Making “Bring Your Own Device” Work for the Enterprise
Last year, in October of 2011, the wireless-industry association CTIA reported the number of wireless subscriber connections in the US had, for the first time, exceeded the number of people. It reported 322.9 million such connections in a country of 315.5 million. From the previous year, the number of wireless-enabled tablets and laptops increased to 15.2 million from 12.9 million (a 17 percent increase), while the number of active data-capable devices (e.g., smartphones) increased to 278.3 million from 264.5 million (just a 5 percent increase).1

The ability to get—and share—information anywhere and at anytime has become ensconced in 21st century life, both personal and professional. This didn’t happen overnight, and it represents a confluence of multiple technological trends: miniaturization of components, wireless technology, social networking, and cloud computing, among others. Perhaps the most important of these trends: ease of use. Anyone who has ever watched a toddler playing with an Apple® iPad mobile digital device knows we have seen the last generations computers can intimidate.

Over the last 20 years, technology has evolved from the command-line interface to drop-down menus to applications that look simple on the surface but mask a lot of complexity. The upshot is more people have a higher level of comfort in using technology than ever before. For corporate IT, this means addressing new demands from employees who want corporate applications to reflect the same kind of simplicity as Facebook® and Flickr®—also known as the consumerization of IT. It also means addressing their demands for accessing corporate data without forcing them to carry two different mobile devices, one for work and one for personal use.

The bring-your-own-device (BYOD) boom can be traced to two converging trends: the desire for employees to be responsive to customers and colleagues in a global, always-connected world still wrestling with time zones; and the desire to save money by not replicating a device employees may already own.

Just as mobility erases geographical boundaries, BYOD erases time boundaries, allowing employees not only to be productive after working hours (a boon for the enterprise) but also to time-shift commitments, enabling them to attend a child’s soccer game in the afternoon and work later in the evening (a boon for employees). Mobility brings a significant advantage to productivity, but as with many advantages, there are tradeoffs.
What are those tradeoffs? Let’s look at the pros and cons of BYOD. Foremost among the positive aspects is convenience. Equipped with a smartphone, employees literally have everything they need in the palm of their hand—contacts, schedules, e-mail, access to corporate data, search engines and applications. The ability to access data wherever work takes them means employees can not only get closer to customers, but do so without the physical barrier of a desk or even a laptop between them. For professionals from salespeople to physicians, this is a distinct plus.

Mobile devices are also more powerful than ever before, thanks to the latest processors. Their performance has made them equivalents to—rather than poor substitutes for—desktop and laptop alternatives.

Because mobile devices are more popular than ever before, both companies and consumers benefit from manufacturers’ economies of scale. Mobile devices are now available at a reasonable cost, especially compared to a desktop computer. Gone are the days when special-purpose tablets came highly customized with a price tag to match; mobile devices now use standard parts in standard configurations, making it simpler for IT to configure them for the corporate network.

Perhaps most important, users love them. Even as recently as a few years ago, it was common to hear stories of employees balking at the deployment of new application because they required a marked shift in the way employees did their job. With technology that’s much more intuitive than ever before and increased ease-of-use within applications, the learning curve is lower and the time-to-value for new applications is shorter. User acceptance is higher, which not only improves productivity but also enhances the relationship between IT and employees.

So what’s the downside? As forward-thinking IT departments have come to understand, it can be considerable, because it spans the triad of people, process and technology.

First, there’s the issue of users’ expectations. They may expect a complex corporate supply chain or workflow application to work with the same simplicity as their online banking application, even though it’s unfair to compare single-purpose applications with ones that have multiple moving parts. Further, they may buy a mobile device expecting it to be the epitome of simplicity and reliability and then, encountering frustration with some of its features, expect IT to close the reality gap—on a device with which it may have little experience.

Then there’s the fragmentation of the marketplace. This is really the flipside of choice. It’s not just the plethora of operating systems and devices—Apple® iOS, Android™, Windows® Phone, RIM®, etc.—it’s the permutations. For instance, Google® licenses the Android™ operating system to device manufacturers, who have the right to tweak it, adding security or connectivity capabilities that may not appear in other Android™ devices.

And device fragmentation doesn’t even begin to take into account operating system versions. So to truly support BYOD, IT must be able to accommodate the very latest versions of Apple® iOS and Android™ as well as the earlier ones. This leads to complexities in technical support issues. Can IT really afford to train its technicians to be proficient in what may be the most daunting matrix of devices, operating systems and applications ever conceived? This isn’t the equivalent of the old days when IT had IBM® mainframes, DEC minicomputers, and Windows® PCs installed—because at least then, users weren’t deeply involved in systems deployment and management.

Another facet of fragmentation affects application development. Companies face multiple questions around developing mobile
apps and look for advice and guidance from companies like Accenture. When users can use any device they choose, how can IT craft an app development strategy that encompasses so many options? Does IT develop more-extensive applications or simpler widgets for each platform, or focus on cross-platform capabilities using Web-based development tools? If it decides to focus on specific platforms, how does it deal with an ever-changing landscape of device types and operating systems?

Furthermore, how do they deal with functionality? Given the limited screen size of most smartphones, drop-down menus and other expansive options may not be viable. That means application development has to accommodate concise and straightforward features. Getting the user experience right is a key driver for mobile application development in a BYOD world. These are the kinds of technical and functional questions Accenture's clients deal with every day.

A different kind of fragmentation affects the data on mobile devices: how do you keep corporate data separate from personal data? How do you make sure employees are using proper security measures when they access public sites and applications, so as to avoid infecting the device with malware that in turn impacts corporate data? And how do you make sure that, when employees leave the company, IT can erase all vestiges of corporate data without affecting personal data?

Add to that security and connectivity issues, the major challenge when it comes to wireless and mobile access to back-end corporate data. Ensuring authentication and authorization sometimes abrogates the basic simplicity of mobile devices, limiting user satisfaction. At the same time, virtual private network and security certificate technology for mobile devices are still immature.

Finally, at the heart of BYOD is the question of cost subsidies. If the company and the employee are sharing the device, shouldn’t they also share the cost? In terms of subsidizing calling plans, are all employees created equal? Should employees in sales—who may be on the road a significantly higher percentage of the time than other mid-level employees—have a higher subsidy? What's fair? If the subsidies are inequitable, how should they be explained? With its ongoing focus on the question of mobility, Accenture can offer comprehensive answers to many of these concerns.
Given the rapid pace of progress in technology, these drawbacks are not insurmountable. Already device manufacturers, software developers, and companies like Accenture are working on solutions to overcome BYOD’s biggest drawbacks. Some of them may be interim solutions; others may be long-term advances that become industry-standard capabilities. Enterprises that want the competitive advantage mobility brings should be aware of these solutions and incorporate them into their ongoing mobility strategy.

Consider Partitioning

Mobile technology has taken a page from virtualization through the use of partitioning. By creating a virtual barrier between personal data and corporate data, IT can ensure users get proper access to corporate data, while still keeping personal data separate and untouched. Done well, partitioning can allow IT or employees themselves to wipe the part of the device containing corporate information when employees leave the company or if they lose the device. Another option is known as application containment, which partitions applications into separate areas, sometimes called “sandboxes,” so that anything done within that area doesn’t affect other facets of the device.

Create Enterprise Application Catalogs

To reduce the possibility of employees downloading applications that might contain malware or otherwise compromise the mobile device, IT can combine the concept of partitioning with enterprise application catalogs. These catalogs, utilized only within the company, contain corporate applications that have been tested and approved for corporate use and potential access to approved public applications. Non-authorized applications means fewer support issues stemming from unfamiliar downloads.

Designate Supported Devices

The abbreviation of BYOD is rapidly evolving in many corporations to BYOSD (bring your own supported device) or CYOD (choose your own device, but still from a designated list). This involves enterprises setting clear parameters for which mobile devices they’ll support. For employees who may be on renewable year-to-year contracts with their personal device, it’s fairly easy to make the transition to a company-supported device within a reasonable amount of time. For enterprises, this now means a narrower universe of devices to support, create applications for, and understand. It’s a win-win for both, because employees still have choice, while enterprises still have control. (An adjunct to this is CYOSP, which means “choose your own service plan”; this lets employees choose from a number of minutes-and-megabytes plans, depending on their anticipated usage, with subsidies based on their roles and responsibilities.)

Identify Development Needs

In an additional effort to place rational parameters on mobile devices, IT should also identify how it is going to develop applications for mobile devices. By hewing to development tools specifically tailored for the hardware itself, they can incorporate convenience and performance capabilities. However, this requires a somewhat bifurcated development strategy, especially if an enterprise allows devices running all four major operating systems (Windows®, BlackBerry®, Apple®, and Google®). By focusing on say, two operating systems, enterprises can still offer choice for employees but limit the dilution of their development resources.
Deploy Mobile Device Management ("MDM")

These tools simplify the tracking of devices and components, a capability highly valuable when an enterprise is accommodating a wide variety of devices. Most MDM systems provide the capability to download updates to mobile devices.

Protect Secure Documents

Just as enterprises should set up application catalogs that only allow downloads from that server, they should also set up systems that preclude employees from sending corporate data in any form to unknown or unprotected applications or e-mail systems. This ensures corporate data can’t accidentally or intentionally be transferred to an unsafe computer, website or application provider.

Deploy Mobile Application Management

While mobile device management is about configuring, securing and monitoring the overall status of mobile devices, mobile application management focuses on a single mobile application by enabling the procurement, deployment, configuration, performance monitoring, usage tracking, updating and uninstallation of specific mobile applications. This functionality is sometimes included in other tools such as mobile enterprise application platform, mobile consumer application platform and mobile device management, but it’s also available from pure-play software vendors.
One of the ways CIOs can best master the BYOD phenomenon is to be proactive. Users are going to bring mobile devices into the organization (just as they may have done with PCs years ago). They’re going to demand connectivity and support. Contrary to how they may seem to IT, they want to be more productive in their work. It’s incumbent upon IT then to be ready when those requests start to stack up—if they haven’t already. When users see IT understanding and accommodating their technology needs—especially now, when they also see the value that mobility provides—it can go a long way to improving relations between the business units and IT.

Accenture can help IT attain that proactive stance. We’ve been on the cutting edge of mobility, and understand both its promise and its pitfalls (and we can help IT avoid the latter). We can help IT accommodate both its needs in terms of security and manageability, while at the same time help IT serve the needs of employees in terms of accessibility, connectivity and reliability. Accenture can not only help you accommodate your enterprise’s current needs, but help create a foundation upon which it can build future mobile technology as it evolves, while keeping development and deployment costs down.

Here are some of the specific capabilities we offer enterprises to accommodate a cogent BYOD strategy.

**Accenture Application Factory**

The Accenture Application Factory incorporates a full suite of crucial development tools for mobile applications. It includes HTML5, the latest technology for building cross-platform applications, as well as middleware for connecting them to back-end applications, which can reduce development costs and deliver faster time-to-market. It also delivers application development methodologies for rapid and agile creation and update of applications.

**Accenture Enterprise Application Catalog**

Once enterprises have built applications, they can place them in a repository from which employees can download applications as easily as they would from a consumer application store. The Accenture Enterprise Application Catalog also handles the capabilities inherent in mobile device management—downloading updates and tracking what’s on mobile devices to confirm they haven’t picked up malware.

**Mobility Consulting**

Accenture offers in-depth strategy and planning capabilities, which help companies effectively analyze and respond to trends by developing strategies, frameworks and roadmaps to accommodate their business needs. With these strategies and tactics in place, companies can:

- Frequently use multiple channels to help increase revenue opportunities
- Leverage technology investments by extending existing applications
- Help increase sales effectiveness and productivity
- Improve quality of information through automation and more timely communication
- Help increase customer satisfaction through improved responsiveness

**Other Tools**

Accenture offers other tools to support and secure communication through mobile devices, including the Secure Content Reader, which encrypts documents and restricts their access, and Secure Messenger, which combines the best of text messages and e-mail, while supporting governance by ensuring internal messages are tracked and traced properly.

In a way, mobility has solved one of the hardest aspects of deploying applications—getting users excited. By combining users’ keen interests with IT’s knowledge of the business and Accenture’s insight on the tools and technologies, enterprises can establish a foundation for a proactive and highly responsive mobility strategy.
About Accenture

Accenture is a global management consulting, technology services and outsourcing company with over 259,000 people serving clients in more than 120 countries. Combining unparalleled experience, comprehensive capabilities across all industries and business functions, and extensive research on the world’s most successful companies, Accenture collaborates with clients to help them become high-performance businesses and governments. The company generated net revenues of US$27.9 billion for the fiscal year ended Aug. 31, 2012. Its home page is www.accenture.com.

About Accenture Mobility

Accenture is focused on enabling its clients to achieve breakthrough growth throughout the rapidly changing mobile ecosystem. Accenture Mobility offers five mobility services including consulting, software services—applications, software services—devices and platforms, managed services, and business integration services. These are designed to help organizations embrace business-to-employee (B2E), business-to-consumer (B2C), business-to-business (B2B) and machine to machine (M2M) business opportunities. Accenture offers mobility and embedded software services across a wide range of industries and platforms, including Android™, Apple® iOS, Blackberry®, Linux®, Meego™, Symbian®, Windows® Phone and Windows® Phone 8.

For more information about how Accenture Mobility can help, contact:

Nisha Sharma
Lead – Product and Offer Development, Enterprise Mobility Managed Services
Accenture Mobility
nisha.sharma@accenture.com

We would like to thank Accenture employees Evan Carstedt, Diegane Dione, Teresa Rinella and David Ruthkowski for their contribution to this publication.

This document makes descriptive reference to trademarks that may be owned by others. The use of such trademarks herein is not an assertion of ownership of such trademarks by Accenture and is not intended to represent or imply the existence of an association between Accenture and the lawful owners of such trademarks.