8. Using Mobile Technology to Build a Government on the Go

By Tom Suder

Introduction

Imagine a government that can respond to its citizens and its workers in entirely different ways, reducing cycle time and cost and increasing efficiency and service quality:

- What if benefits came to citizens via smartphone, enabling them to find out easily which of government's myriad benefits they might be eligible for, or to get real-time updates to claims they submitted?
- What if government field workers could access and input any information from citizens on a handheld device, in-person and in real time?
- What if an injured veteran returning from overseas could file and monitor a claim from a handheld device? What if the same device could also remind the veteran when to take medications, or allow a video consultation with a doctor anytime, anywhere?
- What if there were no need to visit a Social Security office and wait in line because a question could be answered by a video chat?
- What if responses to the next natural disaster could be tracked and coordinated through mobile technology? Citizens could be equipped to be first responders, uploading pictures of structural damage to dams and other infrastructure; emergency crews could be deployed by proximity and save lives; supplies and food could be tracked and redirected in real time.

These visions of the future are achievable today. The country is embracing mobile technology faster than it has adopted virtually any other technology innovation in history. The Apple iPad was released in 2010 and the tablet is changing the way consumers digest information. Apple released the iPad Mini in late 2012 to specifically address, among other things, the desire to put a smart tablet into a coat pocket or purse. Since the iPad was introduced, numerous other manufacturers such as Samsung and Lenovo and operating systems such as Android and Windows Mobile 8 entered the game in many shapes and sizes. Enterprise service providers like IBM have established entire practices devoted to leveraging mobile devices and systems; Amazon released the Kindle using its own version of Android, and Microsoft released a new tablet called Surface.

In a report on the use of mobile technology released by Pew Research Center's Internet and American Life Project in October 2012, 22 percent of all adults in the United States say they now own a tablet. Two years ago, the adoption rate was four percent. It is believed that during the 2012 Christmas season, this number may have reached 30 to 35 percent. The tablet is indeed one of the fastest adoptions of technology in history.

As the general public has rapidly embraced these various forms of mobile technology during the past five years, federal agencies are now adapting the way they do business to take advantage of the opportunities new mobile technologies present for reducing the time and cost of government

operations. As a first step, President Obama released a Digital Government Strategy in May 2012 to begin laying the groundwork for the federal government to develop an infrastructure to support the use of mobile devices and offer services through these devices.

Creating a Citizen-Facing Mobile Services Delivery Strategy

The President's 2012 Digital Government Strategy sets out to accomplish three objectives:

- **To enable the American people and an increasingly mobile workforce both in the general population and within government itself to access high-quality digital government information and services anywhere, anytime, on any device.** The emphasis of the strategy document is on the information, not the technology. By emphasizing an information-centric approach, government agencies can design interoperable, open systems and modernize their content publication model, thus delivering better, device-agnostic digital services at a lower cost.
- **To ensure that as the government adjusts to this new mobile digital world, it can seize the opportunity to procure and manage devices, applications, and data in smart, secure, and affordable ways.** Based on lessons from the e-government transition of the early 2000s, when government information and services were moved online, government now has an opportunity to:
  - Break free from the inefficient, costly, and fragmented practices of the past
  - Build a sound governance structure for mobile digital services
  - Do mobile right from the beginning
- **To create a path to unlock the power of government data to spur innovation across our nation and improve the quality of services for the American people.** Early digital strategies—such as those developed when the World Wide Web came into prominence in the mid-1990s—were completely uncoordinated, sometimes within an agency itself, with government working in silos and making the same mistakes over and over again. A big part of the Digital Government Strategy has been to share best practices and work to establish government-wide guidance from the outset. The focus on the Digital Government Strategy from the beginning has been on the customer. In the case of outward-facing services, the customer is the citizen. From the inward-facing perspective, the customer is the individual federal employee.

In 2010, the General Services Administration (GSA) set up a mobile apps gallery to incubate the development and sharing of government apps so agencies would not be designing them on their own for their own uses. Over 260 government apps were created and uploaded to this gallery (http://apps.usa.gov).

… federal agencies are now adapting the way they do business to take advantage of the opportunities new mobile technologies present for reducing the time and cost of government operations.

Creating a Government-Facing Mobile Strategy

The early success of citizen-facing mobile initiatives highlighted the opportunity to change the way government does its business—and speed service delivery—by adopting a mobile digital strategy internally. A government-industry working group developed a series of papers outlining steps agencies could take.

Allow employees to use their personal devices. Often called Bring Your Own Device (BYOD), this policy approach short-circuits the traditional approach of government agencies having to procure, manage, and track technology equipment themselves. The administration released guidance in August 2012 as a "toolkit for agencies contemplating implementation of BYOD programs." Three government organizations—two federal and one state—were cited in the toolkit for their BYOD efforts:

- The Department of the Treasury's Alcohol and Tobacco Tax and Trade Bureau created a virtual desktop that allowed a BYOD solution with minimal policy or legal implications.
- The U.S. Equal Employment Opportunity Commission (EEOC) was among the first of several federal agencies to implement a BYOD pilot that allowed employees to opt out of the government-provided mobile device program and install third-party software on their own smartphones that enabled the use of their device for official work purposes. EEOC instituted a voluntary policy for BYOD among employees who had been issued an EEOC-provided BlackBerry at a cost of $80 per user. Basically, personal devices could be used at the employee's own expense, but the employee would forgo the government-issued device. A total of 27 percent of EEOC employees took the BYOD option.
- The state of Delaware initiated an effort to not only embrace the concept of BYOD but to realize significant cost savings by having employees turn in their state-owned device in favor of a personally owned device, which could save the state approximately half of its current wireless expenditure.

Develop government enterprise apps (GEAs*).* GEAs are doing-your-job apps for the government worker. They can include areas such as field services, internal collaboration, internal training, case management, and the creation of digital libraries. For example, field services can range from simply replacing a clipboard data collection system that includes an "I have to file my paperwork at the end of the day" component to a robust law enforcement case management system that is available at one's fingertips rather than back at the office or in the squad car.

These types of apps not only provide information when government workers need it, but can also reduce duplicative data entry with its attendant errors. GEAs also have introduced new possibilities to the government worker. Blue Force Tracking, a military term for a GPS enabled application for locating people in the field, can assist agencies in deploying personnel more effectively. Knowing where all your people are at any given moment is a safety issue, as well. Delivering technical or other training in bite-sized parcels to be easily fit into the schedule of the user is another promising area for the use of GEAs.

GEAs can be developed at a fraction of the cost of the traditional desktop application. The information-in-the-palm of your hand argument is compelling. Research and practice are showing that GEAs allow the user to do more of whatever they are doing, whether it is collecting data or providing training.

It is impossible to deliver game-changing applications to mobile devices without an infrastructure in place to support it. Recently, the Department of Agriculture and the Department of Veterans Affairs (VA) have awarded contracts to build mobile device management/mobile

application store infrastructures to support their respective agencies. The Defense Information Services Agency (DISA) is currently trying to award a contract to build a similar infrastructure in the defense environment. Meanwhile, the VA is also wiring all its facilities—including its hospitals and nursing care facilities—with WiFi to allow veterans and employees connectivity to their mobile devices. The Pentagon recently did the same thing, but is also looking to add an in-building cellular component in 2013.

Other examples of agencies making significant progress in using mobile technologies include the Federal Air Marshals Service, which has created a mobile Web app allowing its marshals to access its systems; and the Nuclear Security Administration, which has developed an app allowing its employees to track nuclear materials.

Implementing a Government-Facing Mobile Strategy

One element of the President's 2012 Digital Government Strategy was to "evaluate opportunities to accelerate the secure adoption of mobile technologies into the Federal environment at reduced cost." A small "tiger team" of agency experts from across the government came together and identified three benefits that a mobile strategy would offer:

- Enhanced mobility and quicker access to information for a user population that is dispersed nationally and internationally
- The ability to provide previously unavailable services and applications to support mission operations in the field
- Increased resilience regarding concerns about relying on a single smartphone vendor

The Strategy identified three factors that agencies should consider:

1. Capabilities. What capabilities or functionality and mission needs will be supported by the new technology or devices? The group recognized that mobility has the chance "to present opportunities to enable a mobile workforce and deliver information and services to customers, partners, and the public, improving the ability to accomplish the agency's mission."

It also noted that some of the barriers to capabilities were "technical limitations focused on the pace of technological change and relative immaturity of the product space, including 'mobile device management' (MDM) solutions, mobile application stores, and the variety of device configurations." In addition, it raised the lack of ubiquitous wireless connectivity "as a barrier to delivery of web applications and a virtualized desktop, since both require a continuous network connection."

Ultimately, as agencies put the necessary infrastructure in place, mobile devices will offer the possibility to really change how government does its business.

2. Cost. What would be the total cost of ownership—which includes planning, acquisition, and operations and maintenance costs? This is a big issue in any agency these days, and the group determined that there were two interrelated barriers:

- **Need for an accurate cost-benefit analysis model.** Developing an accurate cost-benefit analysis is always a challenging issue to any government agency, and price models with mobile are rapidly dropping as the Mobile Device Management-Mobile Application Store (MDM/MAS) becomes a commodity.
- **Need for a government-wide contract vehicle.** Fortunately, the lack of a government-wide contract vehicle is being addressed by both the General Services Administration (GSA) and the Defense Information Services Agency in separate contract vehicles. GSA is expected to

award a Wireless Federal Strategic Sourcing Initiative shortly while DISA is expected to do the same with its MDM-MAS.

3. Security. How can agency leaders be assured that any security risks in moving to a mobile strategy can be managed effectively? The Strategy highlighted a number of important gaps that currently exist in various areas. These gaps need to be addressed to enable more effective use of mobile technologies to meet government missions. The gaps include:

- **Security and privacy**. Gaps exist between federal security and privacy requirements and the availability of commercially developed products that implement the required protections. These include:
  - *User authentication:* Lack of a robust user identity authentication mechanism that complies with federal mandates and maintains mobile device ease of use
  - *Data encryption:* Growing need for validated, secure, and efficient cryptography suitable for mobile devices
  - *Application security testing and evaluation:* Lack of automated tools for efficient assessment and authorization of mobile applications
  - *Device sanitization:* Lack of agency processes and tools to follow requirements on device sanitization.
- **Policy and legal issues**. There will need to be a continued focus on ensuring that existing policies accommodate agency needs in a mobile environment, including:
  - *Guidance and best practices for mobility:* More robust engagement mechanisms should be created to help share best practices for mobile devices and supporting tools across the federal enterprise
  - *Business and technical requirements:* Lack of identified mission use cases and technical requirements that are consistent across the federal landscape
  - *Legal:* Lack of legal precedence, policies, or guidance established on electronic discovery of information on mobile devices related to mixed official and personal use for both Government Furnished Equipment (GFE) and BYOD (e.g., compensation, liability for data or equipment loss, etc.).
- **Application and infrastructure**. Gaps exist between the goals of supporting multiple devices and the cross-platform infrastructure needed for applications and devices:
  - *Legacy applications:* Lack of compatibility and ease of use accessing legacy applications from mobile platforms has hindered access to data and the overall transition to mobility.
  - *Infrastructure for mobile devices and mobile application distribution:* Lack of cross-platform compatible industry solutions that satisfy government authentication, security, and management requirements
  - *Network connectivity:* Lack of adequate wireless data network through WiFi or cellular data to always allow networking capabilities for the mobile worker relying on mobile applications

As discussed above, there are many disparate issues involved in implementing a mobile work environment in government, but there are answers to every specific issue that exist today. The challenge for an agency is to work all the issues in parallel and not consecutively. For example, you can't work all your policy and legal issues, get your app's security solution solved, and then have no useful capability because you don't have WiFi in any of your facilities!

A Checklist for Implementing Government Enterprise Apps (GEA)

GEAs have the potential to change the way the government conducts its business internally, but they encounter many barriers such as security, human capital, policy, technology, and infrastructure.

Some of the questions that agencies have to answer include:

- How do I monitor and credential devices on my network?
- How do I set up an internal enterprise app store? Who runs it?
- How do I set up ubiquitous wireless connectivity in all my facilities? More importantly, how do I pay for it?
- How does working with smart devices affect my older workers? Are there any union issues?
- Can I support a Bring Your Own Device (BYOD) Strategy?
- What capabilities should I use to go mobile?
- How do I secure the devices? How do I ensure the apps don't contain malware?
- How do I interface back to my legacy systems using Application Programming Interfaces (APIs)?

The Potential Impact of the Digital Government Strategy on Improving Government Operations

The Obama administration understands the difficulty of implementing a digital mobile strategy and is working to solve problems and share best practices. It created a working group in 2011 to look at the following areas of opportunity for improving mobility within the federal government:

- **Mobile device management**. Improvements in tools and processes are necessary to support enterprise-level configuration management and controls for federal agencies.
- **Application services**. Better tools and processes are needed to accredit and distribute applications required for government missions, leveraging commercial market cycles, and commercial and federal application stores. The National Institute of Standards and Technology will soon release guidelines that provide a methodology for testing and vetting third-party applications that are distributed through various federal agency-operated app stores.
- **Identity access management**. The use of Personal Identity Verification (PIV) standard for user authentication has not yet been adopted for mobile technologies.
- **Improved governance and standards**. The federal government must work collaboratively with industry to bridge the security gaps present in today's smartphones, tablets, and other mobile devices, while continuing to identify policy and legal issues that may need to be addressed to accommodate these new technologies and better fulfill agency mission requirements.

Each of these issues is being addressed by various working groups within the federal community. The identity access management issue may be the most difficult to overcome philosophically. As agencies unroll PIV cards to ensure proper identity management on desktop and laptops, this solution does not lend itself to going in a new direction … such as the smartphone itself being the identifying mechanism.

Conclusion

Mobility offers many possibilities for an agency to enhance its mission, reduce the time it takes to serve citizens, and save money. Here are three of the top things that federal executives should do if they want to create a truly mobile-first environment in their agency.

- **Collaborate internally and externally**. No department or agency can have all the answers in a new technology that is changing very fast. Agencies should set up a structure internally to collaborate on mobility. For example, in the Department of Justice it makes sense for those offices that have similar types of missions to share information and possibly procurements. The department recently had a mobility summit to share ideas and best practices.
- **Move from pilot to production.** The purpose of a mobility pilot should be to go to production. The DoD has had at least 50 mobile pilots, but until organizations have a plan to institutionalize the capability, these pilots will dead-end at some point. Instead of a "Rogue Pilot," it would be best to work with all the stakeholders that can bring to bear all the elements of mobility. Then issues can be worked in parallel.
- **Identify executive champions.** It is almost impossible to do anything in an organization without executive support, but this is especially true in the case of mobility, a new technology that changes the way business is done in so many ways. This isn't just an IT issue. It touches almost every aspect of an organization with many legal, workforce (union), cultural, mission, security, privacy, procurement, and funding issues.

Tom Suder *is President and Founder of Mobilegov, a company that provides cutting-edge mobile solutions to its customers. In addition to his work with Mobilegov, Tom is also Strategic Advisor to the University of Central Florida's Institute for Simulation and Training.*