Stop Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

AMENDMENT AND REQUEST FOR RECONSIDERATION UNDER 35 U.S.C. § 1.111

Sir:

In response to the Office Action mailed on December 19, 2013, Applicants respectfully request reconsideration in light of the:

Listing of the Claims, reflecting current amendments, beginning on page 2; and

Remarks beginning on page 6 of this paper.

Listing of Claims:

This listing of claims will replace all prior versions and listings of claims in the application.

1. (Presently Amended) A method for providing device management services comprising steps of:

gathering, from a network, status information related to each of a plurality of mobile devices, each mobile device utilizing one of a plurality of different mobile operating systems;

storing the status information in an electronic database accessible to a server;

evaluating at the server a first compliance state of at least one of the mobile devices from the status information using a plurality of administrator-defined rules; and

initiating at least one action defined by the [[user]] administrator-defined rules in response to the step of evaluating,

wherein the step of ~~evaluation~~ evaluating is performed by [[a]] the server automatically, in response to changes in the status information in the electronic database .

2. (Original) The method of claim 1, wherein the at least one action is selectable from a plurality of actions, comprising blocking access by the at least one of the mobile devices to a corporate resource.

3. (Original) The method of claim 1, wherein the at least one action is selectable from a plurality of actions, comprising blocking e-mail access for the at least one of the mobile devices.

4. (Original) The method of claim 1, wherein the at least one action is selectable from a plurality of actions, comprising wiping information from the at least one of the mobile devices.

5. (Original) The method of claim 1, wherein the at least one action is selectable from a plurality of actions, comprising warning a user of the at least one of the mobile devices that further action may be taken.

Petitioner Ex 1002, p. 331
Zimperium v. Taasera, IPR2024-00007

6. (Original) The method of claim 1, wherein the step of gathering status information, for the at least one mobile device, comprises gathering information from that mobile device and at least one other source on the network.

7. (Original) The method of claim 1, further comprising the step of subsequently evaluating a second compliance state of at least one of the mobile devices to determine if the at least one action should be revoked.

8. (Currently Amended) The method of claim 1, wherein the plurality of different mobile operating systems comprise at least operating systems compliant with Android and iOS specifications.

9. (Original) The method of claim 1, wherein the status information comprises location information about each mobile device.

10. (Currently Amended) A method for providing device management services comprising steps of:

making a determination that an attribute of a mobile device has changed;

evaluating the attribute, by a processor at a server in response to the determination, to determine if it triggers at least one of a plurality of administrator defined rules, which indicates that the attribute is out of compliance; and

automatically initiating, at the server, an action defined by the at least one of a plurality of administrator defined rules if the attribute is out of compliance,

wherein the attribute is stored in a data store accessible to the server, that includes substantially real-time data, gathered from a network, pertaining to a plurality of attributes of a plurality of mobile devices, comprising devices having different mobile operating systems.

11. (Original) The method of claim 10, wherein the step of automatically initiating an action comprises warning a user of the mobile device that the device is out of compliance and subsequently causing the action to be performed if the attribute remains out of compliance after a period of time defined in the at least one rule.

Petitioner Ex 1002, p. 332
Zimperium v. Taasera, IPR2024-00007

12. (Original) The method of claim 10, further comprising the step of automatically revoking the action if the attribute is brought back into compliance.

13. (Original) The method of claim 12, wherein the step of automatically revoking the action comprises determining if another of the plurality of rules is triggered.

14. (Original) The method of claim 10, further comprising the step of gathering the plurality of attributes for at least one of the plurality of mobile device by gathering attribute information from that mobile device and at least one other source on a network.

15. (Currently Amended) The method of claim 10, wherein the plurality of different mobile operating systems comprise at least operating systems compliant with Android and iOS specifications.

16. (Original) The method of claim 10, wherein the attribute comprises location information about the mobile device.

17. (Currently Amended) A system for providing device management services comprising:

a data store configured to be accessible by a server;

a CPU of the server coupled to a memory configured to execute computer readable instructions;

computer readable instructions for execution on the server comprising instructions configured to:

automatically make a determination that an attribute of a mobile device stored in the data store has changed;

evaluate the attribute, in response to the determination, to determine if it triggers at least one of a plurality of administrator defined rules, which indicates that the attribute is out of compliance; and

automatically initiate an action defined by the at least one of a plurality of administrator defined rules if the attribute is out of compliance,

Petitioner Ex 1002, p. 333
Zimperium v. Taasera, IPR2024-00007

wherein the data store is configured to ~~include~~ gather, from a network, substantially real-time data pertaining to a plurality of attributes of a plurality of mobile devices, comprising devices having different mobile operating systems.

18. (Original) The system of claim 17, wherein the computer readable instructions further comprise instructions configured to present a user interface to an administrator to allow selection of at least one attribute and one available action to define the at least one of the plurality of administrator defined rules.

19. (Original) The system of claim 18, wherein at least one of the actions comprises warning a user of the mobile device that the device is out of compliance and causing subsequent action to be performed if the attribute remains out of compliance after a period of time defined in the at least one rule.

20. (Original) The system of claim 17, wherein the computer readable instructions further comprise instructions configured to automatically revoke the action if the attribute is brought back into compliance.

21. (Original) The system of claim 17, wherein the computer readable instructions further comprise instructions configured to gather the plurality of attributes for at least one of the plurality of mobile device by gathering attribute information from that mobile device and at least one other source on a network.

22. (Currently Amended) The system of claim 17, wherein the plurality of different mobile operating systems comprise at least operating systems compliant with Android and iOS specifications.

23. (Original) The system of claim 17, wherein the attribute comprises location information about the mobile device.

Petitioner Ex 1002, p. 334
Zimperium v. Taasera, IPR2024-00007

REMARKS

Claims 1-23 were pending in the application. Claims 1, 8, 10, 15, 17, and 22 have been amended. Support for these amendments can be found throughout the application, including but not limited to paragraphs 25-27 and Figs 1-4 and related disclosure. No new matter has been introduced. Accordingly, upon entry of this amendment, claims 1-23 are before the Examiner.

Claim Objections

Claims 8, 15, and 22 are objected to because the trademark ANDROID™ is not permissible in claim language. Applicants respectfully submit that the use of Android is descriptive of the type of devices and operating system used on these devices. Accordingly, it does not render the claim indefinite, because a person of ordinary skill in the art would understand the claim limitation to identify a typo of mobile device operating system. *See, e.g.,* MPEP 608.1(v) ("Names used in trade are permissible in patent applications if: (B) In this country, their meanings are well-known and satisfactorily defined in the literature."); MPEP 2173.05(u) ("The presence of a trademark or trade name in a claim is not, per se, improper under 35 U.S.C. 112, second paragraph,").

Furthermore, claims 8, 15, and 22 have been amended to make clear that they are not referring to a source of goods or a particular material or product, but rather operating systems compliant with popular mobile OS specifications. Accordingly, Applicants respectfully request withdrawal of this objection.

Rejections Under 35 U.S.C. § 101

Claims 17-23 stand rejected under 35 U.S.C. § 101 as allegedly being directed to non-statutory subject matter. Applicants would like to thank the Examiner for his suggested change. This change has been adopted. Accordingly, Applicants respectfully request withdrawal of this rejection.

Rejections Under 35 U.S.C. § 102

Claims 1-2, 6, 9-10, 14, 16-18, 21, and 23 stand rejected under 35 U.S.C. § 102(b) as allegedly being anticipated by Thomas et al. (U.S. Patent Publication No. 2010/0242088).

Petitioner Ex 1002, p. 335
Zimperium v. Taasera, IPR2024-00007

Independent claims, 1, 10, and 17 have been amended. Thomas fails to teach all elements of these claims, at least because it fails to teach "storing the status information in an electronic database accessible to a server" and that a "step of evaluating is performed by the server automatically, in response to changes in the status information in the electronic database." [Claim 1, exemplary] By responding automatically at the server to changes in status information in a database, the claimed invention is fundamentally different from the system taught be Thomas, and certain benefits may exist, as would be apparent to a person of ordinary skill (e.g., scalability, centralized evaluation and enforcement of policies).

Thomas teaches a system that provides for centralized policy updates to client facilities, to allow these client facilities to implement and/or participate in the application of the policies. For example, the system of Thomas utilizes a centralized threat management facility 100 "to facilitate the setting, updating and control of such policies the corporation only needs to be concerned with keeping the threat management facility 100 up to date on such policies. The threat management facility 100 can take care of updating all of the other corporate computing assets." Thomas [23]. "[T]he threat management facility 100 may create definition updates," "the client facility 144 may be updated with new definition files periodically to provide the client facility 144 with the most recent malicious code definitions." Thomas at [40].

While Thomas teaches policy management that is handled by a server (e.g., the threat management facility), the enforcement of rules is taught as done on the clients or done in a distributed manner with the assistance of the client. For example, the central management facility can directly access the state information of the client facility, such as by scanning files on the client. "The security management facility 122 [part of facility 100] may have the ability to scan the client facility 144 files for malicious code, remove or quarantine certain applications and files, prevent certain actions, perform remedial actions and perform other security measures. In embodiments, scanning the client facility 144 may include scanning some or all of the files stored to the client facility 144 on a periodic basis, may scan applications once the application has been requested to execute, may scan files as the files are transmitted to or from the client facility 144, or the like. The scanning of the applications and files may be to detect known malicious code or known unwanted applications." Thomas at [28]. Thomas also teaches other enforcement actions that a person of ordinary skill in the art

Petitioner Ex 1002, p. 336
Zimperium v. Taasera, IPR2024-00007

would understand as being performed at the client facility, such as URI filtering and monitoring [29], monitoring behavior before allowing execution of software [30], monitoring outgoing files [42], etc.

A person of ordinary skill in the art would understand Thomas a teaching a scheme whereby a server updates policy information, but enforcement is generally performed locally on the clients (e.g. scanning for local malware, monitoring outgoing network communication, etc.) – not evaluating, by a server, a compliance state of mobile devices in response to changes in status information that is stored in a database accessible to the server. For example, Thomas teaches that an end-point computer security facility is an application that is adapted to the OS of the endpoint device and loaded thereon. Thomas at [50]. Because Thomas teaches updated policy information distributed to client facilities, local software that allows scanning of data on client devices, and the ability for clients to monitor activity and apply policies at the client devices, there is simply no need for Thomas to utilize a database that contains information about the status of mobile devices. Such a database is not taught nor would such a modification be obvious, because it would likely frustrate scheme already taught by Thomas.

Applicants respectfully contend that the paragraphs cited by the Examiner do not teach a server-accessible database that stores status information about mobile devices. For example, Paragraphs 44-47 discuss a database of rules (e.g. network access rule 124). Paragraphs 84-85 discuss generic databases, clients, and servers. Thomas does not teach that status information about mobile devices is gathered and stored in that database or that the server evaluates rules based on changes to this status information. Rather, Thomas teaches that a database of rules can help facilitate the central management of rules that can be enforced at client facilities, as discussed above. Because Thomas fails to teach a database of mobile device status information, it further fails to teach evaluating, by the server, a compliance state based on administrator defined rules, in response to changes in that mobile device status information in the database.

For at least these reasons, Thomas fails to teach all the elements of independent claims 1, 10, and 17. Applicants also believe that any further discussion of the patentability of the additional elements in the independent claims in light of infirmities of the prior art is not needed as moot.

Petitioner Ex 1002, p. 337
Zimperium v. Taasera, IPR2024-00007

Applicants further submit that, because claims 2, 6, 7, 9, 14, 16, 18, 21, and 23 depend from and incorporate all of the limitations of the respective independent claims, these dependent claims are non-obvious over the cited references for at least the reasons stated above with respect to the independent claims. Applicants also believe that any further discussion of the patentability of the additional elements in the dependent claims in light of infirmities of the prior art is not needed as moot. However, Applicants reserve the right to discuss these individual elements further if the Examiner disagrees with Applicants current arguments with respect to the independent claims.

Accordingly, Applicants respectfully request that the rejections associated with claims 1-2, 6, 9-10, 14, 16-18, 21, and 23 be withdrawn and allowance of these claims be swiftly granted.

Rejections Under 35 U.S.C. § 103

Claim 3 stands rejected under 35 U.S.C. § 103(a) as allegedly being obvious over Thomas in view of Moghaddam et al. (U.S. Patent Publication No. 2008/0114862).

Claims 4, 8, 15, and 22 stand rejected under 35 U.S.C. § 103(a) as allegedly being obvious over Thomas in view of Naiman et al. (International Patent Publication No. WO 2011/022053).

Claims 5, 11, and 19 stand rejected under 35 U.S.C. § 103(a) as allegedly being obvious over Thomas in view of Yaqub et al. (U.S. Patent Publication No. 2007/0206552).

Claims 7, 12, 13, and 20 stand rejected under 35 U.S.C. § 103(a) as allegedly being obvious over Thomas in view of Germano et al. (U.S. Patent Publication No. 2007/0266422).

Applicants further submit that, because each of these claim depend from and incorporate all of the limitations of the respective independent claims, these dependent claims are non-obvious over the cited references for at least the reasons stated above with respect to the independent claims. See MPEP §2143.03 (stating that if an independent claim is nonobvious under 35 U.S.C. §103, then any claim depending therefrom is nonobvious). Applicants also believe that any further discussion of the patentability of the additional elements in the dependent claims in light of infirmities of the prior art is not needed as moot. However, Applicants reserve the right to discuss these individual elements further if the Examiner disagrees with Applicants current arguments with respect to the independent claim.

Petitioner Ex 1002, p. 338
Zimperium v. Taasera, IPR2024-00007

Accordingly, Applicants respectfully request that the rejections associated with these remaining claims be withdrawn and allowance of these claims be swiftly granted.

CONCLUSION

Early reconsideration and allowance of all pending claims is respectfully requested. The Examiner is requested to contact the undersigned attorney if an interview, telephonic or personal, would facilitate allowance of the claims.

AUTHORIZATION

The Commissioner is hereby authorized to charge any additional fees which may be required for this response, or credit any overpayment, to deposit account no. 50-0436.

Respectfully Submitted

By: /Jay R. Mitchell, Reg. No. 54316/
Jay R. Mitchell
Registration No. 54,316

Dated: **May 19, 2014**

PEPPER HAMILTON LLP
3000 Two Logan Square
Eighteenth and Arch Street
Philadelphia, PA 19103-279
Telephone: (215) 981-4664
Facsimile: (610) 640-7835

Petitioner Ex 1002, p. 339
Zimperium v. Taasera, IPR2024-00007

Electronic Patent Application Fee Transmittal

Application Number:	13540142
Filing Date:	02-Jul-2012
Title of Invention:	RULES BASED ACTIONS FOR MOBILE DEVICE MANAGEMENT
First Named Inventor/Applicant Name:	Jatin MALIK
Filer:	Jay R. Mitchell/Sara Harvell
Attorney Docket Number:	130839.02101

Filed as Small Entity

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Extension - 2 months with $0 paid	2252	1	300	300

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
		Total in USD ($)		**300**

Electronic Acknowledgement Receipt

EFS ID:	19067699
Application Number:	13540142
International Application Number:	
Confirmation Number:	4198
Title of Invention:	RULES BASED ACTIONS FOR MOBILE DEVICE MANAGEMENT
First Named Inventor/Applicant Name:	Jatin MALIK
Customer Number:	86308
Filer:	Jay R. Mitchell/Sara Harvell
Filer Authorized By:	Jay R. Mitchell
Attorney Docket Number:	130839.02101
Receipt Date:	19-MAY-2014
Filing Date:	02-JUL-2012
Time Stamp:	16:32:28
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	$300
RAM confirmation Number	3530
Deposit Account	500436
Authorized User	MITCHELL, JAY
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees) Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)	

Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees)	
Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Extension of Time	2101Extension.pdf	148876 0e60f3dfc085f87cca5b138a2c63fdd6f265b003	no	2
Warnings:					
Information:					
2		2101Response.pdf	120486 ba567f2fbcb79db25cde209266e5fdd2ba977ea7	yes	10

Multipart Description/PDF files in .zip description

Document Description	Start	End
Amendment/Req. Reconsideration-After Non-Final Reject	1	1
Claims	2	5
Applicant Arguments/Remarks Made in an Amendment	6	10

Warnings:					
Information:					
3	Fee Worksheet (SB06)	fee-info.pdf	30322 f5b1bb624b239b7f2af84a9346f506628324a732	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	299684		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PTO/SB/22 (03-13)
Approved for use through 3/31/2013. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PETITION FOR EXTENSION OF TIME UNDER 37 CFR 1.136(a)

Docket Number (Optional): 130839.02101

Application Number: 13/540,142

Filed: July 2, 2012

For: RULES BASED ACTIONS FOR MOBILE DEVICE MANAGEMENT

Art Unit: 2441

Examiner: KATSIKIS, KOSTAS J.

This is a request under the provisions of 37 CFR 1.136(a) to extend the period for filing a reply in the above-identified application.

The requested extension and fee are as follows (check time period desired and enter the appropriate fee below):

	Fee	Small Entity Fee	Micro Entity Fee	
☐ One month (37 CFR 1.17(a)(1))	$200	$100	$50	$
☑ Two months (37 CFR 1.17(a)(2))	$600	$300	$150	$ 300
☐ Three months (37 CFR 1.17(a)(3))	$1,400	$700	$350	$
☐ Four months (37 CFR 1.17(a)(4))	$2,200	$1,100	$550	$
☐ Five months (37 CFR 1.17(a)(5))	$3,000	$1,500	$750	$

☑ Applicant asserts small entity status. See 37 CFR 1.27.

☐ Applicant certifies micro entity status. See 37 CFR 1.29.
Form PTO/SB/15A or B or equivalent must either be enclosed or have been submitted previously.

☐ A check in the amount of the fee is enclosed.

☑ Payment by credit card. Form PTO-2038 is attached.

☐ The Director has already been authorized to charge fees in this application to a Deposit Account.

☑ The Director is hereby authorized to charge any fees which may be required, or credit any overpayment, to Deposit Account Number 50-0436.

☑ Payment made via EFS-Web.

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

I am the

☐ applicant/inventor.

☐ assignee of record of the entire interest. See 37 CFR 3.71. 37 CFR 3.73(b) statement is enclosed (Form PTO/SB/96).

☑ attorney or agent of record. Registration number 54316.

☐ attorney or agent acting under 37 CFR 1.34. Registration number _____.

/Jay R. Mitchell, Reg. #54316/ — Signature

May 19, 2014 — Date

Jay R. Mitchell — Typed or printed name

215.981.4664 — Telephone Number

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications. Submit multiple forms if more than one signature is required, see below*.

☑ * Total of 1 forms are submitted.

This collection of information is required by 37 CFR 1.136(a). The information is required to obtain or retain a benefit by the public, which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 6 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Electronic Acknowledgement Receipt

EFS ID:	19067699
Application Number:	13540142
International Application Number:	
Confirmation Number:	4198
Title of Invention:	RULES BASED ACTIONS FOR MOBILE DEVICE MANAGEMENT
First Named Inventor/Applicant Name:	Jatin MALIK
Customer Number:	86308
Filer:	Jay R. Mitchell/Sara Harvell
Filer Authorized By:	Jay R. Mitchell
Attorney Docket Number:	130839.02101
Receipt Date:	19-MAY-2014
Filing Date:	02-JUL-2012
Time Stamp:	16:32:28
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	$300
RAM confirmation Number	3530
Deposit Account	500436
Authorized User	MITCHELL, JAY

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees)	
Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Extension of Time	2101Extension.pdf	148876 0e60f3dfc085f87cca5b138a2c63fdd6f265b003	no	2
Warnings:					
Information:					
2		2101Response.pdf	120486 ba567f2fbcb79db25cde209266e5fdd2ba977ea7	yes	10

Multipart Description/PDF files in .zip description

Document Description	Start	End
Amendment/Req. Reconsideration-After Non-Final Reject	1	1
Claims	2	5
Applicant Arguments/Remarks Made in an Amendment	6	10

Warnings:					
Information:					
3	Fee Worksheet (SB06)	fee-info.pdf	30322 f5b1bb624b239b7f2af84a9346f506628324a732	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	299684		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PTO/SB/06 (09-11)
Approved for use through 1/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 13/540,142	Filing Date 07/02/2012	☐ To be Mailed

ENTITY: ☐ LARGE ☒ SMALL ☐ MICRO

APPLICATION AS FILED – PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	RATE ($)	FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X $ =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).			
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))				
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL	

APPLICATION AS AMENDED – PART II

AMENDMENT **05/19/2014**

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	* 23	Minus	** 23	= 0	X $40 =	0
Independent (37 CFR 1.16(h))	* 3	Minus	***3	= 0	X $210 =	0
☐ Application Size Fee (37 CFR 1.16(s))						
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
					TOTAL ADD'L FEE	0

AMENDMENT

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	*	Minus	**	=	X $ =	
Independent (37 CFR 1.16(h))	*	Minus	***	=	X $ =	
☐ Application Size Fee (37 CFR 1.16(s))						
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
					TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".
The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

LIE
/POLIN ANG/

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**
If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/540,142	07/02/2012	Jatin MALIK	130839.02101	4198

86308 7590 09/08/2014

Pepper Hamilton LLP
400 Berywn Park
899 Cassatt Road
Berwyn, PA 19312-1183

EXAMINER	
KATSIKIS, KOSTAS J	
ART UNIT	PAPER NUMBER
2441	

MAIL DATE	DELIVERY MODE
09/08/2014	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No. 13/540,142	Applicant(s) MALIK ET AL.	
	Examiner KOSTAS KATSIKIS	Art Unit 2441	AIA (First Inventor to File) Status No

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTHS FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *19 May 2014*.

☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims*

5)☒ Claim(s) *1-23* is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6)☐ Claim(s) _____ is/are allowed.

7)☒ Claim(s) *1-23* is/are rejected.

8)☐ Claim(s) _____ is/are objected to.

9)☐ Claim(s) _____ are subject to restriction and/or election requirement.

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov.

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

a)☐ All b)☐ Some** c)☐ None of the:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

** See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Information Disclosure Statement(s) (PTO/SB/08a and/or PTO/SB/08b) Paper No(s)/Mail Date _____.

3) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

4) ☐ Other: _____.

Petitioner Ex 1002, p. 352
Zimperium v. Taasera, IPR2024-00007

DETAILED ACTION

1. This communication is in response to the Amendment filed on May 19, 2014, in which claims 1, 8, 10, 15, 17 and 22 have been amended. Accordingly, claims 1-23 remain pending for examination.

Status of Claims

2. Claims 1-23 are pending, of which Claims 1-2, 6, 9-10, 14, 16-18, 21 and 23 are rejected under 35 U.S.C. 102(b). Claims 3-5, 8, 11, 15, 19 and 22 are rejected under 35 U.S.C. 103.

3. **Examiner's Note:** Examiner has cited particular paragraphs and/or columns and line numbers in the references applied to the claims above for the convenience of the applicant. Although the specified citations are representative of the teachings of the art and are applied to specific limitations within the individual claim, other passages and figures may apply as well. It is respectfully requested from the applicant in preparing responses, to fully consider the references in entirety as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior art or disclosed by the Examiner.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

5. Claims 1-2, 6, 9-10, 14, 16-18, 21 and 23 rejected under 35 U.S.C. 102(b) as being anticipated by Thomas et al. (United States Patent Application Publication No. US 2010/0242088 A1), hereinafter "Thomas".

Regarding claim 17, **Thomas** discloses a system for providing device management services comprising *(wherein **Thomas** discloses unified threat management facility 100 (See FIG. 1))* **(Thomas, FIG. 1, paragraph [0023])**:

a data store configured to be accessible by a server *(wherein threat management facility 100 further includes network access rules facility 124. **Thomas** further discloses that the threat management facility 100 has multiple databases (See again, FIG. 1 - at least items 112 and 124). Particularly policy management facility 112 may include a database, a text file, or at least a combination of databases and text files. **Thomas** teaches that a policy database may be a block list, a black list, an allowed list, a white list, or the like that may provide a list of enterprise facility 102 external network locations/applications that may or may not be accessed by the client facility 144. The*

policy management facility 112 may further include rules that may be interpreted with respect to an enterprise facility 102 network access request to determine if the request should be allowed or denied. In addition, the network access rules facility 124 may include databases such as a block list, a black list, an allowed list, a white list, an unacceptable network site database, an acceptable network site database, a network site reputation database, or the like of network access locations that may or may not be accessed by the client facility 144. Furthermore, the security management facility 122 may be used to scan an outgoing file and verify that the outgoing file is permitted to be transmitted per the enterprise facility 102 rules and policies. By checking outgoing files, ***Thomas*** *teaches that the security management facility 122 may be able discover malicious code infected files that were not detected as incoming files as a result of the client facility 144 having been updated with either new definition files or policy management facility 112 information. Moreover, the policy management facility 112 is able to block non-malicious applications, such as VoIP 164, instant messaging 162, peer-to-peer file-sharing, and the like, that may undermine productivity and network performance within the enterprise facility 102)* **(Thomas, FIG. 1, paragraphs [0034], [0042], [0044]-[0045])**;

a CPU of the server coupled to a memory configured to execute computer readable instructions *(wherein* ***Thomas*** *further teaches that the inventive teachings can at least be deployed on a machine that executes computer software on a server, that the software may be associated with a server that may include a file server, print server, domain server, internet server, intranet server and other variants such as secondary*

server, host server, distributed server and the like, that the server may further include at least one or more of memories and processors, and that the methods, programs or codes may be executed by the server) **(Thomas, paragraphs [0082]-[0084])**;

computer readable instructions for execution on the server comprising instructions configured to *(wherein again,* ***Thomas*** *discloses the computer readable software and instructions)* **(Thomas, paragraph [0084])**:

automatically make a determination that an attribute of a mobile device stored in the data store has changed *(wherein again, threat management facility executes a program or application to remediate against a threat or policy violation, and record interactions for subsequent evaluation. More particularly, as discussed above,* ***Thomas*** *teaches that as threats are identified and characterized, the threat management facility 100 may create definition updates used to detect and remediate the latest malicious software, unwanted applications, configuration and policy changes, and the like. The threat definition facility 114 may contain threat identification updates, also referred to as definition files, or, virus identity files that may include definitions of known or potential malicious code, as defined in paragraph [0040]. The definition files may be accessed by security management facility 122 when scanning files or applications within the client facility 144 for the determination of malicious code that may be within the file or application. The definition files may contain a number of commands, definitions, or instructions, to be parsed and acted upon, or the like.* ***Thomas*** *teaches that new and altered malicious code and malicious applications may be continually created and distributed to networks worldwide, and that the definition files that maintain the*

definitions of the malicious code and malicious application information for the protection of the networks and client facilities 144 may need continual updating to provide continual defense of the network and client facility 144 from the malicious code and malicious applications. The definition files management facility 114 may provide for automatic updates of the definition files, updated as a result of an alert of a new malicious code or malicious application) **(Thomas, paragraphs [0040]-[0042] and [0046]-[0047])**;

evaluate the attribute, in response to the determination, to determine if it triggers at least one of a plurality of administrator defined rules *(wherein again, threat management is based on policy violations. In particular,* ***Thomas*** *teaches that corporate policy management is one of the dimensions for which the threat management facility 100 can control. The corporation may institute a policy that prevents certain people (e.g. employees, groups of employees, types of employees, guest of the corporation, etc.) from accessing certain types of computer programs. For example,* ***Thomas*** *discloses that the corporation may elect to prevent its accounting department from using a particular version of an instant messaging service or all such services. In the given example, the policy management facility 112 may be used to update the policies of all corporate computing assets with a proper policy control facility or it may update a select few. Policy management facility 112 may be able to block applications such as VoIP 164 and instant messaging 162 (IM) that, although non-malicious, may nonetheless still undermine productivity and network performance within the enterprise facility 102. Again, the rules of policy management facility 112 may indicate to enterprise facility 102*

access permissions for the client facility 144, such as access permissions associated with the network, applications, external computer devices, and the like, and rules that may be interpreted with respect to an enterprise facility 102 network access request to determine if the request should be allowed. In a particular example, ***Thomas*** *teaches that when a website is requested by the client facility 144, a security facility may access the rules within a policy facility to determine if the requested access is related to a sporting website. The security facility (within threat management facility 100) may analyze the requested website to determine if the website matches with any of the policy facility rules, thereby effectively enforcing policies.* ***Thomas*** *further teaches that the policies may be administrator-defined, that is, maintained by the administration facility 134, through the threat management facility 100, in association with a third party, or the like)* **(Thomas, paragraphs [0023] and [0034]-[0035])**, which indicates that the attribute is out of compliance *(wherein compliance is determined)* **(Thomas, paragraphs [0034]-[0035])**; and

automatically initiate an action defined by the at least one of a plurality of administrator defined rules if the attribute is out of compliance *(wherein again, remedial action facility 128 acts on policy violations)* **(Thomas, paragraph [0046])**, wherein the data store is configured to gather, from a network, substantially real-time data pertaining to a plurality of attributes of a plurality of mobile devices *(wherein threat management facility 100 performing increasingly automated and frequently testing. Again, the updates are received from the network, as a result of alerts of new malicious codes or malicious applications)* **(Thomas, paragraphs [0025], [0040]-[0041] and [0048])**,

comprising devices having different mobile operating systems *(wherein security facility 152 may be an application loaded onto the computer platform or computer support component, where the application may accommodate the plurality of computer platforms)* **(Thomas, paragraph [0050])**.

Claim 10 includes a "method" claim that performs limitations substantially as described in "system" claim 17, and does not appear to contain any additional features with regard to novelty and/or inventive step; therefore, it is rejected under the same rationale.

Regarding claim 1, **Thomas** discloses a method for providing device management services comprising steps of:

gathering, from a network, status information related to each of a plurality of mobile devices, each mobile device utilizing one of a plurality of different mobile operating systems *(wherein as discussed above with regard to claim 17, **Thomas** discloses Internet correspondence (See FIG. 1), as well as security management facility 122 having the ability to scan the client facility 144 files for malicious code, remove or quarantine certain applications and files. See also FIG. 3, step 304, accessing security compliance info. Updates may be received from the network, as a result of alerts of new malicious codes or applications)* **(Thomas, FIG. 1 and FIG. 3, paragraphs [0025], [0028], [0040]-[0041], [0048] and [0058])**;

storing the status information in an electronic database accessible to a server

(wherein unified threat management facility 100 further includes network access rules facility 124 and policy management facility 112, each including databases) **(Thomas, FIG. 1, paragraphs [0034] and [0042])**;

evaluating at the server a first compliance state of at least one of the mobile devices from the status information using a plurality of administrator-defined rules *(wherein again, threat management is based on policy violations. In particular,* ***Thomas*** *teaches that corporate policy management is one of the dimensions for which the threat management facility 100 can control. The corporation may institute a policy that prevents certain people (e.g. employees, groups of employees, types of employees, guest of the corporation, etc.) from accessing certain types of computer programs. For example,* ***Thomas*** *discloses that the corporation may elect to prevent its accounting department from using a particular version of an instant messaging service or all such services. In the given example, the policy management facility 112 may be used to update the policies of all corporate computing assets with a proper policy control facility or it may update a select few. Policy management facility 112 may be able to block applications such as VoIP 164 and instant messaging 162 (IM) that, although non-malicious, may nonetheless still undermine productivity and network performance within the enterprise facility 102. Again, the rules of policy management facility 112 may indicate to enterprise facility 102 access permissions for the client facility 144, such as access permissions associated with the network, applications, external computer devices, and the like, and rules that may be interpreted with respect to an enterprise facility 102 network access request to determine if the request should be allowed. In a*

particular example, ***Thomas*** *teaches that when a website is requested by the client facility 144, a security facility may access the rules within a policy facility to determine if the requested access is related to a sporting website. The security facility (within threat management facility 100) may analyze the requested website to determine if the website matches with any of the policy facility rules, thereby effectively enforcing policies.* ***Thomas*** *further teaches that the policies may be administrator-defined, that is, maintained by the administration facility 134, through the threat management facility 100, in association with a third party, or the like)* **(Thomas, paragraphs [0023] and [0034]-[0035])**; and

initiating at least one action defined by the administrator-defined rules in response to the step of evaluating, wherein the step of evaluating is performed by the server automatically, in response to changes in the status information in the electronic database *(wherein again, remedial action facility 128 acts on policy violations. Again, upon scanning outgoing files and verifying that the outgoing files are permitted to be transmitted per the enterprise facility 102 rules and policies, security is achieved. By checking outgoing files,* ***Thomas*** *teaches that the security management facility 122 may be able discover malicious code infected files that were not detected as incoming files as a result of the client facility 144 having been updated with either new definition files or policy management facility 112 information. In addition, the network access rules may be developed by the enterprise facility 102, or pre-packaged by a supplier, and managed by the threat management facility 100 in conjunction with the administration facility 134. Network access rules and control may be responsible for determining if a*

client facility 144 application should be granted access to a requested network location. When network access for a client facility 144 is denied, the network access control may send an information file to the client facility 144, the information file may contain data or commands that may provide instructions for the remedial action facility 128) **(Thomas, paragraphs [0042]-[0043] and [0046])**.

Regarding claim 2, **Thomas** discloses the method of claim 1, wherein the at least one action is selectable from a plurality of actions, comprising blocking access by the at least one of the mobile devices to a corporate resource *(wherein again, Thomas discloses blocking access)* **(Thomas, paragraphs [0046] and [0064])**.

Regarding claim 21, **Thomas** discloses the system of claim 17, wherein the computer readable instructions further comprise instructions configured to gather the plurality of attributes for at least one of the plurality of mobile device by gathering attribute information from that mobile device and at least one other source on a network *(wherein again, security management facility scans client's files 144, clients are mobile, and security compliance information is derived from security policy to compare scanned files (See FIG. 3, item 304))* **(Thomas, FIG. 3, paragraphs [0028], [0058] and [0074])**.

Claims 6 and 14 includes a “method” claims that perform limitations substantially as described in “system” claim 21, and do not appear to contain any additional features with regard to novelty and/or inventive step; therefore, they are rejected under the same

rationale.

Regarding claim 23, **Thomas** discloses the system of claim 17, wherein the attribute comprises location information about the mobile device *(wherein user location is monitored)* **(Thomas, paragraphs [0043] and [0047])**.

Claims 9 and 16 include "method" claims that perform limitations substantially as described in "system" claim 21, and do not appear to contain any additional features with regard to novelty and/or inventive step; therefore, they are rejected under the same rationale.

Regarding claim 18, **Thomas** discloses the system of claim 17, wherein the computer readable instructions further comprise instructions configured to present a user interface to an administrator to allow selection of at least one attribute and one available action to define the at least one of the plurality of administrator defined rules *(wherein **Thomas** discloses a web portal accessible by an administrator as a user interface)* **(Thomas, paragraph [0053])**.

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. This application currently names joint inventors. In considering patentability of the claims under pre-AIA 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of pre-AIA 35 U.S.C. 103(c) and potential pre-AIA 35 U.S.C. 102(e), (f) or (g) prior art under pre-AIA 35 U.S.C. 103(a).

8. Claim 3 is rejected under 35 U.S.C. 103(a) as being unpatentable over Thomas in view of Moghaddam et al. (United States Patent Application Publication No. US 2008/0114862 A1), hereinafter "Moghaddam".

Regarding claim 3, **Thomas** discloses the method of claim 1, but does not expressly disclose wherein the at least one action is selectable from a plurality of actions, comprising blocking e-mail access for the at least one of the mobile devices.

However **Moghaddam** discloses at least one action is selectable from a plurality of actions, comprising blocking e-mail access for the at least one of the mobile devices

*(wherein **Moghaddam** discloses restricting email)* **(Moghaddam, paragraph [0045])**.

Thomas and **Moghaddam** are analogous art because they are from the same problem solving area, namely, systems and methods for configuring and using the mobile usage data and filtering and blocking access/content.

At the time of the invention, it would have been obvious to one of ordinary skill in the art, having the teachings of **Thomas** and **Moghaddam** before him or her, to modify the security system of **Thomas**, to include email restriction of **Moghaddam**, with reasonable expectation that this would result in a system that enabled users to customize their mobile devices such that usage restrictions were configurable **(Moghaddam, paragraph [0012])**. This approach to improving the computer security system of **Thomas** was well within the ordinary ability of one of ordinary skill in the art based on the teachings of **Moghaddam**.

Therefore, it would have been obvious to one of ordinary skill in the art to combine the teachings of **Thomas** with **Moghaddam** to obtain the invention as specified in claim 3.

9. Claims 4, 8, 15 and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Thomas in view of Naiman et al. (WIPO Patent Application Publication No. 2011022053), hereinafter "Naiman".

Regarding claim 4, **Thomas** discloses the method of claim 1, but does not expressly disclose wherein the at least one action is selectable from a plurality of

actions, comprising wiping information from the at least one of the mobile devices.

However **Naiman** discloses that at least one action is selectable from a plurality of actions, comprising wiping information from the at least one of the mobile devices *(wherein **Naiman** teaches a control policy to wipe files)* **(Naiman, page 11, paragraph 2)**.

Thomas and **Naiman** are analogous art because they are from the same problem solving area, namely, systems and methods of mobile device management.

At the time of the invention, it would have been obvious to one of ordinary skill in the art, having the teachings of **Thomas** and **Naiman** before him or her, to modify the security system of **Thomas**, to include the email restrictions of **Naiman**, with reasonable expectation that this would result in a system that prevented jail breaking and hacking and improved security **(Naiman, page 5, paragraph 2)**. This approach to improving the computer security system of **Thomas** was well within the ordinary ability of one of ordinary skill in the art based on the teachings of **Naiman**.

Therefore, it would have been obvious to one of ordinary skill in the art to combine the teachings of **Thomas** with **Naiman** to obtain the invention as specified in claim 4.

Regarding claim 22, **Thomas** discloses the system of claim 17, but does not expressly disclose wherein the plurality of different mobile operating systems comprise at least operating systems compliant with Android and iOS specifications.

However **Naiman** discloses a plurality of different mobile operating systems that

comprise at least operating systems compliant with Android and iOS specifications *(wherein **Naiman** discloses iPhone and ADROID™ operating systems)* **(Naiman, page 10)**.

Thomas and **Naiman** are analogous art because they are from the same problem solving area, namely, systems and methods of mobile device management.

At the time of the invention, it would have been obvious to one of ordinary skill in the art, having the teachings of **Thomas** and **Naiman** before him or her, to modify the security system of **Thomas**, to include the additional mobile operating systems of **Naiman**, with reasonable expectation that this would result in increased versatility and providing greater marketability to service providers that used various operating systems **(Naiman, page 5, paragraph 2)**. This approach to improving the computer security system of **Thomas** was well within the ordinary ability of one of ordinary skill in the art based on the teachings of **Naiman**.

Therefore, it would have been obvious to one of ordinary skill in the art to combine the teachings of **Thomas** with **Naiman** to obtain the invention as specified in claim 22.

Claims 8 and 15 include “method” claims that perform limitations substantially as described in “system” claim 21, and do not appear to contain any additional features with regard to novelty and/or inventive step; therefore, they are rejected under the same rationale.

10. Claims 5, 11 and 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Thomas in view of Yaqub et al. (United States Patent Application Publication No. US 2007/0206552 A1), hereinafter "Yaqub".

Regarding claim 5, **Thomas** discloses the method of claim 1, wherein the at least one action is selectable from a plurality of actions *(wherein remedial action may take a plurality of forms)* **(Thomas, paragraph [0046])**, but does not explicitly disclose comprising warning a user of the at least one of the mobile devices that further action may be taken.

However **Yaqub** discloses that at least one action is selectable from a plurality of actions, comprising warning a user of the at least one of the mobile devices that further action may be taken *(wherein **Yaqub** teaches warning a user if QoS violations have occurred)* **(Yaqub, paragraph [0081])**.

Thomas and **Yaqub** are analogous art because they are from the same problem solving area, namely, systems and methods of mobile device management.

At the time of the invention, it would have been obvious to one of ordinary skill in the art, having the teachings of **Thomas** and **Yaqub** before him or her, to modify the security system of **Thomas**, to include the email restrictions of **Yaqub**, with reasonable expectation that this would result in improved quality of service. This approach to improving the computer security system of **Thomas** was well within the ordinary ability of one of ordinary skill in the art based on the teachings of **Yaqub**.

Therefore, it would have been obvious to one of ordinary skill in the art to

combine the teachings of **Thomas** with **Yaqub** to obtain the invention as specified in claim 5.

Regarding claim 19, **Thomas** discloses the system of claim 18, wherein at least one of the actions comprises warning a user of the mobile device that the device is out of compliance and causing subsequent action to be performed if the attribute remains out of compliance *(wherein again, the QoS warning. Furthermore, **Yaqub** discloses that if violation persists, access is denied)* **(Yaqub, paragraph [0081])**. **Yaqub** does not expressly disclose causing subsequent action to be performed if the attribute remains out of compliance after a period of time defined in the at least one rule.

However it would be an obvious matter of design choice to modify **Thomas-Yaqub** to include causing subsequent action to be performed if the attribute remains out of compliance after a period of time defined in the at least one rule, in order to prevent unauthorized access from unsecured devices (please note, in the instant Application, paragraphs [0066]-[0067] and [0080]-[0081], Applicants have not given any stated advantage for the claimed limitation).

Claim 11 includes a “method” claim that performs limitations substantially as described in “system” claim 19, and does not appear to contain any additional features with regard to novelty and/or inventive step; therefore, it is rejected under the same rationale.

11. Claims 7, 12-13 and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Thomas in view of Germano et al. (United States Patent Application Publication No. US 2007/0266422 A1), hereinafter "Germano".

Regarding claim 7, **Thomas** discloses the method of claim 1, but does not expressly disclose further comprising the step of subsequently evaluating a second compliance state of at least one of the mobile devices to determine if the at least one action should be revoked.

However **Germano** discloses a step of subsequently evaluating a second compliance state of at least one of the mobile devices to determine if the at least one action should be revoked *(wherein **Germano** discloses that mobile device enforcement agent will continue to limit access to network resources to those identified within the limited access security policy, until such a time as either: (a) the security policies change, the changed policies are synchronized with the mobile device, and the enforcement agent is able to verify that the mobile device is in compliance with the security policy set applicable to that mobile device; or (b) the mobile device comes into compliance via user action or via the implementation of self-corrective measures, such as automated restoration of deleted files or other configuration changes)* **(Germano, paragraph [0037])**.

Thomas and **Germano** are analogous art because they are from the same problem solving area, namely, systems and methods of mobile device security.

At the time of the invention, it would have been obvious to one of ordinary skill in

the art, having the teachings of **Thomas** and **Germano** before him or her, to modify the security system of **Thomas**, to continue to limit access until compliance is restored, such as disclosed in **Germano**, with reasonable expectation that this would result in protecting enterprise data from malicious attacks **(Germano, paragraph [0016])**. This approach to improving the computer security system of **Thomas** was well within the ordinary ability of one of ordinary skill in the art based on the teachings of **Germano**.

Therefore, it would have been obvious to one of ordinary skill in the art to combine the teachings of **Thomas** with **Germano** to obtain the invention as specified in claim 7.

Regarding claim 20, **Thomas-Germano** discloses the system of claim 17, wherein the computer readable instructions further comprise instructions configured to automatically revoke the action if the attribute is brought back into compliance *(wherein again, the mobile device enforcement agent will continue to limit access to network resources to those identified within the limited access security policy, until such a time as either: (a) the security policies change, the changed policies are synchronized with the mobile device, and the enforcement agent is able to verify that the mobile device is in compliance with the security policy set applicable to that mobile device; or (b) the mobile device comes into compliance via user action or via the implementation of self-corrective measures, such as automated restoration of deleted files or other configuration changes)* **(Germano, paragraph [0037])**. The motivation regarding the

obviousness of claim 7 is also applied to claim 20.

Claim 12 includes a "method" claim that performs limitations substantially as described in "system" claim 20, and does not appear to contain any additional features with regard to novelty and/or inventive step; therefore, it is rejected under the same rationale.

Regarding claim 13, **Thomas-Germano** discloses the method of claim 12, wherein the step of automatically revoking the action comprises determining if another of the plurality of rules is triggered *(wherein again, until such a time as the security policies change, the changed policies are synchronized with the mobile device, and the enforcement agent is able to verify that the mobile device is in compliance with the security policy set applicable to that mobile device)* **(Germano, paragraph [0037])**. The motivation regarding the obviousness of claim 7 is also applied to claim 13.

Response to Arguments

12. Applicants' arguments, see page 6, filed May 19, 2014, with respect to Claim Objections have been fully considered and are persuasive. The Objections of Claims 8, 15 and 22, as set forth in the previous Office Action, have been withdrawn.

13. Applicants' arguments, see page 6, filed May 19, 2014, with respect to Claim Rejections under 35 U.S.C. 101 have been fully considered and are persuasive. The Rejections of Claims 17-23, as set forth in the previous Office Action, have been withdrawn.

14. Applicants' arguments, see pages 6-9, filed May 19, 2014, with respect to Claim Rejections under 35 U.S.C. 102(b) have been fully considered but they are not persuasive.

(A) Applicants argued on page 7 of Remarks, "***Thomas*** *fails to teach all elements of these claims, at least because it fails to teach 'storing the status information in an electronic database accessible to a server' and that a 'step of evaluating is performed by the server automatically, in response to changes in the status information in the electronic database'.*

"*While* ***Thomas*** *teaches policy management that is handled by a server (e.g., the threat management facility), the enforcement of rules is taught as done on the clients or done in a distributed manner with the assistance of the client. For example, the central management facility can directly access the state information of the client facility, such as by scanning files on the client. 'The security management facility 122 [part of facility 100] may have the ability to scan the client facility 144 files for malicious code, remove or quarantine certain applications and files, prevent certain actions, perform remedial actions and perform other security measures. In embodiments, scanning the client*

*facility 144 may include scanning some or all of the files stored to the client facility 144 on a periodic basis, may scan applications once the application has been requested to execute, may scan files as the files are transmitted to or from the client facility 144, or the like. The scanning of the applications and files may be to detect known malicious code or known unwanted applications.' **Thomas** at [28]*" **(Recited from page 7 of Remarks)**.

As to point **(A)**,Examiner respectfully disagrees. To begin with, Examiner notes Applicants appear to be arguing that the claimed limitations of "*storing the status information in an electronic database accessible to a server*," and that a "*step of evaluating is performed by the server automatically, in response to changes in the status information in the electronic database*," are features that necessarily preclude a teaching that "*the enforcement of rules is taught as done on the clients or done in a distributed manner with the assistance of the client*". However, the teaching of "*the enforcement of rules being taught as **not** done on the clients or **not** done in a distributed manner with the assistance of the client*" is not recited in the rejected claims. Put otherwise, claim 1 fails to recite that, "*the enforcement of rules is taught as done on the **server and not done in a distributed manner** with the assistance of the client*". Particularly, in response to Applicants' argument that the references fail to show certain features of Applicants' invention, it is noted that the features upon which applicant relies (i.e., "*wherein the enforcement of rules is **not** done on the clients or **not** done in a distributed manner with the assistance of the client*") are not recited in the rejected

claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993). The instant limitations that have been argued against are reproduced below:

"*storing the status information in an electronic database accessible to a server;*" and

"*evaluating at the server a first compliance state of at least one of the mobile devices from the status information using a plurality of administrator-defined rules*".

As discussed above, **Thomas** discloses that each of policy management facility 112 and network access rules facility 124 may include databases storing status information regarding at least usage/access privileges. Particularly, as given above, policy management facility 112 may include a policy database, such as, and/or including a block list, a black list, an allowed list, a white list, or the like that may provide a list of enterprise facility 102 external network locations/applications that may or may not be accessed by the client facility 144. The policy management facility 112 may further include rules that may be interpreted with respect to an enterprise facility 102 network access request to determine if the request should be allowed or denied. Likewise, network access rules facility 124 may also include databases such as a block list, a black list, an allowed list, a white list, an unacceptable network site database, an acceptable network site database, a network site reputation database, or the like of network access locations that may or may not be accessed by the client facility 144 **(See again Thomas, FIG. 1, paragraphs [0034] and [0044])**. Furthermore, also as

pointed out in the above rejection of claim 1, **Thomas** teaches that threat management is based on policy violations. In particular, **Thomas** teaches that corporate policy management is one of the dimensions for which the threat management facility 100 can control. The corporation may institute a policy that prevents certain people (e.g. employees, groups of employees, types of employees, guest of the corporation, etc.) from accessing certain types of computer programs. For example, **Thomas** discloses that the corporation may elect to prevent its accounting department from using a particular version of an instant messaging service or all such services. In the given example, the policy management facility 112 may be used to update the policies of all corporate computing assets with a proper policy control facility or it may update a select few. **Thomas** teaches that policy management facility 112 may be able to block applications such as VoIP 164 and instant messaging 162 (IM) that, although non-malicious, may nonetheless still undermine productivity and network performance within the enterprise facility 102. Again, the rules of policy management facility 112 may indicate to enterprise facility 102 access permissions for the client facility 144, such as access permissions associated with the network, applications, external computer devices, and the like, and rules that may be interpreted with respect to an enterprise facility 102 network access request to determine if the request should be allowed. In a particular example, **Thomas** teaches that when a website is requested by the client facility 144, a security facility may access the rules within a policy facility to determine if the requested access is related to a sporting website. The security management facility 122 (within threat management facility 100) may analyze the requested website to

determine if the website matches with any of the policy facility rules, thereby effectively enforcing policies. **Thomas** further teaches that the policies may be administrator-defined, that is, maintained by the administration facility 134, through the threat management facility 100, in association with a third party, or the like **(See again, Thomas, paragraphs [0025] and [0034]-[0035])**.

In addition, Examiner respectfully submits that if the limitation of "***the enforcement of rules is done on the server and not done in a distributed manner with the assistance of the client***" is in fact a critical feature of the invention, then it should indeed be present in the claim language. Again, Examiner points out that the instant argued-against limitations recite nothing to any effect of "***enforcement***" in any place within the claim language. In any event however, Examiner has sufficiently shown that **Thomas** does teach that the threat management facility 100 of FIG. 1 not only comprises a database as that claimed, does the evaluating (analyzing), but also teaches that policy enforcement is done together with the policy management facility 112, as well as the security management facility 122.

Therefore, Examiner respectfully submits that **Thomas** does disclose, teach, and/or suggest "*storing the status information in an electronic database accessible to a server*," and that a "*step of evaluating is performed by the server automatically, in response to changes in the status information in the electronic database*". Due to the amendment however, Examiner has updated citations to more accurately reflect claim mappings, and has elaborated on the interpretation of the claims, as well as application

of the reference to further assist the reader in understanding the rejection.

Conclusion

15. Applicants' arguments, as well as request for reconsideration, filed May 19, 2014, have been fully considered but they are not deemed to be persuasive.

16. Further references of interest are cited on Form PTO-892, which is an attachment to this Office Action.

17. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

18. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kostas Katsikis whose telephone number is (571)270-5434. The examiner can normally be reached on Monday - Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Wing Chan can be reached on (571)272-7493. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/KOSTAS KATSIKIS/
Primary Examiner, Art Unit 2441

September 4, 2014

Notice of References Cited	Application/Control No. 13/540,142	Applicant(s)/Patent Under Reexamination MALIK ET AL.	
	Examiner KOSTAS KATSIKIS	Art Unit 2441	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-2003/0115322 A1	06-2003	Moriconi et al.	709/224
	B	US-			
	C	US-			
	D	US-			
	E	US-			
	F	US-			
	G	US-			
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Petitioner Ex 1002, p. 380
Zimperium v. Taasera, IPR2024-00007

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13540142	MALIK ET AL.
	Examiner	Art Unit
	KOSTAS KATSIKIS	2441

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	12/16/2013	09/04/2014							
	1	✓	✓							
	2	✓	✓							
	3	✓	✓							
	4	✓	✓							
	5	✓	✓							
	6	✓	✓							
	7	✓	✓							
	8	✓	✓							
	9	✓	✓							
	10	✓	✓							
	11	✓	✓							
	12	✓	✓							
	13	✓	✓							
	14	✓	✓							
	15	✓	✓							
	16	✓	✓							
	17	✓	✓							
	18	✓	✓							
	19	✓	✓							
	20	✓	✓							
	21	✓	✓							
	22	✓	✓							
	23	✓	✓							

Petitioner Ex 1002, p. 381
Zimperium v. Taasera, IPR2024-00007

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S1	1	"13540142"	US-PGPUB; USPAT	ADJ	ON	2013/12/13 15:50
S2	1	"20130007245"	DERWENT	ADJ	ON	2013/12/13 15:50
S3	41873	709/223$	US-PGPUB; USPAT	ADJ	ON	2013/12/13 15:51
S4	43047	709/224$	US-PGPUB; USPAT	ADJ	ON	2013/12/13 15:51
S5	1	"20100242088"	US-PGPUB; USPAT	ADJ	ON	2013/12/13 15:57
S6	960	H04L41/0816.cpc.	US-PGPUB; USPAT	ADJ	ON	2013/12/13 16:01
S7	3684	H04L43/0817.cpc.	US-PGPUB; USPAT	ADJ	ON	2013/12/13 16:01
S8	2594	H04L41/0893.cpc.	US-PGPUB; USPAT	ADJ	ON	2013/12/13 16:02
S9	31	H04L41/0618.cpc.	US-PGPUB; USPAT	ADJ	ON	2013/12/13 16:21
S10	577	455/26.1$	US-PGPUB; USPAT	ADJ	ON	2013/12/13 16:26
S11	3571	455/425$	US-PGPUB; USPAT	ADJ	ON	2013/12/13 16:28
S12	3995	455/456.5$	US-PGPUB; USPAT	ADJ	ON	2013/12/13 16:31
S13	22104	(gather$3 or collect$3 or assembl$3 or aggregat$3) near4 (status)	US-PGPUB; USPAT	ADJ	ON	2013/12/13 16:38
S14	358	(evaluat$3 or assess$3 or determin$3) near20 (compl$5 or conform$4) near20 (polic$3 or rule$1) near20 (violat$3 or break$3 or infract$3)	US-PGPUB; USPAT	ADJ	ON	2013/12/13 16:42
S15	0	S13 same3 S14	US-PGPUB; USPAT	ADJ	ON	2013/12/13 16:43
S16	24731	(polic$3 or rule$1) near20 (violat$3 or break$3 or infract$3)	US-PGPUB;	ADJ	ON	2013/12/13 16:43

Petitioner Ex 1002, p. 382
Zimperium v. Taasera, IPR2024-00007

			USPAT			
S17	92	S13 same3 S16	US-PGPUB; USPAT	ADJ	ON	2013/12/13 16:44
S18	1883	(compl$5 or conform$4) near20 (polic$3 or rule$1) near20 (violat$3 or break$3 or infract$3)	US-PGPUB; USPAT	ADJ	ON	2013/12/13 16:47
S19	2	S13 same3 S18	US-PGPUB; USPAT	ADJ	ON	2013/12/13 16:47
S20	110055	(polic$3 or rule$1) near20 (violat$3 or break$3 or infract$3 or compl$5 or conform$3)	US-PGPUB; USPAT	ADJ	ON	2013/12/13 16:50
S21	1750	(gather$3 or collect$3) near20 (status or state) near20 (((subscriber or mobile or wireless) adj1 (station or device)) or ((user or subscriber) adj1 equipment) or "MS" or "UE" or "MA")	US-PGPUB; USPAT	ADJ	ON	2013/12/13 16:54
S22	31	S20 same3 S21	US-PGPUB; USPAT	ADJ	ON	2013/12/13 16:55
S23	2	S3 and S22	US-PGPUB; USPAT	ADJ	ON	2013/12/13 16:55
S24	2	"20120151041"	US-PGPUB; USPAT	ADJ	ON	2013/12/13 16:57
S25	2	S4 and S22	US-PGPUB; USPAT	ADJ	ON	2013/12/13 16:57
S26	1	S6 and S22	US-PGPUB; USPAT	ADJ	ON	2013/12/13 16:58
S27	1	S7 and S22	US-PGPUB; USPAT	ADJ	ON	2013/12/13 16:58
S28	1	S8 and S22	US-PGPUB; USPAT	ADJ	ON	2013/12/13 16:59
S29	0	S9 and S22	US-PGPUB; USPAT	ADJ	ON	2013/12/13 16:59
S30	0	S10 and S22	US-PGPUB; USPAT	ADJ	ON	2013/12/13 16:59
S31	0	S11 and S22	US-PGPUB; USPAT	ADJ	ON	2013/12/13 16:59
S32	0	S12 and S22	US-PGPUB; USPAT	ADJ	ON	2013/12/13 16:59
S33	3	((JATIN) near2 (MALIK)).INV.	US-PGPUB; USPAT	ADJ	ON	2013/12/13 18:01
S34	3	((RATNESH) near2 (SINGH)).INV.	US-PGPUB; USPAT	ADJ	ON	2013/12/13 18:01

Petitioner Ex 1002, p. 383
Zimperium v. Taasera, IPR2024-00007

S35	1	((RAJAKUMAR) near2 (BOPALLI)).INV.	US-PGPUB; USPAT	ADJ	ON	2013/12/13 18:01
S36	1	S33 and S34 and S35	US-PGPUB; USPAT	ADJ	ON	2013/12/13 18:01
S37	1	S33 and ((status adj1 information) and gathering and initiating).clm.	US-PGPUB; USPAT	ADJ	ON	2013/12/13 18:02
S38	1	S34 and ((status adj1 information) and gathering and initiating).clm.	US-PGPUB; USPAT	ADJ	ON	2013/12/13 18:02
S39	1	S33 and (status and information and gathering and initiating).clm.	US-PGPUB; USPAT	ADJ	ON	2013/12/13 18:03
S40	1	S34 and (status and information and gathering and initiating).clm.	US-PGPUB; USPAT	ADJ	ON	2013/12/13 18:03
S41	2204	(polic$3 or rule$1) near20 (violat$3 or break$3 or infract$3 or compl$5 or conform$3)	FPRS; EPO; JPO	ADJ	ON	2013/12/13 18:05
S42	238	(gather$3 or collect$3) near20 (status or state) near20 (((subscriber or mobile or wireless) adj1 (station or device)) or ((user or subscriber) adj1 equipment) or "MS" or "UE" or "MA")	FPRS; EPO; JPO	ADJ	ON	2013/12/13 18:05
S43	0	S41 same3 S42	FPRS; EPO; JPO	ADJ	ON	2013/12/13 18:05
S44	0	S41 and S42	FPRS; EPO; JPO	ADJ	ON	2013/12/13 18:05
S45	33818	(status or state) near20 (((subscriber or mobile or wireless) adj1 (station or device)) or ((user or subscriber) adj1 equipment) or "MS" or "UE" or "MA")	FPRS; EPO; JPO	ADJ	ON	2013/12/13 18:05
S46	8	S41 same3 S45	FPRS; EPO; JPO	ADJ	ON	2013/12/13 18:05
S47	1	"20100242088"	US-PGPUB; USPAT	ADJ	ON	2013/12/16 12:39
S48	2	"20080114862"	US-PGPUB; USPAT	ADJ	ON	2013/12/16 13:17
S49	1	"20070206552"	US-PGPUB; USPAT	ADJ	ON	2013/12/16 13:53
S50	0	((alert$3 or warning) near4 compliance near20 qos) same3 ((time or grace) adj1 period)	US-PGPUB; USPAT	ADJ	ON	2013/12/16 14:14
S51	0	((alert$3 or warning) near20 compliance near20 qos) same3 ((time or grace) adj1 period)	US-PGPUB; USPAT	ADJ	ON	2013/12/16 14:14
S52	3	((alert$3 or warning) near20 qos) same3 ((time or grace) adj1 period)	US-PGPUB; USPAT	ADJ	ON	2013/12/16 14:14
S53	1	"20070266422"	US-PGPUB; USPAT	ADJ	ON	2013/12/16 14:20

Petitioner Ex 1002, p. 384
Zimperium v. Taasera, IPR2024-00007

S54	1894	((policy or policies or rule$1) near3 (violation or conform$3 or enforc$5)) near20 (corporat$3 or enterprise)	US-PGPUB; USPAT	ADJ	ON	2014/09/04 19:49
S55	63128	(data$1store or database or (data adj1 store)) near20 (policies or rules)	US-PGPUB; USPAT	ADJ	ON	2014/09/04 19:51
S56	116338	(user or client) near20 access near20 (permission$1 or request$3)	US-PGPUB; USPAT	ADJ	ON	2014/09/04 19:52
S57	127	S54 same3 S55 same3 S56	US-PGPUB; USPAT	ADJ	ON	2014/09/04 19:52
S58	46591	709/223$	US-PGPUB; USPAT	ADJ	ON	2014/09/04 19:52
S59	48367	709/224$	US-PGPUB; USPAT	ADJ	ON	2014/09/04 19:52
S60	8	S57 and S58	US-PGPUB; USPAT	ADJ	ON	2014/09/04 19:52
S61	14	S57 and S59	US-PGPUB; USPAT	ADJ	ON	2014/09/04 19:52
S62	0	S57 and (response near20 update$1 near20 (rule$1 or polic$3))	US-PGPUB; USPAT	ADJ	ON	2014/09/04 19:55
S63	95	S57 and (update$1 near20 (rule$1 or polic$3))	US-PGPUB; USPAT	ADJ	ON	2014/09/04 19:56
S64	6	S63 and S58	US-PGPUB; USPAT	ADJ	ON	2014/09/04 19:56
S65	12	S63 and S59	US-PGPUB; USPAT	ADJ	ON	2014/09/04 19:56
S66	2	"20030115322"	US-PGPUB; USPAT	ADJ	ON	2014/09/04 19:58
S67	3	((Jatin) near2 (MALIK)).INV.	US-PGPUB; USPAT	ADJ	ON	2014/09/04 19:59
S68	3	((Ratnesh) near2 (SINGH)).INV.	US-PGPUB; USPAT	ADJ	ON	2014/09/04 19:59
S69	1	((Rajakumar) near2 (BOPALLI)).INV.	US-PGPUB; USPAT	ADJ	ON	2014/09/04 19:59
S70	1	S67 and S68 and S69	US-PGPUB; USPAT	ADJ	ON	2014/09/04 19:59
S71	1	S67 and (rules and database and server).clm.	US-PGPUB; USPAT	ADJ	ON	2014/09/04 20:01
S72	2	S68 and (rules and database and server).clm.	US-PGPUB; USPAT	ADJ	ON	2014/09/04 20:01

Petitioner Ex 1002, p. 385
Zimperium v. Taasera, IPR2024-00007

S73	1	S69 and (rules and database and server).clm.	US-PGPUB; USPAT	ADJ	ON	2014/09/04 20:01
S74	49	((policy or policies or rule$1) near3 (violation or conform$3 or enforc$5)) near20 (corporat$3 or enterprise)	FPRS; EPO; JPO	ADJ	ON	2014/09/04 20:02
S75	5071	(data$1store or database or (data adj1 store)) near20 (policies or rules)	FPRS; EPO; JPO	ADJ	ON	2014/09/04 20:02
S76	16773	(user or client) near20 access near20 (permission$1 or request$3)	FPRS; EPO; JPO	ADJ	ON	2014/09/04 20:02
S77	0	S74 and S75 and S76	FPRS; EPO; JPO	ADJ	ON	2014/09/04 20:03
S78	2	S74 and S75	FPRS; EPO; JPO	ADJ	ON	2014/09/04 20:03
S79	0	S74 and S76	FPRS; EPO; JPO	ADJ	ON	2014/09/04 20:03
S80	113	S75 and S76	FPRS; EPO; JPO	ADJ	ON	2014/09/04 20:03
S81	1158	H04L41/0816.cpc.	US-PGPUB; USPAT	ADJ	ON	2014/09/04 20:04
S82	4025	H04L43/0817.cpc.	US-PGPUB; USPAT	ADJ	ON	2014/09/04 20:04
S83	2946	H04L41/0893.cpc.	US-PGPUB; USPAT	ADJ	ON	2014/09/04 20:04
S84	36	H04L41/0618.cpc.	US-PGPUB; USPAT	ADJ	ON	2014/09/04 20:04
S85	646	455/26.1$	US-PGPUB; USPAT	ADJ	ON	2014/09/04 20:04
S86	3960	455/425$	US-PGPUB; USPAT	ADJ	ON	2014/09/04 20:05
S87	4582	455/456.5$	US-PGPUB; USPAT	ADJ	ON	2014/09/04 20:05

9/4/2014 8:12:57 PM
C:\Users\kkatsikis1\Documents\EAST\Workspaces\13540142.wsp

Petitioner Ex 1002, p. 386
Zimperium v. Taasera, IPR2024-00007

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13540142	MALIK ET AL.
	Examiner	Art Unit
	KOSTAS KATSIKIS	2441

CPC- SEARCHED		
Symbol	Date	Examiner
H04L41/0816	12/13/2013 (Updated 9/4/2014)	KK
H04L43/0817	12/13/2013 (Updated 9/4/2014)	KK
H04L41/0893	12/13/2013 (Updated 9/4/2014)	KK
H04L41/0618	12/13/2013 (Updated 9/4/2014)	KK

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner
709	223, 224	12/13/2013 (Updated 9/4/2014)	KK
455	26.1, 425, 456.5	12/13/2013 (Updated 9/4/2014)	KK

SEARCH NOTES		
Search Notes	Date	Examiner

/KOSTAS KATSIKIS/ Examiner.Art Unit 2441	/KOSTAS KATSIKIS/ Primary Examiner.Art Unit 2441

SEARCH NOTES

Search Notes	Date	Examiner
Examiner conducted thorough EAST search.	12/13/2013 and 12/16/2013 (Updated 9/4/2014)	KK
EAST (USPAT, US-PGPUB) - see search history printout.	12/13/2013 and 12/16/2013 (Updated 9/4/2014)	KK
EAST (EPO, JPO, FPRS) - see search history printout.	12/13/2013 (Updated 9/4/2014)	KK
709/223 (text search - see search history printout).	12/13/2013 (Updated 9/4/2014)	KK
709/224 (text search - see search history printout).	12/13/2013 (Updated 9/4/2014)	KK
H04L41/0816 (text search - see search history printout).	12/13/2013	KK
H04L43/0817 (text search - see search history printout).	12/13/2013	KK
H04L41/0893 (text search - see search history printout).	12/13/2013	KK
H04L41/0618 (text search - see search history printout).	12/13/2013	KK
Examiner conducted Inventor Name search in EAST.	12/13/2013	KK
455/26.1 (text search - see search history printout).	12/13/2013 (Updated 9/4/2014)	KK
455/425 (text search - see search history printout).	12/13/2013	KK
455/456.5 (text search - see search history printout).	12/13/2013	KK

INTERFERENCE SEARCH

US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner

/KOSTAS KATSIKIS/ Examiner.Art Unit 2441	/KOSTAS KATSIKIS/ Primary Examiner.Art Unit 2441

DOCKET NO.: 130839.02101
Application No.: 13/540,142
Response to Office Action dated: September 8, 2014

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: **Jatin MALIK et al.**

Title: **RULES BASED ACTIONS FOR MOBILE DEVICE MANAGEMENT**

Application No.: **13/540,142** Group Art Unit: **2441**

Filed: **July 2, 2012** Examiner: **Kostas J. Katsikis**

Confirmation: **4198** Filed by EFS on: **February 9, 2015**

Mail Stop AF
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

AMENDMENT AND REQUEST FOR RECONSIDERATION UNDER 35 U.S.C. § 1.116

Sir:

In response to the Office Action mailed on September 8, 2014, Applicants respectfully request reconsideration in light of the:

Listing of the Claims, reflecting current amendments, beginning on page 2; and

Remarks beginning on page 7 of this paper.

Listing of Claims:

This listing of claims will replace all prior versions and listings of claims in the application.

1. (Presently Amended) A method for providing device management services comprising steps of:

gathering, at a server, from a network, status information related to an operating state of each of a plurality of mobile devices, each mobile device utilizing one of a plurality of different mobile operating systems, wherein the status information for each mobile device is gathered from a plurality of sources including each mobile device in a substantially real time manner;

formatting the status information for each of the mobile devices, such that rules can be substantially uniformly applied to the status information across the plurality of different mobile operating systems;

storing the status information in an electronic database accessible to [[a]] the server;

evaluating, at the server, a first compliance state of ~~at least one~~ each of the mobile devices from the status information using a plurality of administrator-defined rules, wherein each of the rules applies to mobile devices regardless of mobile operating system; and

initiating, at the server, at least one action defined by the administrator-defined rules in response to the step of evaluating,

wherein the step of evaluating is performed by the server automatically, in response to changes in the status information in the electronic database.

2. (Original) The method of claim 1, wherein the at least one action is selectable from a plurality of actions, comprising blocking access by the at least one of the mobile devices to a corporate resource.

3. (Original) The method of claim 1, wherein the at least one action is selectable from a plurality of actions, comprising blocking e-mail access for the at least one of the mobile devices.

4. (Original) The method of claim 1, wherein the at least one action is selectable from a plurality of actions, comprising wiping information from the at least one of the mobile devices.

Petitioner Ex 1002, p. 390
Zimperium v. Taasera, IPR2024-00007

5. (Original) The method of claim 1, wherein the at least one action is selectable from a plurality of actions, comprising warning a user of the at least one of the mobile devices that further action may be taken.

6. (Original) The method of claim 1, wherein the step of gathering status information, for the at least one mobile device, comprises gathering information from that mobile device and at least one other source on the network.

7. (Original) The method of claim 1, further comprising the step of subsequently evaluating a second compliance state of at least one of the mobile devices to determine if the at least one action should be revoked.

8. (Previously Presented) The method of claim 1, wherein the plurality of different mobile operating systems comprise at least operating systems compliant with Android and iOS specifications.

9. (Original) The method of claim 1, wherein the status information comprises location information about each mobile device.

10. (Presently Amended) A method for providing device management services comprising steps of:

receiving, at a server, a plurality of attributes related to an operating state of each of a plurality of mobile devices, each mobile device utilizing one of a plurality of different mobile operating systems, wherein the attributes for each mobile device are gathered from a plurality of sources including each mobile device;

making a determination that an attribute of a mobile device has changed;

evaluating the attribute, by a processor at [[a]] the server in response to the determination, to determine if [[it]] the attribute change triggers at least one of a plurality of administrator-defined rules, which indicates that the attribute is out of compliance, wherein each of the rules applies to mobile devices regardless of mobile operating system; and

automatically initiating, at the server, an action defined by the at least one of a plurality of administrator defined rules if the attribute is out of compliance,

Petitioner Ex 1002, p. 391
Zimperium v. Taasera, IPR2024-00007

wherein the attribute is stored in a data store accessible to the server, that includes substantially real-time data, gathered from the plurality of sources on a network[[,]] and pertaining to a plurality of attributes of a plurality of mobile devices, ~~comprising devices having~~ wherein the substantially real-time data is formatted, such that the rules can be substantially uniformly applied to the plurality of attributes across the plurality of different mobile operating systems.

11. (Original) The method of claim 10, wherein the step of automatically initiating an action comprises warning a user of the mobile device that the device is out of compliance and subsequently causing the action to be performed if the attribute remains out of compliance after a period of time defined in the at least one rule.

12. (Original) The method of claim 10, further comprising the step of automatically revoking the action if the attribute is brought back into compliance.

13. (Original) The method of claim 12, wherein the step of automatically revoking the action comprises determining if another of the plurality of rules is triggered.

14. (Original) The method of claim 10, further comprising the step of gathering the plurality of attributes for at least one of the plurality of mobile device by gathering attribute information from that mobile device and at least one other source on a network.

15. (Previously Presented) The method of claim 10, wherein the plurality of different mobile operating systems comprise at least operating systems compliant with Android and iOS specifications.

16. (Original) The method of claim 10, wherein the attribute comprises location information about the mobile device.

17. (Presently Amended) A system for providing device management services comprising:

a data store configured to be accessible by a server;

Petitioner Ex 1002, p. 392
Zimperium v. Taasera, IPR2024-00007

a CPU of the server coupled to a memory configured to execute computer readable instructions;

computer readable instructions for execution on the server comprising instructions configured to:

automatically make a determination that an attribute of a mobile device stored in the data store has changed;

evaluate the attribute, in response to the determination, to determine if [[it]] the attribute change triggers at least one of a plurality of administrator-defined rules, which indicates that the attribute is out of compliance, wherein each of the rules applies to mobile devices regardless of mobile operating system; and

automatically initiate an action defined by the at least one of a plurality of administrator defined rules if the attribute is out of compliance,

wherein the data store is configured to gather~~, from a network,~~ substantially real-time data pertaining to a plurality of attributes [[of a]] related to an operating state of each of the plurality of mobile devices, the attributes for each mobile device being gathered from a plurality of sources including each mobile device, ~~comprising devices having~~ wherein each mobile device utilizes one of a plurality of different mobile operating systems, and the substantially real-time data is formatted, such that the rules can be substantially uniformly applied to the plurality of attributes across the plurality of different mobile operating systems.

18. (Original) The system of claim 17, wherein the computer readable instructions further comprise instructions configured to present a user interface to an administrator to allow selection of at least one attribute and one available action to define the at least one of the plurality of administrator defined rules.

19. (Original) The system of claim 18, wherein at least one of the actions comprises warning a user of the mobile device that the device is out of compliance and causing subsequent action to be performed if the attribute remains out of compliance after a period of time defined in the at least one rule.

Petitioner Ex 1002, p. 393
Zimperium v. Taasera, IPR2024-00007

20. (Original) The system of claim 17, wherein the computer readable instructions further comprise instructions configured to automatically revoke the action if the attribute is brought back into compliance.

21. (Original) The system of claim 17, wherein the computer readable instructions further comprise instructions configured to gather the plurality of attributes for at least one of the plurality of mobile device by gathering attribute information from that mobile device and at least one other source on a network.

22. (Previously Presented) The system of claim 17, wherein the plurality of different mobile operating systems comprise at least operating systems compliant with Android and iOS specifications.

23. (Original) The system of claim 17, wherein the attribute comprises location information about the mobile device.

Petitioner Ex 1002, p. 394
Zimperium v. Taasera, IPR2024-00007

REMARKS

Claims 1-23 were pending in the application. Claims 1, 10, and 17 have been amended. Support for these amendments can be found throughout the application, including but not limited to paragraphs 26, 44-46, 58, and related disclosure. No new matter has been introduced. Accordingly, upon entry of this amendment, claims 1-23 are before the Examiner.

This communication is also being filed with the attached Certification and Request for Consideration under the After Final Consideration Pilot Program 2.0.

Rejections Under 35 U.S.C. § 102

Claims 1-2, 6, 9-10, 14, 16-18, 21, and 23 stand rejected under 35 U.S.C. § 102(b) as allegedly being anticipated by Thomas et al. (U.S. Patent Publication No. 2010/0242088).

Applicants respectfully disagree for the reasons set forth in the May 19, 2014 amendment. However, in the interest of expediting prosecution, claims 1, 10, and 17 have been amended to so that there can be no question that the pending claims are patentable over the prior art of record.

As previously discussed, Thomas does not handle mobile status information at a server in the claimed manner. Thomas teaches a system that provides for centralized policy updates to client facilities, to allow these client facilities to implement and/or participate in the application of the policies. *See, e.g.,* Thomas at 23, 40, (a centralized threat management facility 100 "facilitate[s] the setting, updating and control of such policies the corporation only needs to be concerned with keeping the threat management facility 100 up to date on such policies. The threat management facility 100 can take care of updating all of the other corporate computing assets." Thomas at 23; "the client facility 144 may be updated with new definition files periodically to provide the client facility 144 with the most recent malicious code definitions." Thomas at 40). Client facilities then use the security information received from the server to ensure compliance. For example, software can be provided to perform disk scans of client files on disk, or as they are sent to or from the client. *See, e.g.,* Thomas at 28. Thomas further teaches URI filtering and monitoring [*Id.* at 29], monitoring behavior before allowing execution of software [*Id.* at 30], monitoring outgoing files [*Id.* at 42]. These are all processes that necessarily take place at the client. In contrast, the rule enforcement and actions in the pending claims take place on the server, in response to real-time status information received from mobile devices.

Petitioner Ex 1002, p. 395
Zimperium v. Taasera, IPR2024-00007

The pending claims provide specific limitations as to how this information is handled by the server that are simply not taught by Thomas.

Taking claim 1 as an example, claim 1 requires "gathering, at a server, from a network, status information related to an operating state of each of a plurality of mobile devices." Thomas does not teach that any status information is ever gathered at a server, instead teaching that compliance definitions are sent from a server, which allows enforcement at a client. Additionally, claim 1 also requires that this "information for each mobile device is gathered from a plurality of sources including each mobile device in a substantially real time manner." Since Thomas fails to teach that mobile device status information is gathered by a server, Thomas certainly fails to teach that the gathering of information for an individual mobile device includes multiple sources (e.g., the mobile device and at least one other source, such as another server that has access to device status information (e.g., Apple's MDM server that monitors iOS devices – *see, e.g.,* Application at 45-46). Nor does Thomas teach that the absent gathering occurs in a substantially real-time manner.

Because Thomas is unconcerned with gathering mobile device status information at a server, Thomas further fails to teach formatting that information such that rules at the server can be uniformly applied across multiple mobile device operating systems. Furthermore, because Thomas is silent as to rules enforced (rather than simply maintained) at the server, Thomas also fails to teach that these rules are applied regardless of mobile operating system or that resulting actions are initiated at the server.

In addition, regarding claims 10 and 17, Thomas is silent as to gathering of mobile device attributes in the manners discussed with respect to claim 1 and Thomas further fails to teach that those mobile device attributes are stored in a data store accessible to the server, in the claimed manner.

Accordingly, in addition to the distinctions previously discussed in the last amendment, the newly amended independent claims 1, 10, and 17 have several elements that are not taught by Thomas and would not be obvious in light of Thomas. Furthermore, no conceivable combination of Thomas and the remaining cited references could solve these infirmities. Therefore, Applicants respectfully submit that independent claims 1, 10, and 17 are allowable in their present form.

Applicants further submit that, because claims 2, 6, 7, 9, 14, 16, 18, 21, and 23 depend from and incorporate all of the limitations of the respective independent claims, these dependent

Petitioner Ex 1002, p. 396
Zimperium v. Taasera, IPR2024-00007

claims are non-obvious over the cited references for at least the reasons stated above with respect to the independent claims. Applicants also believe that any further discussion of the patentability of the additional elements in the dependent claims in light of infirmities of the prior art is not needed as moot. However, Applicants reserve the right to discuss these individual elements further if the Examiner disagrees with Applicants' current arguments with respect to the independent claims.

Accordingly, Applicants respectfully request that the rejections associated with claims 1-2, 6, 9-10, 14, 16-18, 21, and 23 be withdrawn and allowance of these claims be swiftly granted.

Rejections Under 35 U.S.C. § 103

Claim 3 stands rejected under 35 U.S.C. § 103(a) as allegedly being obvious over Thomas in view of Moghaddam et al. (U.S. Patent Publication No. 2008/0114862).

Claims 4, 8, 15, and 22 stand rejected under 35 U.S.C. § 103(a) as allegedly being obvious over Thomas in view of Naiman et al. (International Patent Publication No. WO 2011/022053).

Claims 5, 11, and 19 stand rejected under 35 U.S.C. § 103(a) as allegedly being obvious over Thomas in view of Yaqub et al. (U.S. Patent Publication No. 2007/0206552).

Claims 7, 12, 13, and 20 stand rejected under 35 U.S.C. § 103(a) as allegedly being obvious over Thomas in view of Germano et al. (U.S. Patent Publication No. 2007/0266422).

None of these references solve the above infirmities with Thomas, discussed above, in any conceivable combination. Therefore, Applicants respectfully submit that, because each of these claim depend from and incorporate all of the limitations of the respective independent claims, these dependent claims are non-obvious over the cited references for at least the reasons stated above with respect to the independent claims. See MPEP §2143.03 (stating that if an independent claim is nonobvious under 35 U.S.C. §103, then any claim depending therefrom is nonobvious). Applicants also believe that any further discussion of the patentability of the additional elements in the dependent claims in light of infirmities of the prior art is not needed as moot. However, Applicants reserve the right to discuss these individual elements further if the Examiner disagrees with Applicants' current arguments with respect to the independent claim.

Accordingly, Applicants respectfully request that the rejections associated with these remaining claims be withdrawn and allowance of these claims be swiftly granted.

Petitioner Ex 1002, p. 397
Zimperium v. Taasera, IPR2024-00007

CONCLUSION

Early reconsideration and allowance of all pending claims is respectfully requested. The Examiner is requested to contact the undersigned attorney if an interview, telephonic or personal, would facilitate allowance of the claims.

AUTHORIZATION

The Commissioner is hereby authorized to charge any additional fees which may be required for this response, or credit any overpayment, to deposit account no. 50-0436.

Respectfully Submitted

By: /Michael K. Jones, Reg. No. 41100/
Michael K. Jones
Registration No. 41,100

Dated: **February 9, 2015**
PEPPER HAMILTON LLP
3000 Two Logan Square
Eighteenth and Arch Street
Philadelphia, PA 19103-279
Telephone: (215) 981-4405
Facsimile: (610) 640-7835

Petitioner Ex 1002, p. 398
Zimperium v. Taasera, IPR2024-00007

PTO/AIA/22 (03-13)
Approved for use through 7/31/2016. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PETITION FOR EXTENSION OF TIME UNDER 37 CFR 1.136(a)

Docket Number (Optional): 130839.02101

Application Number: 130839.02101

Filed: July 2, 2012

For: RULES BASED ACTIONS FOR MOBILE DEVICE MANAGEMENT

Art Unit: 2441

Examiner: Kostas J. Katsikis

This is a request under the provisions of 37 CFR 1.136(a) to extend the period for filing a reply in the above-identified application.

The requested extension and fee are as follows (check time period desired and enter the appropriate fee below):

	Fee	Small Entity Fee	Micro Entity Fee	
☐ One month (37 CFR 1.17(a)(1))	$200	$100	$50	$
☑ Two months (37 CFR 1.17(a)(2))	$600	$300	$150	$ 600
☐ Three months (37 CFR 1.17(a)(3))	$1,400	$700	$350	$
☐ Four months (37 CFR 1.17(a)(4))	$2,200	$1,100	$550	$
☐ Five months (37 CFR 1.17(a)(5))	$3,000	$1,500	$750	$

☐ Applicant asserts small entity status. See 37 CFR 1.27.

☐ Applicant certifies micro entity status. See 37 CFR 1.29.
Form PTO/SB/15A or B or equivalent must either be enclosed or have been submitted previously.

☐ A check in the amount of the fee is enclosed.

☑ Payment by credit card. Form PTO-2038 is attached.

☐ The Director has already been authorized to charge fees in this application to a Deposit Account.

☑ The Director is hereby authorized to charge any fees which may be required, or credit any overpayment, to Deposit Account Number 50-0436.

☑ Payment made via EFS-Web.

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

I am the

☐ applicant.

☑ attorney or agent of record. Registration number 41,100.

☐ attorney or agent acting under 37 CFR 1.34. Registration number _____.

/Michael K. Jones, Reg. #41100/ — Signature

February 9, 2015 — Date

Michael K. Jones — Typed or printed name

215.981.4405 — Telephone Number

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications. Submit multiple forms if more than one signature is required, see below*.

☑ * Total of 1 forms are submitted.

This collection of information is required by 37 CFR 1.136(a). The information is required to obtain or retain a benefit by the public, which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 6 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Mail Stop PCT, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Doc Code: A.NE.AFCP
Document Description: After Final Consideration Pilot Program Request

PTO/SB/434 (05-13)

CERTIFICATION AND REQUEST FOR CONSIDERATION UNDER THE AFTER FINAL CONSIDERATION PILOT PROGRAM 2.0

Practitioner Docket No.:	Application No.:	Filing Date:
130839.02101	13/540,142	July 2, 2012
First Named Inventor:	**Title:**	
Jatin Malik	RULES BASED ACTIONS FOR MOBILE DEVICE MANAGEMENT	

APPLICANT HEREBY CERTIFIES THE FOLLOWING AND REQUESTS CONSIDERATION UNDER THE AFTER FINAL CONSIDERATION PILOT PROGRAM 2.0 (AFCP 2.0) OF THE ACCOMPANYING RESPONSE UNDER 37 CFR 1.116.

1. The above-identified application is (i) an original utility, plant, or design nonprovisional application filed under 35 U.S.C. 111(a) [a continuing application (*e.g.*, a continuation or divisional application) is filed under 35 U.S.C. 111(a) and is eligible under (i)], or (ii) an international application that has entered the national stage in compliance with 35 U.S.C. 371(c).
2. The above-identified application contains an outstanding final rejection.
3. Submitted herewith is a response under 37 CFR 1.116 to the outstanding final rejection. The response includes an amendment to at least one independent claim, and the amendment does not broaden the scope of the independent claim in any aspect.
4. This certification and request for consideration under AFCP 2.0 is the only AFCP 2.0 certification and request filed in response to the outstanding final rejection.
5. Applicant is willing and available to participate in any interview requested by the examiner concerning the present response.
6. This certification and request is being filed electronically using the Office's electronic filing system (EFS-Web).
7. Any fees that would be necessary consistent with current practice concerning responses after final rejection under 37 CFR 1.116, *e.g.*, extension of time fees, are being concurrently filed herewith. [There is no additional fee required to request consideration under AFCP 2.0.]
8. By filing this certification and request, applicant acknowledges the following:
   - Reissue applications and reexamination proceedings are not eligible to participate in AFCP 2.0.
   - The examiner will verify that the AFCP 2.0 submission is compliant, *i.e.*, that the requirements of the program have been met (see items 1 to 7 above). For compliant submissions:
     - The examiner will review the response under 37 CFR 1.116 to determine if additional search and/or consideration (i) is necessitated by the amendment and (ii) could be completed within the time allotted under AFCP 2.0. If additional search and/or consideration is required but cannot be completed within the allotted time, the examiner will process the submission consistent with current practice concerning responses after final rejection under 37 CFR 1.116, *e.g.*, by mailing an advisory action.
     - If the examiner determines that the amendment does not necessitate additional search and/or consideration, or if the examiner determines that additional search and/or consideration is required and could be completed within the allotted time, then the examiner will consider whether the amendment places the application in condition for allowance (after completing the additional search and/or consideration, if required). If the examiner determines that the amendment does not place the application in condition for allowance, then the examiner will contact the applicant and request an interview.
       - The interview will be conducted by the examiner, and if the examiner does not have negotiation authority, a primary examiner and/or supervisory patent examiner will also participate.
       - If the applicant declines the interview, or if the interview cannot be scheduled within ten (10) calendar days from the date that the examiner first contacts the applicant, then the examiner will proceed consistent with current practice concerning responses after final rejection under 37 CFR 1.116.

Signature	Date
/Michael K. Jones, Reg. #41100/	February 9, 2015
Name (Print/Typed) Michael K. Jones	**Practitioner Registration No.** 41,100

***Note**: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4(d) for signature requirements and certifications. Submit multiple forms if more than one signature is required, see below*.*

☑ * Total of 1 forms are submitted.

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Electronic Patent Application Fee Transmittal

Application Number:	13540142
Filing Date:	02-Jul-2012
Title of Invention:	RULES BASED ACTIONS FOR MOBILE DEVICE MANAGEMENT
First Named Inventor/Applicant Name:	Jatin MALIK
Filer:	Michael Kenneth Jones/Sara Harvell
Attorney Docket Number:	130839.02101

Filed as Large Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension - 2 months with $0 paid	1252	1	600	600
Miscellaneous:				
		Total in USD ($)		**600**

Electronic Acknowledgement Receipt

EFS ID:	21439357
Application Number:	13540142
International Application Number:	
Confirmation Number:	4198
Title of Invention:	RULES BASED ACTIONS FOR MOBILE DEVICE MANAGEMENT
First Named Inventor/Applicant Name:	Jatin MALIK
Customer Number:	86308
Filer:	Michael Kenneth Jones
Filer Authorized By:	
Attorney Docket Number:	130839.02101
Receipt Date:	09-FEB-2015
Filing Date:	02-JUL-2012
Time Stamp:	16:53:28
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	$600
RAM confirmation Number	3628
Deposit Account	500436
Authorized User	JONES, MICHAEL K.
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees) Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)	

Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		2101Response.pdf	122861 08ab0e9b07ac6bb1a5ae15a1ce72d6a5440d91aa	yes	10

Multipart Description/PDF files in .zip description

Document Description	Start	End
Response After Final Action	1	1
Claims	2	6
Applicant Arguments/Remarks Made in an Amendment	7	10

Warnings:					
Information:					
2	Extension of Time	2101Extension.pdf	127590 8a7aaa1313736cbeb0b7c31757db7afe6a9482ef	no	2
Warnings:					
Information:					
3	After Final Consideration Program Request	2101AFCP.pdf	202238 53dda3dde446ce42a8e4092dc4af7b2a926afa2a	no	2
Warnings:					
Information:					
4	Fee Worksheet (SB06)	fee-info.pdf	31003 6741fe408a8ac55134e9c04c27776da71cfdd0db	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	483692		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PTO/SB/06 (09-11)
Approved for use through 1/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 13/540,142	Filing Date 07/02/2012	☐ To be Mailed

ENTITY: ☐ LARGE ☒ SMALL ☐ MICRO

APPLICATION AS FILED – PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	RATE ($)	FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X $ =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).			
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))				
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL	

APPLICATION AS AMENDED – PART II

AMENDMENT	02/09/2015	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	* 23	Minus	** 23	=	X $ =	
	Independent (37 CFR 1.16(h))	* 3	Minus	***3	=	X $ =	
	☐ Application Size Fee (37 CFR 1.16(s))						
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
						TOTAL ADD'L FEE	

AMENDMENT		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	*	Minus	**	=	X $ =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	X $ =	
	☐ Application Size Fee (37 CFR 1.16(s))						
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
						TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".
The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

LIE
/PEGGY YARBOROUGH/

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**
If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	13540142
Filing Date	2012-07-02
First Named Inventor	Jatin Malik
Art Unit	2441
Examiner Name	Kostas J. Katsikis
Attorney Docket Number	130839.02101

U.S.PATENTS

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button.

U.S.PATENT APPLICATION PUBLICATIONS

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20070143851	A1	2007-06-21	Nicodemus et al.	
	2	20070156659	A1	2007-07-05	Lim	
	3	20080109871	A1	2008-05-08	Jacobs	
	4	20110145920	A1	2011-06-16	Mahaffey et al.	

If you wish to add additional U.S. Published Application citation information please click the Add button.

FOREIGN PATENT DOCUMENTS

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] ¡	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99**)		
	Application Number	13540142
	Filing Date	2012-07-02
	First Named Inventor	Jatin Malik
	Art Unit	2441
	Examiner Name	Kostas J. Katsikis
	Attorney Docket Number	130839.02101

	1	2005064498	WO	A1	2005-07-14	Shahbazi		☐

If you wish to add additional Foreign Patent Document citation information please click the Add button

NON-PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1	Supplementary European Search Report mailed 5 February 2015 in corresponding European Patent Application No. 12808145.2	☐

If you wish to add additional non-patent literature document citation information please click the Add button

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99**)		
	Application Number	13540142
	Filing Date	2012-07-02
	First Named Inventor	Jatin Malik
	Art Unit	2441
	Examiner Name	Kostas J. Katsikis
	Attorney Docket Number	130839.02101

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☒ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☐ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☐ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Michael K. Jones, Reg. #41100/	Date (YYYY-MM-DD)	2015-02-12
Name/Print	Michael K. Jones	Registration Number	41100

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
14 July 2005 (14.07.2005)

PCT

(10) International Publication Number
WO 2005/064498 A1

(51) International Patent Classification[7]: G06F 17/30

(21) International Application Number:
PCT/US2004/042565

(22) International Filing Date:
22 December 2004 (22.12.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/531,668 23 December 2003 (23.12.2003) US

(71) Applicant *(for all designated States except US)*: **TRUST DIGITAL, LLC** [US/US]; 7900 Westpark Drive, Suite A50, McLean, VA 22102 (US).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **SHAHBAZI, Majid** [US/US]; 13119 Misty Glen Lane, Fairfax, Virginia 22033 (US).

(74) Agent: **BABAYI, Robert S.**; VENABLE LLP, P.O. Box 34385, Washington, DC 20043-9998 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

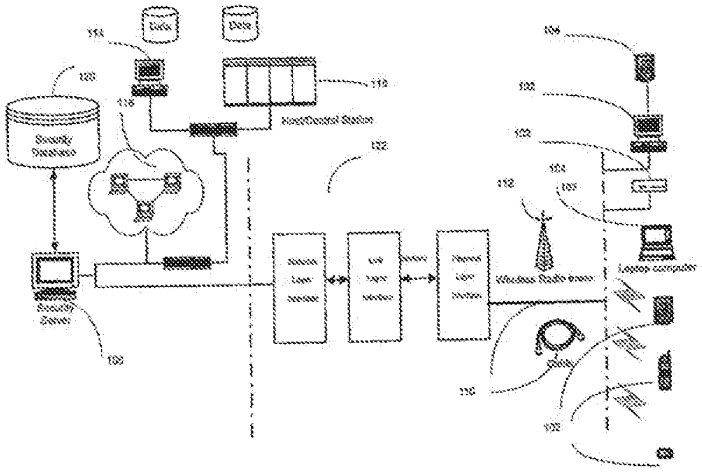
(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii)) for all designations*

[Continued on next page]

(54) Title: SYSTEM AND METHOD FOR ENFORCING A SECURITY POLICY ON MOBILE DEVICES USING DYNAMICALLY GENERATED SECURITY PROFILES



(57) Abstract: A system and method for enforcing security parameters that collects information from a source relating to a mobile device (104). Based on the collected information, an identity status for the mobile device (104) is determined that uniquely identifies the mobile device (104) and distinguishes it from other mobile devices. The identity status of the mobile device (104) can be determined when the mobile device (104) connects to a computing node source (102) or when the mobile device (104) accesses a resource (124) within the network. A security profile based on the identity status of the mobile device (104) is generated and the security profile is applied to the mobile device (104).

WO 2005/064498 A1

— *as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii)) for all designations*
— *of inventorship (Rule 4.17(iv)) for US only*

Published:
— *with international search report*
— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

SYSTEM AND METHOD FOR ENFORCING A SECURITY POLICY ON MOBILE DEVICES USING DYNAMICALLY GENERATED SECURITY PROFILES

TECHNICAL FIELD

The present invention relates in general to the field of data security and more particularly to providing data security to mobile devices.

BACKGROUND

Recent advances in hardware and communication technologies have brought about the proliferation of powerful mobile devices ranging from notebook computers to much smaller personal digital assistants (PDAs) that operate over wired and wireless networks. The productivity enhancements associated with exponential growth of mobile technologies have fundamentally changed the security landscape -- no longer are devices and data landlocked, the free flow and distribution of information to any place, at any time, to any device, creates a unique set of challenges which will continue to evolve. These mobile devices (also known as handheld devices) operate on various platforms, such as palm computing platform, Windows CE, etc. Other types of mobile devices include paging and messaging devices, laptop computers, data-capable smart phones, etc. These devices can provide users with network access connectivity, which allows them to be quickly notified of changing events, and provide them with the resources necessary to respond even when in transit. In this way, users can be given the power to access mission critical information in quick and reliable manner. For example, data generated by client applications running on a wide variety of mobile devices may be transported over networks having various access protocols and wired and wireless links. One such protocol is Transmission Control Protocol/Internet Protocol (TCP/IP), which is designed to connect computer systems that use different operating

Petitioner Ex 1002, p. 415
Zimperium v. Taasera, IPR2024-00007

systems and network technologies. Many popular network applications have been built directly on top of TCP over the past decade, making TCP/IP a de-facto network access protocol standard.

Many personal computer users use Personal Information Management (PIM) applications such as an address book, a daily organizer, and a To-Do list application on their personal computers and mobile devices. The data for these PIMS are stored in corresponding databases at the personal computers and mobile devices. Often, data in these databases must be synchronized in order to maintain data uniformity. The synchronization of data between devices of this type is known. For example, U.S. Patent Number 6,006,274 describes a "Method and Apparatus Using a Pass Through Personal Computer Connected to Both a Local Communication Link and a Computer Network for Identifying and Synchronizing a Preferred Computer with a Portable Computer." Also, U.S. Patent Numbers 6,000,000 and 5,884,323 both describe an "Extendible Method and Apparatus for Synchronizing Multiple Files on Two Different Computer Systems." Generally, the synchronization process is activated either by detecting a mobile device on a cradle or by the manual press of a button. The synchronization process proceeds to synchronize data for several different applications that run on the mobile devices with data for corresponding application on other computers.

As society continues to adopt handheld devices as a standard computing platform and applications become more powerful with the standardization of wired and wireless computing, security threats to data stored in and access by these types of mobile devices have become a serious concern and have created a heightened awareness and increased need for security. In fact, the U.S. Air Force Research Laboratory (AFRL), which develops some of the government's most advanced technologies, is crafting a policy to deal with security risks for data stored in mobile devices.

Petitioner Ex 1002, p. 416
Zimperium v. Taasera, IPR2024-00007

Various types of security software incorporating different data security encryption standards have been used in the past for securing network, desktop, laptop, and PDA environments. On such suit of software is called the Trusted Mobility Suite™ offered by Trust Digital™, which is used to set access control, encryption, and other parameters and push them to such mobile devices as Palm Pilot™, Pocket PC™ , Blackberry™ or Symbian™ OS devices to protect against fraud, theft, sabotage, malicious hacking, and other adverse exposure caused by data compromise. Mobile DesktopSecure™ is a security and encryption software designed to protect files, data, applications, databases, directories, or an entire hard drive. It is also used to push security profiles containing defined security policies from a server to protect laptops and desktops within a network. Generally, Trusted Mobility Suite™ implements security using a graphical user interface (GUI) that allows administrators and users to secure all or selected applications. In this way, the users and administrators can selectively secure application(s) from unwanted and unauthorized access.

Trusted Mobility Suite™ manages data security for mobile devices at different levels. At a higher server level, Trusted Mobility Server™ deploys, manages, and secures networks containing mobile devices using a centralized management solution. A policy-profile editor is used to set security parameters for groups of users based on defined security policies. At a lower device level, PDASecure™ encrypts the data on the mobile device itself and offers security-management for those devices through the Trust Mobility Server. Once installed on a mobile device, PDASecure™ provides for universal integration with all available mobile devices on the network, without the requirement for moving data into separate, secured applications. Also, Trusted Mobility Software Development Kit™ allows software developers to incorporate Trust Digital's Mobility Framework, comprising security,

Petitioner Ex 1002, p. 417
Zimperium v. Taasera, IPR2024-00007

encryption, and centralized rule-based management technologies into their products, for mobile / PDA users.

Also, U.S. Patent No. 6,158,010 discloses a system and method for maintaining security in a distributed computing environment that comprises a policy manager located on a server for managing and distributing a security policy, and an application guard located on a client for managing access to securable components as specified by the security policy. A global policy specifies access privileges of the user to securable components. The policy manager may then preferably distribute a local client policy based on the global policy to the client. An application guard located on the client then manages access to the securable components as specified by the local policy.

Implementation of comprehensive security policies in networks that support a large number of mobile devices has become an important issue for many enterprises, particularly in view of the complexities associated with supporting various hardware and software platforms in terms of network architectures, protocols, device types, etc. Add to this complexity, the various situations under which data security may be breached, either on the network side or on the device side. Additionally, due to limited memory availability and fewer processing resources, creating security programs for mobile devices is much more complicated than with larger computers. There exists a need for an efficient and flexible system and method for securing data in mobile devices used under varying operating environments.

BRIEF DESCRIPTION OF DRAWINGS

FIG. 1 is a diagram of a system that implements security control and management of the present invention.

Petitioner Ex 1002, p. 418
Zimperium v. Taasera, IPR2024-00007

FIG. 2 is a block diagram of a computing node and devices that operate within the system shown in FIG. 1.

FIG. 3 is an exemplary security profile for setting security parameters for the computing node and device.

FIG. 4 is an exemplary diagram of an interface for setting security parameters for a computing node.

FIG. 5 is a diagram for interfacing with applications in a mobile device.

FIG. 6 is a diagram of an interface for setting security parameters in a mobile device.

FIG. 7 is a block diagram of an exemplary security system in accordance with the present invention.

FIG. 8 is a block diagram of network security management using the policy engine.

SUMMARY OF THE INVENTION

Briefly, according to one aspect of the invention, a system and method for enforcing security parameters collects information from a source relating to a mobile device. The source can be an internal source to the mobile device or external source to the mobile device. In one embodiment, the source is a back-up source. Based on the collected information, an identity status for the mobile device is determined that uniquely identifies the mobile device and distinguishes it from other mobile devices similar to the way DNA information identifies an organism. The identity status of the mobile device can be determined when the mobile device connects to a computing node source or when the mobile device accesses a resource within the network. Thus, the identity status can correspond to a connection attribute between the mobile device and computing node or an access attribute to the resource. A security profile based on the identity status of the mobile device is generated and the security

Petitioner Ex 1002, p. 419
Zimperium v. Taasera, IPR2024-00007

profile is applied to the mobile device. In another embodiment, the identity status of the mobile device is determined internal to the mobile device or external to the mobile device.

According to some of the more detailed features of this aspect of the invention, the collected information relates to static attributes of the device or dynamic attributes of the device. The static attributes of the mobile device could at least include physical device identification, device manufacturer, device model number, device serial number, input-output ports, and device capabilities. The dynamic attribute of the mobile device could at least include installed operating system, application, attached peripheral, usage pattern, historical activities, synchronization, location, network, communication link, domain, and security policies. The device security profile can include a parameter relating to protection of the mobile device, restriction on use of an internal resource and external resource, and configuration of a resource.

According to other more detailed features of this aspect of the invention, the mobile device is controlled according to a parameter in the device security profile that relates to an unauthorized resource in the mobile device. The mobile device can be controlled by deleting the unauthorized resource, hard or soft resetting the mobile device, locking the mobile device, preventing the unauthorized resource from running on the mobile device, deleting or removing one or more files that are associated with the unauthorized resource, and hiding the unauthorized resource. Moreover, the mobile device can be controlled according to a parameter that relates to an unauthorized external resource. The unauthorized external resource can be a computing node resource, an external application program, and an external database. Corresponding device security profiles for different identity statuses of the mobile device are administered by a security policy engine. The device security profile can be

Petitioner Ex 1002, p. 420
Zimperium v. Taasera, IPR2024-00007

transferred, by wire or wirelessly, to the mobile device after access to the computing node is granted.

According to another aspect of the invention, a password protected mobile device associated with a security station is unlocked by authenticating the user of the mobile device and by authenticating the mobile device according to a device authentication code that is generated based on a device attribute that corresponds to a device identity status that uniquely identifies the mobile device. Upon authentication, an unlock code is generated that unlocks the password protected mobile device. The user can be authenticated by a user authentication response, a biometric parameter, or a security identification parameter. The user authentication response and the device authentication code can be communicated by the user or the mobile device. The unlock code can be communicated by the security station or an administrator.

According to yet another aspect of the invention, a mobile device is protected by transmitting a request from the mobile device in response to a security threat, such as a virus attack. In response to the request, a device security profile is created based on the security threat and is transmitted to the mobile device. The request includes information related to at least one or more of attributes of the mobile device, such as communication link used by the mobile device, serial number of the mobile device, location, software and hardware on the mobile device. The attributes of the mobile device can also relate to active directory information of the mobile device, including firewall settings of the mobile device, current security settings of the mobile device, and a security parameter of the mobile device.

According to still another aspect of the invention, a mobile device that connects to a computing node is protected by transmitting a login information that is the same for the computing node and the mobile device. When new computing node login information, such

Petitioner Ex 1002, p. 421
Zimperium v. Taasera, IPR2024-00007

as new password, is set for the computing node, the new computing node login information is transmitted to the mobile device. According to one feature of this aspect of the present invention, the new computing node login is transmitted via a device security profile. The new computing node login information from the device security profile is retrieved at the mobile device and the new computing node login information is set as the new login information for the mobile device in order to eliminate the need for using multiple login information. The new computing node login information can be new network login information that is transmitted to the mobile device from a security station to set the new login information of the mobile device.

According to one more aspect of the invention, a network is protected by detecting access to one or more resources by a mobile device. Once detected, the mobile device is authenticated for access to the resources, and a device security profile is transmitted to the mobile device with rules for accessing the one or more resources. The one or more resources can be a communication resource, a data storage resource, a peripheral resource, or a wireless link resource.

According to yet one more aspect of the invention, a computing node that connects to different mobile devices is secured by applying security rules to the different mobile devices in accordance with corresponding device parameters contained in a security signature file. When a change is detected in device parameters of the mobile device, the security policies that are applied to the mobile device are modified in accordance with one or more device parameters of an updated security signature file at the computing node. The device parameters include serial number, security settings, manufacturer, and a model number.

DETAILED DESCRIPTION OF THE INVENTION

Petitioner Ex 1002, p. 422
Zimperium v. Taasera, IPR2024-00007

The present invention relates to a security and compliance framework that links all relevant security technologies to intelligently create and enforce security and data protection policies across the dynamic set of mobile devices and end points in a timeless, network and device independent manner, with low maintenance requirement.

The invention uses a data description method, a query language for understanding the data description and for applying rules to it, and an extensible enforcement structure for real-time policy enforcement that enables real-time analysis and enforcement of security and data protection policies based on an infinite number of environmental, physical, chronological and system parameters. This automates the application of sound security practices in a transparent way to eliminate accidental disclosures, internal threats, and ensure regulatory compliance with minimal impact to IT. Once implemented, the system manages the necessary changes based on existing practices and provides alerts based on pre-determined event thresholds.

Referring to FIG. 1, an exemplary system 100 that advantageously implements the present invention is shown. The system of the invention supports security amongst computing nodes 102 and mobile devices 104, which are also referred to as user-devices. The computing nodes 102 can be any type of wired or wireless network node, a client station connected, a server station, a router, a hub, or an access point. The computing node 102 can also be a stand-alone computer. The computing node 102 possesses the processing power to execute programs and applications in accordance with the present invention. A security server 106 provides central functionality for implementing security parameters in accordance with the present invention. The computing node 102 can be connected to the computing node directly or via a network 122.

Petitioner Ex 1002, p. 423
Zimperium v. Taasera, IPR2024-00007

The mobile devices 104 can be of any type. For example, the present invention can support any handheld device, personal digital assistant, phone, smart phone, pager, etc., where various types of mobile devices operating within the system 100 can be discovered, located or detected for managing security.

Various types of data, files, and profiles can be transferred between the computing nodes 102 and mobile devices 104 over any supported transport, network, or link layer and physical connection. The transport protocol can be any suitable protocol, including TCP/IP, various telephony transport protocols, etc. The links can be wired or wireless links 110, 112. The wired links 110 can be twisted pair, coaxial cable, optical cable, etc. The wireless links 112 can support any protocols, such as IEEE 802.x, GSM, Bluetooth, etc.

In an exemplary embodiment, the system 100 is implemented over a network. The network includes server stations 114, client stations 116, and a host or central station 118 that are linked together by a set of standard or proprietary protocols either directly or via any collection of interconnected (public and/or private) networks, such as the Internet. The network can also support a website that serves informational content using the standard protocols of the World Wide Web. Typically, a website corresponds to a particular Internet domain name and includes the content associated with a particular organization. The system 100 also includes a guest network, for example, a separate Local Area network (LAN), used by guest mobile devices that do not belong to the network. This allows guests or visitors to access the guest wireless network without compromising the security of the entire network.

As shown in FIG. 1, the security server 106 can access a security database 120, which stores various data, including security profiles for the computing nodes 102 and mobile devices 104. The database 120 can also store collected and discovered information from computing nodes 102 and mobile devices 104, including historical information about the

Petitioner Ex 1002, p. 424
Zimperium v. Taasera, IPR2024-00007

mobile devices, synchronization history, event log and audit log information, etc. The security station 106 communicates with the devices through a network layer interface 122. It should be noted that the present invention does not have to be implemented over a network. In fact, the present invention can use a computing node alone or as a part of a network. When the computing node is not connected to any network, the mobile device access between the computing node 102 and the mobile device 104 is an off-line access.

Managing Security between Computing Node and Mobile Devices

Referring to FIG. 2, a block diagram for managing security between the computing node 102, mobile devices 104 and the resource device 124 is shown. The computing node 102 acts as a gateway between the mobile devices 104 and other network resources 124. A node security program or agent 202 is executed in the computing node 102 for interfacing with a corresponding device security program or agent 204 that is executed at the mobile device 104 or resource device 124. The device security program 204 interprets a device security profile 206 to implement mobile device security. The node security program 202 interprets a node security profile 208 to determine one or more security parameters for managing the security between the computing node 102, resource device 124, and mobile devices 104, including controlling transfer of data, files, device profiles, applications, and programs between the computing node 102, resource device 124, and the mobile devices 104. For example, the security parameters derived from interpreting the node security profile 208 may require preventing data synchronization between the mobile device 104 and resource device 124. The node security program 202 can also prevent remote execution, utilization of any application, or file on the mobile device 104 or resources 124. The computing node security program 202 can also enable or disable synchronizing of particular kind of data. For

Petitioner Ex 1002, p. 425
Zimperium v. Taasera, IPR2024-00007

example, the security parameters can specify that address book data of the mobile device 104 cannot be synchronized with the computing node 102.

The information contained in the node security profile 208 can include information that alone or in combination identifies an authorized or unauthorized computing node, an authorized or unauthorized user, an authorized or unauthorized mobile device, an authorized or unauthorized central station, or an authorized or unauthorized network or resource, such as storage devices or a camera. The identity of the mobile device and computing node may be specified by physical address, serial number, model number, device type, server, network resource ID, software license number (registration number), user ID, etc. The authorized or unauthorized computing node can be specified relative to mobile device parameters, such as device type, etc. For example, certain computing nodes 102 may be authorized to synchronize data with certain specified mobile device types, but not authorized to synchronize data with other device types, and vice versa.

As stated above, the computing node 102 can be any type of wired or wireless node, including a client station connected to the security server 106 directly or via a wired or wireless network. Also, the computing node 102 can itself be a mobile device 102 that is responsible for managing security for other mobile devices 104. The node security profile 208 can set user access rights by enabling/disabling or password protecting users' ability to configure the computing node 104 and/or its profile. Depending upon the security parameters set in the node security profile 208, corresponding changes are made to the registry key, file, or database entries of the computing node 102 or its configuration file to enforce the node security profile parameters. Registry key, file, or database entries along with functionality associated with the computing node 102 are used to control and monitor all data synchronization, transfer, access, modification, or execution of files, applications, programs,

Petitioner Ex 1002, p. 426
Zimperium v. Taasera, IPR2024-00007

security profiles and processes that occur through the computing node by any data transport that relates to applications that interface with the devices 104 and 124. The computing node security program 202 can also periodically check, for example, for security profile updates.

A computing node monitoring module in the security station 106 tracks all computing nodes within its network by gathering data on the list of mobile devices that connect to the computing nodes for synchronization and gathers mobile device information on various synchronization and data transfer parameters, e.g., the nature and size of data that was synced, etc. The computing node collects the data along with device specific information from the mobile device for transfer to the security server 106. The server 106 monitors the computing node to determine whether the security of the computing node, and in effect the security of the network, has been compromised. The server 106 may also track data traffic load on the computing nodes to give the administrator information about abnormal traffic patterns that may correspond to unauthorized data transfers. Traffic load analysis may help in effective load balancing.

The device security profile 206 sets the security parameters for the devices 104 and 124, as interpreted by the device security programs 204. The device security parameters include encryption preferences, global (device) password, local (application or resource) password, access control to applications and resources, access control to the device, integrity protection against hackers and traps, file encryption options, port protection, communication protection (i.e., send and receive), ability to use wireless connections like Wi-Fi, 802.11, Bluetooth, controlling the content of the device, like restricting installation of some applications, etc.

Multiple device profiles can be loaded, stored, and transferred to the mobile device from the computing node or the security server. The mobile device itself can be a repository

Petitioner Ex 1002, p. 427
Zimperium v. Taasera, IPR2024-00007

of multiple security profiles. For example, multiple security profiles may be used for handling multiple users that share the mobile device. Each user sharing the mobile device may have a different security and user profile. Only one device profile can be active at a time. As described later in detail, the appropriate profile can become active dynamically based on time, day, date, location, or other attributes that define the "identity status" of the mobile device at the time a connection is made to the computing node. For example, as soon as the mobile device is moved to a secure location, the mobile device activates a device profile that provides security parameters and rules for the secure location.

Creating Security Profiles

The device and node security profiles 206, 208 can be created at the central station 118, the server station 106, or at a computing node 102, using any suitable tool, such those that create .ini, binary, or XML files.

FIG. 3 shows an exemplary security profile. FIG. 4 illustrates an exemplary interface for setting security parameters for a computing node in accordance with the invention. For example, the server access tab, as illustrated, shows security parameters for communicating with a server. Other shown tabs can be used to set device discovery, security policy transfer and event log parameters. FIG. 5 illustrates an interface on a mobile device for activating various applications. FIG. 6 illustrates an interface for a device security profile that applies security parameters to an "Address" and "Expense" application.

Often, not all information in a security profile needs to be updated. Thus, security profiles can be partitioned into basic security rules and extended security rules. The basic security rules may include password settings, device access settings, etc., whereas extended security rules may include application access settings, data transfer restrictions,

Petitioner Ex 1002, p. 428
Zimperium v. Taasera, IPR2024-00007

communication settings etc. The partitioning of the security profile simplifies creation and transfer of security profiles to mobile devices and computing nodes.

The security of system 100 can be managed based on a central security policy, for example, one promulgated by a network administrator. One or more security profiles can be created defining the governing security rules and parameters according to the central policy. The computing node security profile 208 and the device security profile 206 can be updated periodically by checking one or more designated web/ftp sites or by accessing a central station or server station. In a similar manner, the device security profile 206 can be updated by accessing the computing node 102. The device security program 204 can also automatically request device security profile 206 in real time.

A created policy can be deployed via a wireless transport, for example, Bluetooth. Wireless transmission of security profiles allows the security profile to be updated without requiring the mobile device to physically synchronize with the computing node. This provides the administrator flexibility and control to enforce security restrictions on the user in real time. By encapsulating the security profile in a Multimedia Messaging Service (MMS) message or other similar services, new security profiles may be sent and applied to the mobile device.

Static and Dynamic Security Policy Implementation

Conventionally, a security policy is applied statically. A static security policy implementation applies the same security rules every time the mobile devices connect to the computing nodes.

One aspect of the present invention applies or otherwise enforces the security policy dynamically. More specifically, different security rules and parameters are applied depending on a determined "identity status," which is unique to each mobile device. For

Petitioner Ex 1002, p. 429
Zimperium v. Taasera, IPR2024-00007

example, the identity status of the mobile device can be derived based on collected information that relates to the device itself, its status, configuration, and capabilities, as well as its historical activity, as further described below. As describe later in detail, the unique identity status of the mobile device can be connection specific and determined at the time of connection. The unique identity status of the mobile device is used for preventing intrusion, controlling admission, and access to the network, as well as for enforcing a suitable, consistent, and platform independent security policy across the system. For example, based on the unique identity status of the mobile device access to the computing node or to the network via a wireless network can be prevented.

The identity status of the mobile device can correspond to its essential or generic character in different instances, for example, when it connects to a computing node. Such identity status distinguishes the character or personality of the mobile device from others. As such, the identity status of the mobile device, as determined based on collected information, uniquely characterizes the mobile device based on the attributes of the mobile device. The identity status also corresponds to variant identities, roles, phases or versions of the mobile device as a continuing basic entity, similar to an avatar identity status. This unique identity status of the mobile device is akin to DNA information of an organism that distinguishes it from other organisms, even those of the same type. Similar to the DNA information, the collected information characterizes or identifies different mobile devices. For example, two mobile devices of the same type, e.g., two blackberries, may have their own unique identity status or so called DNA information based on other attributes, e.g., features and capabilities, location, etc. Based on device identity status or DNA information, all cloned devices (mobile devices of the same type) can be detected to apply security profiles that ensure integrity according to a promulgated security policy. Such unique information of the device is also

Petitioner Ex 1002, p. 430
Zimperium v. Taasera, IPR2024-00007

helpful in detecting any device activity and device usage. Also, the collected information can be processed to analyze security vulnerabilities, correlate events, and predict risk. The information regarding the identity status of the mobile device can also be structured for use by other systems. The unique identity status of the mobile device can be represented by various types of indicia, e.g., numbers, characters, names, symbols, etc.

Referring to FIG. 7, a block diagram of a mobile edge security architecture 700 in accordance with the present invention is shown. The security policy in the architecture is centrally managed by a system administrator 702, which enforces a unified and cohesive security policy on the mobile devices. The security administrator 702 selects security policy for the network based on standards or varying pre-determined event security thresholds. Selections by the security administrator 702 are indicated by an administrator input 703 and transmitted to a security policy engine 704. The security policy engine 704 generates alarms and reports based on information from the network, the mobile devices 104, and the security thresholds to inform the administrator 702 or the security server of the security of the network and any threats being experienced by the network. Also, the security policy engine 704, which runs on either the computing node 102 or security server 106, generates a device security profile according to the security policy and promulgates the device security profile to the mobile device 104. The security policy engine 704 dynamically analyzes the identity status of the mobile device 104 when generating the device security profile. The security policy engine 704 generates corresponding device security profiles based on the unique identity status of each mobile device 104, for example, at a given connection or access to a resource, etc.

The unique identity status of each mobile device 104 is determined based on device specific information collected from various sources in the computing node 102, network 122,

Petitioner Ex 1002, p. 431
Zimperium v. Taasera, IPR2024-00007

IT infrastructure 706, and the mobile device 104. A data collector 708 collects device specific information from sources that are external to the mobile device 104. Data collector 710 collects device specific information from sources that are internal to the mobile device 104. Node Security Program 712 interacts with policy engine 704, mobile device 104, and data collectors 708, 710 for policy enforcement and for data collection. Node security program 712 also interacts with mobile device 104 for intrusion protection, data protection, and end point security.

Data collection at data collectors 708, 710 is initiated independent of the underlying platform that connects the mobile device 104 to the computing node 102. The data collection may be initiated by the computing node 102, the security server 106, or the mobile device 104. The collected information can be classified based on various attributes. Such attributes can be static attributes of the device, which are fixed and not changeable. One example of a static device attribute is Physical Device ID. Conversely, dynamic device attributes are non-fixed, i.e., they are changeable. Examples of dynamic device attributes include installed operating system and applications, which can be changed, if required. Another class of attributes relates to the capabilities of the device and defines its personality, for example, in terms of supported storage devices, peripherals, ports, and I/O capabilities. Information relating storage media, capabilities, and port attributes of the computing node device, e.g., CD-R, Floppy Drive, SD Card, USB, IR, etc, can be collected and analyzed using well known techniques. The analysis also applies to the capabilities and features of the mobile device's operating system, platform, applications, storage, ports, and peripherals, e.g., Bluetooth, IR, USB, phone, camera, etc.

Yet another class of attributes relates to behavior of the mobile device, for example, in terms of its usage patterns. Usage patterns of the device can include specific analysis of

Petitioner Ex 1002, p. 432
Zimperium v. Taasera, IPR2024-00007

usage logs captured on the device, a review of recent device application usage as well as detection of a device reset log from when the device is reset causing erasure or changes to system level software. Reset logs occur when a user either purposefully or accidentally, e.g., when a battery runs out, resets the mobile device.

Information regarding historical mobile device activities and behavior can be collected and analyzed by accessing various internal and external sources, including back-up databases and storage areas. One example of collected information relates to synchronization history of the mobile device, which reflects when data between one or more applications running the mobile device and a computing node is synchronized. This information can be collected from synchronization logs that are maintained within the mobile device or computing node.

The device attributes can also be classified based on location of the device in order to enforce different security profiles in various physical locations. Different positioning technologies, such as, for example, GPS, may be used to determine the location of the mobile device and to enforce the corresponding security profile for that location. In a wireless network, the location of the mobile device may be determined based on the location of the computing node or access point to which the mobile is connected. A number of wireless computing nodes may exist at any location or proximity, e.g., in office, home, city, etc., forming a number of wireless networks, such a server wireless network, a work group wireless network, or a guest wireless network, etc. Accordingly, at one location, a device security program that applies the rules of the device security profile for that location could restrict access only to an authorized wireless network, but not to any other. Similarly, at a different location, another device security profile could restrict all foreign mobile devices to the guest wireless network.

Petitioner Ex 1002, p. 433
Zimperium v. Taasera, IPR2024-00007

In one embodiment, the location of the mobile device may be obtained from the security server 106 based on which computing node the mobile device is attached. A positioning system may be used to determine the location of the mobile device, the location of the computing node (or access point), or both. Based on the location of the mobile device, the server determines security restrictions for the network and may send a security profile to the mobile device corresponding to that network.

Other collected and classified information includes information on the network in which the mobile device operates, security level, and historical information of the mobile device. Accordingly, this aspect of the invention collects and classifies information that uniquely characterizes a mobile device in terms of a device identity status, which is specific to the mobile device. According to one feature of the present invention, the unique device identity status is used for implementing a platform-independent and dynamic security policy, which is centrally and cohesively applied across the entire system.

The collected information is compiled, categorized, correlated, and updated each time the mobile device connects to the network. By processing and correlating the collected information, the unique identity status of the mobile device is determined. In one exemplary embodiment, the unique identity status of the mobile device is determined when the mobile device connects to the computing node, whereby the identity status is unique to the connection between the mobile device and computing node at the time of connection. The unique identity status can also be determined in any other instances, when the mobile device tries to access a network resource or a communication link. The unique identity status of the mobile device is used for controlling admission and access to the network. If it is determined that the unique identity status of the mobile device allows access to the network, the mobile device is authenticated, for example, by the user entering a correct password.

Petitioner Ex 1002, p. 434
Zimperium v. Taasera, IPR2024-00007

Once the mobile device is allowed access to the computing node and is authenticated, the policy engine 702 automatically creates and distributes a security profile to the mobile device 104 that corresponds to the unique identity status of the mobile device 104 for the connection. The device security profile is based on the authenticated user and the identity status of the mobile device 104.

Referring to FIG. 8, a block diagram illustrates management of network security. The policy engine 704 receives inputs including mobile identity status, and enterprise security 802. The enterprise security 802 includes information from the administrator 702, and other information from the IT infrastructure 706. The policy engine dynamically analyzes the device identity status and the enterprise security to generate real-time policies for mobile device security. The policy engine also uses the information on enterprise security and mobile identity status for reporting and events. Reporting and events include alarms and reports based on defined security thresholds indicating the security of the network.

The device security profile created based on the unique identity status can protect the mobile device in accordance with defined security rules or parameters. The protection can be applied by encrypting data, file, folder, volume, or hard disk. Additionally, the security profile may protect the installed applications in the mobile device by performing an integrity and validity check.

The device security profile created based on the unique identity status of the mobile device can also restrict the capabilities and operation of the mobile device 104. Such device restrictions include limiting access to peripherals, drive, ports, and other capabilities based on the identity status of the mobile device. The applied restrictions could remove access to various resources or password-protect data, applications, or communication links. The restriction can also be applied to protect output data by determining whether or not to encrypt

Petitioner Ex 1002, p. 435
Zimperium v. Taasera, IPR2024-00007

the output data. The applied restriction can also define acceptable/unacceptable devices with which the mobile device can interface.

The device security profile created based on the unique identity status can also configure various features or software in the mobile device, including a firewall, anti-virus software, a virtual private network (VPN), or by downloading and executing other software patches.

The computing node or the mobile device may store a repository of multiple security profiles corresponding to various identity statuses of the mobile device. The multiple security profiles can be stored in the mobile device to enforce different security policies based on time, location, user, role, etc. In one embodiment, the identity status of the mobile device is determined internally by the mobile device itself. For example, the mobile device can determine different identity statuses for itself based on internal resources, such as a clock or GPS receiver, which provide information regarding time and position, respectively. Based on its identity status, the mobile device can apply a corresponding security profile from its own profile repository. For example, if a user is not to access specific applications after a particular time, a restrictive security profile may replace a previous one and deny access to the applications after that time. Alternatively, the mobile device can request a security profile that corresponds to its internally determined identity status from external resources, e.g., the computing node.

Alternatively, the identity status of the mobile device can be determined externally, for example by a computing node or security station. The device security profile corresponding to the identity status can be generated externally and transferred to the mobile device by wire or wireless link. Such externally determined identity status can also be communicated to the mobile device over a link. If the device security profile associated with

Petitioner Ex 1002, p. 436
Zimperium v. Taasera, IPR2024-00007

the communicated identity status is already stored in the mobile device's profile repository, the device security program can retrieve and apply the security profile. Otherwise, the mobile device can send a request to the computing node to receive the device security profile that is associated with the identity status. Once received, the mobile device stores the device security profile for later use.

Control Communication Sessions

With the multitude of available transport technologies, transfer of data to/from a device is relatively easy. An unauthorized mobile device may gain access to the network via wireless access points to steal data or send virus files that corrupt the network. One aspect of the present invention controls access via communication links or use of other resources to prevent unauthorized activity unless authenticated. If, for example, a virus is detected that originates from a particular communications link, this embodiment requires the mobile devices to authenticate themselves before using the communication link to access the network.

Thus, another aspect of the present invention controls access, interface, and use of various wired or wireless communication links, such as the serial connection, Wi-Fi, 802.11, Bluetooth, etc, or other resources. A series of network "sniffers" can be used to scan and detect the use of the communication resources of the system, for example, by detecting the packets that are being communicated from one or more mobile devices over any one of various communication links. Once a mobile device using a particular communication link resource is detected, the mobile device using the link is authenticated before permitting access to the wireless network, for example by a password. By using password authentication, mobile devices misusing the system resources can be identified and held responsible. Additionally, the computing node or security server may also log the usage

Petitioner Ex 1002, p. 437
Zimperium v. Taasera, IPR2024-00007

details of the resources by the authenticated mobile device, including the time and duration of usage.

After password authentication, the security server generates a device security profile for the authenticated mobile device that controls access to the resources. Varying levels of access can be provided to the authenticated mobile device, as defined by the generated device security profile. The device security profile transmitted to the mobile device defines access and resource usage rules, for example, whether the mobile device may synchronize with computing nodes within the network, what kind of data/files the mobile device may be allowed to synchronize with, or the maximum file size allowed for synchronization, etc. This feature allows the administrator to password protect the resources and limit the access only to the authenticated mobile devices. Besides communication resources, other resources can also be password protected, including access to information stored on a network server, or other storage devices and peripherals, including, for example, a data storage device.

Remotely Unlocking a Password Protected Mobile Device

Conventionally, when a user forgets a password for a mobile device, the mobile device cannot be unlocked or accessed without losing the data on the mobile device. According to another aspect of the invention, a password protected mobile device is unlocked without loss of data by authenticating the user and the mobile device. In one embodiment, the user is authenticated by biometric means, e.g., fingerprint or via a secure ID. In another embodiment, the user provides response to one or more queries that authenticate the user. The mobile device is authenticated by an authentication code that is generated based on a physical attribute of the device and a code associated with the security station. Once the user authentication response and the device authentication code are verified, an unlock code is generated that is used to unlock the password protected mobile device to allow access to the

Petitioner Ex 1002, p. 438
Zimperium v. Taasera, IPR2024-00007

device. Verification of the user authentication response and the device authentication code requires communicating them either to the user, e.g., verbally or textually, or by the mobile device automatically. The communicated user authentication response and the device authentication code can be directed to the security station or a network administrator, as the case may be. Similarly, the generated unlock code can be communicated by the administrator to the user or by the security station to the mobile device. The unlock code can be communicated to the mobile device automatically or verbally.

The user authentication queries and answers are created based on information that is known to the user and not to the general public. For each user, the authentication queries and answers are stored in the security database 120 for access by the security server 106 or the administrator. In one exemplary embodiment, each user is allowed to create their own authentication queries and answers in terms of one or more questions and corresponding answer sets using an appropriate interface. Questions in the user defined question set may include mother's maiden name, social security number, state identification card information, favorite pet's name/sports team, or any other personal information or non-personal information that authenticates the user. The authentication queries and answer set may also be stored locally at the mobile device, or may be received from the computing node or the security server.

The user responses are communicated via a wired/wireless links for verification by the security server 106. Alternatively, the user may call the administrator using the telephone network to respond to the query. The responses may also be communicated via an interface, e.g., a website, and be transmitted to the security server 106 to authenticate the user.

The device authentication code is generated based on a series of device attributes, such as the serial number of the mobile device. In another embodiment, the device

Petitioner Ex 1002, p. 439
Zimperium v. Taasera, IPR2024-00007

authentication code can be generated based on calculations that also take into account other parameters, such as the current time. This authentication code is generated by first receiving a device specific code either manually read to the administrator or provided via wired or wireless communications. Upon receipt of this code, the server applies a set of known algorithms to produce a second number, which for a specified time period if entered into the mobile device will unlock the device. This second number can be read manually to the user for entry, or it could be sent via wired or wireless networks. In one embodiment, the device authentication code is encrypted based on the security station 106 identification code. The device authentication code is then transferred in real-time or non-real-time to the security station 106. Alternatively, the device authentication code can be displayed to the user, and the user can communicate the code to the server or administrator via telephone. After receiving the device authentication code, the security server or administrator may then verify the encrypted code to authenticate the mobile device.

After successful authentication of both the user and the mobile device, the security server 106 or administrator generates the unlock code. The unlock code can be a user password for the mobile device, a default password code for unlocking the mobile device, or a default reset code allowing the user to reset the password of the mobile device. As an additional feature, the unlock code may be time sensitive and expire if not entered into the mobile device within a specified amount of time.

Upon receipt, the unlock code may automatically unlock the mobile device without further user input. Alternatively, the administrator may convey the unlock code to the user over the telephone for manual input at the mobile device, or textually via the Internet. Upon entry of the unlock code, a security program on the mobile device unlocks the mobile device to allow the user access to the mobile device.

Petitioner Ex 1002, p. 440
Zimperium v. Taasera, IPR2024-00007

Control Application Usage and Install

According to a further aspect of the present invention, the device security program controls the mobile device according to a device security profile that governs the use and installation of unauthorized resources, including installed applications. Application programs may be computer programs for individual use by the mobile device, such as, for example, an audio program, or they may be computer programs that access external resources, such as, an information server or other computing nodes.

More specifically, when a mobile device attempts to connect to a computing node, the mobile device is authenticated. After authentication, the mobile device receives a device security profile from the server or computing node and activates a device security program. Upon activation, the device security program may identify and list all of the applications, files, and resources that are available on the mobile device, and control the mobile device according to the parameters of the security profile.

After identifying the installed application programs, the unauthorized installed application programs are detected, as determined from the device security profile. Once detected, the security program can delete the unauthorized installed application program, hard or soft reset the mobile device, lock the mobile device, prevent the unauthorized installed application from running, delete one or more files associated with the unauthorized installed application program, or hide the unauthorized installed application program. For example, if the user is connected to a wireless network at a library, the device security program may allow a user to connect to the Internet, but may prevent the user from activating an audio program.

Similarly, after connecting to the computing node, the user may attempt to access application programs from local or remote information resources or install various

Petitioner Ex 1002, p. 441
Zimperium v. Taasera, IPR2024-00007

application programs received via e-mail on the mobile device. The device security program uses the device security profile to determine if installation or access to any of these application programs is allowed. If not, the device security program may prevent or stop the installation of the application program.

An administrator may select allowed or restricted access to the application programs or resources for a particular network by setting a security policy with rules for installation or usage by each mobile device within the network. The administrator, or alternatively a security server, can control the installation of application programs and its usage for all mobile devices that operate within the system. For example, based on the security policy, a security profile for each mobile device connecting to computing nodes of a corporate network can be created. The security profile sets the security rules for the mobile device based a mobile device attribute and/or the user.

The device security program controls application usage and installation according to the security rules of the device security profile, either statically or dynamically, as described above. Under this arrangement, the computing node security program of the computing node can control usage and installation of mobile device applications while the mobile device is connected to the computing node.

The device security profile can also define rules associated with interfacing with unauthorized internal or external resources. The unauthorized external resource can be a computing node resource, an external application program, an external database, and an e-mail server, among others containing proprietary information. The unauthorized internal resources can be an internal camera. According to this embodiment, the device security profile can prevent access to the unauthorized internal or external resources, prevent

Petitioner Ex 1002, p. 442
Zimperium v. Taasera, IPR2024-00007

installation of the unauthorized internal or external resources, and prevent interface or communication with the unauthorized internal or external resources.

The device security program prevents the mobile device from accessing or using unauthorized internal or external resources according to the rules of the device security profile. As an example, the device security profile may prevent the user from using the internal camera in an art gallery. In another example, the device security profile may give the user the right to access promotional data of a company's product from a wireless corporate network, but restrict the mobile device from accessing engineering designs of the product or from accessing devices that may be used to test the product. Additionally, the security profile may protect the corporate network by preventing the mobile device from sending a restricted application program within the network.

Request Based Security Profile Creation

According to still another aspect, a mobile device can request a device security profile for protecting the mobile device from an imminent security threat, such as a virus attack. After receiving the request from the mobile device, the security server may respond by transmitting a suitable device security profile that prevents or lessens the effect of the virus threat. As such, the mobile device may dynamically adjust to various types of network security threats.

If a probability of an attack is seen, then the device security program on the mobile device may request a security profile that provides appropriate protection. The request may include information related to attributes of the mobile device, for example, information on a communication link used by the mobile device, a serial number of the mobile device, or any other information identifying software or hardware on the mobile device. The mobile device attribute information can also include active directory information, for example, firewall

Petitioner Ex 1002, p. 443
Zimperium v. Taasera, IPR2024-00007

settings of the mobile device, current security settings of the mobile device, security parameters, or other security settings of the mobile device.

The request for the security profile may be sent from the mobile device using TCP/IP or any communication connection over any available transport media. A security profile generation module is activated upon receipt of the security profile request from the mobile device to create an appropriate device security profile. The resultant security profile may be transmitted to the mobile device using the same transport media on which the request is received or any alternative transport media.

Unified Login for Mobile Devices

According to another aspect of the invention, the login information is unified between the mobile device and computing node to prevent the need for using multiple login information. This feature eliminates the need to remember multiple passwords for both the mobile device and the computing node. When a user selects new computing node login information, the computing node transmits the new computing node login information to the mobile device. According to one feature of this aspect of the present invention, the new computing node login is transmitted via a device security profile. The mobile device retrieves the new computing node login information from the device security profile and sets it as its new login information. The new computing node login information can be a new password for the computing node. Alternatively, the new login information can be a network login. If so, the new login information is transmitted to the security server. When received, the security server changes the old network login to the new one and transmits the new login information to the mobile device in a device security profile that applies the change to the mobile device.

Petitioner Ex 1002, p. 444
Zimperium v. Taasera, IPR2024-00007

The present embodiment also allows the user to change the password information on their computing node, e.g., a personal computer, and to update the mobile device with the changed password through an updated security profile. When the user changes the password at the computing node, the change is transmitted across the network to update the login information database. After updating the password of the computing node in the database, the server receives notification of the updated network login information and automatically sends an updated device security profile to the mobile device. Alternatively, the server may transmit an updated device security profile to the mobile device at the next time the mobile device connects to the network. The updated security profile may contain the network login information so that the computing node and the mobile device use the same password for network access, thereby preventing the need for the user having to use multiple passwords.

The user may use network login information to log on to the network using a mobile device connected to or disconnected from a computing node. Conventionally, a mobile device cannot directly access the corporate network login information without being connected to a computing node. The mobile device of the present invention may be disconnected from the computing node, but may still access the network using the unified login information, which is used to access the mobile device.

Security Signature files

Mobile devices that connect to computing nodes can have different operations and functionalities. As newer mobile devices enter the market the range of operations and functionalities expands making them hard to track. Such expanded range of functionalities often impact security program or profiles, such that security programs and profiles developed for the previous versions become obsolete. To support the newer versions of the mobile devices, different security programs and different types of security profile may be necessary.

Petitioner Ex 1002, p. 445
Zimperium v. Taasera, IPR2024-00007

The device can be identified based on it behavior and capabilities and make use it will have a unique signature that can be used for tracking within our system.

In order to eliminate the need for replacing the older version security programs and profiles, the present invention uses security signature files to accommodate newer versions of mobile devices that enter the market. The security signature file may, for example, identify a mobile device model, a mobile device manufacturer, and other information specific to the mobile device model and manufacturer.

The security signature file that contains various device parameters of the different devices and the modifications that need to be made to correctly set the rules, when a device parameter is changes added or deleted. Device parameters may include, for example, a serial number, security settings, manufacturer, model, or any other information that may identify the device. The computing node security program may periodically check the server program for updated signature files, or the server may automatically send updated files to the computing node.

Therefore, a system and method for securing a computing node that connects to different mobile devices applies security rules to the different mobile devices in accordance with corresponding device parameters contained in a security signature file. The device parameters include serial number, security settings, manufacturer, model number, etc. When a change in device parameters is detected, the security rules applied to the mobile device are modified in accordance with one or more device parameter of an updated security signature file at the computing node.

The embodiments and examples discussed herein are non-limiting examples.

The invention is described in detail with respect to exemplary embodiments, and it will now be apparent from the foregoing to those skilled in the art that changes and

Petitioner Ex 1002, p. 446
Zimperium v. Taasera, IPR2024-00007

modifications may be made without departing from the invention in its broader aspects, and the invention, therefore, as defined in the claims is intended to cover all such changes and modifications as fall within the true spirit of the invention.

Petitioner Ex 1002, p. 447
Zimperium v. Taasera, IPR2024-00007

Claims:

1. A method for enforcing security parameters in a system that includes one or more mobile devices and one or more computing nodes, comprising:

collecting information from a source relating to a mobile device;

based on the collected information, determining an identity status for the mobile device that is unique to the mobile device and distinguishes it from other mobile devices;

generating a security profile based on the identity status of the mobile device; and

applying the security profile to the mobile device.

2. The method of claim 1, wherein the source is at least one of an internal source to the mobile device or external source to the mobile device.

3. The method of claim 2, wherein the source is a back-up source.

4. The method of claim 1, wherein the identity status of the mobile device is determined internal to the mobile device or external to the mobile device.

5. The method of claim 1, wherein the collected information relates to at least one of a static attribute of the device and a dynamic attribute of the device.

6. The method of claim 5, wherein the static attribute of the mobile device comprises an attribute relating to at least one of physical device identification, device

Petitioner Ex 1002, p. 448
Zimperium v. Taasera, IPR2024-00007

manufacturer, device model number, device serial number, input-output port, and a device capability.

7. The method of claim 5, wherein the dynamic attribute of the mobile device comprises an attribute that relates to at least one of installed operating system, application, attached peripheral, usage pattern, historical activity, synchronization, location, network, communication link, domain, security policy, and a connection attribute between the mobile device and computing node.

8. The method of claim 1, wherein the device security profile includes a parameter relating to at least one of protection of the mobile device, restriction on use of a resource, and configuration of a resource.

9. The method of claim 1, wherein the identity status of the mobile device is determined when the mobile device connects to a computing node source or when the mobile device accesses a resource.

10. The method of claim 1, further including controlling the mobile device according to a parameter in the device security profile that relates to an unauthorized resource in the mobile device.

11. The method of claim 10, wherein controlling the mobile device comprises at least one of deleting the unauthorized resource, hard or soft resetting the mobile device, locking the mobile device, preventing the unauthorized resource from running on the mobile

Petitioner Ex 1002, p. 449
Zimperium v. Taasera, IPR2024-00007

device, deleting one or more files that are associated with the unauthorized resource, and hiding the unauthorized resource.

12. The method of claim 1, further including controlling the mobile device according to a parameter that relates to an unauthorized external resource.

13. The method of claim 12, wherein the unauthorized external resource comprises at least one of a computing node resource, an external application program, and an external database.

14. The method of claim 1, wherein corresponding device security profiles for different identity statuses of the mobile device are administered by a security policy engine.

15. The method of claim 1, wherein the device security profile is transferred to the mobile device after access to the computing node is granted.

16. The method of claim 15, wherein the device security profile is transferred wirelessly.

17. A method for unlocking a password protected mobile device associated with a security station, comprising:

authenticating a user of the mobile device;

Petitioner Ex 1002, p. 450
Zimperium v. Taasera, IPR2024-00007

authenticating the mobile device according to a device authentication code that is generated based on an identity status of the mobile device that uniquely characterizes the mobile device; and

generating an unlock code for unlocking the password protected mobile device.

18. The method of claim 17, wherein the user is authenticated by at least one of a user authentication response, a biometric parameter, or a security identification parameter.

19. The method of claim 17, further including communicating at least one of the user authentication response and the device authentication code by at least one of the user or the mobile device.

20. The method of claim 17, further including communicating the unlock code by at least one of the security station and an administrator.

21. A method for protecting a mobile device, comprising:

transmitting a request from the mobile device in response to a security threat;

creating a device security profile in response to the request based on the security threat; and

transmitting the device security profile to the mobile device.

Petitioner Ex 1002, p. 451
Zimperium v. Taasera, IPR2024-00007

22. The method of claim 21, wherein the request comprises information related to one or more attributes of the mobile device.

23. The method of claim 22, wherein one of the one or more attributes of the mobile device relates to at least one of a communication link used by the mobile device, a serial number of the mobile device, software and hardware on the mobile device.

24. The method of claim 22, wherein one of the one or more attributes of the mobile device relates to active directory information of the mobile device.

25. The method of claim 24, wherein the active directory information of the mobile device comprises firewall settings of the mobile device, current security settings of the mobile device, and a security parameter of the mobile device.

26. The method of claim 21, wherein the device security profile protects the mobile device from a virus threat.

27 A method for protecting a mobile device that connects to a computing node, comprising:

transmitting a new computing node login information to the mobile device in a device security profile;

retrieving the new computing node login information from the device security profile at the mobile device; and

Petitioner Ex 1002, p. 452
Zimperium v. Taasera, IPR2024-00007

setting the new computing node login information as the new login information for the mobile device.

28. The method of claim 27, wherein the new computing node login information comprises a new password.

29. The method of claim 27, wherein the new computing node login information comprises a new network login information.

30. The method of claim 17, wherein the new network login information is transmitted to the mobile device from a security station to set the new login information of the mobile device.

31. A method for protecting a network comprising, comprising:

detecting access by a mobile device to one or more resources within the network;

authenticating the mobile device for access to the one or more resources; and

transmitting a device security profile to the mobile device upon authentication, said security profile comprising rules for accessing the one or more resources.

32. The method of claim 31, wherein the one or more resources comprise at least one of a communication resource, a data storage resource, and a peripheral resource.

Petitioner Ex 1002, p. 453
Zimperium v. Taasera, IPR2024-00007

33. The method of claim 31, wherein the communication resource comprises a wireless link resource.

34. A method for securing a computing node that connects to different mobile devices, comprises:

applying security rules to the different mobile devices in accordance with corresponding device parameters contained in a security signature file;

detecting a change in at least one of the device parameters of a mobile device; and

modifying the security rules applied to the mobile device at the computing node in accordance with one or more device parameters of an updated security signature file.

35. The method of claim 34, wherein the one or more device parameters comprise at least one of a serial number, security settings, manufacturer, and a model number.

Petitioner Ex 1002, p. 454
Zimperium v. Taasera, IPR2024-00007

Data
Data
114
120
118
116
Security Database
Host/Central Station
122
Network Layer Interface
Link Layer Interface
Physical Layer Interface
Wireless Radio Tower
Laptop computer
Security Server
106
Cable
110
102
104
152
112
153

FIG. 1

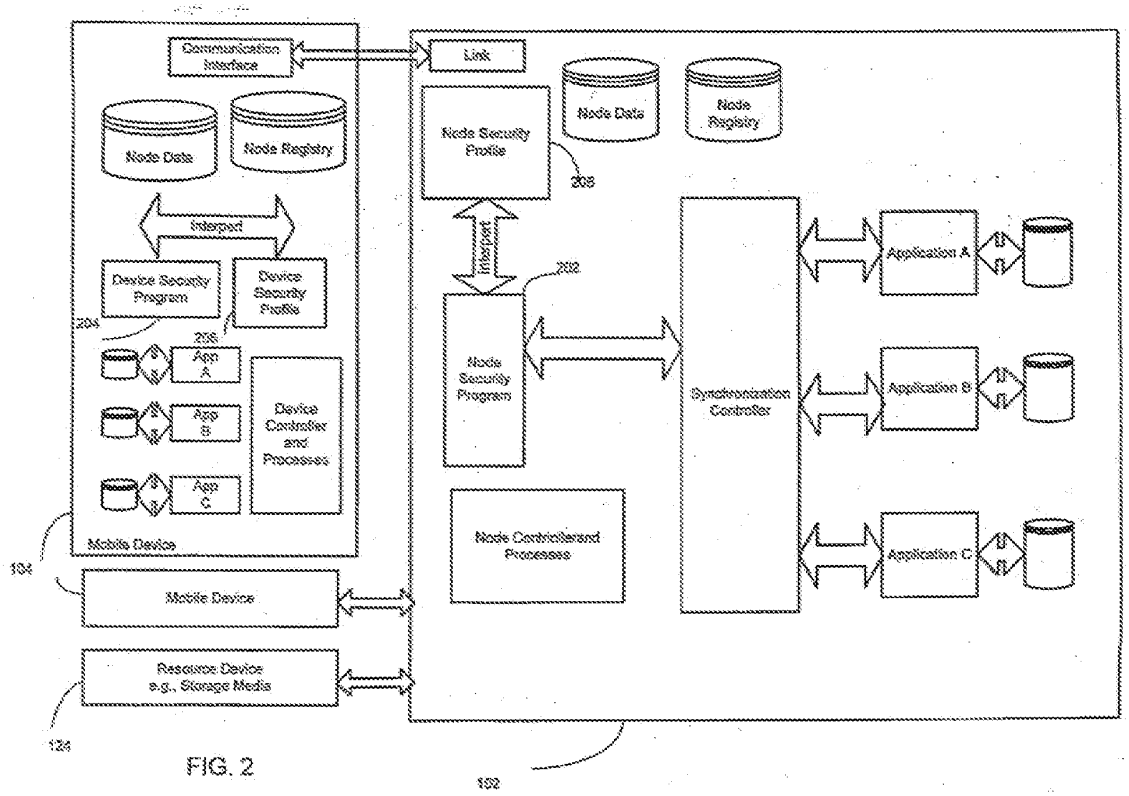


FIG. 2

Petitioner Ex 1002, p. 456
Zimperium v. Taasera, IPR2024-00007

```
- <{_8F032CDD-DAEB-452F-83E5-FC8804907AC7>
  - <PolicyEditor>
      <IsCommonPolicy value="true" />
      <DeviceType value="Pocket PC" />
      <CreationStamp value="2003-08-26 17:34:46" />
      <UserName value="Pocket PC" />
      <HotSyncName value="Pocket PC" />
      <Version value="21" />
      <MagicValue value="1004695628" />
      <SerialNumber value="N-882683AUW72882" />
      <AdminPassword value="[1]" />
      <SessionKey value="a021a791bed695fc300f872cfcc5866518d3dbc68" />
      <NewAdminPassword value="[1]" />
      <ChangePassword value="false" />
      <ForceGlobalPasswordChange value="false" />
      <ExpirationPeriod value="0" />
      <MinPasswordLength value="1" />
      <FolderName value="SecureFolder" />
      <CryptoMethod value="RC4" />
      <StorageSize value="65536" />
      <UserCanSeeSettings value="true" />
      <RestrictionStartTime value="0" />
      <RestrictionEndTime value="0" />
      <PasswordRestriction value="33686018" />
      <GlobalPasswordRestriction value="2" />
      <LocalPasswordRestriction value="2" />
      <BackdoorPasswordRestriction value="2" />
      <WipePasswordRestriction value="2" />
      <WorkingDays value="0" />
      <Company value="Trust Digital" />
      <Address value="" />
```

FIG. 3

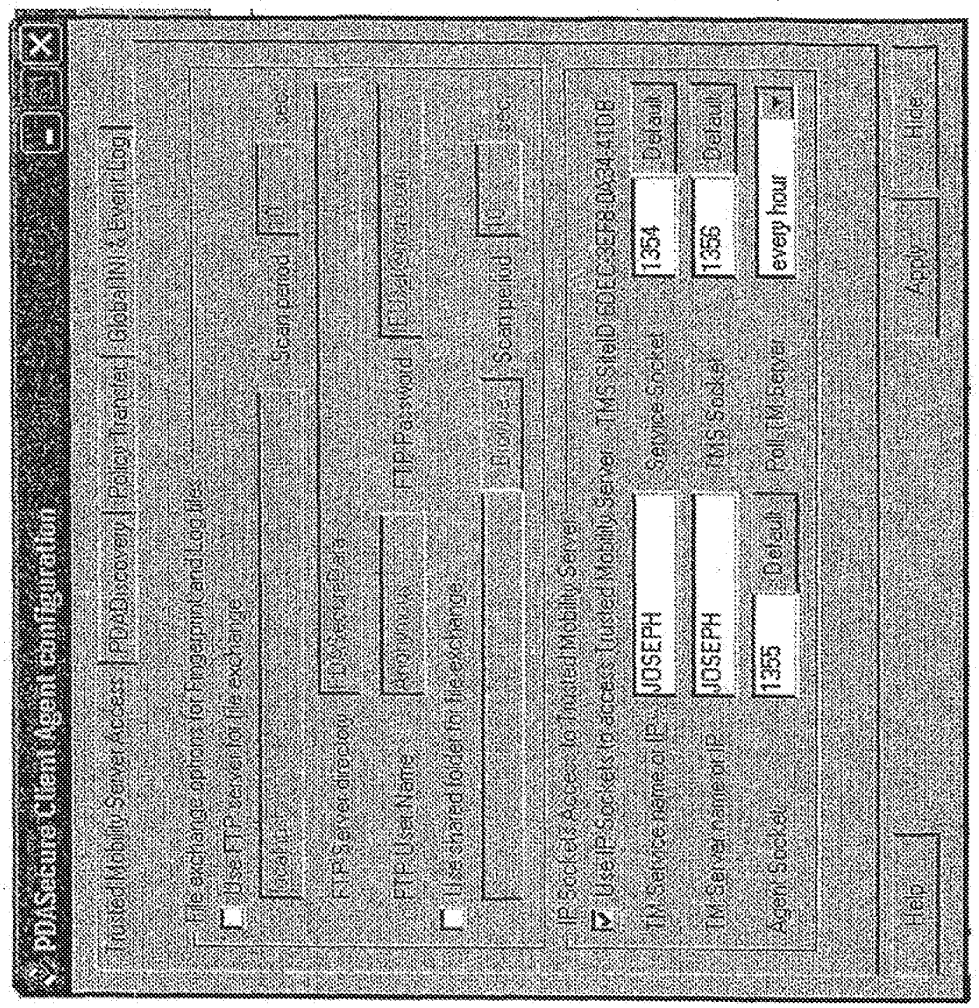

PDASecure Client Agent configuration
Trusted Mobility Server Access
PDA Discovery
Policy Transfer
Global NMS Event Log
Use FTP server for file exchange
Scan period
sec
FTP Server address
FTP User Name
FTP Password
Use shared folder for file exchange
Browse...
Scan period
sec
IP Socket Access to Trusted Mobility Server
Use IP Sockets for access to Trusted Mobility Server - TMS Shell 0x0E0E3EF8 0x34410E
TM Service name or IP:
JOSEPH
Service Socket
1354
Default
TM Server name or IP:
JOSEPH
TMS Socket
1356
Default
Agent Socket
1355
Default
Poll TM server
every hour
Help
Apply
Hide

FIG. 4

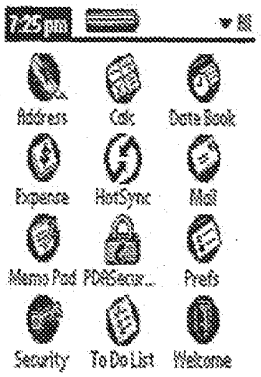

Address
Calc
Date Book
Expense
HotSync
Mail
Memo Pad
PDASecure...
Prefs
Security
To Do List
Welcome

FIG. 5

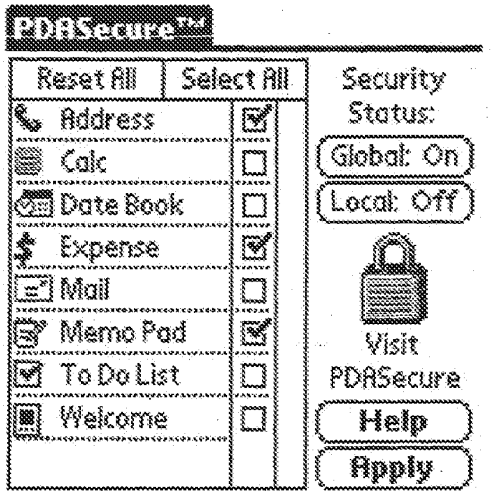

PDASecure™
Reset All
Select All
Address
Calc
Date Book
Expense
Mail
Memo Pad
To Do List
Welcome
Security Status:
Global: On
Local: Off
Visit PDASecure
Help
Apply

FIG. 6

700
System Administrator
702
Administrator Input
703
IT Infrastructure
706
DATA Collecter
708
Policy Engine
704
710
DATA Collecter
Node Security Program
712
Mobile Edge
104

FIG. 7

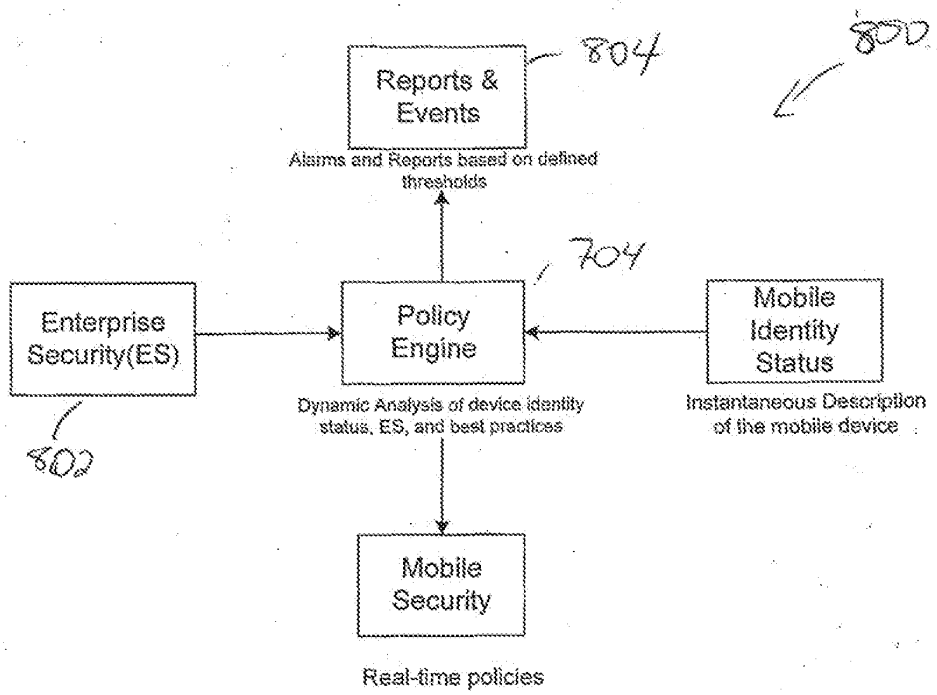

800
804
Reports & Events
Alarms and Reports based on defined thresholds
704
Enterprise Security(ES)
802
Policy Engine
Dynamic Analysis of device identity status, ES, and best practices
Mobile Identity Status
Instantaneous Description of the mobile device
Mobile Security
Real-time policies

FIG. 8

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US04/42565

A. CLASSIFICATION OF SUBJECT MATTER
IPC(7) : G06F 17/30
US CL : 707/1, 707/10, 707/100, 707/102
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
U.S. : 707/1, 707/10, 707/100, 707/102

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
East Database v.1.4.1

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X, E	US Pub. No. 2005/0022012 A1 (BLUESTONE et al.) 27 January 2005 (25.01.2005), page 1, paragraph 0006, page 3, paragraph 0036, page 4, paragraphs 0039-0040, page 5, paragraphs 0047-0050, page 6, paragraph 0057.	1-35
A, P	US Pub. No. 2004/0076128 A1 (RAO et al.) 22 April 2004 (22.04.2004).	1-35

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
11 May 2005 (11.05.2005)	25 MAY 2005
Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450 Alexandria, Virginia 22313-1450 Facsimile No. (703) 305-3230	Authorized officer Neveen Abel-Jalil Telephone No. 571-272-4074

Form PCT/ISA/210 (second sheet) (January 2004)

Electronic Acknowledgement Receipt

EFS ID:	21478073
Application Number:	13540142
International Application Number:	
Confirmation Number:	4198
Title of Invention:	RULES BASED ACTIONS FOR MOBILE DEVICE MANAGEMENT
First Named Inventor/Applicant Name:	Jatin MALIK
Customer Number:	86308
Filer:	Michael Kenneth Jones/Sara Harvell
Filer Authorized By:	Michael Kenneth Jones
Attorney Docket Number:	130839.02101
Receipt Date:	12-FEB-2015
Filing Date:	02-JUL-2012
Time Stamp:	16:04:09
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Form (SB08)	2101SIDS2.pdf	63431 531080d685e277ea2f3b7184bc0de3316803908b	no	4

Warnings:	
Information:	

This is not an USPTO supplied IDS fillable form					
2	Other Reference-Patent/App/Search documents	2101EESR.pdf	1980871 9702cebf6c8618d1c6be56ff7b58631b9b3b4412	no	3
Warnings:					
Information:					
3	Foreign Reference	2005064498A1.pdf	6190957 dd6a285097af11d020a63ce85a9d9029f4e2ae64	no	50
Warnings:					
Information:					
		Total Files Size (in bytes):	8235259		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

NOTICE OF ALLOWANCE AND FEE(S) DUE

86308 7590 02/23/2015

Pepper Hamilton LLP
400 Berywn Park
899 Cassatt Road
Berwyn, PA 19312-1183

EXAMINER
KATSIKIS, KOSTAS J

ART UNIT	PAPER NUMBER
2441	

DATE MAILED: 02/23/2015

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/540,142	07/02/2012	Jatin MALIK	130839.02101	4198

TITLE OF INVENTION: RULES BASED ACTIONS FOR MOBILE DEVICE MANAGEMENT

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$480	$0	$0	$480	05/26/2015

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED. THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.

THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED. SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE DOES NOT REFLECT A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE IN THIS APPLICATION. IF AN ISSUE FEE HAS PREVIOUSLY BEEN PAID IN THIS APPLICATION (AS SHOWN ABOVE), THE RETURN OF PART B OF THIS FORM WILL BE CONSIDERED A REQUEST TO REAPPLY THE PREVIOUSLY PAID ISSUE FEE TOWARD THE ISSUE FEE NOW DUE.

HOW TO REPLY TO THIS NOTICE:

I. Review the ENTITY STATUS shown above. If the ENTITY STATUS is shown as SMALL or MICRO, verify whether entitlement to that entity status still applies.

If the ENTITY STATUS is the same as shown above, pay the TOTAL FEE(S) DUE shown above.

If the ENTITY STATUS is changed from that shown above, on PART B - FEE(S) TRANSMITTAL, complete section number 5 titled "Change in Entity Status (from status indicated above)".

For purposes of this notice, small entity fees are 1/2 the amount of undiscounted fees, and micro entity fees are 1/2 the amount of small entity fees.

II. PART B - FEE(S) TRANSMITTAL, or its equivalent, must be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed and an extra copy of the form should be submitted. If an equivalent of Part B is filed, a request to reapply a previously paid issue fee must be clearly made, and delays in processing may occur due to the difficulty in recognizing the paper as an equivalent of Part B.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: Utility patents issuing on applications filed on or after Dec. 12, 1980 may require payment of maintenance fees. It is patentee's responsibility to ensure timely payment of maintenance fees when due.

Petitioner Ex 1002, p. 465
Zimperium v. Taasera, IPR2024-00007

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: Mail **Mail Stop ISSUE FEE**
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

86308 7590 02/23/2015
Pepper Hamilton LLP
400 Berywn Park
899 Cassatt Road
Berwyn, PA 19312-1183

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission
I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

(Depositor's name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/540,142	07/02/2012	Jatin MALIK	130839.02101	4198

TITLE OF INVENTION: RULES BASED ACTIONS FOR MOBILE DEVICE MANAGEMENT

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$480	$0	$0	$480	05/26/2015

EXAMINER	ART UNIT	CLASS-SUBCLASS
KATSIKIS, KOSTAS J	2441	709-223000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).
- ❑ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.
- ❑ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list
(1) The names of up to 3 registered patent attorneys or agents OR, alternatively,
(2) The name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.
1 _____
2 _____
3 _____

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE (B) RESIDENCE: (CITY and STATE OR COUNTRY)

Please check the appropriate assignee category or categories (will not be printed on the patent) : ❑ Individual ❑ Corporation or other private group entity ❑ Government

4a. The following fee(s) are submitted:
- ❑ Issue Fee
- ❑ Publication Fee (No small entity discount permitted)
- ❑ Advance Order - # of Copies _____

4b. Payment of Fee(s): **(Please first reapply any previously paid issue fee shown above)**
- ❑ A check is enclosed.
- ❑ Payment by credit card. Form PTO-2038 is attached.
- ❑ The director is hereby authorized to charge the required fee(s), any deficiency, or credits any overpayment, to Deposit Account Number _____ (enclose an extra copy of this form).

5. **Change in Entity Status** (from status indicated above)
- ❑ Applicant certifying micro entity status. See 37 CFR 1.29 — NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.
- ❑ Applicant asserting small entity status. See 37 CFR 1.27 — NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.
- ❑ Applicant changing to regular undiscounted fee status. — NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature _____ Date _____

Typed or printed name _____ Registration No. _____

PTOL-85 Part B (10-13) Approved for use through 10/31/2013. OMB 0651-0033 U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Petitioner Ex 1002, p. 466
Zimperium v. Taasera, IPR2024-00007

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/540,142	07/02/2012	Jatin MALIK	130839.02101	4198

86308 7590 02/23/2015

Pepper Hamilton LLP
400 Berywn Park
899 Cassatt Road
Berwyn, PA 19312-1183

EXAMINER	
KATSIKIS, KOSTAS J	
ART UNIT	PAPER NUMBER
2441	

DATE MAILED: 02/23/2015

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(Applications filed on or after May 29, 2000)

The Office has discontinued providing a Patent Term Adjustment (PTA) calculation with the Notice of Allowance.

Section 1(h)(2) of the AIA Technical Corrections Act amended 35 U.S.C. 154(b)(3)(B)(i) to eliminate the requirement that the Office provide a patent term adjustment determination with the notice of allowance. See Revisions to Patent Term Adjustment, 78 Fed. Reg. 19416, 19417 (Apr. 1, 2013). Therefore, the Office is no longer providing an initial patent term adjustment determination with the notice of allowance. The Office will continue to provide a patent term adjustment determination with the Issue Notification Letter that is mailed to applicant approximately three weeks prior to the issue date of the patent, and will include the patent term adjustment on the patent. Any request for reconsideration of the patent term adjustment determination (or reinstatement of patent term adjustment) should follow the process outlined in 37 CFR 1.705.

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.

Petitioner Ex 1002, p. 467
Zimperium v. Taasera, IPR2024-00007

OMB Clearance and PRA Burden Statement for PTOL-85 Part B

The Paperwork Reduction Act (PRA) of 1995 requires Federal agencies to obtain Office of Management and Budget approval before requesting most types of information from the public. When OMB approves an agency request to collect information from the public, OMB (i) provides a valid OMB Control Number and expiration date for the agency to display on the instrument that will be used to collect the information and (ii) requires the agency to inform the public about the OMB Control Number's legal significance in accordance with 5 CFR 1320.5(b).

The information collected by PTOL-85 Part B is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450. Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Notice of Allowability	Application No. 13/540,142	Applicant(s) MALIK ET AL.	
	Examiner KOSTAS KATSIKIS	Art Unit 2441	AIA (First Inventor to File) Status No

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *the After Final filed 02/09/2015*.
   ☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on_____.
2. ☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.
3. ☒ The allowed claim(s) is/are *1-23*. As a result of the allowed claim(s), you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov .
4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

   Certified copies:

   a) ☐ All b) ☐ Some *c) ☐ None of the:
   1. ☐ Certified copies of the priority documents have been received.
   2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
   3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☒ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date 02/12/2015
3. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
4. ☒ Interview Summary (PTO-413), Paper No./Mail Date *02/11/2015* .
5. ☐ Examiner's Amendment/Comment
6. ☐ Examiner's Statement of Reasons for Allowance
7. ☒ Other *See attached PTOL-2323 form*.

/KOSTAS KATSIKIS/
Primary Examiner, Art Unit 2441

Petitioner Ex 1002, p. 469
Zimperium v. Taasera, IPR2024-00007

Examiner-Initiated Interview Summary	Application No.	Applicant(s)	
	13/540,142	MALIK ET AL.	
	Examiner	Art Unit	
	KOSTAS KATSIKIS	2441	

All participants (applicant, applicant's representative, PTO personnel):

(1) *KOSTAS KATSIKIS*. (3)_____.

(2) *MICHAEL K. JONES (Reg. No. 41,100)*. (4)_____.

Date of Interview: *11 February 2015*.

Type: ☒ Telephonic ☐ Video Conference
☐ Personal [copy given to: ☐ applicant ☐ applicant's representative]

Exhibit shown or demonstration conducted: ☐ Yes ☒ No.
If Yes, brief description: _____.

Issues Discussed ☐101 ☐112 ☐102 ☐103 ☒Others
(For each of the checked box(es) above, please describe below the issue and detailed description of the discussion)

Claim(s) discussed: *1,10 and 17*.

Identification of prior art discussed: *SINHA*.

Substance of Interview
(For each issue discussed, provide a detailed description and indicate if agreement was reached. Some topics may include: identification or clarification of a reference or a portion thereof, claim interpretation, proposed amendments, arguments of any applied references etc...)

Examiner brought Applicant's attention to newly cited reference to SINHA (US 2011/0167474 A1) which is a continuation-in-part of 13/051,519, and disclosing a mobile device management system. Particularly, paragraphs [0062]-[0064] with reference to FIG. 5, were indicated by Examiner to disclose newly amended limitations of claims 1, 10 and 17. However, Applicant and Examiner agreed that the cited portions of SINHA that were relied upon by Examiner were not supported by the Parent Application, 13/051,519.

Applicant recordation instructions: It is not necessary for applicant to provide a separate record of the substance of interview.

Examiner recordation instructions: Examiners must summarize the substance of any interview of record. A complete and proper recordation of the substance of an interview should include the items listed in MPEP 713.04 for complete and proper recordation including the identification of the general thrust of each argument or issue discussed, a general indication of any other pertinent matters discussed regarding patentability and the general results or outcome of the interview, to include an indication as to whether or not agreement was reached on the issues raised.

☐ Attachment

/KOSTAS KATSIKIS/ Primary Examiner, Art Unit 2441	

Petitioner Ex 1002, p. 470
Zimperium v. Taasera, IPR2024-00007

Notice of References Cited	Application/Control No. 13/540,142	Applicant(s)/Patent Under Reexamination MALIK ET AL.	
	Examiner KOSTAS KATSIKIS	Art Unit 2441	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-2011/0167474 A1	07-2011	SINHA et al.	726/1
*	B	US-2012/0179802 A1	07-2012	NARASIMHAN et al.	709/223
*	C	US-2012/0240183 A1	09-2012	SINHA, Amit	726/1
*	D	US-8,499,331 B1	07-2013	Yehuda et al.	726/1
*	E	US-2013/0305101 A1	11-2013	Gupta et al.	714/47.3
*	F	US-2015/0006681 A1	01-2015	Lim et al.	709/219
	G	US-			
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Petitioner Ex 1002, p. 471
Zimperium v. Taasera, IPR2024-00007

AFCP 2.0 Decision	Application No.	Applicant(s)
	13/540,142	MALIK ET AL.
	Examiner	Art Unit
	KOSTAS KATSIKIS	2441

This is in response to the After Final Consideration Pilot request filed 09 February 2015.

1. **Improper Request** – The AFCP 2.0 request is improper for the following reason(s) and the after final amendment submitted with the request will be treated under pre-pilot procedure.

   ☐ An AFCP 2.0 request form PTO/SB/434 (or equivalent document) was not submitted.

   ☐ A non-broadening amendment to at least one independent claim was not submitted.

   ☐ A proper AFCP 2.0 request was submitted in response to the most recent final rejection.

   ☐ Other:

2. **Proper Request**

   A. After final amendment submitted with the request will not be treated under AFCP 2.0.
   The after final amendment cannot be reviewed and a search conducted within the guidelines of the pilot program.

   ☐ The after final amendment will be treated under pre-pilot procedure.

   B. Updated search and/or completed additional consideration.
   The examiner performed an updated search and/or completed additional consideration of the after final amendment within the time authorized for the pilot program. The result(s) of the updated search and/or completed additional consideration are:

   ☒ 1. All of the rejections in the most recent final Office action are overcome and a Notice of Allowance is issued herewith.

   ☐ 2. The after final amendment would not overcome all of the rejections in the most recent final Office action. See attached interview summary for further details.

   ☐ 3. The after final amendment was reviewed, and it raises a new issue(s). See attached interview summary for further details.

   ☐ 4. The after final amendment raises new issues, but would overcome all of the rejections in the most recent final Office action. A decision on determining allowability could not be made within the guidelines of the pilot. See attached interview summary for further details, including any newly discovered prior art.

   ☐ 5. Other:

   Examiner Note: Please attach an interview summary when necessary as described above.

Petitioner Ex 1002, p. 472
Zimperium v. Taasera, IPR2024-00007

Receipt date: 02/12/2015
Doc code: IDS
Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99**)		
	Application Number	13540142
	Filing Date	2012-07-02
	First Named Inventor	Jatin Malik
	Art Unit	2441
	Examiner Name	Kostas J. Katsikis
	Attorney Docket Number	130839.02101

U.S.PATENTS

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button.

U.S.PATENT APPLICATION PUBLICATIONS

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20070143851	A1	2007-06-21	Nicodemus et al.	
	2	20070156659	A1	2007-07-05	Lim	
	3	20080109871	A1	2008-05-08	Jacobs	
	4	20110145920	A1	2011-06-16	Mahaffey et al.	

If you wish to add additional U.S. Published Application citation information please click the Add button.

FOREIGN PATENT DOCUMENTS

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] ¡	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.K./

Receipt date: 02/12/2015	Application Number	13540142
INFORMATION DISCLOSURE STATEMENT BY APPLICANT	Filing Date	2012-07-02
	First Named Inventor	Jatin Malik
(Not for submission under 37 CFR 1.99)	Art Unit	2441
	Examiner Name	Kostas J. Katsikis
	Attorney Docket Number	130839.02101

	1	2005064498	WO	A1	2005-07-14	Shahbazi		☐

If you wish to add additional Foreign Patent Document citation information please click the Add button

NON-PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1	Supplementary European Search Report mailed 5 February 2015 in corresponding European Patent Application No. 12808145.2	☐

If you wish to add additional non-patent literature document citation information please click the Add button

EXAMINER SIGNATURE

Examiner Signature	/Kostas Katsikis/	Date Considered	02/13/2015

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.K./

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13540142	MALIK ET AL.
	Examiner	Art Unit
	KOSTAS KATSIKIS	2441

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☒ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	12/16/2013	09/04/2014	02/11/2015						
	1	✓	✓	=						
	2	✓	✓	=						
	3	✓	✓	=						
	4	✓	✓	=						
	5	✓	✓	=						
	6	✓	✓	=						
	7	✓	✓	=						
	8	✓	✓	=						
	9	✓	✓	=						
	10	✓	✓	=						
	11	✓	✓	=						
	12	✓	✓	=						
	13	✓	✓	=						
	14	✓	✓	=						
	15	✓	✓	=						
	16	✓	✓	=						
	17	✓	✓	=						
	18	✓	✓	=						
	19	✓	✓	=						
	20	✓	✓	=						
	21	✓	✓	=						
	22	✓	✓	=						
	23	✓	✓	=						

Petitioner Ex 1002, p. 475
Zimperium v. Taasera, IPR2024-00007

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13540142	MALIK ET AL.
	Examiner	**Art Unit**
	KOSTAS KATSIKIS	2441

CPC						
Symbol					**Type**	**Version**
H04L		43	/	0817	F	2013-01-01
H04L		41	/	0816	I	2013-01-01
H04L		41	/	0893	I	2013-01-01
H04L		63	/	10	A	2013-01-01
H04L		63	/	20	A	2013-01-01
H04W		12	/	08	A	2013-01-01
H04W		12	/	12	A	2013-01-01
			/			
			/			
			/			
			/			
			/			
			/			
			/			
			/			

CPC Combination Sets							
Symbol				**Type**	**Set**	**Ranking**	**Version**
			/				
			/				

NONE		**Total Claims Allowed:**	
(Assistant Examiner)	(Date)	23	
/KOSTAS KATSIKIS/ Primary Examiner.Art Unit 2441	02/11/2015	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	1

Petitioner Ex 1002, p. 476
Zimperium v. Taasera, IPR2024-00007

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13540142	MALIK ET AL.
	Examiner	**Art Unit**
	KOSTAS KATSIKIS	2441

US ORIGINAL CLASSIFICATION		INTERNATIONAL CLASSIFICATION										
CLASS	SUBCLASS	CLAIMED					NON-CLAIMED					
709	223	G	0	6	F	15 / 173 (2006.01.01)						
CROSS REFERENCE(S)												
CLASS	SUBCLASS (ONE SUBCLASS PER BLOCK)											

NONE (Assistant Examiner)	(Date)	**Total Claims Allowed:** 23	
/KOSTAS KATSIKIS/ Primary Examiner.Art Unit 2441 (Primary Examiner)	02/11/2015 (Date)	O.G. Print Claim(s) 1	O.G. Print Figure 1

Petitioner Ex 1002, p. 477
Zimperium v. Taasera, IPR2024-00007

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13540142	MALIK ET AL.
	Examiner	**Art Unit**
	KOSTAS KATSIKIS	2441

☒ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original
	1		17												
	2		18												
	3		19												
	4		20												
	5		21												
	6		22												
	7		23												
	8														
	9														
	10														
	11														
	12														
	13														
	14														
	15														
	16														

NONE (Assistant Examiner)	(Date)	**Total Claims Allowed:** 23	
/KOSTAS KATSIKIS/ Primary Examiner.Art Unit 2441 (Primary Examiner)	02/11/2015 (Date)	O.G. Print Claim(s) 1	O.G. Print Figure 1

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S1	1	"13603630"	US-PGPUB; USPAT	ADJ	ON	2014/07/12 11:07
S2	1	"20140068025"	DERWENT	ADJ	ON	2014/07/12 11:07
S3	7599	(proxy near (function or server)) same3 (service near (provider$1 or provider$1))	US-PGPUB; USPAT	ADJ	ON	2014/07/28 08:53
S4	1697	(proxy near (function or server)) near20 (service near (provider$1 or provider$1))	US-PGPUB; USPAT	ADJ	ON	2014/07/28 08:56
S5	1420	((provider near information) near10 (identifier$1 or id$1))	US-PGPUB; USPAT	ADJ	ON	2014/07/28 08:58
S6	1	S4 same3 S5	US-PGPUB; USPAT	ADJ	ON	2014/07/28 08:58
S7	21	S4 and S5	US-PGPUB; USPAT	ADJ	ON	2014/07/28 08:59
S8	20193	709/220$	US-PGPUB; USPAT	ADJ	ON	2014/07/28 08:59
S9	75	S4 and S8	US-PGPUB; USPAT	ADJ	ON	2014/07/28 08:59
S10	43	((Di) near2 (LIU)).INV.	US-PGPUB; USPAT	ADJ	ON	2014/07/28 10:34
S11	879	((Xiao) near2 (LI)).INV.	US-PGPUB; USPAT	ADJ	ON	2014/07/28 10:34
S12	1	((Ruth) near2 ("PALLARES DEL EGIDO")).INV.	US-PGPUB; USPAT	ADJ	ON	2014/07/28 10:34
S13	1	S10 and S11 and S12	US-PGPUB; USPAT	ADJ	ON	2014/07/28 10:36
S14	1	S10 and (service and provider and proxy and function).clm.	US-PGPUB; USPAT	ADJ	ON	2014/07/28 10:37
S15	1	S11 and (service and provider and proxy and function).clm.	US-PGPUB; USPAT	ADJ	ON	2014/07/28 10:37
S16	1	S12 and (service and provider and proxy and function).clm.	US-PGPUB; USPAT	ADJ	ON	2014/07/28 10:37

Petitioner Ex 1002, p. 479
Zimperium v. Taasera, IPR2024-00007

S17	141	(proxy near (function or server)) same3 (service near (provider$1 or provider$1))	FPRS; EPO; JPO	ADJ	ON	2014/07/28 10:39
S18	66	(proxy near (function or server)) near20 (service near (provider$1 or provider$1))	FPRS; EPO; JPO	ADJ	ON	2014/07/28 10:39
S19	66	S17 and S18	FPRS; EPO; JPO	ADJ	ON	2014/07/28 10:39
S20	145	((provider near information) near10 (identifier$1 or id$1))	FPRS; EPO; JPO	ADJ	ON	2014/07/28 10:39
S21	2	S19 and S20	FPRS; EPO; JPO	ADJ	ON	2014/07/28 10:40
S22	3	("TDF" or (traffic adj1 (detect$3 or control or monitor$3) adj1 function)) near20 ("CDN" or (content adj1 delivery adj1 network))	US-PGPUB; USPAT	ADJ	ON	2015/02/05 14:05
S23	132	(traffic adj1 detection adj1 function)	US-PGPUB; USPAT	ADJ	ON	2015/02/05 14:22
S24	4	(traffic adj1 detection adj1 function) same3 cdn	US-PGPUB; USPAT	ADJ	ON	2015/02/05 14:22
S25	3002	(configur$3 or provision$3) near4 (proxy adj1 (function$1 or server$1))	US-PGPUB; USPAT	ADJ	ON	2015/02/05 14:23
S26	586410	(set or group) near3 (providers or servers or elements)	US-PGPUB; USPAT	ADJ	ON	2015/02/05 14:24
S27	304	S25 same3 S26	US-PGPUB; USPAT	ADJ	ON	2015/02/05 14:24
S28	21685	709/220$	US-PGPUB; USPAT	ADJ	ON	2015/02/05 14:26
S29	6700	709/222$	US-PGPUB; USPAT	ADJ	ON	2015/02/05 14:26
S30	2924	h04l67/327.cpc.	US-PGPUB; USPAT	ADJ	ON	2015/02/05 14:27
S31	4763	h04l67/28.cpc.	US-PGPUB; USPAT	ADJ	ON	2015/02/05 14:27
S32	14	S27 and S28	US-PGPUB; USPAT	ADJ	ON	2015/02/05 14:27
S33	7	S27 and S29	US-PGPUB; USPAT	ADJ	ON	2015/02/05 14:27
S34	6	S27 and S30	US-PGPUB; USPAT	ADJ	ON	2015/02/05 14:27
S35	9	S27 and S31	US-PGPUB; USPAT	ADJ	ON	2015/02/05 14:27
S36	6	S27 and S30	US-PGPUB;	ADJ	ON	2015/02/05 14:32

Petitioner Ex 1002, p. 480
Zimperium v. Taasera, IPR2024-00007

			USPAT			
S37	5	(proxy adj1 (server or mechanism or function)) near10 ((configuration adj1 file) or database or datastore) near10 (address adj1 information)	US-PGPUB; USPAT	ADJ	ON	2015/02/05 14:41
S38	20	(first adj1 proxy adj1 (server or mechanism or function)) near4 (configur$3 or provision$3 or initializ$3 or initialis$3)	US-PGPUB; USPAT	ADJ	ON	2015/02/05 14:46
S39	25	(second adj1 proxy adj1 (server or mechanism or function)) near4 (configur$3 or provision$3 or initializ$3 or initialis$3)	US-PGPUB; USPAT	ADJ	ON	2015/02/05 14:47
S40	14	S38 same3 S39	US-PGPUB; USPAT	ADJ	ON	2015/02/05 14:47
S41	315	(second adj1 proxy adj1 (server or mechanism or function))	US-PGPUB; USPAT	ADJ	ON	2015/02/05 14:47
S42	18	S38 same3 S41	US-PGPUB; USPAT	ADJ	ON	2015/02/05 14:47
S43	215	(proxy near (server or function or mechanism)) near20 (configuration file)	US-PGPUB; USPAT	ADJ	ON	2015/02/06 14:54
S44	21685	709/220$	US-PGPUB; USPAT	ADJ	ON	2015/02/06 15:26
S45	6700	709/222$	US-PGPUB; USPAT	ADJ	ON	2015/02/06 15:26
S46	215	(proxy near (server or function or mechanism)) near20 (configuration file)	US-PGPUB; USPAT	ADJ	ON	2015/02/06 15:26
S47	23	S44 and S46	US-PGPUB; USPAT	ADJ	ON	2015/02/06 15:26
S48	11	S45 and S46	US-PGPUB; USPAT	ADJ	ON	2015/02/06 15:26
S49	1	(first near server) near20 (configuration adj1 file) near20 (address or location) near20 (second near server)	US-PGPUB; USPAT	ADJ	ON	2015/02/06 15:40
S50	1	"20070143851"	US-PGPUB; USPAT	ADJ	ON	2015/02/13 19:39
S51	2	"20070156659"	US-PGPUB; USPAT	ADJ	ON	2015/02/13 19:40
S52	2	"20080109871"	US-PGPUB; USPAT	ADJ	ON	2015/02/13 19:41
S53	1	"20110145920"	US-PGPUB; USPAT	ADJ	ON	2015/02/13 19:42

2/13/2015 7:44:51 PM

Petitioner Ex 1002, p. 481
Zimperium v. Taasera, IPR2024-00007

C:\ Users\ kkatsikis1\ Documents\ EAST\ Workspaces\ 13603630.wsp

Petitioner Ex 1002, p. 482
Zimperium v. Taasera, IPR2024-00007

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S1	1	"13540142"	US-PGPUB; USPAT	ADJ	ON	2013/12/13 15:50
S2	1	"20130007245"	DERWENT	ADJ	ON	2013/12/13 15:50
S3	41873	709/223$	US-PGPUB; USPAT	ADJ	ON	2013/12/13 15:51
S4	43047	709/224$	US-PGPUB; USPAT	ADJ	ON	2013/12/13 15:51
S5	1	"20100242088"	US-PGPUB; USPAT	ADJ	ON	2013/12/13 15:57
S6	960	H04L41/0816.cpc.	US-PGPUB; USPAT	ADJ	ON	2013/12/13 16:01
S7	3684	H04L43/0817.cpc.	US-PGPUB; USPAT	ADJ	ON	2013/12/13 16:01
S8	2594	H04L41/0893.cpc.	US-PGPUB; USPAT	ADJ	ON	2013/12/13 16:02
S9	31	H04L41/0618.cpc.	US-PGPUB; USPAT	ADJ	ON	2013/12/13 16:21
S10	577	455/26.1$	US-PGPUB; USPAT	ADJ	ON	2013/12/13 16:26
S11	3571	455/425$	US-PGPUB; USPAT	ADJ	ON	2013/12/13 16:28
S12	3995	455/456.5$	US-PGPUB; USPAT	ADJ	ON	2013/12/13 16:31
S13	22104	(gather$3 or collect$3 or assembl$3 or aggregat$3) near4 (status)	US-PGPUB; USPAT	ADJ	ON	2013/12/13 16:38
S14	358	(evaluat$3 or assess$3 or determin$3) near20 (compl$5 or conform$4) near20 (polic$3 or rule$1) near20 (violat$3 or break$3 or infract$3)	US-PGPUB; USPAT	ADJ	ON	2013/12/13 16:42
S15	0	S13 same3 S14	US-PGPUB; USPAT	ADJ	ON	2013/12/13 16:43
S16	24731	(polic$3 or rule$1) near20 (violat$3 or break$3 or infract$3)	US-PGPUB;	ADJ	ON	2013/12/13 16:43

Petitioner Ex 1002, p. 483
Zimperium v. Taasera, IPR2024-00007

			USPAT			
S17	92	S13 same3 S16	US-PGPUB; USPAT	ADJ	ON	2013/12/13 16:44
S18	1883	(compl$5 or conform$4) near20 (polic$3 or rule$1) near20 (violat$3 or break$3 or infract$3)	US-PGPUB; USPAT	ADJ	ON	2013/12/13 16:47
S19	2	S13 same3 S18	US-PGPUB; USPAT	ADJ	ON	2013/12/13 16:47
S20	110055	(polic$3 or rule$1) near20 (violat$3 or break$3 or infract$3 or compl$5 or conform$3)	US-PGPUB; USPAT	ADJ	ON	2013/12/13 16:50
S21	1750	(gather$3 or collect$3) near20 (status or state) near20 (((subscriber or mobile or wireless) adj1 (station or device)) or ((user or subscriber) adj1 equipment) or "MS" or "UE" or "MA")	US-PGPUB; USPAT	ADJ	ON	2013/12/13 16:54
S22	31	S20 same3 S21	US-PGPUB; USPAT	ADJ	ON	2013/12/13 16:55
S23	2	S3 and S22	US-PGPUB; USPAT	ADJ	ON	2013/12/13 16:55
S24	2	"20120151041"	US-PGPUB; USPAT	ADJ	ON	2013/12/13 16:57
S25	2	S4 and S22	US-PGPUB; USPAT	ADJ	ON	2013/12/13 16:57
S26	1	S6 and S22	US-PGPUB; USPAT	ADJ	ON	2013/12/13 16:58
S27	1	S7 and S22	US-PGPUB; USPAT	ADJ	ON	2013/12/13 16:58
S28	1	S8 and S22	US-PGPUB; USPAT	ADJ	ON	2013/12/13 16:59
S29	0	S9 and S22	US-PGPUB; USPAT	ADJ	ON	2013/12/13 16:59
S30	0	S10 and S22	US-PGPUB; USPAT	ADJ	ON	2013/12/13 16:59
S31	0	S11 and S22	US-PGPUB; USPAT	ADJ	ON	2013/12/13 16:59
S32	0	S12 and S22	US-PGPUB; USPAT	ADJ	ON	2013/12/13 16:59
S33	3	((JATIN) near2 (MALIK)).INV.	US-PGPUB; USPAT	ADJ	ON	2013/12/13 18:01
S34	3	((RATNESH) near2 (SINGH)).INV.	US-PGPUB; USPAT	ADJ	ON	2013/12/13 18:01

Petitioner Ex 1002, p. 484
Zimperium v. Taasera, IPR2024-00007

S35	1	((RAJAKUMAR) near2 (BOPALLI)).INV.	US-PGPUB; USPAT	ADJ	ON	2013/12/13 18:01
S36	1	S33 and S34 and S35	US-PGPUB; USPAT	ADJ	ON	2013/12/13 18:01
S37	1	S33 and ((status adj1 information) and gathering and initiating).clm.	US-PGPUB; USPAT	ADJ	ON	2013/12/13 18:02
S38	1	S34 and ((status adj1 information) and gathering and initiating).clm.	US-PGPUB; USPAT	ADJ	ON	2013/12/13 18:02
S39	1	S33 and (status and information and gathering and initiating).clm.	US-PGPUB; USPAT	ADJ	ON	2013/12/13 18:03
S40	1	S34 and (status and information and gathering and initiating).clm.	US-PGPUB; USPAT	ADJ	ON	2013/12/13 18:03
S41	2204	(polic$3 or rule$1) near20 (violat$3 or break$3 or infract$3 or compl$5 or conform$3)	FPRS; EPO; JPO	ADJ	ON	2013/12/13 18:05
S42	238	(gather$3 or collect$3) near20 (status or state) near20 (((subscriber or mobile or wireless) adj1 (station or device)) or ((user or subscriber) adj1 equipment) or "MS" or "UE" or "MA")	FPRS; EPO; JPO	ADJ	ON	2013/12/13 18:05
S43	0	S41 same3 S42	FPRS; EPO; JPO	ADJ	ON	2013/12/13 18:05
S44	0	S41 and S42	FPRS; EPO; JPO	ADJ	ON	2013/12/13 18:05
S45	33818	(status or state) near20 (((subscriber or mobile or wireless) adj1 (station or device)) or ((user or subscriber) adj1 equipment) or "MS" or "UE" or "MA")	FPRS; EPO; JPO	ADJ	ON	2013/12/13 18:05
S46	8	S41 same3 S45	FPRS; EPO; JPO	ADJ	ON	2013/12/13 18:05
S47	1	"20100242088"	US-PGPUB; USPAT	ADJ	ON	2013/12/16 12:39
S48	2	"20080114862"	US-PGPUB; USPAT	ADJ	ON	2013/12/16 13:17
S49	1	"20070206552"	US-PGPUB; USPAT	ADJ	ON	2013/12/16 13:53
S50	0	((alert$3 or warning) near4 compliance near20 qos) same3 ((time or grace) adj1 period)	US-PGPUB; USPAT	ADJ	ON	2013/12/16 14:14
S51	0	((alert$3 or warning) near20 compliance near20 qos) same3 ((time or grace) adj1 period)	US-PGPUB; USPAT	ADJ	ON	2013/12/16 14:14
S52	3	((alert$3 or warning) near20 qos) same3 ((time or grace) adj1 period)	US-PGPUB; USPAT	ADJ	ON	2013/12/16 14:14
S53	1	"20070266422"	US-PGPUB; USPAT	ADJ	ON	2013/12/16 14:20

Petitioner Ex 1002, p. 485
Zimperium v. Taasera, IPR2024-00007

S54	1894	((policy or policies or rule$1) near3 (violation or conform$3 or enforc$5)) near20 (corporat$3 or enterprise)	US-PGPUB; USPAT	ADJ	ON	2014/09/04 19:49
S55	63128	(data$1store or database or (data adj1 store)) near20 (policies or rules)	US-PGPUB; USPAT	ADJ	ON	2014/09/04 19:51
S56	116338	(user or client) near20 access near20 (permission$1 or request$3)	US-PGPUB; USPAT	ADJ	ON	2014/09/04 19:52
S57	127	S54 same3 S55 same3 S56	US-PGPUB; USPAT	ADJ	ON	2014/09/04 19:52
S58	46591	709/223$	US-PGPUB; USPAT	ADJ	ON	2014/09/04 19:52
S59	48367	709/224$	US-PGPUB; USPAT	ADJ	ON	2014/09/04 19:52
S60	8	S57 and S58	US-PGPUB; USPAT	ADJ	ON	2014/09/04 19:52
S61	14	S57 and S59	US-PGPUB; USPAT	ADJ	ON	2014/09/04 19:52
S62	0	S57 and (response near20 update$1 near20 (rule$1 or polic$3))	US-PGPUB; USPAT	ADJ	ON	2014/09/04 19:55
S63	95	S57 and (update$1 near20 (rule$1 or polic$3))	US-PGPUB; USPAT	ADJ	ON	2014/09/04 19:56
S64	6	S63 and S58	US-PGPUB; USPAT	ADJ	ON	2014/09/04 19:56
S65	12	S63 and S59	US-PGPUB; USPAT	ADJ	ON	2014/09/04 19:56
S66	2	"20030115322"	US-PGPUB; USPAT	ADJ	ON	2014/09/04 19:58
S67	3	((Jatin) near2 (MALIK)).INV.	US-PGPUB; USPAT	ADJ	ON	2014/09/04 19:59
S68	3	((Ratnesh) near2 (SINGH)).INV.	US-PGPUB; USPAT	ADJ	ON	2014/09/04 19:59
S69	1	((Rajakumar) near2 (BOPALLI)).INV.	US-PGPUB; USPAT	ADJ	ON	2014/09/04 19:59
S70	1	S67 and S68 and S69	US-PGPUB; USPAT	ADJ	ON	2014/09/04 19:59
S71	1	S67 and (rules and database and server).clm.	US-PGPUB; USPAT	ADJ	ON	2014/09/04 20:01
S72	2	S68 and (rules and database and server).clm.	US-PGPUB; USPAT	ADJ	ON	2014/09/04 20:01

Petitioner Ex 1002, p. 486
Zimperium v. Taasera, IPR2024-00007

S73	1	S69 and (rules and database and server).clm.	US-PGPUB; USPAT	ADJ	ON	2014/09/04 20:01
S74	49	((policy or policies or rule$1) near3 (violation or conform$3 or enforc$5)) near20 (corporat$3 or enterprise)	FPRS; EPO; JPO	ADJ	ON	2014/09/04 20:02
S75	5071	(data$1store or database or (data adj1 store)) near20 (policies or rules)	FPRS; EPO; JPO	ADJ	ON	2014/09/04 20:02
S76	16773	(user or client) near20 access near20 (permission$1 or request$3)	FPRS; EPO; JPO	ADJ	ON	2014/09/04 20:02
S77	0	S74 and S75 and S76	FPRS; EPO; JPO	ADJ	ON	2014/09/04 20:03
S78	2	S74 and S75	FPRS; EPO; JPO	ADJ	ON	2014/09/04 20:03
S79	0	S74 and S76	FPRS; EPO; JPO	ADJ	ON	2014/09/04 20:03
S80	113	S75 and S76	FPRS; EPO; JPO	ADJ	ON	2014/09/04 20:03
S81	1158	H04L41/0816.cpc.	US-PGPUB; USPAT	ADJ	ON	2014/09/04 20:04
S82	4025	H04L43/0817.cpc.	US-PGPUB; USPAT	ADJ	ON	2014/09/04 20:04
S83	2946	H04L41/0893.cpc.	US-PGPUB; USPAT	ADJ	ON	2014/09/04 20:04
S84	36	H04L41/0618.cpc.	US-PGPUB; USPAT	ADJ	ON	2014/09/04 20:04
S85	646	455/26.1$	US-PGPUB; USPAT	ADJ	ON	2014/09/04 20:04
S86	3960	455/425$	US-PGPUB; USPAT	ADJ	ON	2014/09/04 20:05
S87	4582	455/456.5$	US-PGPUB; USPAT	ADJ	ON	2014/09/04 20:05
S88	2	(gather$3 or collect$3 or captur$3) near20 ((status or state) adj1 (information or data)) near20 (operat$3 near (state or status)) near20 (((mobile or user or portable) adj1 (handset or device or equipment)) or ue)	US-PGPUB; USPAT	ADJ	ON	2015/02/10 16:35
S89	2032	(gather$3 or collect$3 or captur$3) near20 ((location or status or state) adj1 (information or data)) near20 (((mobile or user or portable) adj1 (handset or device or equipment)) or ue or mn)	US-PGPUB; USPAT	ADJ	ON	2015/02/10 17:19
S90	3520	(corporat$3 or organization) near20 (polic$3 or rule$1) near20 (enforc$3 or compliance)	US-PGPUB; USPAT	ADJ	ON	2015/02/10 18:09
S91	2198	(gather$3 or collect$3 or captur$3) near20 ((location or status or state or configuration) adj1 (information or	US-PGPUB; USPAT	ADJ	ON	2015/02/10 18:10

Petitioner Ex 1002, p. 487
Zimperium v. Taasera, IPR2024-00007

		data)) near20 (((mobile or user or portable) adj1 (handset or device or equipment)) or ue or mn)				
S92	174	(vary$3 or differ$3) near10 (mobile adj1 ("OS" or (operating adj1 system)))	US-PGPUB; USPAT	ADJ	ON	2015/02/10 18:12
S93	0	(uniform$2 or evenly) near20 appl$4 near20 (rule$1 or polic$3) near20 (mobile adj1 ("OS" or (operating adj1 system)))	US-PGPUB; USPAT	ADJ	ON	2015/02/10 18:14
S94	0	(uniform$2 or evenly) near20 (rule$1 or polic$3) near20 (mobile adj1 ("OS" or (operating adj1 system)))	US-PGPUB; USPAT	ADJ	ON	2015/02/10 18:14
S95	1	S91 same3 S92	US-PGPUB; USPAT	ADJ	ON	2015/02/10 18:14
S96	1	S90 and S91 and S92	US-PGPUB; USPAT	ADJ	ON	2015/02/10 18:15
S97	1	S90 same3 S91	US-PGPUB; USPAT	ADJ	ON	2015/02/10 18:15
S99	6	S90 and S92	US-PGPUB; USPAT	ADJ	ON	2015/02/10 18:15
S100	3520	(corporat$3 or organization) near20 (polic$3 or rule$1) near20 (enforc$3 or compliance)	US-PGPUB; USPAT	ADJ	ON	2015/02/11 14:53
S101	2198	(gather$3 or collect$3 or captur$3) near20 ((location or status or state or configuration) adj1 (information or data)) near20 (((mobile or user or portable) adj1 (handset or device or equipment)) or ue or mn)	US-PGPUB; USPAT	ADJ	ON	2015/02/11 14:53
S102	30	S100 and S101	US-PGPUB; USPAT	ADJ	ON	2015/02/11 14:53
S103	1329	H04L41/0816.cpc.	US-PGPUB; USPAT	ADJ	ON	2015/02/11 15:48
S104	4229	H04L43/0817.cpc.	US-PGPUB; USPAT	ADJ	ON	2015/02/11 15:48
S105	3217	H04L41/0893.cpc.	US-PGPUB; USPAT	ADJ	ON	2015/02/11 15:48
S106	42	H04L41/0618.cpc.	US-PGPUB; USPAT	ADJ	ON	2015/02/11 15:48
S107	677	455/26.1$	US-PGPUB; USPAT	ADJ	ON	2015/02/11 15:48
S108	4167	455/425$	US-PGPUB; USPAT	ADJ	ON	2015/02/11 15:48
S109	4882	455/456.5$	US-PGPUB; USPAT	ADJ	ON	2015/02/11 15:49

Petitioner Ex 1002, p. 488
Zimperium v. Taasera, IPR2024-00007

S110	42139	(gather$3 or collect$3 or captur$3) near20 ((location or status or state or configuration) adj1 (information or data))	US-PGPUB; USPAT	ADJ	ON	2015/02/11 15:54
S111	3520	(corporat$3 or organization) near20 (polic$3 or rule$1) near20 (enforc$3 or compliance)	US-PGPUB; USPAT	ADJ	ON	2015/02/11 15:54
S112	188	S110 and S111	US-PGPUB; USPAT	ADJ	ON	2015/02/11 15:55
S113	2	S112 and S103	US-PGPUB; USPAT	ADJ	ON	2015/02/11 15:55
S114	3	S112 and S104	US-PGPUB; USPAT	ADJ	ON	2015/02/11 16:00
S115	17	S112 and S105	US-PGPUB; USPAT	ADJ	ON	2015/02/11 16:02
S116	0	S112 and S106	US-PGPUB; USPAT	ADJ	ON	2015/02/11 16:04
S117	0	S112 and S107	US-PGPUB; USPAT	ADJ	ON	2015/02/11 16:04
S118	0	S112 and S108	US-PGPUB; USPAT	ADJ	ON	2015/02/11 16:04
S119	0	S112 and S109	US-PGPUB; USPAT	ADJ	ON	2015/02/11 16:04
S121	174	(vary$3 or differ$3) near10 (mobile adj1 ("OS" or (operating adj1 system)))	US-PGPUB; USPAT	ADJ	ON	2015/02/11 16:05
S122	83	S111 and ((mobile adj1 device adj1 management) or (mdm adj1 system))	US-PGPUB; USPAT	ADJ	ON	2015/02/11 16:06
S123	2	S121 and S122	US-PGPUB; USPAT	ADJ	ON	2015/02/11 16:06
S124	5	"13051519"	US-PGPUB; USPAT	ADJ	ON	2015/02/11 16:28
S125	3	"12178772"	US-PGPUB; USPAT	ADJ	ON	2015/02/11 16:34
S126	3	((Jatin) near2 (MALIK)).INV.	US-PGPUB; USPAT	ADJ	ON	2015/02/11 17:29
S127	3	((Ratnesh) near2 (SINGH)).INV.	US-PGPUB; USPAT	ADJ	ON	2015/02/11 17:29
S128	1	((Rajakumar) near2 (BOPALLI)).INV.	US-PGPUB; USPAT	ADJ	ON	2015/02/11 17:29
S129	1	S126 and S127 and S128	US-PGPUB;	ADJ	ON	2015/02/11 17:29

Petitioner Ex 1002, p. 489
Zimperium v. Taasera, IPR2024-00007

			USPAT			
S130	0	S126 and (mobile adj1 device adj1 management).clm.	US-PGPUB; USPAT	ADJ	ON	2015/02/11 17:29
S131	2	S126 and (mobile adj1 device adj1 management)	US-PGPUB; USPAT	ADJ	ON	2015/02/11 17:30
S132	1	S127 and (mobile adj1 device adj1 management)	US-PGPUB; USPAT	ADJ	ON	2015/02/11 17:30
S133	1	S128 and (mobile adj1 device adj1 management)	US-PGPUB; USPAT	ADJ	ON	2015/02/11 17:31
S145	3520	(corporat$3 or organization) near20 (polic$3 or rule$1) near20 (enforc$3 or compliance)	US-PGPUB; USPAT	ADJ	ON	2015/02/11 17:36
S146	89	(corporat$3 or organization) near20 (polic$3 or rule$1) near20 (enforc$3 or compliance)	FPRS; EPO; JPO	ADJ	ON	2015/02/11 17:47
S147	157	(mobile adj1 device adj1 management)	FPRS; EPO; JPO	ADJ	ON	2015/02/11 17:47
S148	0	S146 same3 S147	FPRS; EPO; JPO	ADJ	ON	2015/02/11 17:47
S149	0	S146 and S147	FPRS; EPO; JPO	ADJ	ON	2015/02/11 17:47
S150	0	(mobile adj1 device adj1 management) same3 (mobile adj1 ("OS" or (operating adj1 system)))	FPRS; EPO; JPO	ADJ	ON	2015/02/11 17:48
S151	0	(mobile adj1 device adj1 management) and (mobile adj1 ("OS" or (operating adj1 system)))	FPRS; EPO; JPO	ADJ	ON	2015/02/11 17:48

2/11/2015 6:01:32 PM
C:\Users\kkatsikis1\Documents\EAST\Workspaces\13540142.wsp

Petitioner Ex 1002, p. 490
Zimperium v. Taasera, IPR2024-00007

OK TO ENTER: /K.K./ 02/11/2015

DOCKET NO.: 130839.02101
Application No.: 13/540,142
Response to Office Action dated: September 8, 2014

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: **Jatin MALIK et al.**

Title: **RULES BASED ACTIONS FOR MOBILE DEVICE MANAGEMENT**

Application No.: **13/540,142** Group Art Unit: **2441**

Filed: **July 2, 2012** Examiner: **Kostas J. Katsikis**

Confirmation: **4198** Filed by EFS on: **February 9, 2015**

Mail Stop AF
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

AMENDMENT AND REQUEST FOR RECONSIDERATION UNDER 35 U.S.C. § 1.116

Sir:

In response to the Office Action mailed on September 8, 2014, Applicants respectfully request reconsideration in light of the:

Listing of the Claims, reflecting current amendments, beginning on page 2; and

Remarks beginning on page 7 of this paper.

EAST Search History

EAST Search History (Interference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S134	0	(gather$3 and server and plurality and rules and mobile and device and operating and system and uniformly and applied and status and information and formatting and regardless and action and compliance and real$1time).clm.	USPAT; UPAD	ADJ	ON	2015/02/11 17:31
S135	0	(gather$3 and server and plurality and rules and mobile and device and operating and system and uniformly and applied and status and information and formatting and regardless and action and compliance and (real adj1 time)).clm.	USPAT; UPAD	ADJ	ON	2015/02/11 17:31
S136	0	(gather$3 and server and plurality and rules and mobile and device and operating and system and uniformly and applied and status and information and formatting and regardless and action and compliance).clm.	USPAT; UPAD	ADJ	ON	2015/02/11 17:32
S137	0	(gather$3 and server and plurality and rules and mobile and device and operating and system and uniformly and applied and status and information and formatting and regardless and action).clm.	USPAT; UPAD	ADJ	ON	2015/02/11 17:32
S138	0	(gather$3 and server and plurality and rules and mobile and device and operating and system and uniformly and applied and status and information and formatting and regardless).clm.	USPAT; UPAD	ADJ	ON	2015/02/11 17:32
S139	0	(gather$3 and server and plurality and rules and mobile and device and operating and system and uniformly and applied and status and information and formatting).clm.	USPAT; UPAD	ADJ	ON	2015/02/11 17:32
S140	0	(gather$3 and server and plurality and rules and mobile and device and operating and system and uniformly and applied and status and information).clm.	USPAT; UPAD	ADJ	ON	2015/02/11 17:32
S141	0	(gather$3 and server and plurality and rules and mobile and device and operating and system and uniformly and applied and status).clm.	USPAT; UPAD	ADJ	ON	2015/02/11 17:32
S142	0	(gather$3 and server and plurality and rules and mobile and device and operating and system and uniformly and applied).clm.	USPAT; UPAD	ADJ	ON	2015/02/11 17:32
S143	0	(gather$3 and server and plurality and rules and mobile and device and operating and system and uniformly).clm.	USPAT; UPAD	ADJ	ON	2015/02/11 17:32
S144	2	(gather$3 and server and plurality and rules and mobile and device and operating and system).clm.	USPAT; UPAD	ADJ	ON	2015/02/11 17:32

Petitioner Ex 1002, p. 492
Zimperium v. Taasera, IPR2024-00007

2/ 11/ 2015 6:01:43 PM
C:\ Users\ kkatsikis1\ Documents\ EAST\ Workspaces\ 13540142.wsp

Petitioner Ex 1002, p. 493
Zimperium v. Taasera, IPR2024-00007

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

BIB DATA SHEET

CONFIRMATION NO. 4198

SERIAL NUMBER	FILING or 371(c) DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
13/540,142	07/02/2012 RULE	709	2441	130839.02101

APPLICANTS

INVENTORS

Jatin MALIK, Bangalore, INDIA;
Ratnesh SINGH, Bangalore, INDIA;
Rajakumar BOPALLI, Bangalore, INDIA;

**** CONTINUING DATA ***************************

This appln claims benefit of 61/503,729 07/01/2011

**** FOREIGN APPLICATIONS ***************************

**** IF REQUIRED, FOREIGN FILING LICENSE GRANTED **** ** SMALL ENTITY **
07/13/2012

Foreign Priority claimed	❑ Yes ☑ No	❑ Met after Allowance	STATE OR COUNTRY	SHEETS DRAWINGS	TOTAL CLAIMS	INDEPENDENT CLAIMS
35 USC 119(a-d) conditions met	❑ Yes ☑ No		INDIA	10	23	3
Verified and Acknowledged	/KOSTAS J KATSIKIS/ Examiner's Signature	Initials				

ADDRESS

Pepper Hamilton LLP
400 Berywn Park
899 Cassatt Road
Berwyn, PA 19312-1183
UNITED STATES

TITLE

RULES BASED ACTIONS FOR MOBILE DEVICE MANAGEMENT

FILING FEE RECEIVED		
685	FEES: Authority has been given in Paper No._____ to charge/credit DEPOSIT ACCOUNT No._____ for following:	❑ All Fees ❑ 1.16 Fees (Filing) ❑ 1.17 Fees (Processing Ext. of time) ❑ 1.18 Fees (Issue) ❑ Other _____ ❑ Credit

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13540142	MALIK ET AL.
	Examiner	Art Unit
	KOSTAS KATSIKIS	2441

CPC- SEARCHED		
Symbol	Date	Examiner
H04L41/0816	12/13/2013 (Updated 9/4/2014) (Further updated 2/11/2015)	KK
H04L43/0817	12/13/2013 (Updated 9/4/2014) (Further updated 2/11/2015)	KK
H04L41/0893	12/13/2013 (Updated 9/4/2014) (Further updated 2/11/2015)	KK
H04L41/0618	12/13/2013 (Updated 9/4/2014) (Further updated 2/11/2015)	KK

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner

/KOSTAS KATSIKIS/ Examiner.Art Unit 2441	/KOSTAS KATSIKIS/ Primary Examiner.Art Unit 2441

US CLASSIFICATION SEARCHED			
Class	**Subclass**	**Date**	**Examiner**
709	223, 224	12/13/2013 (Updated 9/4/2014)	KK
455	26.1, 425, 456.5	12/13/2013 (Updated 9/4/2014) (Further updated 2/11/2015)	KK

SEARCH NOTES		
Search Notes	**Date**	**Examiner**
Examiner conducted thorough EAST search.	12/13/2013 and 12/16/2013 (Updated 9/4/2014) (Further updated 2/10 & 2/11/2015)	KK
EAST (USPAT, US-PGPUB) - see search history printout.	12/13/2013 and 12/16/2013 (Updated 9/4/2014) (Further updated 2/10 & 2/11/2015)	KK
EAST (EPO, JPO, FPRS) - see search history printout.	12/13/2013 (Updated 9/4/2014) (Further updated 2/11/2015)	KK
709/223 (text search - see search history printout).	12/13/2013 (Updated 9/4/2014)	KK
709/224 (text search - see search history printout).	12/13/2013 (Updated 9/4/2014)	KK
H04L41/0816 (text search - see search history printout).	12/13/2013 (Further updated 2/11/2015)	KK
H04L43/0817 (text search - see search history printout).	12/13/2013 (Further updated 2/11/2015)	KK

/KOSTAS KATSIKIS/ Examiner.Art Unit 2441	/KOSTAS KATSIKIS/ Primary Examiner.Art Unit 2441

SEARCH NOTES		
Search Notes	**Date**	**Examiner**
H04L41/0893 (text search - see search history printout).	12/13/2013 (Further updated 2/11/2015)	KK
H04L41/0618 (text search - see search history printout).	12/13/2013 (Further updated 2/11/2015)	KK
Examiner conducted Inventor Name search in EAST.	12/13/2013 (Further updated 2/11/2015)	KK
455/26.1 (text search - see search history printout).	12/13/2013 (Updated 9/4/2014) (Further updated 2/11/2015)	KK
455/425 (text search - see search history printout).	12/13/2013 (Further updated 2/11/2015)	KK
455/456.5 (text search - see search history printout).	12/13/2013 (Further updated 2/11/2015)	KK

INTERFERENCE SEARCH			
US Class/ CPC Symbol	**US Subclass / CPC Group**	**Date**	**Examiner**
	See Interference Search History Printout.	2/11/2015	KK

/KOSTAS KATSIKIS/ Examiner.Art Unit 2441	/KOSTAS KATSIKIS/ Primary Examiner.Art Unit 2441

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: Mail **Mail Stop ISSUE FEE**
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

PEPPER HAMILTON LLP
3000 Two Logan Square
Eighteenth and Arch Streets
Philadelphia, Pennsylvania 19103-2799

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

(Depositor's name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/540,142	07/02/2012	Jatin Malik	130839.02101	4198

TITLE OF INVENTION: RULES BASED ACTIONS FOR MOBILE DEVICE MANAGEMENT

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	UNDISCOUNTED	$960.00			$960.00	05/23/2015

EXAMINER	ART UNIT	CLASS-SUBCLASS
K. J. Katsikis	2441	709-223

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).
- [ ] Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.
- [ ] "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list
(1) The names of up to 3 registered patent attorneys or agents OR, alternatively,
(2) The name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1 Pepper Hamilton LLP
2
3

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE: FIBERLINK COMMUNICATIONS CORPORATION

(B) RESIDENCE: (CITY and STATE OR COUNTRY): BLUE BELL, PENNSYLVANIA

Please check the appropriate assignee category or categories (will not be printed on the patent) : [ ] Individual [X] Corporation or other private group entity [ ] Government

4a. The following fee(s) are submitted:
- [X] Issue Fee
- [ ] Publication Fee (No small entity discount permitted)
- [ ] Advance Order - # of Copies _____

4b. Payment of Fee(s): **(Please first reapply any previously paid issue fee shown above)**
- [ ] A check is enclosed.
- [X] Payment by credit card. Form PTO-2038 is attached.
- [X] The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment, to Deposit Account Number 50-0436 (enclose an extra copy of this form).

5. **Change in Entity Status** (from status indicated above)
- [ ] Applicant certifying micro entity status. See 37 CFR 1.29 — NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.
- [ ] Applicant asserting small entity status. See 37 CFR 1.27 — NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.
- [X] Applicant changing to regular undiscounted fee status. — NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature /Michael K. Jones, Reg. #41100/ Date May 22, 2015

Typed or printed name Michael K. Jones Registration No. 41,100

Petitioner Ex 1002, p. 498
Zimperium v. Taasera, IPR2024-00007

Electronic Patent Application Fee Transmittal

Application Number:	13540142
Filing Date:	02-Jul-2012
Title of Invention:	RULES BASED ACTIONS FOR MOBILE DEVICE MANAGEMENT
First Named Inventor/Applicant Name:	Jatin MALIK
Filer:	Michael Kenneth Jones/Sara Harvell
Attorney Docket Number:	130839.02101

Filed as Large Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Utility Appl Issue Fee	1501	1	960	960

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension-of-Time:				
Miscellaneous:				
		Total in USD ($)		**960**

Electronic Acknowledgement Receipt

EFS ID:	22422869
Application Number:	13540142
International Application Number:	
Confirmation Number:	4198
Title of Invention:	RULES BASED ACTIONS FOR MOBILE DEVICE MANAGEMENT
First Named Inventor/Applicant Name:	Jatin MALIK
Customer Number:	86308
Filer:	Michael Kenneth Jones/Sara Harvell
Filer Authorized By:	Michael Kenneth Jones
Attorney Docket Number:	130839.02101
Receipt Date:	22-MAY-2015
Filing Date:	02-JUL-2012
Time Stamp:	10:50:57
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	$960
RAM confirmation Number	8148
Deposit Account	500436
Authorized User	JONES, MICHAEL K.
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees) Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)	

Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Notification of loss of entitlement to small entity status	2101EntityStatus.pdf	72497 420381c547ecedf9ab6477564b20ba93c05b40d6	no	1
Warnings:					
Information:					
2	Issue Fee Payment (PTO-85B)	2101IssueFeeTransmittal.pdf	107244 af95aad4c283e0b5ed313cfb19839e4562f2868e	no	1
Warnings:					
Information:					
3	Fee Worksheet (SB06)	fee-info.pdf	30651 bca1b5436af6a9f9dfdb975817175 3f6c5cafd2b	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	210392		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

DOCKET NO.: 130839.02101
Application No.: 13/540,142

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: **Jatin Malik et al.**

Title: **RULES BASED ACTIONS FOR MOBILE DEVICE MANAGEMENT**

Application No.: **13/540,142** Group Art Unit: **2441**

Filed: **July 2, 2012** Examiner: **K. J. Katsikis**

Confirmation No.: **4198** Filed by EFS on: **May 22, 2015**

Mail Stop Issue Fee
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

NOTIFICATION OF LOSS OF SMALL ENTITY STATUS UNDER 37 C.F.R. §1.27(g)(2)

Sir:

Notification under 37 C.F.R. §1.27(g)(2) is hereby given that small entity status is no longer appropriate for the above-identified application.

The Issue Fee is being paid concurrently herewith at the large entity rate.

Respectfully Submitted

By: /Michael K. Jones, Reg. No. 41100/
Michael K. Jones
Registration No. 41,100

Dated: **May 22, 2015**
PEPPER HAMILTON LLP
3000 Two Logan Square
Eighteenth and Arch Street
Philadelphia, PA 19103-279
Telephone: (215) 981-4405
Facsimile: (610) 640-7835

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	ISSUE DATE	PATENT NO.	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/540,142	06/30/2015	9071518	130839.02101	4198

86308 7590 06/10/2015

Pepper Hamilton LLP
400 Berywn Park
899 Cassatt Road
Berwyn, PA 19312-1183

ISSUE NOTIFICATION

The projected patent number and issue date are specified above.

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(application filed on or after May 29, 2000)

The Patent Term Adjustment is 0 day(s). Any patent to issue from the above-identified application will include an indication of the adjustment on the front page.

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (http://pair.uspto.gov).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Application Assistance Unit (AAU) of the Office of Data Management (ODM) at (571)-272-4200.

APPLICANT(s) (Please see PAIR WEB site http://pair.uspto.gov for additional applicants):

Jatin MALIK, Bangalore, INDIA;
Ratnesh SINGH, Bangalore, INDIA;
Rajakumar BOPALLI, Bangalore, INDIA;

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The USA offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to encourage and facilitate business investment. To learn more about why the USA is the best country in the world to develop technology, manufacture products, and grow your business, visit SelectUSA.gov.

OPAP
OCT 25 2018
PATENT & TRADEMARK OFFICE

IFW

PTO/SB/81A (12-08)
Approved for use through 01/31/2018. OMB 0651-0035
U.S. Patent and Trademark Office, U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995 no persons are required to respond to a collection of information unless it displays a valid OMB control number

PATENT - POWER OF ATTORNEY OR REVOCATION OF POWER OF ATTORNEY WITH A NEW POWER OF ATTORNEY AND CHANGE OF CORRESPONDENCE ADDRESS

Patent Number	9,071,518 / 13/540142
Issue Date	June 30, 2015
First Named Inventor	Jatin Malik
Title	RULES BASED ACTIONS FOR MOBILE DEVICE MANAGEMENT
Attorney Docket No.	AUS920145107US2

I hereby revoke all previous powers of attorney given in the above-identified patent.

☐ A Power of Attorney is submitted herewith.

OR

☒ I hereby appoint Practitioner(s) associated with the Customer Number identified in the box at right as my/our attorney(s) or agent(s) with respect to the patent identified above, and to transact all business in the United States Patent and Trademark Office connected therewith. **26502**

OR

☐ I hereby appoint Practitioner(s) named below as my/our attorney(s) or agent(s) with respect to the patent identified above, and to transact all business in the United States Patent and Trademark Office connected therewith:

Practitioner(s) Name	Registration Number

Please recognize or change the correspondence address for the above-identified patent to

☒ The address associated with the above-identified Customer Number.

OR

☐ The address associated with the Customer Number identified in the box at right:

OR

☐ Firm or Individual Name					
Address					
City		State		Zip	
Country					
Telephone		Email			

I am the

☐ Inventor, having ownership of the patent.

OR

☒ Patent owner.

Statement under 37 CFR 3.73(b) (Form PTO/SB/96) submitted herewith or filed on _____

SIGNATURE of Inventor or Patent Owner

Signature	/Timothy M. Farrell/	Date	10/24/2018
Name	Timothy M. Farrell, Reg. No. 37,321	Telephone	(801) 763-7150
Title and Company	Counsel, International Business Machines Corporation		

NOTE Signatures of all the inventors or patent owners of the entire interest or their representative(s) are required. If more than one signature is required, submit multiple forms, check the box below, and identify the total number of forms submitted in the blank below

☒ A total of 1 forms are submitted

This collection of information is required by 37 CFR 1.31, 1.32, and 1.33. The information is required to obtain or retain a benefit by the public, which is to update (and by the USPTO to process) the file of a patent or reexamination proceeding. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 15 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

OPAP AKIMA-1 OCT 25 2018 PATENT & TRADEMARK OFFICE

PTO/SB/96 (07-09)
Approved for use through 07/31/2012 OMB 0651-0031
U S Patent and Trademark Office; U.S DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number

STATEMENT UNDER 37 CFR 3.73(b)

Applicant/Patent Owner: International Business Machines Corporation

Application No /Patent No 9,071,518 Filed/Issue Date June 30, 2015

Titled: RULES BASED ACTIONS FOR MOBILE DEVICE MANAGEMENT

International Business Machines Corporation, a corporation
(Name of Assignee) (Type of Assignee, e.g., corporation, partnership, university, government agency, etc.

states that it is

1. ☒ the assignee of the entire right, title, and interest in;

2. ☐ an assignee of less than the entire right, title, and interest in (The extent (by percentage) of its ownership interest is _____ %), or

3 ☐ the assignee of an undivided interest in the entirety of (a complete assignment from one of the joint inventors was made)

the patent application/patent identified above, by virtue of either:

A. ☐ An assignment from the inventor(s) of the patent application/patent identified above The assignment was recorded in the United States Patent and Trademark Office at Reel _____, Frame _____, or for which a copy therefore is attached

OR

B ☒ A chain of title from the inventor(s), of the patent application/patent identified above, to the current assignee as follows

1 From Jatin Malik; Ratnesh Singh; Rajakumar Bopalli To: Fiberlink Communications Corporation

The document was recorded in the United States Patent and Trademark Office at
Reel 028981, Frame 0607, or for which a copy thereof is attached

2 From Fiberlink Communications Corporation To International Business Machines Corporation

The document was recorded in the United States Patent and Trademark Office at
Reel 039001, Frame 0462, or for which a copy thereof is attached

3 From _____ To: _____

The document was recorded in the United States Patent and Trademark Office at
Reel _____, Frame _____, or for which a copy thereof is attached

☐ Additional documents in the chain of title are listed on a supplemental sheet(s)

☒ As required by 37 CFR 3.73(b)(1)(i), the documentary evidence of the chain of title from the original owner to the assignee was, or concurrently is being, submitted for recordation pursuant to 37 CFR 3 11

[NOTE A separate copy (*i.e.*, a true copy of the original assignment document(s)) must be submitted to Assignment Division in accordance with 37 CFR Part 3, to record the assignment in the records of the USPTO See MPEP 302 08]

The undersigned (whose title is supplied below) is authorized to act on behalf of the assignee

Signature 10/24/2018 Date

Timothy M. Farrell, Reg. No 37,321 Counsel
Printed or Typed Name Title

This collection of information is required by 37 CFR 3 73(b) The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U S C 122 and 37 CFR 1 11 and 1 14 This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U S Department of Commerce, P O Box 1450, Alexandria, VA 22313-1450 DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
13/540,142	07/02/2012	Jatin MALIK	AUS920145107US2

CONFIRMATION NO. 4198

POA ACCEPTANCE LETTER

26502
IBM CORPORATION
IPLAW SHCB/256-3
1701 NORTH STREET
ENDICOTT, NY 13760

OC000000103664731

Date Mailed: 11/08/2018

NOTICE OF ACCEPTANCE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 10/25/2018.

The Power of Attorney in this application is accepted. Correspondence in this application will be mailed to the above address as provided by 37 CFR 1.33.

Questions about the contents of this notice and the requirements it sets forth should be directed to the Office of Data Management, Application Assistance Unit, at **(571) 272-4000** or **(571) 272-4200** or **1-888-786-0101**.

/ldvan/

Petitioner Ex 1002, p. 507
Zimperium v. Taasera, IPR2024-00007

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
13/540,142	07/02/2012	Jatin MALIK	AUS920145107US2

CONFIRMATION NO. 4198

86308
Pepper Hamilton LLP
400 Berywn Park
899 Cassatt Road
Berwyn, PA 19312-1183

POWER OF ATTORNEY NOTICE

OC000000103664711

Date Mailed: 11/08/2018

NOTICE REGARDING CHANGE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 10/25/2018.

- The Power of Attorney to you in this application has been revoked by the assignee who has intervened as provided by 37 CFR 3.71. Future correspondence will be mailed to the new address of record(37 CFR 1.33).

Questions about the contents of this notice and the requirements it sets forth should be directed to the Office of Data Management, Application Assistance Unit, at **(571) 272-4000** or **(571) 272-4200** or **1-888-786-0101**.

/ldvan/

AMENDED

AO 120 (Rev. 08/10)

TO:	REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK
Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court for the Eastern District of Texas, Marshall Division on the following

☐ Trademarks or ☑ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
2:22-cv-00063	7/5/2022	for the Eastern District of Texas, Marshall Division

PLAINTIFF	DEFENDANT
TAASERA LICENSING LLC	CHECK POINT SOFTWARE TECHNOLOGIES LTD.

	PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1	6,842,796	1/11/2005	Taasera Licensing LLC
2	8,327,441	12/4/2012	Taasera Licensing LLC
3	8,955,038	2/10/2015	Taasera Licensing LLC
4	8,990,948	3/24/2015	Taasera Licensing LLC
5	9,092,616	7/28/2015	Taasera Licensing LLC

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1		
2		
3		
4		
5		

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE

Copy 1—Upon initiation of action, mail this copy to Director Copy 3—Upon termination of action, mail this copy to Director
Copy 2—Upon filing document adding patent(s), mail this copy to Director Copy 4—Case file copy

Petitioner Ex 1002, p. 509
Zimperium v. Taasera, IPR2024-00007

AMENDED

AO 120 (Rev. 08/10)

TO:	Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court for the Eastern District of Texas, Marshall Division on the following

☐ Trademarks or ☑ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
2:22-cv-00063	7/5/2022	for the Eastern District of Texas, Marshall Division

PLAINTIFF	DEFENDANT
TAASERA LICENSING LLC	CHECK POINT SOFTWARE TECHNOLOGIES LTD.

	PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1	9,608,997	3/28/2017	Taasera Licensing LLC
2	9,923,918	3/20/2018	Taasera Licensing LLC
3	9,071,518	6/30/2015	Taasera Licensing LLC
4			
5			

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1		
2		
3		
4		
5		

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE

Copy 1—Upon initiation of action, mail this copy to Director Copy 3—Upon termination of action, mail this copy to Director
Copy 2—Upon filing document adding patent(s), mail this copy to Director Copy 4—Case file copy

Petitioner Ex 1002, p. 510
Zimperium v. Taasera, IPR2024-00007

AMENDED

AO 120 (Rev. 08/10)

TO:	REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK
Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court for the Eastern District of Texas, Marshall Division on the following

☐ Trademarks or ☑ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
2:22-cv-00063	7/5/2022	for the Eastern District of Texas, Marshall Division

PLAINTIFF	DEFENDANT
TAASERA LICENSING LLC	CHECK POINT SOFTWARE TECHNOLOGIES LTD.

	PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1	9,608,997	3/28/2017	Taasera Licensing LLC
2	9,923,918	3/20/2018	Taasera Licensing LLC
3	9,071,518	6/30/2015	Taasera Licensing LLC
4			
5			

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1		
2		
3		
4		
5		

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT		
CLERK	(BY) DEPUTY CLERK	DATE

Copy 1—Upon initiation of action, mail this copy to Director **Copy 3—Upon termination of action, mail this copy to Director**
Copy 2—Upon filing document adding patent(s), mail this copy to Director **Copy 4—Case file copy**

Petitioner Ex 1002, p. 511
Zimperium v. Taasera, IPR2024-00007

AO 120 (Rev. 08/10)

TO:	REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK
Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court for the Eastern District of Texas, Marshall Division on the following

☐ Trademarks or ☑ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
2:22-cv-00427	10/31/2022	for the Eastern District of Texas, Marshall Division

PLAINTIFF	DEFENDANT
TAASERA LICENSING LLC	MUSARUBRA US LLC, D/B/A TRELLIX

	PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1	7,673,137	3/2/2010	Taasera Licensing LLC
2	8,327,441	12/4/2012	Taasera Licensing LLC
3	8,850,517	9/30/2014	Taasera Licensing LLC
4	8,955,038	2/10/2015	Taasera Licensing LLC
5	8,990,948	3/24/2015	Taasera Licensing LLC

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1		
2		
3		
4		
5		

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE

Copy 1—Upon initiation of action, mail this copy to Director Copy 3—Upon termination of action, mail this copy to Director
Copy 2—Upon filing document adding patent(s), mail this copy to Director Copy 4—Case file copy

Petitioner Ex 1002, p. 512
Zimperium v. Taasera, IPR2024-00007

AO 120 (Rev. 08/10)

TO:	REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK
Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court for the Eastern District of Texas, Marshall Division on the following

☐ Trademarks or ☑ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
2:22-cv-00427	10/31/2022	for the Eastern District of Texas, Marshall Division

PLAINTIFF	DEFENDANT
TAASERA LICENSING LLC	MUSARUBRA US LLC, D/B/A TRELLIX

	PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1	9,071,518	6/30/2015	Taasera Licensing LLC
2	9,092,616	7/28/2015	Taasera Licensing LLC
3	9,608,997	3/28/2017	Taasera Licensing LLC
4	9,923,918	3/20/2018	Taasera Licensing LLC
5			

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1		
2		
3		
4		
5		

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE

Copy 1—Upon initiation of action, mail this copy to Director Copy 3—Upon termination of action, mail this copy to Director
Copy 2—Upon filing document adding patent(s), mail this copy to Director Copy 4—Case file copy

Petitioner Ex 1002, p. 513
Zimperium v. Taasera, IPR2024-00007