



IT Best Practices: Mobile Policies and Processes for Employee- owned Smartphones

By: Maribel Lopez, Principal Analyst

April 2010

Mobile Growth Will Lead to Employee-Owned Smartphones In The Enterprise

Mobility has moved from a luxury to mainstream globally with worldwide subscribers reaching over 4.5 billion at the end of 2009. The availability of unlimited data and text messaging plans has pushed consumer mobile usage beyond voice to text messaging, multimedia applications and Internet access. Today's smartphones offer a wide range of functionality, device types, as well as prices to fit every budget. Sleeker designs, richer multimedia applications and compelling carrier promotions are encouraging consumers to buy smartphones as they upgrade. As a result, over 165 million smartphones were shipped worldwide in 2009.

Today's smartphones aren't just for business users. Consumers are using smartphones for entertainment as well as productivity tools such as email and calendar. Employees are buying smartphones and asking IT to connect these personal devices to the network. This is creating a new category of endpoints that IT needs to manage and secure. These devices may be called one of several names including employee-liable, employee-owned, personal-liable, individually-liable, as well as individually-owned smartphones. For this report, we will refer to this category of user as employee-owned smartphones. Lopez Research defines employee-owned smartphones as:

Mobile devices that are used for both personal and corporate voice, data and messaging use that are purchased and owned by an employee. These devices have a monthly plan that is paid for by the individual, but may or may not be expensed back to the company.

Traditionally, IT only supported corporate-liable devices, which are mobile devices where the company pays for the device and its associated monthly plan. To manage support costs and telecom expense, corporate-liable devices were only given to a small percentage of the workforce. Companies also prohibited the use of personal devices to minimize security risks. While many companies have a policy prohibiting access to company data on personal devices, employee-owned smartphones are making inroads into the company regardless of IT's policy. There are many reasons why employees want to use personal devices. In some cases, employees are bringing in their own devices as a response to a strict corporate lock down. In other cases, employees may want access to mobility and the corporation won't fund it. Even employees that have a corporate-liable smartphone may only want to carry a single device – their personal smartphone. If IT diligently secures access to email and business applications, employees are working around these restrictions by forwarding email to their personal email accounts. The growing popularity of smartphones means IT can't ignore the issue any longer. A company can either choose a restrictive policy that creates opportunity for a security breach or it can put in place policies and controls that allow IT to embrace employee-owned smartphones.

IT Needs To Revise Policy and Processes For Employee-owned Mobility

Many firms already have policies and management procedures to support corporate-liable devices, however these policies need to be revised to account for employee-owned smartphones. While there are numerous areas in a mobile policy, the inclusion of employee-owned devices changes at least 10 sections of a company's security and management policy (see Figure 1). Other policy categories may also need to be changed depending on the industry. IT should review these areas and create new guidelines within each of these sections. The following sections offer guidelines for enabling the use of employee-owned devices.

Who is eligible and what data can be accessed? How will applications be delivered?

The policy should define the criteria for what types of employee can access the network with a personal device. Examples of criteria that companies are using include job title, job function and the number of hours worked. The policy should also define what applications and services can be accessed over what type of device. For example, a firm may allow employee-owned smartphones to access only email while corporate-liable smartphones can access email as well as other business applications such as CRM and sales automation.

In the corporate-liable world, IT selected which applications had access to the network. Many firms take a similar approach
April 2010 IT Best Practices: Mobile Policies and Processes to Support Employee-owned Smartphones 2

with employee-owned devices and forbid any application downloads. In the case of employee-owned phones, IT should expect and accept that users will want to use applications like games and social networks on their handhelds. To deliver this flexibility while maintaining a secure environment, IT should embrace platforms and/or security solutions that will limit the resources that applications can access. It should also consider adding a white-list/blacklist content-filtering approach for mobile browsers.

Figure 1. Guidelines for Policy Changes to Support Employee-owned Devices

	Policy Guideline	Areas to address
1	Who is eligible?	What type of employees can access the company's network (e.g., certain job titles, roles, etc.)?
2	What data and services can be accessed?	Should the company allow employee-owned devices to access email, a subset of business applications, all available mobile applications or only business applications that are web-enabled?
3	How will applications and services be delivered?	Does the solution require a desktop client to deliver applications or will applications be downloaded from a site? Can IT push applications to the device over the air?
4	What does the company pay for?	Will the company reimburse the entire monthly cost, a fixed stipend, the cost of the data plan or a percentage of the voice and data plan?
5	Which operating systems and devices?	How many platforms will IT support (e.g., Android, BlackBerry, iPhone OS, Linux, Symbian, Windows Mobile, etc.)?
6	How is the device secured?	What security measures will be enforced on employee-owned devices (i.e., passwords, device encryption, remote lock, wipe, etc.)?
7	How is the device managed?	Will the device be maintained over the air or through syncing with a desktop or web application?
8	What support is provided?	Will IT assist in the first time device set-up? Will IT provide first or second tier support?
9	What are the privacy issues?	Is the employee's data private? What is the treatment of an employee's data (i.e., is it stored? How can it be used? etc.)?
10	What are the legal concerns?	Is use of a personal phone by non-exempt employees considered overtime? What is my responsibility as a corporation if I discover the employee is involved in illegal activity that isn't related to the corporation?

Once IT has defined who can access the network and what applications a user can access, IT must define the process for how users will access business applications. Will employees go to a secure web portal to download an application? Will the application link be delivered to the user's device over the air? Or will IT need to deploy a desktop application to support application downloads? The procedure for accessing applications may also differ from one type of mobile smartphone to another. For example, RIM's BES allows over the air activation and push of applications while the iPhone requires Active-
 April 2010 IT Best Practices: Mobile Policies and Processes to Support Employee-owned Smartphones **3**

Sync. IT may decide it will only support certain handhelds based on the process of downloading applications to a specific device type.

What does the company pay for?

Unlike corporate-liable devices, the employee purchases and owns the device. If the employee wishes to use their personal device for work-related activities, IT must have a policy that outlines what, if any, portion of the monthly fees that the firm will pay. The greater the business need for mobile voice and data, the more likely the firm is to pay at least part of the monthly fees. A fixed stipend approach is often considered for reimbursement. The move to flat rate voice and data plans has made it easier to set stipend limits. Many companies choose a stipend amount that pays for the data portion of the bill. When determining a stipend, firms must adjust the amounts to equal the variances in data rates across the globe. If the employee has no need to access corporate data, the firm may choose to provide access to the network without any reimbursement. Policies should minimize the amount of time accounting must spend to process reimbursements by setting fixed dollar amounts or tiers of reimbursement expenses.

What mobile operating systems and devices will the company support?

Traditionally, a company would standardize on a small number of smartphones and usually no more than two operating systems to minimize support issues within corporate-liable device programs. But employees want to use whatever device they own. The company needs a strategy that enables choice while minimizing chaos. IT must design a policy that addresses what types of operating systems IT will support (e.g., Android, iPhone OS, Linux, RIM's BlackBerry, Symbian, Windows Mobile, etc.). Given the rapidly changing mobile environment, the policy must also specify what version of the operating system IT will support. For example, Google has released four versions of its Android OS within the past year. This is particularly important as certain corporate applications may only work with certain versions of an operating system.

IT should also define what device characteristics are required and restricted. For example, certain companies restrict the use of camera phones in the building while other firms have applications that may require a certain processing capability and/or removable media for data storage. Also, IT should set a standard for how much free memory must be on the device to support software updates. Firms that want to run mobile voice and data over the wireless LAN may encourage employees to get a device that has Wi-Fi.

How is the device secured and managed?

Businesses are losing control of customer and corporate data as employee-owned smartphones enter the enterprise. Employees accept a predefined set of security and management policies when they are given a corporate-liable smartphone, but employees don't expect the same level of security to be applied when they own the device. IT must create a new policy that states employee-owned smartphones need to be treated the same as any other endpoint on the corporate network. Firms need a comprehensive mobile policy that leverages existing security standards to limit data loss and theft from malicious code that exploits vulnerabilities in mobile technologies such as Bluetooth, SMS, and mobile operating systems (OSs).

Employees must be willing to allow IT to add additional security and management software to the device if necessary. If an employee wants to connect their own device to the network, the employee must be willing to accept the corporate policy and understand its consequences. For example, if the employee loses the device, IT will wipe all data from the device. During the data wipe, the employee could lose personal data such as address book contacts, photos and applications. Employees that want network access must be willing to accept that they could lose personal data and that the company won't be held liable for any lost data. With this knowledge the employee also must agree to report the loss or theft of device as soon as possible. Additionally, employees should be aware that IT may choose to limit access to certain applications. Most employees will agree to whatever terms they are provided, without reading or understanding the consequences of accepting the policy. IT and the company must dedicate resources to educate employees about the potential issues associated with connecting a personal device to a corporate network.

At a minimum IT should require password protection on all devices. While password strength is important, the type of password required should be less cumbersome than the typical PC passwords, which may require 8 characters including numbers and symbols. Besides password protection, IT should be able to remotely lock or remove data from lost or stolen devices. Other types of security policies could include corporate control of what applications reside on the device as well as control over what can be downloaded onto the device (see Figure 2). IT may also choose to encrypt the data on the device as well as the data on any removable media cards. In doing so, IT should be aware that this encryption could slow device responsiveness. To ensure ease of management, IT should consider solutions that enable over the air updates for provisioning and security.

Figure 2. Types of Security Policies

Security Category	Description
Password Protection	The software should be able to enforce a password, define the maximum password length, set maximum time before a security timeout and the maximum number of password attempts as well as set the password length.
Encryption	The software should be able to encrypt data on the device, data on a removable media card and data as it transits the network.
Remote device lock and remote data removal	This is the ability to send a command to a device which will remotely lock the device and/or erase all data from a device.
Application use	Application controls can disable features, like SMS and application viewing, as well as control what application can be downloaded to the device and what resources an application can use.
Hardware use	Hardware controls enable or disable hardware features such as the camera, GPS, Wi-Fi and Bluetooth connections
Auditing	To adhere to compliance and industry standards, firms need the ability to audit and archive phone records, messaging records such as MMS and SMS, as well as emails and voice mails. Firms may also use software to reroute incoming and outgoing cellular calls through the PBX for auditing.

What type of support?

Today, corporate-liable devices are fully supported by IT. Many management features are lost once an employee moves to an individual-liable plan including information on the carrier connection for troubleshooting. The new policy should define what support, if any, IT will provide for employee-owned devices. Today, many corporations are claiming they won't support any employee-owned device or IT is electing to only support email-related issues. The policy should state that IT will not support personal applications and that these applications will be removed if they interfere with device performance. IT should also have a wiki, knowledge base or extranet site that provides a troubleshooting FAQ. While the policy might state IT won't support personal smartphones, the IT staff should plan for a short-term spike in call volume as the policy takes effect.

What are the privacy and legal concerns?

Employee-owned devices blend a mix of personal and corporate data. Unfortunately, IT doesn't have the tools today to effectively partition personal data from corporate data and regulations may require corporations to archive data for auditing purposes. Along with informing employees of the risks of data loss, IT must also alert employees that the company has access to their personal records such as SMS, email, MMS, and phone logs. The policy should clearly state that the company has access to all records on the device and that they may be required to archive this data. The corporation should also consult its legal department for guidance on what actions to pursue if illegal activity is discovered in the process of auditing a device's records. If the employee doesn't agree to these terms, IT should not allow the device to access corporate data.

Can IT accommodate employees' 'personal' needs with existing devices?

Many IT departments have used application control features to restrict the use of entertainment features and application downloads for the company's existing corporate-liable smartphone portfolio. As part of the overall management of a mixed-liability environment, IT departments could appease the broader needs of the employees by loosening several IT policies on the company's standardized devices. For example, a corporate BlackBerry which previously was locked down to provide only email, phone, and PIM information, might be 'opened' to allow white-list applications such as a music player and a camera but not generic application downloads. In this way IT departments may be able to stave off end-users demands for the latest device by allowing the organization's standard issue smartphones to act more like consumer smartphones.

Review Smartphone Vendors Security and Management Features

Once IT has defined what type of security and manageability is required, IT should evaluate each of the mobile operating system platforms against this set of criteria. Specifically, IT should review each smartphone device in three areas:

1. **Provisioning and management.** How simple is the process for on-boarding and off-boarding a user? Does the vendor provide management tools that help you identify what is happening, where it is happening and why? Can you assess if the problem is a device issue or a carrier issue? Do knowledge bases or community resources exist on how to troubleshoot issues in a corporate setting? For example, the more consumer-oriented phones such as Android and iPhone provide minimal resources to help a firm minimize escalation to tier 2-3 support. IT should also review the process for updates. For example, does the management software offer features like over the air updates?
2. **Security.** Mobile device platforms must offer controls that minimize the devastating affect of device loss that exposes customer — or corporate — information. However, IT's ability to secure devices varies dramatically across platforms. IT must review each platforms ability to support essential and advanced features. For example, can you enforce passwords? Can IT remotely lock and remove data from a device? Can IT encrypt data at rest and in transit? How many IT policies does the platform support? Are these the policies that you would use?
3. **Current and planned business-grade application support.** Applications will provide the foundation for new growth. IT should review the different mobile smartphone OS and device vendors' approaches to application support. For example, who are their current partners? Does it have a developer program for business applications? Does the vendor already have a path to support emerging communications scenarios such as fixed mobile convergence? While these platforms may support thousands of applications, IT must review which business applications the platforms currently support and plan to support in the future.

Evaluate Mobile Management Software Solutions and Services

In our discussions with IT managers, they listed increased support costs as a key concern with enabling employee-owned mobility. IT leaders told us it wasn't the increase in the volume of users that troubled the staff but it was the variety of platforms that need to be supported which worries IT. Once IT has an understanding of the strengths and weaknesses of the mo-

bile platforms, it can build a matrix of the security and manageability gaps across the various vendors' platforms. In some platforms, the vendor offers a full suite of security and management features (e.g., Research In Motion's BlackBerry) while in other cases the vendor will provide minimal support (e.g., Google's Android). The level of support may also vary by the version of the operating system.

Due to the extreme variation across the platforms, IT managers are selecting one of two strategies. Depending on the firm's security and compliance requirements, IT will either select a device platform that it feels offers the proper security and standardize on this platform or it will look for ways to support multiple device platforms. For example, in many cases, IT will only allow employee-owned BlackBerry devices to connect to the network. Companies that want to support multiple mobile operating systems must add third-party security and management software to create a consistent baseline across the various device platforms. Several years ago, the functionality needed to support employee-owned mobility was a set of discrete software packages in areas such as mobile security, mobile middleware and mobile device management. However, vendors such as Boxtone, Sybase, Trust Digital and others have entered the space to offer more comprehensive mobility management solutions to bridge multi-device environments. While the multi-vendor offerings are new for many of the vendors, firms should still evaluate how these packages could ease the support issues associated with a multi-platform environment.

Summary

To take advantage of an employee's desire to bring their own smartphones into the office, IT should revise its mobile policy, assess the strengths and weaknesses of each mobile operating system and define a set of approved smartphones. IT must also secure and manage employee-owned devices in the same manner that it would a corporate-liable device. This may require the addition of third-party software or working with a VAR or managed service provider for support.

The good news is that the rise of employee-owned phones will help firms expand mobility beyond the top 10% of users to over half of the firms employees in several years. Embracing employee-owned mobility provides the opportunity to offload the device purchase and a portion of the mobile expense onto the employee. Increased mobility will improve employee productivity and strategically position a company to improve business processes by using applications on smartphones. To reap these rewards, IT must effectively manage the transition with appropriate policies and systems.

About Lopez Research

Quality research, strategic insight and intelligent commentary on the communications environment with a focus on the technology and service trends, issues, processes and players that drive innovation, influence decisions, and impact consumer, SMB and enterprise users. The Lopez Research syndicated research program in 2010 evaluates two key themes: pervasive communications and connected devices, and how they will evolve and change the existing landscape for the consumer, SMB and enterprise markets. We will consider, review and report on the development of converging, ubiquitous, multi-platform, multimedia communications experiences that are deliverable through an ever-widening range of devices.

We also offer primary market research and customized reporting for our clients on issues, trends, technology and processes relevant to the communications industry and your business.

Offices

9793 S. Burberry Way
Littleton, Colorado 80129

2269 Chestnut Street, Suite 202
San Francisco, CA 94123

Call us: 415-894-5781

Visit us at: www.lopezresearch.com