A Guide to Mobility in Government

2011 | ISSUE 1

CENTER FOR DIGITAL GOVERNMENT Special Report IN CONJUNCTION WITH GOVERNMENT TECHNOLOGY'S public cio

A SUPPLEMENT TO **PUBLIC CIO** MAGAZINE

Contents

Sponsored by:

Introduction

"Suspected Murderer Arrested Thanks to New Police Technology"
— Any Day, 2011

John Smith, a suspect in the murder of two people, was arrested today in a routine traffic check. When he presented a license, the officer, thanks to new mobile technology, snapped a photo of Smith and sent it to headquarters for verification.

When Smith's face didn't match the photo on file, the officer followed up and found an outstanding warrant for Smith. Smith was immediately arrested and transported to jail. Examination of the license, which had been expertly duplicated, revealed that the license number was real, but the owner's photo had been replaced with Smith's.

Although the headline and story are fictitious, the technology is real, and so is the possibility of using it to make just such an arrest.

This is just one example of the plethora of ways in which mobility is helping government at all levels address demands for performance and better constituent service in the face of the greatest revenue challenges in decades.

Far from being an expense, mobile equipment is in many cases more than paying for itself by increasing the amount and quality of work employees can do in the field, reducing government task process time from weeks to days or hours, shortening response time to customers, cutting travel time, decreasing equipment expenses and eliminating occupancy costs.

For more than a decade, The Center for Digital Government has specialized in researching, analyzing, documenting and providing expert advice on the role and impact of technology in the public sector. In this Special Report on mobility, CDG continues that effort. The report identifies both the enablers and the threats to mobility, describes its many disparate and occasionally surprising benefits through real government case studies, and provides an overview on how state and local governments can fund mobile technology initiatives.

Mobility is moving at a faster rate than the Internet at its start. It will change the way every government does business. This report shows how.

The Technology Behind the Mobility Movement

MOBILE DEVICES

Long closed to anything but the BlackBerry, the federal government opened up to iPhones, iPads and Android devices in 2011.[1] This change in policy by Washington, D.C., is just the most visible example of consumerization of mobile devices in the workplace, one of the top trends in government mobility in 2011.

For years, the only mobile devices allowed in the offices of enterprises and government have been BlackBerry, with its highly secure e-mail system, and "ruggedized" laptops that could survive a fall from a tall building. With the advent of the iPhone in 2007, however, that all changed. People bought these devices and found them so helpful that they wanted to use them at work as well. This trend started in business first, naturally, but the pressure has steadily grown in government, too.

Now state and local governments are not only adopting consumer smartphones and tablets, but they are also allowing employees to use their own devices, another major trend. According to a recent study, 90 percent of organizations will support business applications on personal devices by 2014. This trend is thought to be driven by consumers who want to use their own smartphones and other portable gadgets at work.[2] By 2013, studies forecast that 80 percent of businesses will support the use of tablets by employees.[3] It is likely that this trend will be reflected in government at a similar level, because the adoption of tablets is part of the overall "bring your own device" (BYOD) trend.

BYOD saves governments money, a benefit they were quick to recognize. Of course, BYOD also creates security problems. However, those problems are being addressed by smart policies that limit the list of acceptable devices and by solutions like mobile

management platforms that automatically apply standard organizational security protocols to every remote device.

Mobile devices are helping governments that are strapped by tight budgets. Civil servants who survived the waves of layoffs now realize that mobility can help them do more work in less time. That has become an imperative, because there are fewer state and local government employees today, but just as much, if not more, work.

2011 may well be the turning point for the government adoption of all manner of consumer mobile devices — smartphones, tablets, netbooks, laptops and all the peripherals and accessories — that make it possible for anyone to work anywhere at any time.

ADVANCED DATA COLLECTION

Asset tracking and inventory might be called the biggest hidden application of mobility. Everyone has heard — or has told from firsthand experience — stories about the $50,000 worth of widgets that got lost in a warehouse, or the extra thousand boxes of office supplies ordered when the first thousand boxes were forgotten. A different class of mobile devices — multiple types of scanners and small special-purpose computers — that automatically collect data and send it to central databases may consign such stories to history.

Scanners most commonly read different types of tags — barcodes, radio-frequency identification (RFID), or quick response (QR). But other types of scanners exist, too, such as fingerprint, image or smartcard readers that attach to mobile computers. Snap-on cameras, especially for law enforcement, also fall in this category. Police officers use them to photograph suspects, drivers' licenses, vehicle accidents, and more.

Asset-tracking computers can be handheld or even wearable on a finger, wrist or arm. They have built-in scanners, and users can type data in on a small keypad. Some include voice recognition, some function as full-fledged smartphones with scanners, and some are ruggedized.

"Assets" can include mobile computers, boxes of pens, bulldozers, animals, prisoners, hospital patients, accident victims, evacuees, and anything else that needs to be tracked. Objects get tagged; people wear bracelets or anklets with built-in tags.

Data from these devices is collected in real time and immediately logged into inventory. The devices can automatically generate work orders and equipment receiving and disposal records, link financial data on assets to work schedules and maintenance, track where equipment is being used and who has responsibility. This creates a built-in workflow for tracking and managing assets, which is especially helpful for managers of equipment that is constantly on the move, such as in facilities or for emergency response.

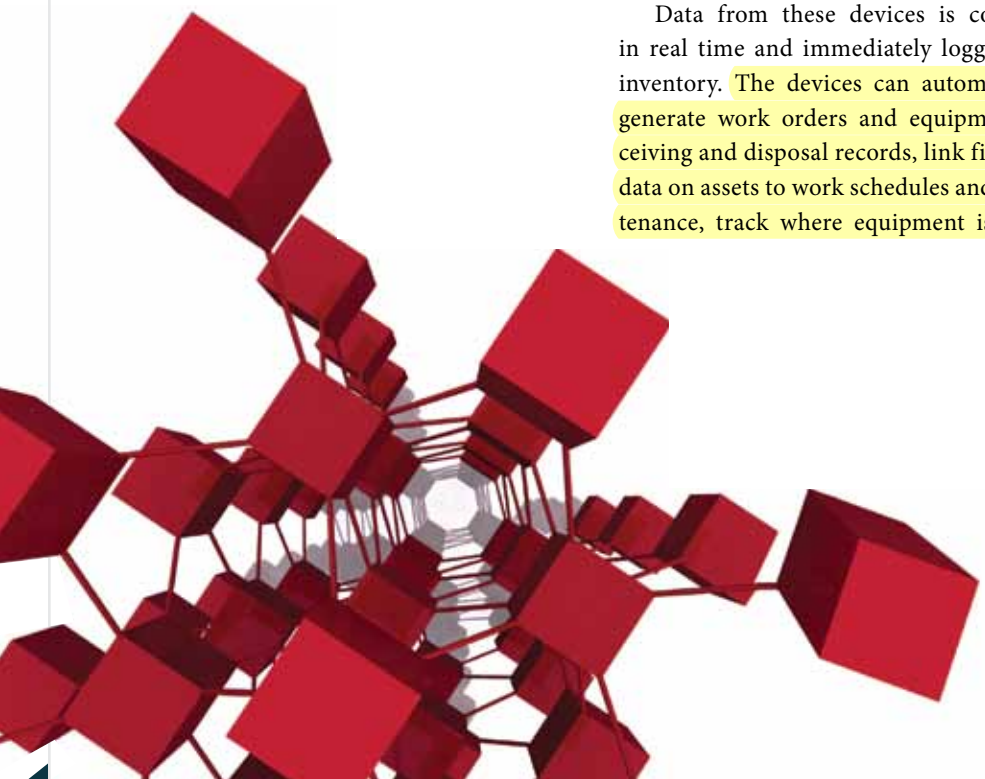
2011 may well be the turning point for the government adoption of all manner of consumer mobile devices that make it possible for anyone to work anywhere at anytime.

Up-to-date databases eliminate the problem of lost or misplaced assets, reducing costs. Scanning increases accuracy and speed, reducing errors and the time needed to manage asset logistics. Accurate information means better audit results and greater transparency into the long list of assets owned by governments. When the "assets" are people, mobile logistics means they do not get lost, even in emergencies.

NETWORKS

The phrase "wireless network" encompasses three generations of telecommunications technologies, ranging in capabilities from short text messages transmitted at 20 kbps to full-scale videoconferencing at 100 Mbps. The technologies include a bewildering array of acronyms and specifications. Briefly comparing these mobility-enabling technologies by generation is a quick way to review them.

Second generation, or 2G networks were introduced in the 1990s. (The first generation, or 1G, networks were analog only.) For the first time, voice and data



could be digitally transmitted. Transmission speeds were between 10 kbps and 20 kbps, enabling functions such as digital voice, short text messages, e-mail and Web browsing. 2.5G networks made basic multi-media possible, such as games, images and audio/video clips. These networks are still around, but are rapidly becoming obsolete in the smartphone era.

3G networks — and 3.5G and 3.75G — transmit data between 144 kbps and 2+ Mbps. They added functions such as full-motion and on-demand video, 3-D gaming, videoconferencing and much faster Web browsing, especially for sites with significant amounts of graphics. These networks were first introduced in 2001 and, after a somewhat slow start, now cannot be deployed fast enough.

4G networks are just now starting deployment. Transmission speed will range from 100 Mbps to 1 Gbps. Those speeds enable high-quality video streaming, videoconferencing and Voice over Internet (VoIP). Another feature differentiating 4G from 3G networks is that providers hope they will solve the rural/remote broadband access challenge.

WiMAX and WiFi are also very important to mobility, but for technical reasons, neither falls into a neat "G" category.

2G, 3G and 4G networks can broadly be said to use the same basic infrastructure of antennas on towers or buildings and base stations that provide power, landline links to the backbone network and other services. However, the transmission coding, the power needed to transmit, the range of the signal, and other characteristics have all vastly improved with each generation.

Although WiMAX also uses the antenna and base station infrastructure, it needs no landline connection to the backbone network. It can make that connection over the air at speeds of 34 Mbps to 1 Gbps.

2G, 3G and 4G networks all feature direct device-to-antenna communications.

With WiMAX, devices (phones) with direct connection just emerged in 2010. If one's mobile device has no built-in WiMAX connectivity, intermediate physical links are needed, either a freestanding indoor or outdoor gateway (similar to a modem) or a small "dongle" that plugs into a mobile device via USB port.

WiFi uses no cell antennae. Instead, it uses "hotspots," or wireless access points (WAPs), that let WiFi-enabled mobile devices connect over the air to a landline network. Usually, the WAP is connected to a router that links up to the landline network, or a router may contain the WAP. WAPs relay data between different wireless devices and the landline network.

Where WiFi networks are used to enable mobility, the number of hotspots needed can vary greatly. Multiple hotspots may be needed in an office building or city center, with fewer needed outdoors or in more pastoral surroundings. However, if too many hotspots are crowded into too small a space, they can interfere with each other, disrupting communications.

Mobile hotspots are now available, embedded in several mobile devices. If there's no network to connect to, a mobile hotspot cannot create one. If a network is available, however, mobile hotspots epitomize "anytime, anywhere" connectivity.

UNIFIED COMMUNICATIONS

Having a single phone number that also integrates with e-mail, voicemail, contact list, calendar, social media, instant messaging and the Web is the consumer version of unified communications. All of that plus integration with organization networks, data centers, line-of-business applications, "presence," and audio and videoconferencing is the enterprise version.

Deploying an enterprise unified communications solution is expensive and can be difficult. As of April 2011, just 11 percent of 150 state and local government respondents to a survey on unified communications said the technology was fully deployed in their organizations.[4]

Governments seeking to deploy unified communications solutions have several options. They can build a solution, starting with upgrading or replacing their existing voice and data networks. The unified messaging platform will integrate these networks, along with applications. Several teams will be involved, including in-house IT, network and telephony providers, and the unified messaging platform vendor.

Alternatively, governments can use a cloud solution, which is the path many organizations, both private and public sector, have chosen. Although a cloud solution does not involve the extensive infrastructure

upgrades that the "build it ourselves with some expert help" approach requires, the complexity should not be underestimated.

Either way, implementing unified communications is challenging. Nevertheless, the benefits, including much greater collaboration capability among employees and remote videoconferencing, seem to be worth the challenges.[5]

VIRTUALIZATION

When people think of computers, they usually think of physical devices. A conventional office computer, for example, typically has a monitor, keyboard and a box full of electronic processors that perform common tasks like storing data, running an operating system and applications, and maintaining the "desktop" you see on the monitor. An office computer also draws power from electrical outlets and has connections to some type of network — wired or wireless or both.

Of all these functions, however, only two are physical — the electrical and network connections. Even though some sort of physical medium is needed for storage of data, apps, etc., the functions of storing those things, running applications and an operating system, and maintaining a desktop are all done in software.

This is the essence of virtualization — using software to duplicate all the functionality of a computer or server except electrical and network connections. The software that enables the virtualization is designed just for this purpose.

Many state and local governments have consolidated multiple data centers into just a few facilities by replacing hundreds and thousands of physical servers with virtual ones. Many virtual servers can reside in a single cabinet or box made specifically for hosting them. The cabinet has the necessary physical connections that provide electrical power and, through software, links each virtual server to the network.

When it comes to mobility, focus shifts to the devices government employees carry with them to do their jobs. It would be very convenient for these employees to have the same computer set-up wherever they go. Going one step further, it would be especially convenient to have the same set-up for different devices, from laptops to smartphones.

Enter the virtual device infrastructure (VDI), which can create just such an identical computer set-up on any physical mobile tool. Just as a server's functions are virtualized to create a virtual server, so can a computer set-up be virtualized using a VDI. The exact set-up of an individual's computer — office, laptop, whatever — can be replicated down to the tiniest detail with a VDI. This software representation of a specific computer set-up, frequently referred to as a virtual desktop — the "desktop" that you see on a computer monitor, not the type of computer that sits on a desk — is then stored on one or more servers in an organization's data center or in a public or government cloud.

A VDI can be used on any device that has a keyboard and a monitor large enough to display the virtual desktop. This means most laptops, netbooks and tablets are fine as they are, but a smartphone would need a docking station with an auxiliary keyboard and monitor.

When running applications on mobile devices, it is transparent to the user that the actual computer is remote. Any change a user makes, such as writing a new document, updating an old one, or even changing the way icons are displayed on the monitor, is stored on the server in the data center instead of on device itself.

Wherever a user goes, and whatever device the user has, as long as he or she can access the data center or cloud that stores the VDI, the same computer set-up is available down to the screen saver and designated alert sounds. Consequently, people can be just as productive in a hotel, remote field office or distant conference as they can be back at the office.

Ultimately, this uniform performance results in increased productivity across the board. That usually correlates with better service for constituents — faster responses to queries and more rapid execution of tasks like permitting, inspections, repair and maintenance.

VDIs also reduce the number of physical devices that a state or local government employee may need to do his or her job. Perhaps only a laptop is needed instead of a desktop and a laptop. Perhaps a smartphone with a dock and auxiliary devices is sufficient for some employees. Perhaps a tablet is fine for some tasks or some employees' entire jobs. So not only does VDI enhance employee productivity and constituent happiness, but it also gives governments the option of reducing expenses for hardware and its upkeep.

There is yet another way that VDI can save money for public sector organizations. All the processing performed with VDI uses the server's processors, not those of the

physical device the user has at hand. Therefore, it does not matter how old a device is; it can still operate current software by VDI because the server back in the data center or cloud is doing all the work. Thus, any equipment, from expensive, ruggedized devices needed for some types of field operations to desktops used in offices, can remain in service and still "run" current applications. Even obsolete hardware can be used.

All the physical device does is access the VDI on the server. The physical device becomes a "thin client" or "dumb terminal" — a box that displays the VDI, but does nothing else. This aspect of VDI means that governments suffering from budget woes can delay equipment replacement, even when it is obsolete, yet still use the latest applications.

THE CLOUD

With all the hype about the cloud, it is no surprise that more than half of 646 public sector employees responding to a survey on the topic confessed to confusion between cloud computing and virtualization.[6]

So what is cloud computing? Clouds are a large pool of easily usable and accessible virtualized resources that can be dynamically reconfigured to adjust to a variable load, allowing for optimum resource utilization. Cloud computing is a pay-per-use model in which guarantees are offered by the provider through service level agreements.[7]

The "public" cloud is available to anyone who can pay the generally low fees. A "private" cloud is often built and used in-house, but the resource may be offered for a price to partners, associates and customers. "Hybrid" cloud solutions use a public cloud for some purposes, such as data storage, but keep other tasks in-house.

Clouds enable mobility in multiple ways. Since a cloud is accessible from anywhere, mobile users can retrieve data stored there, make updates to it and store the new information. A vast array of applications resides in the cloud as well, enabling mobile users to do everything from handling e-mail to collaborative document creation.

The cloud also hosts many types of services, such as printing via e-mail, using databases, or operating an organization's entire back office. The virtual device infrastructures described earlier frequently "live" in the cloud, letting mobile users fire them up whenever and wherever they wish on whatever device they choose. The cloud makes anytime, anywhere access to information, applications, hosted services and virtual devices a reality for mobile users.

We will explore more on the cloud and virtualization in the upcoming Special Report on Cloud Computing.

APPLICATIONS & SOCIAL MEDIA

Adoption of mobile devices is growing at a rate much faster than that of the original Internet, and mobile Internet use will exceed desktop Internet use by 2014.[8] Much of that growth is due to apps and social media, which let consumers do almost anything on their smartphones and tablets and share it with their friends.

What people can do in their personal lives, they want to do in their dealings with government. They seek apps that let them get data, transact business and communicate with government. An ever-growing list of apps lets them do just that.

One example is the widespread and extremely popular "break-fix" apps that allow constituents to photograph a pothole or broken streetlight and send an e-mail of it to the local public works agency. Another app, used in several cities, lets citizens search for vacant parking spaces and even pay the meters with their mobile devices.

On the government side, the first mobile apps sent data out to the public. The next round, like the two described above, enabled two-way communication. The next step, under way now, is the development of apps for government field workers, such as inspectors, law enforcement, emergency responders, health workers, social workers, and utility and public works personnel. A couple of examples include e-citations and electronic permit inspections.

Some governments have a well-thought-out mobile strategy that drives app development. Others are trying out existing apps to see how well this thing called mobility works before developing a strategy.

One current app issue is the "native" vs. Web choice. Native apps — built for specific devices — are more elegant, can store and forward data and can be rolled out faster, but they must be re-built for each operating system and form factor. Web-based apps that any device can use need only be built once, but they are less elegant and can only be used when a device is linked to the Internet.

Just as citizens expect helpful government apps, they also expect to interact with government via social media. On June 12, 2009, then-Federal CIO Vivek Kundra blogged, "If you are on Facebook or MySpace, government should be accessible there, too. This is the core of what we call 'context-driven government.' … That is why the White House has created communities on Twitter, Facebook, MySpace, YouTube and Flickr …"[9]

The message has not been lost on state and local governments, which have flocked to social media in large numbers, blogging, tweeting, and connecting through Facebook and other sites. It's a good way to find out what constituents want and a quick way to get official messsages out.

SECURITY & MOBILE DEVICE MANAGEMENT

Because mobility involves so many separate elements — the cloud, the devices themselves, in-house data centers and back offices, and the network — security is not simple.

Public cloud computing's security has always been a concern for IT, and it still is. In a survey of 643 public sector IT professionals, 62.5 percent of federal and 42.2 percent of state and local government respondents cited security as the biggest barrier to their adoption of the public cloud.[10] Those concerns are only exacerbated by the recent highly publicized breaches of cloud computing provider GoGrid and the cloud where Sony stored the records of 100 million customers. The alleged use by a hacker of Amazon's Elastic Computer Cloud (EC2) service to attack Sony just makes it worse.[11]

Because iron-clad proof of impenetrability is not an attainable goal, careful attention in the choice of a provider is the best route. Making sure the provider has security-specific certifications such as FISMA is important. However, according to the survey described above, over 56 percent of federal IT professionals and over 36 percent of state and local government IT professionals said that existing federal security standards and regulations need to be supplemented with additional cloud security standards and regulations, best practices and guidelines.

Ultimately, government leaders should employ strong due diligence and can conduct their own research by finding other customers of the provider and talking with them. During the trial/demo period, leaders can evaluate the provider's security.

Mobile security can be approached in a couple of ways, depending upon the number of devices. If only a few mobile devices are involved, then security can focus on them, assuming the network and back office/data center are also secure. If many mobile devices are in use, then "endpoint security" becomes unmanageable, and an organization-wide mobile management solution makes device security much easier.

Endpoint security focuses on making the devices themselves as impenetrable as possible. To start with, and no matter the organization size, a device audit is required. Next, just as with computers, strong passwords are needed, and devices must be regularly updated with the latest operating system versions, patches, antivirus software, intrusion prevention, and any other necessary programs. It also helps if the organization encrypts all transmissions. Because most of these steps (except encryption) are voluntary, employees must understand the risks involved and their role as the first line of defense. If the variety of devices makes security overwhelming, management may limit the list of acceptable devices.

Management may impose rules, i.e., develop a policy about the types of data that can be stored and when and where it can be used. Other rules may dictate the online sites, including social media destinations, that may be visited or from where information may be downloaded. Again, with no automated central device control that pushes policy to devices, policy adherence is voluntary.

When the number of devices goes beyond a dozen or two, mobile device management platforms become essential. These solutions reside in the organization's data center or back office and automate all aspects of device security. Devices are automatically provisioned: identity verification, authentication and access privileges. Usage and access can be tracked and logged. If a data-packed smartphone or tablet is lost or stolen, mobile device management platforms can reach out remotely and erase all corporation information, leaving any personal information untouched.

With mobile management platforms, policies are automatically pushed to devices so that, for example, an attempt to access data without appropriate privileges will be denied, as will attempts to access off-limits websites. All software

updates and upgrades are sent out over the air without user involvement. Of course, with or without mobile device management, network and back office/data center security is essential, and encryption is always a good idea. And even with mobile device platforms, IT may choose to limit the types of devices permitted in the organization. What these platforms do is eliminate the voluntary and device-by-device provisioning, updating, upgrading, patching, policy adherence, etc.

Device security can also be obtained through virtual device infrastructures, described previously. With this method, the VDI contains all security features and rules, regardless of the physical device.

Network security, for mobility as for everything else, is mainly about access control and intrusion prevention, such as firewalls and threat detection/denial. The first means proving identity and only using the network in the ways you are allowed to use it — for example, only accessing data you have permission to access. The second means preventing attacks, including keeping malware out.

Network access control is set through provisioning and maintained as all other security is, by strong passwords and keeping software and policies up to date. Intrusion prevention is provided by solutions that detect, recognize and deny threats.

Antivirus software is necessary but insufficient; intrusion prevention requires real-time or near-real-time searches for threats and keeping up to date on the means to deny them access to the network. With a mobile management platform, intrusion prevention will automatically be installed on mobile devices, but it must also be installed on the network, and elsewhere as needed.

Mobile security, like other types of security, is a matter of identifying all possible points of entry and securing each of them. It is also a task that never stops.

STRATEGY & POLICY

Although strategy and policy are not the same thing, they tend to overlap and blur around the edges. Strategy refers to the top-level goals and aims of an organization, and policy refers to the implementation of those goals and aims.

All too often, strategy is lost in the glow of the latest mobile device's "cool factor." Sometimes, everyone from the CIO on down wants it without giving much thought to the organization's goals and if or how the device fits in.

A sensible strategy requires serious thought about two basic questions:

- What is our mission?
- How can mobility help us achieve it?

Governments are well aware that their mission is to serve constituents. Examining how mobility can make that service better, faster, more efficient and less expensive is how strategy is developed.

This is simple, but by no means easy, because it means looking at how jobs are done now and envisioning how they can be done better, cheaper, faster and more efficiently with mobile devices. Sometimes, the ways mobility can improve things do not become clear until after implementation. Many governments have discovered, for instance, that because mobile employees usually no longer need desktop computers, office telephones, or even offices, they can reap significant and unexpected equipment and real estate savings.

Implementing strategy is typically much messier than creating it. Decisions about the types of devices, form factors, ruggedness, data access, security, websites, social media, apps and many other details must be decided, often after a problem has developed. Can employees use their own devices? Can they speak as civil servants on social media and blogs? Can they use commercial apps on their mobile devices or only those developed in house? Can we develop apps in house? This is just a sample of the plethora of specifics that must be addressed.

Challenges to Mobility

THREATS

Mobile-capable versions of blogs, social media and all other sites are vulnerable to hackers bent on disruption and financial gain. Where apps are developed and offered for download without controls, scrutiny and security, they, too may become a vector for attacks. Good security practices are the best prevention against these threats.

Data leakage, i.e., the loss or outside distribution of important or sensitive corporate data, is a common threat to business and government, with or without mobility. Whether the leakage is intentional or unintentional, the best offense is good policy and clear communication with employees about the value and sensitivity of data and the risk its loss entails to the organization and the individual. Prevention of malicious, intentional data leakage might best be accomplished by equally clear communication about punitive actions that can be dealt to the guilty, including civil and criminal penalties.

Electric power outages, node equipment failures, excessive traffic and attacks are common causes of network crashes. Backing up power sources and node equipment, a standard operating procedure, minimizes or eliminates outage time.

Excessive traffic requires additional bandwidth, if it is not from an attack. Network providers continue to build out networks as fast as they can, trying to keep ahead of the blazing rate of mobile adoption. Attacks of any kind can only be dealt with through good security measures, previously described.

Network incompatibilities can generally be solved with new hardware, software intermediaries, network upgrades or network replacements.

Cloud crashes and security breaches arise from causes similar to network failures and breaches. If a cloud provider integral to an organization's business suddenly ceases operation, having a back-up is the only immediate option. If that does not exist or also fails, then waiting until the provider resumes service is the only alternative, unpalatable as it may be.

If due diligence was performed before a cloud engagement, and the security was good, you have done all you could to protect your organization. The best approach to a breach is not to panic, but to find out what damage, if any, has been done and then deal with it.

PRIVACY

Location-aware devices can tell an individual where he or she is at all times. They can just as easily report a person's location back to a home office or headquarters. Such tracking is often implemented for safety reasons, as with law enforcement, social workers and other mobile employees, but it is easy to see how it could quickly become an intrusion into one's privacy.

As with other "slippery slope" issues, the best way to prevent such intrusion is to establish strong rules about when tracking is merited and when it is not. The development of such rules should involve everyone, not just management or IT. Once the rules are established, they should be firmly enforced. Ultimately, each user of a location-aware device must have the right and ability to turn it off and disappear into the landscape.

UNDERSERVED AREAS

Remote or lightly populated areas with little or no network access can build their own networks or wait until a provider installs one. Because it requires no expensive cell towers/antennas, but rather a web of relatively inexpensive hotspots and routers plus a high-speed landline network link, WiFi is one possible way to build a wireless network to support mobility. This is not to say it is cheap, just that it costs less than building a network of cell antennas and base stations.

WiMAX is another option, since it needs no landline network access. It does require antennas, but WiMAX antenna range is greater than cell antenna range, so fewer are required to cover the same area.

The new pre-4G Long Term Evolution and 4G Advanced LTE is a third option, although this technology comes from carriers. Not only does LTE have high-capacity data throughput, but it is also expected to provide long-range communications, requiring fewer antennae. Thus it may be less expensive for carriers to install in remote areas.

Government Mobility in Action

OUT IN THE FIELD: EQUIPPING UTILITY AND OTHER FIELD WORKERS

SALT LAKE CITY

Before Salt Lake City started its mobility initiative in 2006, building contractors might have to wait for days to find out what changes city inspectors required them to make before they could continue work on a project. The mayor's office frequently received complaints from contracting firms about the delays, which cost both time and money.

Prior to 2006, the building inspection process was entirely paper-based. Contractors would call in to request inspections. When an inspector left the city's Building Services and Zoning Enforcement Department in the morning, he would have a stack of forms that comprised his job list for the day. At a job site, the inspector would write

comments and notes on the different sections of the form, including a tear-off portion describing the changes that were necessary. This tear-off section was left at the site for the contractor. The rest of the form went back to the office for transcription. Often this form would be lost on the site or destroyed by weather or other conditions typical on a construction site.

This is the point where nearly all of the delays originated. Forms left at the job site might get lost in any number of ways. If the customer called in to get the changes, he might have to talk to several people before finding the inspector who had examined his job site. The in-office transcription task was also a problem. The city had no dedicated staff for transcribing the inspection reports; it was done by staff members when they had time. "There could be 150 reports a day," said Orion Goff, director of the Building Services and Zoning Enforcement Department. That sometimes resulted in back-ups of three to four days. When that happened, staff had to be dedicated to that task — taking them away from other important work.

In January 2011, Salt Lake City Building Services implemented the second version of an in-house inspection application that is integrated with leading commercial GIS software, such that "almost everything is done with maps," Goff said. "When inspectors open their laptops, all their work (i.e., their list of inspection sites for the day) is already on the laptops based on the GIS map layer and the inspector's assigned locations. The GIS can even map the best route for them. Customers can get inspection result information on their mobile devices. Salt Lake City sends it to them by e-mail. There is hardly any paper now."

The commercial product used for the inspections has an analytical component that gives the Building Services and Zoning Enforcement Department strategic insight into the department's performance and relationship with customers. City executives and managers and staff in the department can also see what is happening in terms of construction and development across the whole of Salt Lake City. The analytical component is an application that shows what is happening with building permits, building licenses and community and economic development, among other things.

The analytics application "ties directly into the inspection database, tying all our data together," said Lisa Shaffer, the development review administrator in the Building Services and Zoning Enforcement Department.

The benefits of the analytics are manifold. "We have used the analytics application to track the number of customers who walk into the building for any purpose to do with development, such as codes and inspections," Shaffer said. "We can see every day the number of customers who come in as well as the number of building permits today vs. the month's average. With the GIS component, we can see where applications are being submitted so we can see where development is happening in the city in real time. We don't need reports. Customers can go online or use their mobile devices to see their permit status, pay fees, and schedule inspections for already-issued permits."

As with the analytics application, civil servants and customers both benefit from the mobile inspection application. "It is saving staff time and paperwork," Goff said. "Inspectors can spend more time with customers on inspections. We have been able to re-assign staff to be more productive. For example, no one is now inputting inspector comments, and eventually no one will be dedicated to moving paper plans around the office." The staff that once had to transcribe inspection reports now "can deal with customers face-to-face and give them more time and help," Goff said. "They can introduce the customers to staff members to get them through the [permitting or other] process faster."

SAN DIEGO COUNTY

One year after Harold Tuck became the CIO of San Diego County, he became the head of the county's new Innovation Council. Founded in 2009, the Council brought together county and business leaders to incorporate advice and expertise from the commercial world and help the county solve the problems of government. "We had multiple goals," Tuck said. "We wanted to enhance workforce effectiveness by using existing technology better and by bringing in new technology. We decided to focus on mobility."

At a Mobility Day event held in the first quarter of 2010, several companies presented their mobile solutions and products to the county. One of the solutions, a mobility VPN (virtual private network) was an answer to a problem faced by all the different inspectors in the Land Use and Environment Group, one of five county business units. This solution gives the ability to access the county's case management systems by medical, social services and other caseworkers who must travel from place to place to do their jobs.

In 2010, San Diego County's Land Use and Environment Group's Agricultural Weights and Measures inspectors became the first county employees to pilot the mobility VPN. These 80 inspectors, of which seven were involved in the pilot, conduct 60,000 inspections per year, monitor pesticides on farms, preview and review public works projects and monitor air pollution, among other things. They all faced the same problem, one created by geography.

"Eastern San Diego County is mountainous and rural and has huge network connectivity problems," said David Lindsay, the information technology manager for the Land Use and Environment Group. "If you lost the network connection, you lost the [inspection] application. Users had to restart the connection five to ten times a day. This wasted about six minutes each time, adding up to about 30 minutes to an hour each day, plus [the inspector] would lose all the work [he'd done]."

The new solution that the Land Use and Environment Group piloted in 2010 "keeps the user engaged in the application even if he is disconnected," Lindsay said. "You don't have to re-connect. It can detect what wireless networks are available and select the best connection [for the user's location], so the user doesn't need to know what network is around," Lindsay said. "It is seamless to the user. The application never crashes."

All these technology improvements have greatly increased inspector performance. This solution has also been adopted by the county's public health nurses, the Department of Animal Services and other organizations within the county.

"The savings of the program in the trial was impressive," Lindsay said. "We increased productivity by 31 percent or approximately 2,500 additional inspections annually. Time spent traveling to the work district was reduced 100 percent, adding a value of $90,000 annually. A 14 percent reduction in miles driven vs. fuel consumed equals an average monthly vehicle mileage savings of 3,354 miles, or approximately 40,000 miles annually. [We have] no need for LAN or desk phone lines. There are also potential reductions in office space with associated savings.

"We estimate the annual savings at $41,200 plus the $90,000 value of staff time redirected to more productive activities for a total value of $131,200 for just one program with seven inspectors. Since the trial, the program has been implemented with other department field staff; however, the savings for the additional programs have not yet been fully calculated," Lindsay said.

The network and case management solutions are just small elements of San Diego County's full-scale Government WithOut Walls (GWOW) mobility strategy. It will ultimately include unified communications, a voice-to-text translator, a Web-based meeting tool, and a re-vamp of the county's Website so that it is much more mobile-friendly and device-agnostic for county employees and constituents. Tuck explains the essence of the GWOW mobility strategy: "It doesn't matter where you are, we want to be there."[12]

RALEIGH, N.C.

When it comes to mobility, the capital city of the Tarheel State is no novice. Raleigh equipped its police force with in-vehicle laptops in the late 90s. In 2006, it did the same with its inspectors.

According to Lawrence Cullipher, the Raleigh Police Department's IT manager, the first laptops installed in police vehicles operated on the old CDPD (19,200 baud) dedicated network. The only function officers could perform was to interface with CAD. Today, each laptop is equipped with broadband aircards. Officers now have access to the Internet, records management system, city e-mail and numerous Web-based public safety applications. Each laptop has the full suite of Microsoft Office products, plus a thermal printer. Now officers can issue electronic citations, complete electronic accident reports, even complete their incident reports online and transmit all this data back to the department's servers. Today, the police cruiser is truly an office on wheels.

> "We are mirroring the trend of consumerizing IT — smartphones and tablets. This is a completely different animal. It is not driven from the top. It is happening organically. Consumers are buying these devices in astronomical quantities despite the economy. People just purchase a device and bring it to work."
>
> JONATHAN MINTER,
> CHIEF TECHNOLOGY OFFICER,
> RALEIGH, N.C.

The city's mobile philosophy is simple, practical and straightforward. "Our strategy is to increase the amount of time employees can work in the field and reduce the time they spend in the office," said Jonathan Minter, the city's chief technology officer.

"The first goal was getting access in the field and connectivity," Minter said. That

was accomplished with commercial broadband data cards in laptops that allowed employees to work beyond the office and still stay in touch with it. The police department used standard laptops. Most inspectors had expensive ruggedized laptops.

"Goal 1B was getting WiFi access in all city buildings," Minter said. "Now we have relatively ubiquitous WiFi."

Today, though, "we are heading into a new era with our mobile strategy," Minter said. "We are mirroring the trend of consumerizing IT — smartphones and tablets. This is a completely different animal. It is not driven from the top. It is happening organically. Consumers are buying these devices in astronomical quantities despite the economy. People just purchase a device and bring it to work."

To take advantage of this groundswell of employees bringing their own devices to work, the city offers an option to reimburse the cost of a smartphone and provide a monthly usage stipend. It will also help employees link their smartphones and tablets to the city network. Those employees who bring their own device to work are responsible for their own contract, device and technical support.

The inspectors' laptops reflect the IT consumerization trend, too, but not by disappearing. "They are moving away from the traditional ruggedized laptops," Minter said. "We aren't getting the value for their cost, which is more than twice as much as commodity laptops. The ruggedized laptops are harder to use, heavier and slower. We have no military applications that need them. So we are moving to less-expensive, medium-level ruggedized or standard laptops — not 100 percent, but there is a move away. Commodity laptops are good enough for the price."

Flexibility and attention to mobile trends are good things in a government, but these characteristics also create new problems for Raleigh. "The question is how do we support all the different devices?" Minter said. "We have a secure WiFi network configuration, but it doesn't support Android. That wasn't a problem two years ago because Android didn't exist. Now it has the biggest market share of all smartphones. So we are tweaking our WiFi and VPN network infrastructures so we can support it."

The "tweaking" consists of changes to the security protocols for both networks. "This is what our mobile strategy is — making sure that our infrastructure is flexible enough for change," Minter said. "We must support this wave of devices that we have no control over. There is no need to convince people that mobility is a great thing."

The first version of the city's mobile strategy was to support employees who work away from offices. Now, Minter said, "we also want to enable knowledge workers to use their preferred technology. As knowledge workers bring new devices in, we want to make sure the infrastructure supports them, as well."

Although the city's field inspectors are moving towards less rugged laptops, Minter said laptops will not disappear in favor of other devices. "Several departments view laptops as key enablers for disaster and recovery operations," he said. "When buildings are closed down, employees can respond with laptops."

This approach was solidly proven when Raleigh was hit by a number of tornadoes on one day during the spring of 2011. Damage assessment is the first thing city inspectors do after such a disaster, and the amount of and timing of help from FEMA depends on those assessments. The time it takes for inspectors and the city to perform the assessments, verify the data they are based on, calculate the dollar total of the damage and create a map of the stricken areas has changed greatly over the last 35 years, thanks to advances in IT, and more recently, to mobile IT.

"In the 1988 tornado, it took about a week to complete the damage assessment, but then several weeks to determine total value," said Colleen Sharpe, Raleigh's GIS manager. "It took six months for us to create one map. With Hurricane Fran in 1996, it took over a week for us to do the damage assessment, another week to key in all the data, and a couple of days to get the value and the map once we entered the data. In the April 2011 tornado, it took two days to complete the damage assessment, a day to verify the data, calculate the total value, and create a map. Overall, we went from weeks to days."[13]

SOCIAL WORK AND HUMAN SERVICES

MICHIGAN DEPARTMENT OF HUMAN SERVICES

From the start, social workers in the Michigan Department of Human Services spent some time in the field with clients, an hour or two a day driving to meet clients, and a lot of time in the office. The clients include children, adults and care facilities. The social workers' tasks include protecting children who live at home or who are fostered, protecting adults, inspecting and licensing the care facilities, and performing other kinds of social work.

"Drive time is about one to two hours a day," said Duane Berger, chief deputy director of the Michigan Department of Human Services. "There are many distractions in coming to the office, such as looking for files, writing reports, and other paperwork. Phone calls take up a lot of time. The social workers can spend half a day returning calls."

If social workers must attend regular in-office meetings, their time in the field with clients is reduced even more. On top of that, by 2010, the ratio of client cases to the approximately 2,200 DHS child welfare social

> "You can't manage mobile workers by walking around, so we are really focusing on management training for supervisors. They can kill it all if there is no change in management style. If, for instance, the manager requires a staff meeting every morning, that defeats the program."
>
> DUANE BERGER, CHIEF DEPUTY DIRECTOR, MICHIGAN DEPARTMENT OF HUMAN SERVICES

workers was more than 20 to 1, which, combined with high levels of attrition, meant that clients were not getting the services they needed.

"The social workers want to take care of these kids," Berger said. "It became obvious that there were many built-in distractions that prevented them from carrying out their core mission, which is out in the field."

"The social workers were always mobile workers, but we gave them office equipment. We are finally equipping them properly. This is not so much a mobile strategy as properly equipping our employees to facilitate their mobility."

DHS' budget does not have a "mobile equipment" category. It does, however, have a "technology refresh" category. "So we are buying mobile technology on a 'refresh budget,'" Berger said.

In late spring and mid-summer 2011, DHS deployed 200 "bundles" of mobile technology, which included smartphones and light-weight laptops. Both devices include cameras. The smartphone cameras are for photographing clients and their homes as part of the social workers' standard work process. The laptop cameras are for planned videoconferences that social workers can attend from the field.

To connect to the state's secure wireless virtual private network, the smartphones contain built-in "hotspots." The laptops connect to the smartphones and use them as the gateway to the network.

"Right now, the social workers take notes in the field and type them back in the office," Berger said. "[The mobile devices] will increase the speed and accuracy of reporting, leading to a significant improvement in the timeliness and currency of information as well as helping social workers care better for children and families. That will increase employee retention as employees can focus on why they were hired, where their passion lies."

The recent hiring of 500 new, next-gen employees to work in child welfare is also expected to reduce attrition. "This was part of the effort to get the 20-plus to one ratio of claims down to a more reasonable 15-to-1 level for child welfare," Berger said. These new workers were the first to get training on the new devices, but all the social workers will receive it by the end of FY 2013.

The training will coincide with the phased purchasing and introduction of additional equipment. Berger plans to add 300 more "bundles" in 2011, then 600 more in 2012 and again in 2013. Yet, Berger is not concerned with the social workers' ability to adapt to mobility.

"The biggest training is not for the workers, but for the supervisors," he said. "You can't manage mobile workers by walking around, so we are really focusing on management training for supervisors. They can kill it all if there is no change in management style. If, for instance, the manager requires a staff meeting every morning, that defeats the program."

A limitation on the mobile strategy is the current client database. "It was not built for mobile technology," Berger said. "So it can't be accessed by the Web. Social workers have to get to the files in another way." This will change by October 2012, with a Web-based application in the works.

"Mobile workers have more flexibility in their job," said David Behen, Michigan's CIO.[14] "They don't have to come to the job, get a job ticket and go to the work site.

Instead, they can go straight to the job and get all the information they need through mobile devices. Organizations and employees will be more efficient, errors will be reduced, services will be sped up and the number of offices needed will be reduced. Customer service will be increased, and we are measuring this. Employee and customer satisfaction will increase, and so will the employees' quality of life."

Besides these benefits, Berger said that with the social workers spending more, and perhaps nearly all, of their time in the field, fewer offices will be needed. Although this is not a primary goal for DHS, Berger said, "We expect to save money on rent, but we may spend some or all of the savings on mobile technology. For every dollar I save, I hope to spend half of it on mobile tools."

For the next two years, DHS will be rolling out its new mobile tools and upgrading its client database. There will also be a different occupancy model. "Employees can work at home, and we'll have hoteling," Berger said. DHS is creating a call center for client support. Right now, when a client calls in with a question, the only person who has all the details needed to correctly help is the individual's social worker. With electronic reporting and data records, however, this information will be available to call center personnel, and clients can get questions answered much faster than when they must wait for the social worker to return their call.

The state's welfare system is also creating a Web-based portal where clients can go to perform transactions that have always before required a trip to a DHS office. Community partners, such as hospitals and nonprofits, will also provide clients with access to the portal in their offices.

"Our role is to help people who need help," Berger said. "We need to be out there to provide that help. It leads to better health and safety for all."[15] All it took was equipping mobile workers with the right tools.

LAW ENFORCEMENT AND EMERGENCY RESPONDERS

OKLAHOMA CITY

Several years ago, Oklahoma City launched a major public safety capital project that focused on enhancing the capabilities of public safety departments through mobility. At that time, police and fire department personnel in Oklahoma City were using old, inflexible, limited data terminals in their vehicles. The city also had a conventional public safety radio communications system with 35 channels (much like different radio channels in your car). Police had assigned channels, and the fire department had different assigned channels. Even in emergencies, the two organizations could not communicate directly with each other.

This system, with police on one channel (or set of channels) and firefighters on another, is identical to the one that existed in New York City on September 11, 2001. The inability of fire, police and other emergency responders to communicate with each other contributed to much of the chaos of that day. Since September 11, public safety and first responder organizations across the country have strived to upgrade communications systems to eliminate these channel incompatibilities.

This was Oklahoma's first goal for the public safety capital project. Another goal was the replacement of the old limited-function mobile data terminals used by police and fire with up-to-date mobile computers. With new devices, public safety personnel could send and receive vital information whenever and wherever necessary. A third goal was the implementation of a new computer-aided dispatch system that was also integrated with a geographic information system.

Ultimately, the city got much more capability than it ever thought possible. Best of all, even with all the added capabilities, the project cost the same as the original proposal. Funding came from a one-half cent sales

tax approved by city citizens that lasted from July 2000 through February 2003.

The city's original plan was to build a new "trunked" radio system, in which all available bandwidth on any specific local or long-distance network is time-shared among users. However, several RFPs suggested the installation of a WiFi network instead of a trunked radio system.

"We implemented the [WiFi] network, which was dedicated to public safety [and not for general municipal use], across a 520-square-mile footprint," said Kerry Wagnon, the city's public safety program manager for IT. "It included fixed routers in the city and mobile routers in the police and fire department vehicles."

Within this 520-square-mile, densely-populated area of the city, approximately 1,700 fixed routers were put in place, working out to roughly 3.25 routers per square mile. The city planned ahead so that any new WiFi networks built for consumers would not interfere with the public safety system. The network automatically adjusts to emergency situations.

Oklahoma City chose not to rely solely on the WiFi network for public safety. "We also use commercial broadband and middleware that lets the computer in a vehicle choose the nearest available router, whether it's WiFi or commercial broadband," Wagnon says.

The new, computer-aided dispatch system, which is integrated with a geographic information system, depends on the WiFi network to identify the location of police and fire vehicles. "The connectivity tells where the vehicle is," Wagnon says. "The dispatches go out to the mobile data computers, and all the information is automatically updated."

With the new network and computer-aided dispatch system, human dispatchers no longer need to canvass police or fire personnel to decide whom to send to an incident. The new mobile data computers give police and fire personnel full offices in their vehicles. Police officers and firefighters can access shared network directories, collaborate on documents and management workflows, and use other Web-based tools, including e-mail.

While in their cars, Oklahoma City Police can obtain information from the local crime database as well as from the FBI's National Fingerprint Database by using their mobile data computers. Similarly, firefighters use the mobile computers to obtain building plans, fire department diagrams and plans for fighting fires in those buildings.

Although specific metrics were not developed to evaluate the performance of the various elements of the public safety capital project, Wagnon said, "Qualitatively, we know there is huge improvement. Most of the improvements have been in terms of cost containment. [The new technology] allows police and firefighters to do their jobs without adding any more employees. They can do more from the field because now they have the information to make decisions in the field."

MICHIGAN STATE POLICE

Across the nation, it is not uncommon for state police's responsibilities to consist exclusively of patrolling interstate and state highways. In Michigan, however, "We also serve as the primary law enforcement in the unincorporated areas where there is no police force," said State Police Inspector Mike Brown.

The majority of these unincorporated areas are the 83 counties of the Great Lakes State. For the last 15 years, Michigan state police officers have been assigned to specific counties and attached to an office, or post, in that county. The troopers had laptops and access to a network, but "it was piggybacked on county mobile technology," Brown said, meaning that both laptops and networks belonged to the counties but the troopers used them to provide police services.

Five years ago, the Michigan State Police began reducing its reliance on counties for computers and network access. That happened as a result of five previous years of effort on the part of the state, beginning in 2001, to build its own network. "In 2006, the state started piloting mobile worker plans and broadband services," said Amy Baumer, director of the Michigan Office of Enterprise Development. In 2010, greater attention was turned to a "more detailed enterprise mobile strategy," Baumer said.[16]

For the state police, that strategy led to greater mobile access to critical data plus electronic filing of vehicle crash reports and traffic citations. "We now have automated

data collection that tells where the officer is and tracks everything he does, whether it's investigating complaints, making arrests, or issuing citations," Brown said. This system functions as a daily log, but it also means that an officer's location is always known. That could save an officer's life.

To support these new, mobile versions of tasks that used to be done on paper in an office, the police also received new hardware. It came in two forms: 1) ruggedized laptops with multiple wireless connectivity options; and 2) three-piece in-vehicle-mounted workstations with detachable keyboards and CPUs that can go in the cabin or in the trunk. The workstations include GPS technology for indicating vehicle location. They also feature multiple wireless modems for connectivity to broadband data networks, either commercial carriers or the one built by the state.

"These tools have expanded the capabilities of the officers," Brown said. "They've increased the accuracy and timeliness of reports, especially for crashes. Those reports are completed five times more quickly from the field than when they're done manually, because of all the delays that get removed. The cars are more cluttered now, but the tools have increased efficiency and access to data. Ten to 15 years ago, when a state trooper stopped someone, he could only check to see if the name on the license was genuine, but there was no way to find out if the person was really who he claimed to be. Now, in the field, we can get pictures of people and see if they really match the license."

Approximately 500 of the 700 state police cruisers have been outfitted with the new computers. In the next year or two, Michigan plans to equip the rest of the vehicles. Ruggedized tablets or small netbooks may also be issued to officers for the times they are working in an office.

Yet another aspect of the greater mobility of the state police is the plan to close 21 of the existing 62 posts, or offices, around the state. This "regionalization" initiative will also involve re-assigning officers from a single county to the new regions, which average about three counties per post. "The officers will live in those areas," Brown said. "They can do all their tasks from their vehicles and the posts."

The regionalization plan, which will be completed in October, is expected to help Michigan address shortfalls in the budget, saving nearly $21 million in general funds.[17] This savings would not be possible without mobility. "We can eliminate posts because there is more capability in the field," Brown said.

The regionalization also ties in with the Great Lakes State's overall mobility goals, which are "to reduce the cost of doing business, increase the productivity and efficiency of employees, reduce occupancy costs, and increase the recruitment of the people we need," said David Behen, Michigan's CIO. "Mobility is a factor in retaining the talent we want. It increases employee satisfaction and the quality of life and reduces commuting time."[18]

For Brown and his 1,200 fellow officers, mobility means they can stay in the field more and thus do a better job of enforcing the law. "We are trying to make the field officer as flexible as possible so he can do 80 percent of his work there," Brown said. "It is very important to have the officers on the street."[19]

FEDERAL BUREAU OF ALCOHOL, TOBACCO, FIREARMS, AND EXPLOSIVES

Although its origins date back to 1789, the mission of the Bureau of Alcohol, Tobacco, Firearms, and Explosives has remained consistent: protecting American citizens from crimes, especially violent ones, relating to illegal trafficking and tax violations in the substances and devices listed in the organization's name.

In today's Bureau, it takes 2,500 law enforcement officers and 700 regulators, plus a large support staff of 1,800 and an additional 2,500 contractors and on-loan task force officers from state and local law enforcement agencies, to accomplish this mission. Under the jurisdiction of the U.S. Department of Justice, the Bureau's special agents investigate crimes, prepare criminal case reports, testify for the government in court or in grand juries, and gather and analyze evidence through a number of methods. Industry operations investigators perform inspections and inquiries related to federal regulations for the industries with which the Bureau is concerned.

> "We want to give field employees better tools, better and faster information access, and a better way for them to record their work."

DR. RICK HOLGATE, ASSISTANT DIRECTOR FOR SCIENCE & TECHNOLOGY AND CHIEF INFORMATION OFFICER, FEDERAL BUREAU OF ATF

For both groups, their work "mostly happens outside the office," said Dr. Rick Holgate, assistant director for science & technology and chief information officer, Federal Bureau of ATF.

Until recently, these Bureau employees' primary mobile tool for working outside the office has been a laptop. "If we can give users easier-to-use tools that are lighter and easier to carry than a laptop that can help them do their jobs better, then they can focus on what they do in the field and what they need," Holgate said.

To do this, the Bureau has examined a number of new consumer mobile technologies in the last two years. First, it looked at alternatives to the government-standard

BlackBerry. In 2010, it began looking at tablets as alternatives to laptops. A number of special agents and inspectors were issued 150 laptops in a pilot effort that was still under way in mid-summer 2011. "We are looking for better tools that provide more capability for less cost," Holgate said.

If the laptop pilot is successful, and if funds are available, Holgate says several thousand of the devices could be issued to mobile workers throughout the Bureau. The inspectors and special agents may not wait that long, however; "there is a significant groundswell for allowing some level of 'bring your own device,'" Holgate said. "If the employee owner will sign up for the same controls and management as the ATF-issued devices, then it doesn't matter to the Bureau. It is attractive not to own all of these devices, but they do have to meet security and policy requirements."

ATF's mobile portal was rolled out about a year ago, but not for consumers or "customers," as with most government portals. It was for the Bureau's mobile employees. "We want to leverage it so it can be a gateway for mobile devices to get to critical ATF information," Holgate said. Initially, access to the portal was going to be through a Web browser.

That thinking has changed. "In some cases, you need to have information available locally on the device," Holgate said. Those cases include functions like e-mail, contact lists, and having documents available for reading and editing without being tied to a website. "With the portal-centric approach, everything is on the website," Holgate said.

So ATF is "now thinking more about apps," he said. The Bureau has no intention of becoming an app-development shop. Instead, "we plan to use apps already built for the devices, such as getting to e-mail attachments, opening and editing documents, or taking advantage of specific business intelligence apps," Holgate said. "It is best to use existing apps for those purposes."

One app that was developed specifically for ATF is e-Trace. It "kicks off the very manual process of tracing a firearm for law enforcement," Holgate said. "It can also track the workflow of the process and package the firearm report at the end." ATF runs about 300,000 such traces every year, and about 30,000 law enforcement officers, including some from other countries, currently use the app.

As ATF continues to experiment with mobile devices, the Bureau seeks to achieve three major goals. First, "We want to give field employees better tools, better and faster information access, and a better way for them to record their work," Holgate said.

A second goal is to develop a "better business case for providing devices for users, for example, replacing laptops with tablets or with a combination of a tablet, smartphone and a client for office workers while also reducing the cost of the device portfolio."

The third goal is to reduce the cost of real estate required for employee workspace. "We want to think more creatively about how space is paid for and provisioned," Holgate said. "What's my model for office space for different types of users, and what should the infrastructure be?" For example, Holgate says that special agents probably need minimal office spaces, less or different office infrastructure (no desk phones), and collaborative work spaces instead of conference/meeting spaces.

"We understand the potential benefits of mobility," Holgate said. "Now we want to know how best to achieve them in the lowest-cost way."[20]

The Portal: Transforming Constituent Interaction with Government

When Arkansas launched its first mobile Web portal in April 2009, the goal was to inform state citizens how stimulus funds would be used. When the current portal, http://mobile.ar.gov, was launched in June 2010, its dual purposes included providing more mobile services to citizens and increasing the knowledge and use of broadband technology in the state.

It took no time at all for the portal to start racking up successes in both directions. "The first transaction for a government entity went online in September 2009, when the game check app, developed by the Game and Fish Commission, became available," said Claire Bailey, the state's director of the Department of Information Systems.

The game check app has been hugely popular, piling up more visits and use than any other mobile app on the portal. It allows hunters to report their harvested game to the state, which is a legal requirement, but they no longer have to physically find a game check station and complete paper forms to obey the law.

On top of that, however, they can share photos of their triumphs — and prove the fish really is that big — with friends on Facebook, which is integrated with the app. Even more, a Twitter feed provides alerts in case of bad weather or other emergencies, so hunters and fishermen can leave remote recreation areas while it is still safe.

In April 2010, http://mobile.ar.gov launched three secure payment transactions. Families and friends of prison inmates could deposit funds to their trust accounts. Parolees can pay fines and make restitution payments through the portal. And the ordinary citizen can pay property taxes with their smartphone or tablet from wherever they happen to be. The number of cities and counties where taxes can be paid through the mobile portal is growing rapidly, and so is the number of citizens taking advantage of it.

Perhaps the biggest impact on state citizens has been the "Youniversal" scholarship app. It could not have happened without a huge effort on the part of the Arkansas Department of Higher Education to simplify the byzantine process for applying for financial aid for college. With the old system, an average of 18,000 students each year received just under $48 million in financial aid from the Arkansas Department of Higher Education. "People didn't know how to apply or how to find the money," said Bailey.

The revamped Universal Financial Aid System, launched on January 1, 2010, consolidates 21 existing aid programs from multiple government agencies into a single database. Then a search engine accepts the necessary information about the student and the parents and starts looking. "For a student applying for financial aid, it performs a search for all scholarships and grants he or she is eligible for," Bailey said. In the new system's first year, every student who was eligible — 30,000 students — received more than $120 million in financial aid.

In April 2011, http://mobile.ar.gov débuted the "Youniversal" smartphone app for the new financial aid system. The Youniversal

app is of course directed towards students, who make up one of the biggest users of the state mobile portal. With this app, current and hopeful students can access the financial aid system anytime, anywhere, with any mobile device. The National Association of State CIOs quickly recognized Youniversal as the winning entry for cross-boundary collaboration and partnership.

As for increasing knowledge of and use of broadband technology in the state, especially in the 17 most depressed counties, "we want to showcase technology for them and show how broadband can be used," Bailey said. The state is partnering with nonprofit organizations seeking to promote Internet access and education to achieve those goals. It is also seeking to ensure sufficient broadband connectivity for all citizens through landlines and fixed and mobile wireless.

Since the mobile portal was launched, the game check application has been downloaded tens of thousands of times and the agency has nearly the same number of followers on Facebook. It has also saved the agency thousands of man hours in manual effort now that real time game check data is available and they no longer have to collect the paper game check forms from check stations.

As new mobile devices appear in the market, http://mobile.ar.gov will respond with new apps. But a bigger goal for Bailey and her team is to open up the massive stores of data the state has collected. "We are figuring out how to expand the data the state has into new areas like mobile, especially for location-based services," she said.[21]

Funding for Mobility Initiatives

Mobility requires technology, and some of it can be costly. Governments need not always raise the funds internally. Collaborative contracts stretch dollars by helping governments obtain better pricing. Grants, which largely come from the federal government, provide funding for a variety of projects. Partnering with businesses or other organizations for equipment, expertise and services benefits all parties. Some government entities have made shared services centers of revenue. Smart use of existing funds can make mobility a reality. Tapping into community ingenuity, almost for free, produces surprising results.

CONTRACTS

Term, state and cooperative contracts operate similarly. Term and state contracts operate within a single state, whereas cooperative purchasing involves multiple entities. In both cases, all state government and tribal entities are eligible. The contract processes start when one or more eligible government entities identify a need.

For term and state contracts, once a need is identified, verified and validated, the state procurement agency releases a request for proposals. Companies vie for the contract by offering very advantageous terms, which they do because of the size of the customer base. Contracts always have end dates, which keep the process competitive and prevents vendors from indefinitely locking up the state business.

Once contract winners are announced, any state government entity can buy from them at much lower costs than if they bought on the open market. Procurement is greatly simplified, with no vendor qualification, competitive bidding or RFP evaluation. The term contract addresses it all.

With cooperative purchasing, different states take the lead in a group solicitation, issuing requests for proposals and awarding contracts based on their own laws and procurement practices. Although the lead state owns and manages the contracts, partnering entities follow their own laws. Many cooperative contracts already exist, and nothing prevents other entities from joining.

State and local entities can benefit from the enormous purchasing leverage of the federal government through the General Services Administration Cooperative Purchasing Program. This program lets state and local government entities purchase information technology hardware, software and services through contracts awarded under GSA Federal Supply Schedule 70. They can also purchase special IT items through GSA Consolidated (formerly Corporate Contracts) Schedule.

US Communities (www.uscommunities.org) is a cooperative purchasing organization comprising local and state government agencies, public school districts, higher education and nonprofits across the United States. Its buying scope is nationwide, giving members very good prices when they purchase products through its contracts. Almost 42,000 public sector entities in the United States participate in US Communities contracts, which annually total more than $1 billion for products and services.

This list of cooperative contract organizations is by no means comprehensive.

- Western States Contracting Alliance, www.aboutwsca.org
- State of Texas CO-OP Purchasing, www.window.state.tx.us/procurement/prog/coop/
- Educational & Institutional Cooperative Purchasing, www.eandi.org
- MiCTA (originally Michigan Collegiate Telecommunications Association, but the organization is now national), www.mictatech.org
- United States General Services Administration, www.gsa.gov
- PEPPM, www.peppm.org
- US Communities, www.uscommunities.org
- National Joint Powers Alliance, www.njpacoop.org.

FEDERAL GRANTS

Grants.gov is the central clearinghouse for all information on federal grants, which is the main source for grants for both state and local governments. (States also make grants to their own local governments, of course.) Grants.gov not only lists all federal grants by agency and program, but it also explains how to determine eligibility, apply and write a proposal.

The federal government offers a vast number of grants for law enforcement, health care, transportation, public assistance (following emergencies), emergency preparedness, social services, juvenile offender rehabilitation, criminal justice, energy projects, environmental projects … and the list continues indefinitely. Almost any of these areas could involve mobile technology. The chances of winning a grant for mobile technology depend heavily upon the rationale provided in the proposal.

PUBLIC-PRIVATE PARTNERSHIPS

In the United States, governments and businesses have been partnering for more than 200 years to provide both services and facilities. Today, these partnerships include information technology[22] and its offspring, mobility.

Effective public-private partnerships do not usually happen overnight, although that has occurred after natural disasters. Most often, they begin when a state or local government faces a developing challenge or identifies a trend that it lacks the expertise to address. At this point, government leaders reach out to the business community for advice, discussion, and insight.

This can be the beginning of a relationship in which both sides realize they can help each other. "The key to that collaborative partnership is trust in the relationship — confidence that builds as both parties are encouraged to explore emerging trends, new ideas and a better understanding of the challenges and issues faced by one another."[23]

As that trust develops, the two parties may form collaborative partnerships. These are "non-legal working relationships that often occur between the public and private sectors to meet a common objective or goal. Primarily goodwill gestures, collaborative partnerships are often used to provide knowledge exchange or collective leverage resources for a specified goal."[24]

At this stage, "It is not uncommon for technology firms and state IT organizations to collaborate to explore new technology that mutually benefits both parties."[25] Companies may be willing to provide devices at low or no cost to demonstrate the product and to gain publicity and good will.

If the collaboration is successful, the partnership may move on to a contractual basis, yet one which still relies upon trust and seeks "win-win" scenarios for both parties. The partnerships may last indefinitely, even if a company does not always have contracts with the public sector partner.

SHARED SERVICES

According to the Chief Information Officers of the States, IT shared services means that a single government entity provides IT services to other government entities.[26] It is not uncommon for a city to have an accounting system, enterprise resource system, data center, private cloud, or other technology asset that can be shared with the county in which it is located, or vice versa. Similarly, one state agency can provide other agencies or local governments in the same state with IT services. In most cases, the organization providing the service charges a fee. Despite paying the fee, the organizations using the services still pay less than if they had to run the service themselves.

An obvious mobility example would be the case where a state, city or county owns and operates a broadband data or WiFi network and shares it, for a fee, with other government entities. Data centers, mobile device management solutions, and similar resources could also be shared for fees.

SMART USE OF FUNDS

Although "mobility" may not appear in the RFP for grants or in an official budget, "technology" may. Mobile devices and supporting technology may also be legitimately covered by grant requirements for better customer service, reducing response time for permits, speeding up delivery of benefits and similar dictates.

In Michigan, a technology refresh budget was used to purchase mobile devices for employees who needed to spend more time in the field. If a legitimate argument can be made for spending money on mobility, no rules or laws are violated, and it better serves the public — smart use of existing funds or a well-written grant application can pay for the technology.

LOW-COST OR FREE APPS

New York City challenged developers to build apps for many public services, resulting in dozens of free apps, such as a 411 directory. Ottawa uses an innovator fund to reward high school and college student winners with small prizes in app-development contests. The Ottawa apps must make use of city and regional data that was recently made public. One app combines data to find the best ice skating location in the winter, based on temperature, thickness of ice and how big the crowd is.

The Ottawa government sees the contests not only as a way to get free apps, but also to attract young people to civil service, create new services and showcase the area's high-tech workforce to attract businesses.

On May 21, 2009, the United States government launched Data.gov with 47 sets of federal information. The goals, according to then-Federal CIO Vivek Kundra, were "to democratize data across the government and tap into the ingenuity of the public to develop tools that help the American people." Today, the site contains nearly 400,000 datasets, and more than 200 apps have been developed to make use of them.[27]

It is clear that the public has depths of app-development abilities and is enthusiastic about putting them to use. Tapping into that skill and enthusiasm is a winning strategy for governments, who get apps for free or little cost, improve services to constituents by making them more accessible via apps and engage the public in the business of government.

The Payoff

"The world is going mobile," said David Behen, chief information officer for the state of Michigan. "Agencies are begging for mobility. They know they can do more."[28]

Although Behen was speaking of Michigan, his words apply equally to every public sector entity in the United

When governments have no budget for innovation, mobility may provide a path for investing in it. This technology of smartphones and tablets also continues the government trends of greater transparency, lower costs, improved service, increased constituent involvement, and more flexibility.

States — federal, state, local, tribal, K-12 and higher education. Not only do they all know they can do more with mobility, they also know they can do it better, faster and for less money.

The case studies presented in this Special Report show how seven states and eight agencies reaped the payoff from mobility almost as soon as they put it into effect.

Salt Lake City vastly sped up its building inspection process. Builders in the city are so happy with the new approach that their frequent complaints to the mayor about delays dried up entirely.

In San Diego County, a mobility pilot involving just seven of 80 county inspectors saved more than $131,000. How much will the county save when all its inspectors are "mobilized"?

Raleigh was able to report total damages from an April tornado in three days vs. more than two weeks with Hurricane Fran in 1996 and more than six months with a 1988 tornado. How much difference does it make if a city gets disaster assistance in a matter of days vs. two or three weeks?

Although it is too early to know the details of how Michigan's social workers and their clients will benefit from mobile technology, having case workers work out in the field more than in the office will increase the time they spend with clients or let them see more clients. That is an improvement in itself.

Oklahoma City's firefighters and police can now spend more time in their vehicles and much less in the office, resulting in increased police presence in a city with one of the largest land areas in the United States.

The same is true for Michigan's State Police and the Federal Bureau of Alcohol, Tobacco, Firearms, and Explosives. MSP's vehicle crash reports, now reported from the field via mobile devices, are processed five times as quickly as when they were done on paper. ATF is seeking similar results as it proceeds through a laptop pilot.

Arkansas' mobile portal brought in a couple million dollars in revenue in its first year. At the same time, in conjunction with major changes in the state's financial aid process for college-bound students, the portal helped to nearly double the number of Arkansas high school students who received financial aid while simultaneously increasing the total dollars awarded by two-and-a-half times.

Although these benefits are impressive, they are just the beginning. When governments have no budget for innovation, mobility may provide a path for investing in it. This technology of smartphones and tablets also continues the government trends of greater transparency, lower costs, improved service, increased constituent involvement and more flexibility.

It took years to realize the benefits of computers in the office. Those benefits may arrive faster with mobility, or they may simply keep accruing as the technology keeps improving.

What might mobility do for your government's mission?

Endnotes

1. Rosenwald, Michael S. "Federal government loosens its grip on the Blackberry," The Washington Post, May 30, 2011.
2. "Gartner Reveals Top Predictions for IT Organizations and Users for 2011 and Beyond," press release, November 30, 2010.
3. "Garter Reveals …" Ibid.
4. "Point, Click, Talk: The 2011 CDW-G Unified Communications Tracking Poll," CDW-G, http://newsroom.cdwg.com/features/feature-04-04-11.html, April, 2011.
5. "Point, Click, Talk," Ibid.
6. "A Pulse on Virtualization and Cloud Computing," Quest Software, prepared by Norwich University School of Graduate and Continuing Studies, April, 2011.
7. "IT-as-a-Service in State and Local Government: Leveraging technology and innovative strategies to lower costs and provision services on demand," Center for Digital Government White Paper, http://www.govtech.com/library/papers/IT-as-a-Service-in-State-and-Local-Government.html. http://www.govtech.com/policy-management/Cloud-and-Virtualization-Definitions-Still-Confuse-Most-Govt-Officials.html, May 24, 2011.
8. Meeker, Mary, Scott Devitt, and Liang Wu, "Internet Trends," Morgan Stanley, http://www.scribd.com/fullscreen/29850507, April 12, 2010.
9. Kundra, Vivek and Katie Stanton, "New Technologies and Participation," http://www.whitehouse.gov/blog/2009/06/12/new-technologies-and-participation, June 12, 2009.
10. "A Pulse on Virtualization and Cloud Computing," Ibid.
11. Galante, Joseph, Olga Kharif and Pavel Alpeyeve, "Sony Network Breach Shows Amazon Cloud's Appeal for Hackers," Bloomberg, http://www.bloomberg.com/news/2011-05-15/sony-attack-shows-amazon-s-cloud-service-lures-hackers-at-pennies-an-hour.html, May 16, 2011.
12. Telephone Interview with Harold Tuck, CIO, San Diego County, and David Lindsay, Land Use and Environmental Group Information Technology Manager, San Diego County, June 14, 2011.
13. Telephone Interview with Jonathan Minter, Chief Technology Officer, Office of Information Technology, Raleigh, NC, June 27, 2011.
14. Telephone Interview with David Behen, Michigan CIO, June 24, 2011.
15. Telephone Interview with Duane Berger, Chief Deputy Director of the Michigan Department of Human Services, July 1, 2011.
16. Telephone Interview with Amy Baumer, Director of Services for the Michigan Office of Enterprise Development, June 24, 2011
17. Press Release, "Official Statement: Michigan State Police Announce Regional Policing Plan," http://www.michigan.gov/msp/0,1607,7-123-58112-253251--,00.html, March 24, 2011.
18. Telephone Interview with David Behen, Ibid.
19. Telephone Interview with Mike Brown, Inspector, Michigan State Police, June 30, 2011.
20. Telephone Interview with Dr. Rick Holgate, Assistant Director for Science & Technology and Chief Information Officer, Federal Bureau of ATF, June 27, 2011.
21. Telephone Interview with Claire Bailey, Director of the Arkansas Department of Information Systems, April 13, 2011.
22. "Top Ten Facts About PPPs," The National Council for Public-Private Partnerships, http://www.ncppp.org/presskit/topten.shtml.
23. "Keys to Collaboration: Building Effective Public-Private Partnerships," NASCIO, www.nascio.org/publications, May, 2006.
24. "Keys to Collaboration," Ibid.
25. "Keys to Collaboration," Ibid.
26. "The 2010 state CIO survey," NASCIO, http://www.nascio.org/publications/surveys.cfm, August, 2010.
27. "From Data to Apps: Putting Government Information to Work for You," Vivek Kundra, The White House Blog, http://m.whitehouse.gov/blog/2011/05/20/data-apps-putting-government-information-work-you, May 20, 2011.
28. Telephone Interview with David Behen, Ibid.

"Mobility is critical to the success of governments today, in terms of empowering workers and serving citizens. As such, mobile solutions must accommodate the needs of both parties – un-tethering the workforce and bringing them into the community with back-office maps and data, while allowing citizens to interact with government and request services anywhere and anytime."

DARRELL LEWIS
VICE PRESIDENT OF PRODUCT MANAGEMENT
ACCELA, INC.

"Mobility has become a necessity for government workers today. Whether they are tracking assets or managing an evacuation, they need the tools and applications that allow them to work from a remote location. Access to wireless networks both public and private, increases the efficiency of workforces and delivers information in real-time for better decision making."

JASON OPPENHEIM
MOTOROLA SOLUTIONS, GOVERNMENT & PUBLIC SAFETY
WIRELESS MOBILITY SALES - NORTH AMERICA
SALES DIRECTOR, EASTERN US / CANADA

"People are now using the same smartphones for both personal and work activities. Therefore, you're adding an additional risk into your environment with these types of devices. You can't manage these as a personal-only phone or a work-only phone anymore."

JOHN BORDWINE
CHIEF TECHNOLOGY OFFICER
FOR PUBLIC SECTOR
SYMANTEC

"Innovative federal, state, and local agencies recognize the importance of mobile and are making essential services available to citizens on the go. We're seeing early success with millions of app downloads and hundreds of mobile-optimized websites being used. Mobile is eGovernment's next frontier and demand for mobile-friendly solutions continues to grow exponentially each month."

RON THORNBURGH
SENIOR VICE PRESIDENT OF SALES & MARKETING
NIC

"Today's increasing preference and requirement for mobile solutions present a potential security challenge. The Public Sector is looking to Industry to bring innovative, secure new technologies that meet their changing needs while delivering more secure solutions. These solutions need to be easily implemented and user-friendly so that adoption is simplified. HP focuses on delivering exactly these critical requirements for our Government and Education customers through industry-leading solutions such as HP e-Print Enterprise Mobile Printing and secure print job authentication through HP Access Control."

LESLEY GOROG HARRIS
VICE PRESIDENT PUBLIC SECTOR
HP IMAGING AND PRINTER GROUP

"Mobile, without a doubt, is a game changer. But achieving that impact requires starting with a mobile strategy, a roadmap, that leads to the best processes and technology. Organizational goals need to drive this new level of information sharing capability to enable the right people (workers, constituents and customers) to access and exchange the right information at the right time (in the field or in their office) at the right cost. It is about more than just devices. It's about creating mobile solutions that align the entire data value stream: creating the most effective processes and technologies to collect it, store it, secure it, access it, integrate it and display it."

CAROL MORGAN
SENIOR VICE PRESIDENT
DAUGHERTY BUSINESS SOLUTIONS

"The key to implementing a high-functioning and efficient mobile framework is flexibility. Though the devices are what get the attention, what is at the back-end of that framework is what allows customers to truly optimize their solutions and meet their specific needs."

ROGER BJORK
ENTERPRISE MOBILITY SOLUTIONS
DELL

"People talk about mobility as if it's a one-dimensional challenge – how far can your device take you? In practice, mobility is a two or three dimensional phenomenon. The relationship between the cloud and the client is what determines the quality of the experience. A laptop PC or other client device is only truly mobile if it's configured to work hand-in-hand with the cloud, contextually aware of its surroundings, and can perform any kind of app or function in a way that appears native to the device. Otherwise, you're just diluting the experience and leaving horsepower of the device on the table."

RICH CHESTON
CHIEF TECHNICAL ARCHITECT
LENOVO, INC.

In an on-the-go world, NIC helps governments go mobile.

NIC is bringing its very successful eGovernment solutions to mobile devices. Like the governments it partners with, NIC knows mobility is an essential everyday solution — for governments and the citizens and businesses they serve. With a proven self-funded approach, NIC is delivering effective government-specific mobile solutions at no cost to state and federal agencies.

Major Mobility
NIC was the first provider to release government-specific native applications for the iPad, iPhone, Android, Windows Mobile, BlackBerry and other mobile platforms. Whether it's a practice driver exam for the iPad, secure payment processing from various devices or financial aid applications via cell phone, NIC can build solutions that make it easy for citizens to interact with government anywhere and at any time.

New Mobile Solutions Every Day
On average, NIC introduces several new mobile solutions each week on behalf of federal, state and local government agencies. NIC has already built hundreds of native applications and Web services that are optimized for smartphone and tablet devices.

Knowledge Is Power
As it charges forward in the mobile world, NIC has a strong knowledge base to draw from. NIC has built websites, online services and secure payment processing solutions for more than 3,000 federal, state and local government agencies. NIC has developed more than 7,500 eGovernment applications and securely processed more than $12 billion in government payments in 2010 alone.

Self-Funding Works
NIC's transaction-based, self-funded approach delivers diverse eGovernment solutions to agencies without requiring taxpayer appropriations, and the majority of services are provided at no cost to citizens. A modest efficiency fee is applied to a limited number of business-facing services, which covers the costs of building, maintaining and enhancing both eGovernment and mobile platforms.

NIC™ the people behind eGovernment®

Learn more about NIC's mobile eGovernment solutions at **www.egov.com.**

Solution Spotlight: **HP**

HP ePrint Enterprise: Printing in the Age of Mobility

Today's workforce is more mobile than ever.

Where, when, and how we work has changed dramatically in recent years, thanks in large part to the use of Internet-connected mobile devices. And these trends are only growing: According to Gartner Research, *by 2014, 90 percent of Global 1000 companies will implement Cloud Print Services for mobile personnel.*[1]

Our smartphones allow us to tap into cloud services, giving us the power to communicate and compute virtually anywhere our work or life takes us. But to the frustration of many mobile employees, printing has traditionally been the exception – until now! HP ePrint Enterprise solves these challenges by bringing the power of printing to mobile devices. By making it easy to print from smartphones as well as other mobile devices, HP ePrint Enterprise delivers on the promise of true mobility for government organizations and employees.

Mobile Productivity in the Office

Using HP ePrint Enterprise and their supported mobile device[2], employees can maintain productivity by:

- Printing without the hassle of booting up a laptop, logging on to a VPN, or installing drivers
- Easily searching for, and sending print jobs to any office location they will be working at
- Converting mobile content into hard copy for easy reading, editing, and sharing on the go

Print on the Go

Because for mobile workers, work happens outside the traditional office space, employees can also print on the go with the same application they use within their organization, to thousands of HP ePrint Mobile Print Locations, including print-and-copy retail stores, hotels, airport lounges, and more.

Public HP ePrint Mobile Print Locations include:

- Thousands of FedEx Office stores
- Other print locations powered by PrinterOn® like Hilton hotels and select Air Canada Maple Leaf Lounges

Enabling Security for Mobile Printing

From anywhere in the world, an HP ePrint Enterprise user can hit Print with enterprise-level security. The document travels through encrypted channels, and HP ePrint Enterprise administrative software hosted on your server processes the document and renders it for printing. Your data never leaves your network, so the process is as secure as your trusted enterprise network. For additional layers of security, the solution can integrate with pull- and PIN-printing solutions requiring user authentication.

When printing to an HP ePrint Mobile Print location, the print job is released only after submitting your print job's unique release code at the location. This allows you to maintain document security.

[1] *Gartner Research, document number G00208968, "Predicts 2011: Increasing Value of Imaging and Print Services Complements Multimedia Communications," November 17, 2010.*

[2] *Usage of HP ePrint services app at mobile print locations requires Internet- and email-capable smartphone with separately purchased wireless Internet service, and the HP ePrint services app. Availability and cost of printing varies by mobile print location. Visit www.hp.com/go/eprintmobile to view the list of applicable smartphones and operating systems.*

To learn more about HP ePrint Enterprise and Mobile Print Location solutions visit **www.hp.com/go/ePrintEnterprise**.

Mobile and Secure

GOVERNMENT IS ON THE GO. Every day, government employees are doing more work via mobile devices — smartphones, laptops, tablets and more. Mobility is making people more productive and efficient. But it's also creating new security challenges. With a growing number of devices connecting to your network from just about anywhere, traditional security isn't enough.

People are using the same mobile devices for both work and personal activities. This dual use creates additional risk. "We have to think more about how people use the personal side of these devices," said John Bordwine, Chief Technology Officer for Public Sector at Symantec. "The way people are using smartphones today is extremely different from the way they were using them two years ago."

With changes in usage and an increasing number of devices, organizations are finding it more difficult to manage their mobile environments. Meanwhile, cyber-criminals are getting smarter and finding new ways to get in. The *Symantec Internet Security Threat Report Volume XVI* showed there were 42 percent more mobile vulnerabilities in 2010 than in 2009. This increase from 115 to 163 new mobile operating system vulnerabilities indicates cyber-criminals are focusing more attention on the mobile space. The report also said several types of attacks traditionally launched against PCs are moving to mobile devices. And it predicts more threats in the future as more people go mobile and cyber-criminals continue to explore mobile environments as a potential profit center.

Phishing attacks, for example, are now targeting mobile devices. "What happens if one of those phishing attacks mutates across from the personal part of your phone to the business part? It's something that people really need to think about," said Bordwine.

Facing a wide range of threats to mobile environments, government agencies need a comprehensive approach to security. Symantec has the knowledge and expertise needed to keep government data safe and secure in the new mobile world.

Symantec Has It Covered

Whether securing your network infrastructure or your endpoints, Symantec provides the tools you need to keep your operations secure — without inhibiting you.

Endpoint Virtualization — Provides on-demand application streaming, so your users have the applications they need without gaining access to your systems. The application comes to them.

Network Access Control — Helps you discover and evaluate endpoints, such as PCs and mobile devices, attempting to access your network. Blocks or quarantines endpoints that are not up to your security standards.

Endpoint Security — Provides protection for those devices you do control, including laptops and handhelds. Includes firewall, malware detection and spam blocking for mobile devices.

Remote Device Management — Helps you push security software and patches to mobile devices. Lets you wipe data from lost or stolen devices.

Data Loss Prevention — Discovers the locations of your most sensitive data and protects it. Data encryption and policy enforcement ensure that sensitive data is not improperly shared.

Storage Solutions to Support Mobility — Makes storage and data backup more efficient in a mobile environment. Symantec cloud-based storage solutions give organizations scalable and efficient storage as mobile application demands increase.

Symantec™

go.symantec.com/publicsector

Portable Productivity

Motorola's wireless devices maximize service efficiencies.

Tight budgets and an increasingly digital constituency are motivating government agencies to turn to technology to help improve service levels. Today's public-sector work force is increasingly mobile, making access to key information sources in the field no longer a luxury, but a necessity.

Public organizations in many service areas have turned to Motorola for mobile computing devices that can withstand harsh physical conditions as well as provide a robust feature set. The all-in-one functionality allows employees to carry one device for both voice communications and network connectivity. Various productivity-boosting applications are available that greatly reduce paperwork and enhance service to the community.

Form Meets Function

Users of Motorola products enjoy desktop-quality performance in a lightweight, rugged device. Download speeds are as fast as 3 Mbps and available memory is as high as 256 MB and 1 GB Flash. Motorola's cost-effective products provide a high-resolution screen for optimal viewing of photos, videos and documents, as well as support for location-based applications.

Government users rely on Motorola's strict security certification to protect sensitive data. Flexible connectivity options let users connect to a wide area network outside the office, and seamlessly switch to a wireless local area network inside the office.

Wireless data capture capabilities include RFID and bar-code scanners, simplifying asset management and maintenance procedures. Forms can be filed on the go, eliminating significant paperwork and processing delays. The duration of many work processes is decreased, and accuracy is increased, resulting in untold efficiencies for employees and citizens.

Rapid Deployment

Training needs are minimal for Motorola users due to the widespread use of mobile devices. Most public employees are already comfortable with the technology, enabling agencies to be up and running faster. Regardless of an organization's needs for mobile information and communication, Motorola offers a range of solutions to optimize the field capabilities of the public work force.

Far-Reaching Mobile Capabilities

Motorola devices have helped increase efficiency in a wide range of public services and operations.

- Law enforcement officers issue tickets or traffic citations using mobile forms, therefore reducing paperwork and expediting processing and revenue collection.
- Firefighters and paramedics use an electronic triage and tracking system to transmit patient medical information and photos in real time to emergency rescue teams and local hospital staff.
- Building, health, environmental and safety inspectors access vital inspection history data in the field and file required forms to address current conditions.
- Maintenance personnel have access to procedure manuals and other materials without a trip back to the office, and provide on-the-spot documentation on work performed.
- Parks staff use the devices to more effectively manage system assets and inventory, and streamline work order processes.

MOTOROLA

Motorola Solutions is a global provider of mission critical communication products and services for enterprise and government customers. Through leading-edge innovation and communications technology, we enable customers to be their best in the moments that matter.

http://www.motorolasolutions.com/government

MORE BANG FOR THE BUCK

Lenovo ThinkPad systems with 2nd gen Intel® Core™ i5 vPro™ processors support your mobile work force while keeping costs down.

Mobile devices can increase efficiency in every government agency. Caseworkers, transportation officials, permitting agents and other mobile employees can spend more time in the field, meaning they spend less time and money returning to the office to do paperwork. Public safety personnel have better decision-making capabilities in the field when they have records and databases at their fingertips. And office employees can be more productive when they can perform computing tasks on the go.

While everyone recognizes the benefits of mobility, agency decision-makers must choose their mobile computing devices carefully. Total cost of ownership is clearly important in today's budget climate. Lenovo's industry-leading reliability, durability, security and broad range of features ensure that mobile government work forces maintain optimum productivity in the field at a reasonable cost.

Military specification durability keeps devices working longer. Most ThinkPad devices meet military specifications for vibration, shock and humidity. They're built to withstand spills, extreme temperatures and outdoor dust and sand. And they're rigorously tested to ensure that your device's useful life won't be cut short by coffee spills or demanding outdoor use. In the unlikely event that a device is ruined, Lenovo offers warranty and accident protection plans to secure your investment.

Benchmark reliability ensures your mobile work force can access systems and information when needed. With Lenovo's long-standing reputation for reliability, you can be confident that the efficiency you gain by deploying mobile devices won't be compromised by device malfunctions. And with the variety of connectivity options offered on ThinkPad laptops, mobile employees can gain access to the materials they need in more places.

Security government demands. The Lenovo Intel solution offers a wide variety of security features so government agencies enjoy the efficiencies offered by mobility without putting sensitive data at risk should a device be lost or stolen. Built-in fingerprint readers, remote data wipe software and hardware-based security solutions are just some of the options government agencies can use to minimize costly and damaging security risks that could impact a mobile work force.

Variety of features and options enable a wide range of tasks. With numerous ThinkPad models with Intel technology available on the WSCA/NASPO contract, agencies can choose the features that meet their needs. Transportation workers, for instance, can have the computing power to handle engineering applications, while agencies can opt for less powerful devices with the same rock-solid reliability and security for employees with less intensive computing needs.

Savings Throughout the Product Life Cycle

ThinkVantage Technologies available for the ThinkPad can reduce ownership costs from deployment to disposal. ThinkVantage tools provide:

- simplified imaging;
- migration of end-user data and settings;
- password management;
- power management;
- system updates;
- system recovery tools;
- security tools; and
- data removal tools for disposal.

Lenovo ThinkPad laptops give government agencies the tools they need to meet demands for efficiency amid tight budgets while maintaining security, productivity and a reasonable cost of ownership.

lenovo FOR THOSE WHO DO.

For more information, please visit **www.LenovoPublicSector.com**.

Government Goes Mobile

Accela offers on-the-go tools for public employees and citizens.

At a time when government workers are being asked to do more with less, the future of e-government is being shaped, in part, by mobile technology that helps facilitate collaboration between workers and citizens.

Mobility isn't just about traditional mobile workers anymore. The fact is that most government professionals are spending less time at their desks. They may be inspectors accessing data, tools and GIS maps in the field; functional experts sharing information with other departments on the fly; or department heads rushing between meetings.

Meanwhile, citizens want 24/7 interaction with local governments on two primary levels:

- to make service requests for inconveniences or safety hazards in their neighborhoods, such as street light outages, code enforcement issues and more.
- to conduct business-to-government transactions, such as obtaining a business license, scheduling inspections, tracking permits or making payments for municipal services.

A wide variety of internal and external interactions can occur in a mobile environment, with the proper tools. Accela has developed a range of mobility solutions, tailored to these audiences' unique needs. These tools are accessible on the devices mobile users prefer, including tablets, smartphones and mobile PCs.

Accela Automation®, a Web- and cloud-based enterprise software platform, provides the foundation for these mobility solutions. It automates numerous agency functions — permitting, licensing, infrastructure asset management, code enforcement and more — and creates better ways for governments to serve their citizens.

Leveraging expertise from working with more than 500 state and local governments, Accela delivers state-of-the-art mobile solutions to support the next phase of e-government.

Maximizing Efficiency

Government Mobility

Accela Mobile Office™ delivers mobile capabilities for inspections, code enforcement, work orders and service requests, to name a few. Direct, real-time access to data and maps from an agency's GIS enables workers to access and update records, work assignments and more — saving time and increasing productivity.

Accela Analytics™ is the first iPad app that lets agency staff access and act upon back-end data related to permits, licenses, planning/zoning, code-enforcement or citizen service requests on the go. An intuitive dashboard features charts, graphs, maps and watch lists. Some of these functions have also been extended to the iPhone.

Citizen Mobility

Accela Mobile 311™ is a native iPhone and iPad app that enables citizens to request services or report incidents to local government, from wherever they are. While most citizen-engagement apps simply capture requests, Accela Mobile 311 connects directly to an agency's Accela Automation system, and routes requests to the appropriate responders. Local governments brand Accela Mobile 311 with their name and logo, and then offer it to their citizens via Apple's App Store.

Accela Mobile Citizen Access™ enables users to check on permit inspections via their smartphones. The app displays permit types and status, work location addresses and other associated data. Users can also schedule or cancel inspection appointments, modify details and add comments, saving valuable time.

ACCELA™ Government Software

accela.com/Mobility

Sponsored by:

The Center for Digital Government, a division of e.Republic, is a national research and advisory institute on information technology policies and best practices in state and local government. Through its diverse and dynamic programs and services, the Center provides public and private sector leaders with decision support, knowledge and opportunities to help them effectively incorporate new technologies in the 21st century.

www.centerdigitalgov.com

Public CIO, a division of e.Republic, is an award-winning platform dedicated to technology thought leadership in federal, state and local government. Through print, online and a portfolio of events, Public CIO provides CIOs and key enterprise leaders with career critical insights on leading and navigating the innovative trends creating efficiencies, driving collaboration and impacting government services.

www.public-cio.com

Acknowledgements:

John Miri
Editor-in-Chief, Center for Digital Government

After a successful career as a private sector software executive, Miri was appointed by the Texas Governor to the top regulatory board overseeing statewide electronic government. He went on to lead transformational projects for two successive Texas State Chief Technology Officers and has become an advisor and close confidant to leading state and local government CIOs around the nation. As the former Director of E-Government and Web Services for the State of Texas, Miri led the state to breakthrough results of 829 online services, 83 million citizen financial transactions, and $5 billion in online revenue. He helped found three web-based technology companies that leveraged Web 2.0 and cloud computing to achieve dramatic results for clients in the commercial markets. Miri has been a passionate advocate of next generation Internet technologies for more than a decade and is a nationally recognized speaker and author on government technology.

Bridget Mintz Testa

Bridget Mintz Testa has been a full-time writer since the dot-com boom. Prior to that, she worked as an aerospace contractor at NASA-Johnson Space Center, first in lunar and planetary exploration and then in space station robotics. She has written on a wide variety of topics, including Internet and networking technology, telecommunications, electronics, energy, residential construction, human resources, urban planning, business strategy and information technology. She has performed feasibility assessments and market research for small businesses seeking capital for start-up or expansion. She currently lives in the greater Houston, Texas, metropolitan area.