



# **Smartphones for Law Enforcement Mobility: Guidelines for Selection**

**Tad Woolley**  
**InterAct Public Safety Systems**

## Introduction

Today, most local law enforcement agencies in the U.S. have laptop computers and mobile data software in their patrol vehicles to allow their officers to “run a plate” at a traffic stop or get background and photos on a person of interest without having to call a dispatcher over the radio. But we are witnessing a paradigm shift in how police officers in the field get this information. This shift is to mobile data on smartphones – commercially-available wireless handheld devices that are both data and voice capable.

This paradigm shift is being propelled by the fact that the total software and hardware acquisition cost of a smartphone is about **one-fifth the cost of an in-car mobile data system**. This makes mobile data on a smartphone very attractive for all departments who want to safely extend the safety and effectiveness of officers beyond the on-duty shift and the limits of a vehicle.

This whitepaper is a concise summary of the advantages of smartphones, as well as data-only handhelds, and the issues any law enforcement agency should consider when developing a deployment strategy for these devices. In the easy-to-follow format of “Top 10” lists, it addresses key issues such as: “future proofing” your investment to ensure you spend your money wisely; scalability; integration with existing systems; and ensuring that your “short term” implementation can migrate to meet your long term needs.

## Benefits of the Smartphone as a Mobile Data Platform

With the continual expansion of cellular network bandwidth and the capabilities of multi-purpose handheld devices like the BlackBerry smartphone, law enforcement agencies across the country are starting to widely deploy mobile data systems on these less costly and more convenient platforms. The trend started first with investigators, foot patrols and other users not primarily assigned to a patrol car. But now, police departments are evaluating the costs and benefits of deploying smartphones even to their vehicle-based officers.

One of the obvious limitations of an in-car system is that it’s only available to the officer when in the car. Because the smartphone is assigned to the person not the vehicle, mobile data on a smartphone is available wherever an officer needs to be. The result – and benefit – is that the officer is no longer tethered to the patrol car and is more visible and accessible in the community.

Another operational advantage is that information access from a smartphone is available at any time - even when the officer isn’t on-duty. The reality is that police officers at the end of their shifts don’t just turn off the vigilance they’re trained to use on the job. Even off-duty, they serve as a force multiplier - extra eyes to help prevent and solve crime.

The following “Top 10” list briefly describes the key benefits that smartphones and other wireless handheld solutions offer for law enforcement.

- 1. Cost:** The total cost of a smartphone enabled with a mobile data application, such as InterActPocketCop<sup>®</sup>, is about 20% of the “up-front” cost of an in-vehicle mobile data system (including laptop, harness and modem hardware, as well as software). This makes mobile data on smartphones a viable alternative to an in-vehicle system for those who don’t need it or a supplement for those who do – giving everyone access wherever they are.
- 2. Extend mobile data capabilities to out-of-vehicle personnel:** With a smartphone you can arm your investigators, special operations, and foot, bike, equestrian and motorcycle personnel with immediate dispatch communications, NCIC lookups, status changes and text messaging.

3. **24x7x365 access to state and NCIC databases:** While officers only have access to an in-vehicle system when they're in a vehicle, a smartphone personally assigned to the officer is available at any time – even off-shift – for quick access to criminal justice information to make well-informed decisions.
4. **Secure, silent communications:** When sending or receiving a voice message could compromise officer safety, the ability to send and receive silent, secure text messages on a smartphone is the only safe alternative. With the prevalence of text messaging on cell phones and smartphones, an officer or investigator in an undercover.
5. **Access to driver's license photos at their fingertips (if available in your state):** Getting a DMV image of an individual to confirm identity before the person is released or booked significantly improves the effectiveness and safety of front-line personnel.
6. **Immediate access to broadcast messages:** Equipping your smartphone users with the ability to receive "be on the lookout" (BOLO) and other broadcast messages gives them access to the same information sent to laptop or MDC users.
7. **Voice & data on one device:** The smartphone can provide phone, push-to-talk (on selected devices) and SMS-based text messaging, as well as mobile data, eliminating the need to purchase and carry a separate cell phone. This benefit, of course, does not apply to (non-smartphone) handholds that are designed to transmit data only.
8. **Multi-function devices run other applications:** This same device can support Internet access, email, address/phone lists, calendar for court appointments, duty schedules, to-do lists and more. Many smartphones also come with a camera, which can be used to take and transmit a photo or video of a person of interest.
9. **Force multiplier:** The ability to collect information wirelessly can reduce the amount of time users spend waiting for a dispatcher to respond or going to the station to complete paperwork.
10. **Smartphones can help protect officer safety:** Using the geographic positioning system (GPS) capabilities available today in most smartphones, agencies can map and track the current location of users in the event of an emergency. Used in conjunction with a feature such as the "Officer Needs Assistance" button in InterActPocketCop, GPS can help get the closest resource quickly to the scene.

## Considerations in Choosing the Right Smartphone Solution

The following "Top 10" list answers key questions you should address to ensure you select the appropriate solution (hardware, software and network) and maximize the capabilities that smartphones and other wireless handheld devices offer. In large part the answers to these questions will be dictated by *who* will be using the solution you deploy. For example, officers who already have land mobile radios may not require a smartphone's voice capabilities (although many officers have both radio and cell phone today). Conversely, the cell phone capability may be essential for officers and investigators on surveillance or undercover who would not want to have a police radio visible.

### 1. Which wireless network should we choose?

This question really boils down to: what is available, and does the coverage (footprint) meet your requirements. Compare coverage maps posted on the websites of the various cellular carriers to get a rough idea of coverage. Note that this is constantly improving as the carriers add to or upgrade their systems. Local representatives from

the carriers you are considering will be able to provide more detailed information concerning current coverage and planned enhancements within your jurisdiction. While multiple carriers serve many of the same metropolitan areas, selecting one (or more) may come down to which support the devices you want to use. An important consideration to include in this selection is choosing a software platform that runs on the available hardware to provide connectivity to your existing system, including your mobile solutions deployed in your cars and state NCIC interfaces. When selecting the software platform, be sure to ask what the supplier's current capabilities are, being sure you understand what they do today from what they are willing to develop. Standard "off the shelf", existing solutions are far simpler, more economical and faster to deploy. A common mistake agencies make is selecting a supplier who commits to build a software solution over one who has an existing solution and can point to satisfied customers.

## **2. How do we ensure that communications are secure?**

Today, many law enforcement agencies use public wireless networks for in-vehicle mobile data computers, or MDCs. Public wireless networks encrypt the data for secure transmission over the air. The technology employs encryption keys that change with each logon to the system, thus providing a high level of security. Additionally, applications designed for handheld products need to have true end-to-end security, i.e., Advanced Encryption Standard (AES) or Federal Information Processing Standards (FIPS) publication 140-2, a specification published by the National Institute for Standards and Technology (NIST) defining security requirements for encrypting information. The FIPS 140-2 standard defines certified encryption from the smartphone to the server and has been adopted By the FBI for securing the NCIC database. The FBI has mandated that all new installations requiring access to NCIC after September 30, 2005 must be compliant with FIPS 140-2. This requirement is also being imposed at the State level, where a number of states are requiring FIPS 140-2 compliance. When considering your software platform options, make sure the application supports true "end to end" data integrity and meets the FIPS 140-2 encryption standard.

## **3. What device hardware should we use?**

There is a wide spectrum of hardware choices available for deployment, with each device having specific advantages that can be maximized with the proper software application. As mentioned above, a critical factor in your choice is whether you intend to provide users with voice capability as well as data. If that is the case then you will be choosing a smartphone, and you should look for device "family" (e.g., BlackBerry) that has a strong presence in the marketplace so that you don't become "orphaned" in the future because the device is no longer supported. (You could technically mix and match device families if your selected software supports them, but the increased complexity of device management that that would cause should be avoided.)

The device selection will be limited and will vary by the wireless network(s) available to you. In the case of smartphones, each carrier supports (and often sells) different device families, but the choice – at least among the national carriers – is wide enough for you to have choices in selecting a suitable platform.

For many agencies, battery life is also a critical factor. The device should remain available for at least a complete shift, assuming moderate use. Other important considerations include those related to "form factor, such as size, weight, ruggedness, and ease of use of the screen and the keypad, as well as factors such as cost, processor speed and memory constraints. If you expect that the deployment will ultimately involve a large number of users, then the device management (e.g., provisioning, disabling a lost or stolen device) capabilities of the platform become more important.

It's impossible to expect an agency to become an expert in all of the alternatives available on the market at any specific time, so the best strategy here is to work with a solution supplier that is a "subject matter expert" on the alternatives. An experienced supplier can point to existing, satisfied customers that have deployed different hardware platforms, helping to ensure that your deployment will not result in implementation and support "surprises" such as cost overruns and delays in deployment.

#### **4. Do we integrate smartphone users with other systems?**

A smartphone-based mobile data system can be designed, implemented and operated as a standalone application. A *fully integrated* smartphone solution becomes an *extension* of your existing systems – CAD, RMS and in-vehicle mobile data. In other words, the handheld device is actually a client on a message switch, just like a mobile data computer in a squad car. In the fully integrated example the smartphone user appears on the Status screens of MDC users and Dispatch when the user is logged on. Like an MDC, the handheld application includes basic messaging such as Talk (one-to-one) and Announce (one-to-many), and, upon receiving a "hit" to an inquiry, instantly sends alarms to all vehicles, without dispatcher intervention. Additional functions, such as CAD integration and access to RMS and other agency data, are available to the smartphone user on an integrated system, which a standalone system would not be able to access. The department benefits by having a scalable, fully integrated solution, not just an "add-on," as well as by maintaining full control over the system and records of the individual devices.

Another important feature smartphones provide your front line personnel is the ability to send BOLOs to users immediately. In a fully integrated system, the same notice that is sent to MDC users will also be sent to these users. Standalone systems often are not capable of supporting sending BOLOs from individual agencies.

Choosing a system that has integrated interfaces with all of the agencies you can pull information from will significantly improve the capability of the device, putting the user on an even playing field and in some cases ahead of with his MDC counterpart operating out of a patrol car.

#### **5. Who do we call when we have a problem?**

Keeping your mission critical software platforms fully functional and up to current revision levels with the appropriate state interfaces can be a full time job and major headache if you do not select your application program supplier wisely. If the prospective vendor's support department equals the programmer who wrote the code (who may be out installing the first system), you had better look elsewhere. Ask the supplier important qualifying questions such as:

- > How many support staff handle the phones?
- > How do they escalate a call if they cannot solve the problem immediately?
- > Do they have a call center? If so, their call center should be well staffed, provide toll-free telephone support, and employ knowledge-based software systems to track calls and assist with troubleshooting problems.
- > Your agency supports your community 24x7 and having anything less from your supplier puts your front line personnel and your community at considerable risk- does the supplier have a 24x7 support infrastructure in place? If so, can they provide you with references of "satisfied customers" who have had the need to use this resource?
- > Do they have field engineers available to support your installation in the event you need "on site support"? Again, be sure to ask for references.

## **6. How do we avoid “technological obsolescence”?**

Wireless technology is the fastest growing area in the technology sector available to your agency. This is especially true of the smartphone devices themselves, which are often replaced by newer models every year or two. For this reason, a purchase made today may be out of date or require updates in 12 to 18 months. Since law enforcement agencies don't have the luxury of updating systems with that frequency, a system that includes a complete software maintenance and upgrade program is extremely valuable- ensuring that you maximize your precious investment. Changes to state interfaces, backend CAD systems and client updates should be included under your software application support plan. Every agency is strapped with ensuring that they spend their budget wisely. Having a support plan in place that provides updates to keep your solution as current as possible and one that includes technical support at no additional charge will ensure that you properly budget for your ongoing maintenance costs, while providing you with “peace of mind,” knowing that your system can grow, adjust or update as required.

A Carrier Subscription Plan is part of most cellular data purchases. With a Subscription Plan, you get airtime, software and support for one monthly fee. No need to worry about managing a private radio network or budgeting for new technology. Depending on the software platform you choose, the handheld hardware and software can be included in the monthly payment. And for customers that purchase hardware separately, a Breakage Protection Plan is an important consideration.

## **7. What is data “parsing” and why is it important?**

The whole point to providing your field staff with a smartphone is to provide them with timely information. If the software solution they are running provides the information in the order of priority they need, then “mission accomplished,” but, on the other hand, if they need to scroll through multiple screens to find the important facts, then the software platform chosen is not suited to run on a handheld device.

Data parsing is the ability to receive data from one or multiple sources, such as the DMV or NCIC, and formatting it for the device that will be receiving it. This can also include “stripping out” unnecessary text. Given the limited screen real estate of a smartphone, parsing is essential to provide for only pertinent data to be shown and minimizes the need to scroll through long strings of data. On a full PC monitor or laptop display, responding with a full screen of text to a query is often desired, but in a handheld application, your officer needs to see the most important information first. What's most important can vary, depending on the results provided to a specific query by the various databases your application accesses.

Also, a single NCIC query can result in multiple secondary queries to other data sources such as NLETS and DMV. Each secondary query can take a different duration to process and report, so that responses are fragmented and received out of sequence. Select a software platform that parses these responses in real time and presents a summarization of the results on the screen displaying all critical information at a glance, while providing the capability to drill down on replies of specific interest.

## **9. How do we handle installation, configuration and training for these devices?**

Identify a vendor that provides a turnkey solution for setting up your department. That means knowing the requirements of your state, coordinating with your chosen carrier, understanding the specifics for provisioning devices and the ability to work with you to maximize the integration of smartphones into your agency's systems and operations. Each device should also include a comprehensive User's Guide. Ask any prospective vendor to show you sample User's Guides and training materials before making a

decision. Once the system is installed, keeping your staff current on the capabilities of the device is important. Look to a supplier who can provide you with ongoing training and technical telephone support. As you upgrade your system, to keep current with carrier, federal, state or local interface changes, select a supplier who provides technical bulletin notifications of important issues that may affect system performance. Ask for samples of their existing technical bulletins to judge their current support capabilities. Explore how they disseminate this information today. Explore whether the suppliers offer e-mail notifications and secure, self-service Web sites so your staff can keep fully informed on system upgrades and changes.

#### **10. How do we choose a reliable mobile data software vendor?**

As with any technology purchase decision, you will need to consider many different factors. But when implementing a mobile data system on an evolving technology such as smartphones, the following vendor criteria become more critical:

- > At least 10 years experience in wireless, handheld mobile data communications
- > Substantial installed base of smartphone customers for reference
- > Extensive track record with state interfaces
- > Strong support organization, both internally and in the field
- > Technical expertise to add additional functionality
- > Strong relationship with smartphone suppliers, ensuring that the mobile data software functionality keeps pace with platform capabilities
- > A supplier who is a “subject matter expert,” able to advise you on the various options for system integration and hardware device alternatives.

## **Conclusion**

If written only a few years ago a whitepaper on this topic would have had to raise and answer the issue of user acceptance of handheld technology. The pace of change – the paradigm shift, if you will – that has occurred in terms of the adoption of smartphones through society has made this much less an issue (although the agency should be mindful that some new users may require more orientation on device features than others). This should not, however, suggest that there aren't important user-related questions – outside the scope of this document - that do need to be addressed. The new capabilities that smartphones bring to law enforcement require clear policies for their use – both on and off-duty. Expectations with respect to when and how often users are expected to check and respond to agency email should be clearly stated. Permitted personal use of the device must also be clearly defined. One InterAct customer agency, for example, has instituted a “user agreement” that the smartphone user (and supervisor) must sign. The agreement covers potential issues, such as personal cell phone use and related charges, as well as non-business Internet browsing and text messaging. Policies that ensure that the smartphone is used appropriately will help make it an even more essential tool for law enforcement.

## Confidential Information

This document contains confidential, proprietary information. Duplication or distribution of any content in this document is prohibited without the express consent of the authors. The methods and systems described in this document represent trade secrets with patent pending.

# InterAct CONNECTIONS FRAMEWORK



102 West Third Street, Suite 750, Winston-Salem, NC 27101 | 1.800.768.3911 | [info@interact911.com](mailto:info@interact911.com) | [www.interact911.com](http://www.interact911.com)

InterAct Public Safety makes Connections for Life™ providing both stand-alone and fully integrated mission-critical public safety and homeland security systems and products. As the pioneers of the first three-screen E911 system 20 years ago, InterAct's passion for innovation is leading the way to Next Generation telephony, dispatch, records management, and mobile data systems. Founded in 1975, InterAct Public Safety continues to extend the definition of public safety with unique applications like intelligent digital video surveillance, alert notification and crisis management systems. InterAct makes it possible for first responders from private, state, local and national agencies to decrease response times and increase their effectiveness in the communities they serve. InterAct is an ISO 9001:2000 certified company.