Why Government-Issued Smartphones for Law Enforcement

Author: The Digital Decision

The Digital Decision

Published August 2023

EXECUTIVE SUMMARY

Many Law enforcement agencies may have a subset of government-issued smartphones deployed. However, these agency-issued devices often go to command-level officers or administrators for base-level functions, like calling, texting, and email. Unfortunately, most first responders in the field (frontline patrol officers, tactical response teams, fire, EMS, and EMA workers, etc.) rely on personally owned smartphones to bring them to work. That's changing as departments realize the challenges with Bring Your Own Devices (BYOD) and the significant return on investment (ROI) that agencies can gain from issuing government-owned smartphones to first responders in the field. The primary concern for BYOD is security. Any time BYOD is used, it puts smartphone data at risk.

All Law enforcement agencies have personnel who operate without a traditional vehicle and, therefore, don't have a platform to support an in-vehicle computer. For law enforcement personnel who work by bicycle, foot patrol, or motorcycle, in plainclothes details, school resource positions, or marine units, smartphones can empower them with real-time mission-critical data, increasing their situational awareness, overall productivity, and personal safety — wherever their operations take them. Many smartphones today offer a rich desktop experience from a mobile device — officers can bring any work and recorded data from the field directly into the office without interrupting their workflow.

For most police officers, ready access to information effectively ends when the officer steps outside the vehicle. And the reality of policing is that the most effective officers are those who don't stay in their mobile "offices" or cruisers. Smartphones, on the other hand, are inherently mobile. They can be placed in an officer's pocket or on their belt in a case/holster. They are small, lightweight, highly functional, and convenient.

Not only do smartphones extend an officer's resources beyond their patrol vehicle, but the FBI's CJIS-compliant **government-issued smartphones should be considered essential technology to be provided to every law enforcement officer and first responder.**

MOBILE APPLICATIONS

Smartphones not only provide real-time access to information, but they also enable features that go well beyond the capabilities of in-vehicle computers.

Many capabilities are made possible with an off-the-shelf consumer smartphone, while others require specialized applications or added accessories. Many smartphone applications are designed to enhance the productivity and safety of law enforcement officers and first responders. From using smartphones as a Miranda warning reference to a first aid guide, apps are constantly developing to provide digital resources for law enforcement. Here's a partial list of what's already available today:

1. High-resolution cameras for capturing images and videos for evidence collection
2. On-scene information collection, recording, and note-taking
3. Timely, mission-critical data retrieval
4. Mobile computer-aided dispatch (CAD) -- extends the smartphone into a fully functional CAD-addressable device.
5. Access to records management systems (RMS)
6. Access to real-time video surveillance providing alerts and enhanced situational awareness:
7. Access to criminal justice databases (requires FBI CJIS compliance).[3]
8. Land Mobile Radio to LTE integration: Interoperability between your portable 2-way LMR radio and your smartphone. Ability to talk on any LMR talk group from your smartphone, which expands coverage on your LMR network from regional to nationwide access.
9. Emergency beacon/alert if it recognizes that an officer is in a foot chase or officer down
10. Voice assistance
11. Improved situational awareness through officer-specific geolocation
12. Next Generation 9-1-1 integration
13. Electronic citations and field-based reporting
14. Basic language translation
15. Access to department policies, and training videos, and so much more!

New rugged, push-to-talk ready smartphones can supplement LMR radios, allowing a single device to support mission-critical voice as well as access to rich multimedia data available wherever officers have access to our 4G LTE/Wi-Fi networks. These carrier-integrated applications make push-to-talk on your smartphone to communicate on any LMR 2-way radio talk group.

Significant improvement in smartphone device technology is happening before our eyes with graphic and chip processing, memory, and the ability for these phones and devices to be as powerful as your laptops and computers. Over the next three years, we believe that the 5G Ultra-Wideband wireless networks being deployed today will dramatically improve the speed of an individual's smartphone download by over 20 times. 5G is opening up a realm of possibilities for mobility applications for law enforcement.

In sum, mobile apps enable officers to do more without tying up radio traffic. Officers can enter searches, update call information, and do other tasks independently from the scene. Even "voice to text" enabled apps (e.g., "Siri" or "Google Assistant") can assist in updating or adding narrative or call notes. Empowering the officer to do more improves officer and overall department efficiency."

BRING YOUR OWN DEVICE (BYOD) CHALLENGES

The BYOD approach has weaknesses.[1] Considerable research and surveys have affirmed that BYOD does not deliver the savings that organizations believe it does. A **strategy of relying on employee's personal devices can stunt mobile maturity, compromise productivity, and create additional security risks for law enforcement agencies.[2]**

As smartphones, tablets, and other devices became mainstream, many organizations have accepted or embraced bring your own device (BYOD) as part of their workplace culture. Despite this acceptance, compliance regulations (like CJIS compliance) will dictate how—or if—an organization can adopt BYOD. BYOD policy has a slightly different look for law enforcement under CJIS compliance. All smartphones and tablets or other devices must use a CJIS-compliant multi-factor authentication (MFA) process, and they must also be enrolled in an agency-controlled mobile device manager (MDM) capable of remotely locking or erasing the memory of a lost or compromised device[3].

MOBILE SECURITY

Departments that use Smartphones to access criminal justice databases must adhere to a different set of compliance rules than other industries. Devices accessing criminal data must follow FBI Criminal Justice Information Services (CJIS) compliance for mobile device security. It's important to note that BYOD creates the possibility that your phone, with your personal information contained within, could potentially become evidence and subject to discovery in court proceedings. A comprehensive BYOD policy must be implemented if BYOD devices are used.[4] Mobile device security is critical to success. All work-related data transmitted or stored on a device needs to be encrypted. The stringent policies of CJIS compliance make BYOD among law enforcement difficult, if not impossible, to achieve.
BYOD carries multiple threats and risks that government-issued devices do not; the difference is where responsibility lands. Who is responsible for the mobile device management around those threats, the deployment of mobile threat detection, or

---

[1] Mobile devices and your employees: To BYOD or not to BYOD? Mobile devices and your employees: To BYOD or not to BYOD? - Samsung Business Insights

[2] Maximizing Your Mobile Value - Maximizing_Mobile_Value_2022-Final.pdf (samsung.com)

[3] CJIS compliance and mobile device security in law enforcement CJIS Compliance & Mobile Device Safety in Law Enforcement | Verizon Business

[4] Establishing an effective BYOD mobility policy Samsung_Establishing-an-effective-BYOD-mobility-policy_WHITE-PAPER-2021-V9

the mitigation of any cyber incident ? Mobile threats—such as phishing, unsecured Wi-Fi usage, or excessive permissions in apps—are potentially a big concern because they can lead to data leakage or data loss, which could result in a significant security issue for law enforcement.

Unique to BYOD are threats caused by cross-contamination. When a mobile device holds both professional and personal credentials, it makes mobile device security more difficult. It may even be used by other family members for personal use. That simple action could potentially put you and your agency in violation of CJIS compliance.

Mobile devices are critical to Law Enforcement and agencies dedicated to keeping citizens safe, but the data they use is extremely sensitive, and stringent mobile device security is a necessary. In other industries, BYOD is seen as a cost-saving measure, but don't expect this to happen in Law Enforcement. First, devices used by law enforcement need to be dependable; Law Enforcement shouldn't use a phone/data service plan or carrier with spotty coverage and unreliable service. They need devices that can support the mobile device security measures necessary to meet FBI CJIS compliance.

Devices used by law enforcement are valuable to criminals, not just cybercriminals. The FBI has well-defined parameters of what constitutes personally identifiable information (PII), and PII's protection is a priority. Any time BYOD is used, it puts the user's PII at risk, especially if the device ends up in the hands of an alleged criminal. Some agencies may decide keeping separate personal and work materials, including not conducting private activities on department-issued devices.

For any agency that embraces intelligence-led policing, **government-issued smartphones are powerful tools to boost officer efficiency.** Mobile devices can augment existing law enforcement technology by providing alternative communications functionality and creating an efficient connected officer capability.

PRIORITY SERVICES & 5G FUTURE CAPABILITIES

Government-issued devices are eligible for a higher level of network priority services than BYOD devices. For example, BYOD devices are typically not eligible for "Preemption" or higher Quality of Service (QoS) levels. In contrast, government-issued devices with public safety price plans are authorized to use the robust priority features (access priority, preemption, QoS) available for public safety users. This means that on "dark sky days," when natural disasters or other catastrophic events impact cellular networks, your government-issued devices will have priority over BYOD devices on the network. Your BYOD devices may have severe challenges connecting to the cellular network in a fully loaded/congested network scenario. 5G ultra-wideband with next-generation stand-alone 5G cores embracing "Voice Over New Radio" (VONR), Network Slicing, and other advanced network capabilities will begin deployment in 2024. Some of these new 5G public safety-centric features, e.g., public safety network slicing and priority services, may not be available for BYOD devices.

CONCLUSION

Much like a Swiss Army knife, **a government-issued smartphone has endless investigatory, tactical, operational, administrative, and alternative communications capabilities.** Using government-issued smartphones can save valuable time during the beginning stages of investigations, increase arrest and prosecution rates, speed up administrative procedures, and make it a much easier and more economical for police personnel to do their job.

As millennials and Gen Z (born after 1995) enter the workforce, Smartphone mobility has become the norm. These mobile devices on 5G networks provide law enforcement unprecedented capabilities to share vital information that will lead to safer, smarter, and more connected communities.

Law enforcement agencies are facing unprecedented pressure to do more with less. **Equipping law enforcement personnel with CJIS-compliant government-issued smartphones provides a new toolset to deliver more efficient and effective services, increase situational awareness for first responders, and enhance the safety of our officers and citizens.**