Mobility momentum

Allowing government employees to use their own mobile devices at work can boost employee productivity and overall government efficiency.

While limited finances and shrinking workforces have battered state and local governments, a growing trend may be just the tonic needed to help them deliver the services their residents expect. Increasingly, governments are creating a bring-your-own-device to work (BYOD) policy, which allows employees to use personal mobile computing devices — smart phones, laptops and PDAs — to connect to the agency's network and use them in their work.

Traditionally, state and local governments have avoided adopting BYOD policies because the prospect of managing employee-owned devices and keeping information secure was a concern for information technology (IT) teams, says Alan Shark, executive director and CEO of the Public Technology Institute. But as consumers continue to embrace smart phones and connectivity access becomes ubiquitous, "employees no longer want to be tethered to their desktops to get the information that they need," says Sundhar Annamalai, executive director of product marketing management for Advanced Mobility Solutions, AT&T.

To some extent, policies that allow government employees to bring their own mobile devices to work are inevitable, Shark says. With inspectors, utility, A BYOD POLICY IS A GOOD WAY FOR GOVERNMENTS TO CONNECT WITH YOUNGER WORKFORCES AND INCREASE EMPLOYEE SATISFACTION.

maintenance, service workers, and similar positions on the payroll, 40 percent to 60 percent of local government workforces are mobile, Shark says. In the past, these workers would have collected information out in the field, completed paperwork by hand and then returned to their offices to input the data on a desktop computer. However, today's mobile devices improve that process, allowing employees to be more productive and responsive to customers, even when they're away from their desks.

"When you look at the limited resources state and local governments have compared to that of a Fortune 10 company, it makes sense to make them more productive while they're out in the field," Annamalai adds.

Measurable Benefits

BYOD policies have tangible and quantitative benefits:

> Productivity and response time to customer service inquiries can be measured, although it may be too early in the implementation phase for most cities and counties to provide statistics, Shark admits.

> BYOD policies help reduce new equipment purchases and shrink IT inventories. People also tend to care for their personal devices more carefully than they would equipment that's owned by their employer. "With people purchasing their own devices, there's less of a refresh rate burden on providing new equipment to a city and county employee," Shark says.

> Yet the boost in employee satisfaction is more important than the cost savings and productivity increases, Shark says. More than 50 percent of mobile handset users use smart phones, according to AT&T. Younger employees, especially Millennials, have access to email and the web via their personal smart phones, so it's only natural for them to want it at work, too. "They have the devices, like to collaborate and are impatient people. When they come to work for a government agency, local, state, city or county and are told, 'here is your desktop computer,' the response is 'I have more power here in my hands than I do on my desktop, and I want to use my device,'" Shark adds.

With that in mind, implementing a BYOD policy is a good way for local governments to stay connected to younger workforces and increase employee satisfaction.

Privacy and Security Solutions

One of the reasons state and local governments historically have shied away from allowing BYOD is concern over privacy and security. Those fears are not unfounded, considering potential loss of confidential information and the risks of contracting viruses or malware that disable government systems. More than 50 percent of organizations that reported data loss in the past year attribute it to insecure mobile devices, according to AT&T.

"One of the key things we've seen among state and local governments is the privacy component in how the devices are being managed is a great concern," Annamalai says.

Yet controls increasingly are being developed to address security and privacy. In some cases, state and local governments mandate the use of passwords on personal devices. Some communities use virtual private networks in which data is encrypted or restricted from being downloaded onto personal devices. Other communities offer mobile device management (MDM) systems that keep track of device whereabouts and restrict usage or provide "kill" switches so that if the device is lost or stolen the device can be wiped clean.

Increasingly, state and local governments are applying container-based systems, in which a single device is assigned separate business and personal identities. Using this system, governments control the access and data allowed for the business side of the device, but the employee has free reign to use his smart phone however he likes through the device's personal persona. For example, if the device is lost, the IT department can wipe all of the government's information off of the phone without having to erase the user's personal information. And, the employee doesn't have to worry about an employer invading his privacy because the employer has no access to personal contacts and applications on the phone.

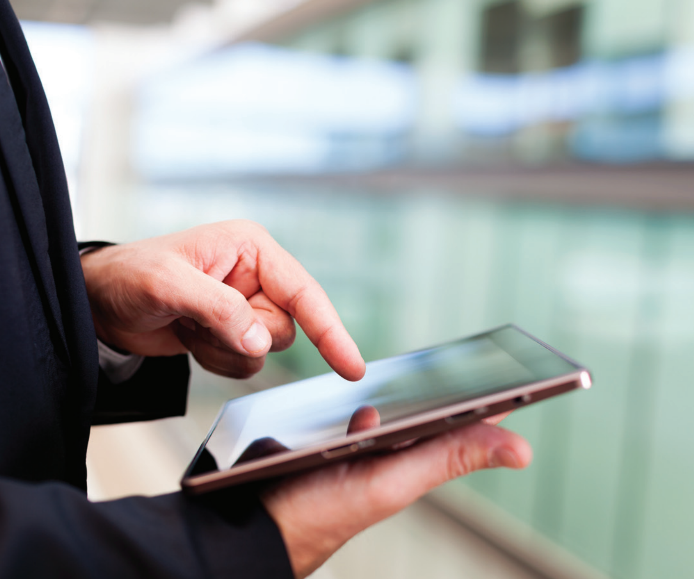
On Board With BYOD

There a few communities that are already pursuing a BYOD strategy to attempt to seize the benefits early. Some cities are exploring solutions that allow personal devices access to the government network in exchange for complete transparency and control over the device itself for

Continue the Mobile Government Conversation

If you missed the live Mobile Government webinar on November 14, you and your colleagues can hear it OnDemand at americancityandcounty.com. *Plus, you can email your questions directly to the speakers,*

> **Bill Wolpin (bill.wolpin@penton.com)**
Editorial Director & Associate Publisher
> **Alan Shark** (ashark@pti.org)
executive director and CEO, Public Technology Institute
> **Sundhar Annamalai** (xxx@att.com)
executive director of product marketing
management for Advanced Mobility Solutions



maximum security. Others are looking at containerization solutions that separate agency and personal data but can put more responsibility and burdens on the employee.

Overland Park, Kan., recently implemented a BYOD policy, and Vicki Irey, chief information officer, says after only three months of the program, employees are wholeheartedly on-board. About 86 personally owned smart phones and 15 personally owned tablets have access to the network to send and retrieve email.

Enrolling a personal device on the MDM system initially takes about 30 minutes and costs $26 per device. Once employees choose to use their personal mobile device at work, they must register it with the IT department's MDM system so the department knows how many users have access to its network; create a password for the device; and agree to let the city wipe the data off of the phone or tablet if the device is lost or stolen. A VPN maintains the city's data in the IT Department, allowing employees to work on a virtual environment but preventing data from being downloaded to individual mobile devices.

Yet Irey believes the security steps, time and cost are minimal. "Almost immediately, the [BYOD] policy increased employee satisfaction and efficiency," she says. "If employees can see their email and respond to requests while they're out in the field or while they're away from the office, that is more efficient than having to wait until you come back to the office."

Currently, only exempt employees have access to email and Web browsing. The Fair Labor Standards Act (FLSA) does not allow non-exempt employees to participate in the program, Irey says. The city plans to deploy applications to specific departments over the next year and a half, based on needs. For example, restaurant inspectors will manage reports through an Apple-based application, whereas the Parks Department will use an Android-based application, based on the jobs they need to accomplish and the applications available.

"We're being careful about what we're deploying, making sure we provide the right applications that each department needs," Irey says.

Nevertheless, she is adamant that "mobile is where we are going" because of the productivity gains and, frankly, employee demands to use their own technology.

Anxious for laws and regulations like FLSA to catch up with technology to allow both exempt and nonexempt employees to take advantage of mobile technology, Irey describes BYOD policies as "like a moving train." Local and state governments can't stop the move toward increased mobility, she cautions. "If an organization tries to stop it, people are going to find ways around it."

Two Sides of Connectivity

Some employees — like police officers, code enforcement officers and building inspectors — in Scottsdale, Ariz., have had wireless connectivity for more than a decade, according to Brad Hartig, chief information officer. So it made sense that as the city was phasing out its use of BlackBerry devices and employees increasingly were carrying smart phones for personal use, it should implement a BYOD policy that allows those personal devices to have two functions.

Hartig says his department was used to having a back-end management system that provided good visibility of mobile devices and wanted something similar to manage BYOD devices. He also wanted a system that wouldn't commingle personal data with city data, because employees expressed concerns that the city would be able to view personal information. Without a way to reassure employees that their personal information would remain private, his department feared that few would subscribe to the BYOD policy. To that end, his team chose a container-based mobile device management system that allows employees to use their own devices at work, but separates city information from personal data.

Under the policy, employees can use their personal devices to access email and the city's password-protected Intranet. Employees incur the cost for data charges when they download city information, as they would when downloading personal data. But because employees are primarily accessing the Intranet and not downloading much data or many applications onto their devices, the costs are minimal.

"At this point a lot of people are accepting the use of the BYOD policy. They want to be able to have mobility and are willing to take on the overhead of data rates," Hartig says.

The program has been in a pilot for eight months. Eventually, the program will be rolled out to the entire organization, at which time he expects a substantial number of employees to take advantage of the BYOD policy and for it to allow more functionality. For instance, employees may soon be able to actively sync their calendars or delve deeper into city information with their personal devices. Adding functions would increase some of the work his department has to do to support the BYOD policy. "There's definitely a support component to implementation," Hartig says, when you take into account choosing a system to manage privacy and security, and working with and supporting the individual to enroll their device. However, "if you look at the advantage of having a mobile workforce, productivity increases, and not having to buy a city-owned phone or carry the monthly airtime, it's definitely worth it," he says.

Ultimately, the success of BYOD policy implementation depends on how invested the government is in providing a security and management solution and in supporting the device, Hartig says, "because the workforce is already making the investment in the device."

Control Plus Freedom of Choice

AT&T's solution to managing mobile devices and BYOD takes a fresh perspective. It strikes the right balance between security control with distinct work and personal balance while limiting the exposure and responsibility of individual employees.

AT&T Toggle is a container-based solution that maintains employee privacy and agency security on personal devices. The company offers security features for the device and network that run across the carrier, OS and OEM devices, including contain lock, wipe and application level management. AT&T limits individual employee burdens by providing split billing within the dual persona container and dual voice and data services right from one device, including separate Toggle data allowances available by the agency to preserve employees personal data.

Toggle is bringing the best of both worlds together by providing government the control they need while giving users the freedom of choice.

AT&T Toggle℠

A complete mobility management solution

In today's world, mobility is no longer a luxury. The line between employees' work and personal lives is fading, a shift that complicates the task of managing mobile devices while enabling collaboration among mobile users.

To take full advantage of the changing culture, agencies need to implement a solution that addresses employee requirements while providing a highly secure platform that protects proprietary information. AT&T Toggle can be that solution.

Dual Persona

AT&T Toggle provides a dual persona experience to address the needs of agencies and their end users. Toggle creates a password-protected work mode on mobile devices through which agencies can control and distribute applications and content. Agency data cannot be used outside the Toggle workspace; meanwhile, administrators cannot access end users' personal activities.

Highly Secure

AT&T Toggle provides an application environment that can address the various security requirements within an agency. By encrypting sensitive information on the device and providing carrier-class security in the network to help ensure end-to-end protection for data at rest and in transit, Toggle can help deliver peace of mind to the most security-conscious agencies.

Built with security at its core, Toggle provides a password-protected workspace supported by the following features:

> Antivirus software – check both personal and agency workspaces for known viruses, malware and other malicious code and applications on Android™ devices.

> Application-Level VPN Enablement – extend the use of the agency's VPN to the Toggle workspace.

> Toggle Secure Gateway – A highly secure gateway integrates existing LDAP/AD environments with the cloud-based Toggle administration console for simplified user device management.

> Together, the Toggle Secure Gateway and Application-Level VPN Enablement allow applications to be tunneled, and help prevent the exposure of the agency Microsoft Exchange environment, including Exchange ActiveSync (EAS), to the Internet.

Mobile Enterprise Management

> With Toggle, agencies can address the full range of needs with one solution:

> Application and content management – Distribute applications and content to an entire workforce or to individuals based on their roles and responsibilities.

> Application wrapping – Highly secure and manage agency and third-party apps for distribution through a custom enterprise application store.

> ToggleHub – Allows simple access to the latest approved mobile apps, tools, and content.

> Toggle Calendar – Enables access to work calendar.

> Toggle Messenger – Includes a user friendly experience such as push alerts from the agency to users.

> Toggle browser – A highly secure interface that allows agencies to allow and control end user access to internet and intranet websites.

> Toggle email – Uses AES 256-bit encryption to protect agency data from personal data. Agency data and email attachments are highly secured and protected within the Toggle workspace.

For more information contact www.att.com/secureworkforce.