Use of Mobile Technology for Information Collection & Dissemination

A Technology Assessment Report

Use of Mobile Technology for
Information Collection and Dissemination

A DACS Technology Assessment Report

DACS Report Number 518055

Contract FA1500-10-D-0010
Prepared for the Defense Technical Information Center

Prepared By
Chet Hosmer, Chief Scientist
Carlton Jeffcoat, Vice President, Cyber Security Division
Matt Davis, Malware Analyst
Wetstone/Allen Corporation of America
10400 Eaton Place
Fairfax, VA 22030

Thomas McGibbon, DACS Director
Quanterion Solutions Inc.
100 Seymour Road
Utica, NY 13502

Distribution Statement A

Approved for public release: distribution is unlimited

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. **PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.**

1. REPORT DATE *(DD-MM-YYYY)*
TBD

2. REPORT TYPE
Technical

3. DATES COVERED *(From - To)*
N/A

4. TITLE AND SUBTITLE
Use of Mobile Technology for Information Collection and Dissemination

5a. CONTRACT NUMBER
FA1500-10-D-0010

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER
N/A

6. AUTHOR(S)
Chet Hosmer, Carlton Jeffcoat, Matt Davis, Thomas McGibbon

5d. PROJECT NUMBER
N/A

5e. TASK NUMBER
N/A

5f. WORK UNIT NUMBER
N/A

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Allen Corporation of America, Cyber Security Division, Coastal Carolina University Foundation Center, 5341 E HWY 501, Suite E 501-509 Conway, SC 29526

Quanterion Solutions, Inc., 811 Court St., Utica, NY 13502

8. PERFORMING ORGANIZATION REPORT NUMBER

DACS DAN #518055

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Defense Technical Information Center
DTIC/AI
8725 John J. Kingman Rd., STE 0944
Ft. Belvoir, VA 22060

10. SPONSOR/MONITOR'S ACRONYM(S)
DTIC

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for Public Release, Distribution Unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

Mobile technology is increasingly being utilized as a tool for information dissemination and collection. Numerous agencies including the Department of Defense (DoD), Department of Homeland Security (DHS), Intelligence community, and law enforcement are utilizing mobile technology are utilizing mobile technology for information management. The three primary mobile devices being utilized today for the purposes of information collection and dissemination are the iPad® / iPhone®, Android™, and Windows Mobile™. The open architecture of these devices is conducive for rapid application development and release. Despite the advanced mobile technology that exists today, factors such as security, usage, and trends must be considered when transitioning to mobile information collection and dissemination architecture.

15. SUBJECT TERMS
TBD

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON** Thomas McGibbon
a. REPORT U	**b. ABSTRACT** U	**c. THIS PAGE** U	UU	77	**19b. TELEPHONE NUMBER** *(include area code)* 315-351-4203

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std. Z39.18

Table of Contents

Table of Tables

Table of Figures

1.0 Abstract

Mobile technology is increasingly being utilized as a tool for information dissemination and collection across the Government. The Department of Defense (DoD), Department of Homeland Security (DHS), Intelligence communities, and law enforcement are among those agencies utilizing mobile technology for information management. The primary mobile devices being utilized are the iPad®, iPhone®, Android™, and Windows Mobile™. The open architecture of these devices is advantageous for rapid application development and release. Despite the advanced mobile technology that exists today, factors such as security, usage, and trends must be considered when transitioning to mobile information collection and dissemination architecture.

2.0 Executive Summary

In today's information-based world, rapid and efficient dissemination of high assurance information is essential. Mobile technology, specifically hand-held cellular based devices, is playing a large role in redefining how information is disseminated. The revolution of mobile technology is changing the primary purpose of mobile devices from making or receiving calls to retrieving the latest information on any subject.

New mobile technologies such as the iPhone®, iPad®, Android™ and similar devices have revolutionized the way information can be distributed. In the past, mobile devices such as Personal Data Assistants (PDAs) primarily focused on data storage and display. Today, an increasingly large number of devices are focusing not only on data storage and display, but also on communication and processing. As a result organizations have begun leveraging mobile technology as a means of information dissemination. These organizations include, but are not limited to, Government organizations such as the Department of Defense (DoD), the United States Army, the Department of Homeland Security (DHS), and a number of critical infrastructure organizations.

Mobile technology offers many advantages for both government and non-governmental organizations over the traditional methods of information dissemination. It is not limited by geographical location and can be accessed anywhere with the appropriate technology. Mobile technology is also more readily available because the devices are always with the user and always on. This connectivity is especially important during military missions and exercises. Crucial information such as adversary intelligence, terrain description, maps, and asset information can be accessed by the warfighter instantly, anytime, anywhere during the course of a battle or campaign. As a result, when messages or other information needs to be distributed, it will reach the maximum number of people when mobile technology is utilized.

Using mobile devices for information collection also offers advantages over traditional forms of information collection. Because mobile technology can be taken anywhere, information can be collected in real-time in the field. Mobile applications help make the collection of information easier and more efficient than traditional collection methods. Utilizing mobile device hardware, information collection applications can take photographs, automatically collect location data, record messages, and transmit information with the single push of a button.

Whether used by government organizations, businesses, or individuals, mobile technology is changing the way we receive and view information today. New applications being developed allow users to be connected in ways not thought possible before.

3.0 Introduction

This report is a technology assessment of the use of mobile technology for information dissemination and collection, with a particular emphasis on government and critical infrastructure applications. Technical considerations in the use of mobile technology are also discussed throughout.

The report is divided into five topics:

- **Current Uses of Mobile Devices** provides an overview of the current uses of mobile applications for information collection and dissemination by various government and non-government organizations.
- **Mobile Information Collection and Dissemination** describes current methods used to disseminate and collect information on mobile devices.
- **Mobile Technology Architectures** provides an overview of the current information architecture being utilized in the Army, DHS, and the Navy to support mobile users.
- **Current Mobile Device Technology** provides a technical overview of current mobile architectures and best practices associated with development on those architectures.
- **Key Aspects of Mobile Information Management** describes key elements and considerations that must be taken into account when transitioning into a mobile-based information environment.

3.1 Mobile Technology

The scope of this report is focused on only information collection and dissemination as it relates to mobile technology. For purposes of this report, the term mobile technology will refer to hand-held cellular communication devices. These devices primarily consist of smart phones and in this report will be expanded to include the iPad® due to its portability and cellular communication capabilities. Not included in the scope of mobile devices for this report will be devices such as laptop computers, portable hard drives, USB thumb drives, and portable music players.

3.2 Intended Audience

The report is intended to provide a technology assessment of mobile technology as it pertains to information collection and dissemination. The intended audience is individuals tasked with making crucial infrastructure decisions related to mobile devices. This would include:

- Individuals looking to migrate from a traditional computer-based infrastructure to a more mobile device-based infrastructure,
- Individuals who are in charge of acquiring and deploying mobile technology to the field,
- Government, Law Enforcement, and DoD Users of Mobile Devices,
- Security Professionals,
- Information Technology Program Managers, and
- System and Network Administrators in charge of mobile devices

This report assumes that the audience has a basic understanding of mobile devices and their usage. However, an overview of the architectures of mobile devices will be provided to give readers a better understanding of the applications and security considerations discussed in this report.

3.2.1 Motivation for Mobile Information

In the aftermath of the World Trade Center crisis a study was conducted to examine the World Trade Center response through the lenses of information, technology, and organizations who utilized them to address this unprecedented urban emergency. [WTC2004] Several key findings of this report related directly to mobile device information and moreover the information received in a crisis including:

- The nature, strengths and weaknesses of information technology in a crisis
- The availability, quality and reliability of information technology in a crisis
- The specific information needs required during such an incident
- Information resources needed to be relevant, accurate, and timely

In the case of the World Trade Center crisis, the loss of the Verizon Central Office disrupted "traditional communications". Therefore, other mobile ad hoc technologies[1] were required to provide communication and information dissemination. In some cases these networks were constructed overnight as either "line of site" networks or with locally deployed "hot spots" providing communication capabilities for those on the ground.

Significant advancements in mobile technology have occurred since September 11, 2001, both in the advancement of the devices and the infrastructures that support them. For example, mobile devices like the Android™ and iPad® can now operate equally and seamlessly via traditional cellular networks, as well as with infrastructure/ad hoc wireless networks.

The devices themselves have evolved from single or dual use (i.e., phone / text) to application rich devices with built in capabilities allowing for communication, smart applications, navigation, video streaming, and storage of gigabytes of information directly on the device. These enhancements provide new opportunities for using these devices in ways for which we have only scratched the surface. The latest devices include Global Positioning System (GPS) navigation, accelerometers, movement detection technologies, and advanced camera systems to both record and transmit video and audio.

[1] A mobile ad hoc network is a self-configuring collection of mobile devices connected by wireless links.

4.0 Current Uses of Mobile Devices

The use of mobile devices as information management tools has gained great popularity recently. These devices have been increasingly adopted by DoD, DHS, Intelligence Agencies, and other Government agencies for the purpose of information collection and dissemination. The unique hardware features offered by mobile devices in terms of information management has proved to be an invaluable resource as new applications have been developed for these platforms.

Also many acquisition organizations, particularly within the DoD, have observed the speed with which the mobile “Apps” development community have developed new software for mobile devices and want to be able to deliver capability to the warfighter faster.

4.1 DoD Applications

DoD believes there are many benefits associated with providing soldiers mobile based technology. Applications can be provided as a convenient and flexible means of receiving training and accessing critical information. In the field, mobile applications provide the ability to access critical operational information regardless of location. This could include anything from classified intelligence to maps of friendly force locations.

The Defense Advanced Research Projects Agency (DARPA) has launched a program known as the **Transformative Apps Program**. The purpose of this program is to place the correct mobile applications into the hands of warfighters. To facilitate this, a military application store is being created to promote collaboration between developers and users in the field.

The applications found in the store will be initially stored in a repository having two distinct sections. The first section will hold beta applications that need to be evaluated and tested. The second section will hold those applications which have been tested and certified for use. To help create a broad set of applications, a wide range of contributors will be utilized. Application development will come from government sources as well as private industry. This will be facilitated by lowering the barrier to entry by loosening requirements of items such as proposals and DoD contracting [ARMY].

DARPA is looking for mobile applications that perform a variety of functions, including command and control, reporting, mission planning, intelligence, geospatial visualization, analysis, language translation, training, and logistics tracking. During initial development, the applications will be focused towards open source mobile platforms.

Another DoD initiative is **Connecting Soldiers to Digital Applications (CSDA)**, sponsored by the Army Capabilities Integration Center (ARCIC) and the Army CIO/G6, with support from the Army Training and Doctrine Command (TRADOC) deputy commanding general for Initial Military Training, and other Army organizations. The purpose of this initiative is to determine the value of giving soldiers applications on mobile devices [ARMY].

During Phase One of the initiative the Army experimented with several types of smart phones to evaluate the effectiveness and usefulness of various mobile applications in the field. Devices tested included the Apple iPhone®, Google Android™ devices, and Microsoft Windows Mobile™ phones [C4ISR]. On these devices, applications were tested which covered a wide range of functions. These included training, leader development, job aids, and administrative tasks. Phase Two of the initiative will look at mobile applications as they relate to tactical operations. Specifically, the Army will examine how to integrate mobile technology with radio networks and battle command systems [ARMY].

DoD is also starting to integrate chemical and biological sensors into mobile devices. Researchers from the University of California, San Diego have developed a **miniature chemical sensor** which can detect harmful gas in the air and automatically send the information about the type and transmitting range of the gas. The chemical sensor is a silicon chip with hundreds of independent miniature sensors. These can identify the molecule of specific toxic gas and then report on it [SENS].

The Army has recognized the need to provide applications to the field faster than currently taking place. As a result, a program called **Apps for the Army** was introduced. The goal of the program is to have an application in the field ninety days after requesting it. During the first thirty days after a request for an application to do a specific function has been made, the developer will create and demonstrate a prototype. The software will then be voted upon and suggestions offered. The developer will have another sixty days to complete development. At this point the application will be deployed. This concept of rapid development was successfully tested in The Apps for the Army challenge [ARMY APPS].

4.1.1 Tactical Networks

Because many of the tactical networks in the field are unreliable, unsecure, or often times not available at all, DoD mobile applications will not be able to connect to large centralized servers. Rather, these applications will rely on distributed compute and storage nodes in vehicles or outposts. Several companies are working on solutions to this problem.

Lockheed Martin, for example, has begun to address the unreliability of field based network connections by developing a new communications system called **MONAX**, a 3G wireless system, designed specifically for warfighters, consisting of a portable sleeve that connects smartphones to base stations on the ground or in the air. All data transferred over the network is protected by exportable encryption (encryption that is able to be employed outside of the U.S.). The MONAX communications system also has its own app store with applications which leverage the new network.

Another company addressing the networking issues is Textron who has released a new communications system, **Forward Airborne Secure Transmissions and Communications (FASTCOM)**. This cellular network has been approved to handle Secret level and below communication. FASTCOM can be powered by an unmanned aircraft, aerostat (moored balloon), or ground vehicle equipped with 3G cellular pods. From these pods, FASTCOM creates a secure cellular network providing its users with full access to the 3G features of their smartphones, and access to any available network-based resources.

4.1.2 Application Examples

The current mobile applications being utilized for collecting and disseminating information, as seen in Table 1, are primarily being developed for either iPhone® or Android™ based mobile devices. Most of the applications developed for use in the field are done so that the application does not need a constant active network connection to fully function as the locations that DoD users use mobile devices sometimes make it impossible to receive communications.

Many DoD applications are designed to work in conjunction with mobile devices to automatically collect location data, known as GeoTagging. This location data can be collected for DoD assets, including equipment, military bases, terrain, and even soldiers themselves. Once collected, the location based information is transmitted to centralized DoD communications networks, processed and correlated, and then made available to other mobile devices. Utilizing this collected and processed location data, soldiers are able to transmit crucial location information back to their mobile devices. This relays information about the upcoming terrain, enemy location, fellow soldier location, and asset locations. All of this data is plotted on a generalized map of the soldier's surroundings for quick access. The applications are excellent at accepting information, correlating it, and then disseminating it to mobile users when the information is most useful and relevant.

Many other DoD mobile applications take advantage of the storage and video playback capabilities of the iPhone® and Android™ based devices to serve as a training tool. Training topics currently used in mobile applications range from exercise regimens to information about military language, ranks, and insignia. Mobile technology is especially useful when utilized as this type of training aid as the information can be viewed virtually anywhere at any time.

Platform	Application Name	Manufacturer	Description
iPhone®	Find Your Embassy	US Embassy	Used to locate and contact the nearest U.S. Embassy anywhere in the world. Also gives international users maps and contact information for U.S. Embassies and consulates along with access to travel alerts and warnings.
iPhone®	Physical Training Program	US Army	Allows soldiers to create their own training program from the application's plans and videos based on the Army's new Physical Readiness Training program.
iPhone®/Android™	Telehealth Mood Tracker	US Army	This app monitors soldiers using a visual rating scale to keep records of their psychological health and address behavioral issues that can stem from deployment or trauma.
Android™	Disaster Relief	US Army	Helps military personnel working in humanitarian relief and civilian affairs campaigns. The

Platform	Application Name	Manufacturer	Description
			dissemination and analysis tool searches, edits and creates maps which are viewable on Google Earth and Google Maps.
Android™	New Recruit	US Army	Provides information for soldiers considering joining the army, including military rank and insignia, Army news feeds, an Army physical fitness test calculator and a Body Mass Index calculator.
Android™	Raytheon Android™ Tactical System (RATS)	Raytheon	RATS is a battlefield networking system that utilizes mobile terminals powered by the Android™ OS to connect soldiers in the field with other soldiers and military assets. With RATS system, soldiers will have access to recon data, friendly unit locations, and biometric/photo analysis.
Android™	Android™ Portable	US Army	Allows potential Army soldiers to learn important information about the Army such as rank and soldier's creed before beginning basic training. The application can also be used as a reference for existing soldiers after they complete their training.
Android™	Grid Nav	US Army	This will allow users the ability to get accurate location data displayed in both angular and MGRS coordinate format. The user also has the ability to convert between decimal degrees and DMS to MGRS format.
Android™	Movement Projection	US Army	A map app for the navigation of roads. It allows soldiers to input obstacles and threats, stops, start and end points, and calculates the best route to a destination.
Android™	Fort Gordon Post Locator	US Army	Allows users to find important locations on the post. It uses

Platform	Application Name	Manufacturer	Description
			Google Maps to show exact locations of popular locations on base.
Android™	go2MWR	US Army	Allows users to locate Morale, Welfare and Recreation locations, display different types of information, and schedule the use of services.
Smartphone	SoldierEyes	Textron	Contains a set of command, control, intelligence and situational awareness tools. It enables soldiers to connect with intelligence databases and uses an open architecture that supports third-party software applications.

Table 1: Examples of DoD Mobile Applications

4.2 Department of Homeland Security

The Department of Homeland Security (DHS) is currently working to expand its mobile application capabilities. Researchers from the **Cell-All** program recently introduced prototypes of mobile phones which could detect chemical and biological threats in the air. When this technology is combined with a phone's Global Positioning System, emergency responders will have a better understanding of the scope of the biological or chemical attack [NASA].

Another DHS agency adopting mobile application technology is the Transportation Security Administration (TSA) which has created an application called **MyTSA**, providing the public access to relevant TSA travel information. The information includes the types of items that may be carried through TSA security checkpoints, checkpoint policies, estimated wait times at checkpoints, and current travel conditions [PIA]. The application will also have the ability to connect to a data feed through the Federal Aviation Administration (FAA) to bring up information about airport delays.

4.3 Intelligence Agencies

One of the challenges facing the intelligence community is how to collect, organize, and archive the vast amounts of data received every day. Mobile applications are excellent in assisting with this task as information can be collected and organized directly in the field. An application called **Counter-Insurgency Intelligence Collection (COIN)** has been developed by MITRE for both the iPhone® and Android™ operating systems to assist with this task. This application allows warfighters to collect, organize, and share user-defined intelligence data such as people, places, and events directly from the battlefield. Prior to this, soldiers carried personal cameras, GPS devices, and other commercial technology to gather the same data. [COIN]

4.4 Other Government

Over the past few years, a shift in technology has caused the government to begin to transition from E-government (also known as Digital Government, referring to how government utilizes telecommunications technologies to enhance efficiency and effectiveness in the public sector) to M-government principals. M-government is defined as “the extension of e-government to mobile platforms, as well as the strategic use of government services and applications which are only possible using cellular/mobile telephones, laptop computers, personal digital assistants (PDAs) and wireless internet infrastructure.” [WIKI]

There are multiple benefits for the government and the people by transitioning to an M-government based approach:

- Mobile technology has a wide reach. Mobile technology adoption exceeds that of the Internet and thus will reach more individuals.
- Unlike computers which are usually connected to a specific location and not always powered on, mobile devices are usually continuously carried and always on. If an urgent message or crisis communication is needed, it would be more effective to disseminate that information on a mobile device than a traditional computer system.
- M-government is cost effective. Sending a text message to citizens is cheaper than sending a stamped letter. Information also flows faster on mobile devices. Government

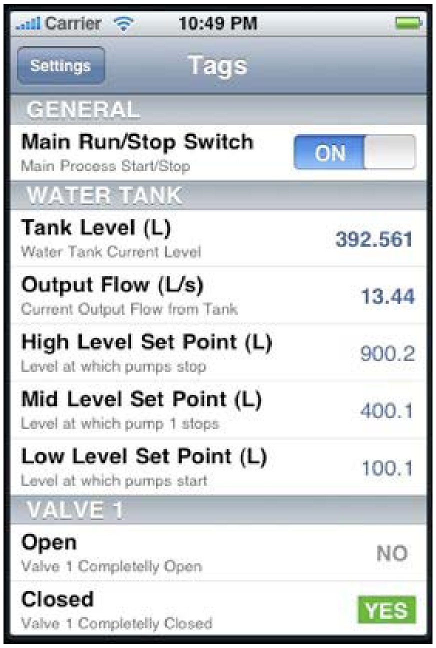
staff can transfer data very rapidly between mobile devices and can also access data electronically rather than physically having to travel to retrieve this data.

- Mobile technology could increase democracy and could be used in everything from voting to policy development. This would allow unprecedented communication between the government and the people.

M-government has already been adopted by many foreign governments. In Estonia, mobile devices are used to manage parking and improve communication between home and school. In Bangladesh, the government sends text messages to warn the public of imminent natural disasters. These are two simple examples of how governments are implementing mobile technology [M-GOVT],

4.5 Utilities and Critical Infrastructure

Mobile technology is also rapidly being adopted into the field of utilities and critical infrastructure. As an example, mobile technology allows users to remotely monitor and control systems from virtually anywhere in the world. An example of this is **ScadaMobile** created by SweetWilliam Automation (Figure 1). **ScadaMobile** is an iPhone® and iPad® application that



GENERAL

Main Run/Stop Switch — ON
Main Process Start/Stop

WATER TANK

Tank Level (L) — 392.561
Water Tank Current Level

Output Flow (L/s) — 13.44
Current Output Flow from Tank

High Level Set Point (L) — 900.2
Level at which pumps stop

Mid Level Set Point (L) — 400.1
Level at which pump 1 stops

Low Level Set Point (L) — 100.1
Level at which pumps start

VALVE 1

Open — NO
Valve 1 Completelly Open

Closed — YES
Valve 1 Completelly Closed

Figure 1: Scada Mobile

allows users to monitor OMRON Programmable Logic Controller processes and systems remotely. OMRON is the world leader in industrial automation. As a result, this application can be used in infrastructure such as mini hydro power plants, water plants, industrial process control, and building automation [SCADA].

4.6 Law Enforcement

There are many applications that state and law enforcement agencies are using to ease their workload. These take advantage of the unique smartphone features including cameras, GPS sensors, clocks, on scene data entry, and voice recording. In the future, voice logging of events and interviews with victims and suspects, local weather and other environmental information may be included.

Two of the more prominent law enforcement mobile applications include **Field Contact** and **USAccident:**

- **Field Contact** allows officers to document and send field contact information including name, address, vehicle information, aliases, and location of incidents. The application also integrates photographs taken with an iPhone®. Officers can quickly search, create, edit, and share contacts from any location. This application can greatly assist in intelligence gathering and distribution.
- **USAccident** allows for the completion of official accident reports along with the submission directly via the smartphone. This will both streamline and improve accuracy of the accident information.

Current law enforcement mobile applications for collecting and disseminating information, as seen in Table 2, tend to be concentrated on the iPhone® platform and make use of many of the hardware's features. Like DoD, many law enforcement applications make use of the GPS sensor to automatically record the locations of traffic accidents, police vehicles, road blocks, and other incidents. This information can then be saved to a law enforcement database. Also utilized is the built in camera to photograph and document crime scenes. Notes can be electronically added to the photographs and uploaded directly to the police station before the officer even leaves the crime scene. Law enforcement applications have also greatly enhanced on-scene data entry.

Whether being used for statements from witnesses or general observations, mobile applications are able to collect and store this information electronically and rapidly distribute this information if desired.

The development, adoption and use of mobile technology by law enforcement is expanding.

Platform	Application Name	Manufacturer	Description
iPhone®	ePocrates	Epocrates, Inc.	Contains databases and other tools for identifying drugs, infectious diseases, and medications.
iPhone®	Field Contact	Law Enforcement	Allows officers to record and send field information including name, address, vehicle information, aliases, and location of incidents, including photographs taken with the iPhone®.
iPhone®	Miranda Warning	Ron Shellnut	Provides officers with the Miranda statement to be read to individuals being arrested. In the future this will be multilingual and provide spoken Miranda warnings from a native language speaker. Replaces the physical Miranda card officers carry.
iPhone®	PoliceOne	PoliceOne.com	Keeps officers informed of events and strategies while on duty. Features include police breaking news, tactical tips, and expert columnist articles.
iPhone®	DUI Warning	Ron Shellnut	Application contains copies of implied consent warning card and field sobriety test instructions for officers.
iPhone®	USAccident Report	Tort Logics	Allows user to complete official accident report and submit the report directly from the phone.
iPhone®	Police Logger Plus	Gary Huntress	Allows users to automatically log the time and date of events.

Platform	Application Name	Manufacturer	Description
iPhone®	Police Notebook	APPiPhany Technologies Corp.	Allows police officers to officially record details and incidents while on patrol.
iPhone®	Auto VIN Decoder	Intersog	Application has the ability to return year, make, model, body style, engine type, manufacturer country when a VIN number is entered.
iPhone®	G360 Accelerometer	ARAS 360	Measures the braking potential on accident scene road surfaces.
iPhone®	Emergency Radio	Edge Rift	Allows users to listen into emergency radio transmissions, police, fire rescue, airport etc. Also provides backup to radio, can only send, but in the future text communication will allow units to communicate when radios fail or are inside, yet WiFi is available.
iPhone®	Pocket First Aid & CPR	American Heart Association	Guide for first responders on CPR and first aid techniques.
iPhone®	FBI Most Wanted	FBI	Includes mug shots and descriptions of many of the FBI top 10 Most Wanted lists. Also contains contact information for local FBI offices and embassies.
Blackberry	OnPatrol	xwave	Keeps law enforcement officials in touch. The application lets officers receive dispatches, send and receive messages, and access national police databases.

Table 2: Examples of Law Enforcement Mobile Applications

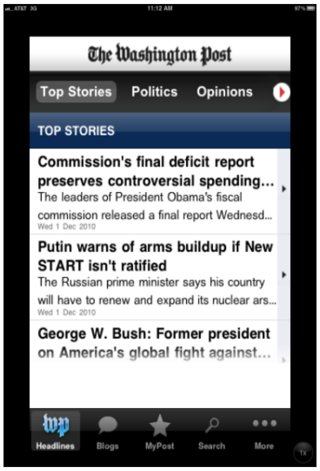
4.7 Libraries

Libraries are classic examples of information collection and dissemination organizations moving to mobile technology. Examining mobile device architectures and uses by libraries is important both from information dissemination and cataloging perspectives:

- Libraries must determine how users would identify publications in their library and then how they wish to receive them. Obviously, these publications could be books, articles, video, pod/screen casts or even interactive applications. The cataloging of publications for easy access is much more complicated than one might consider. For example, an obvious dissemination choice would be to create a web page based catalog with search options. However, a web page may be slow and unwieldy to interface with from a handheld mobile device. Also, the bandwidth of mobile devices whether on 3G, 4G or wireless will further dictate which method of delivery is possible. The available capabilities of the handheld mobile devices are also a consideration. For example, Flash is not supported on iPhones® and iPads® to deliver streaming content.
- Another important consideration with mobile based library applications is collaboration. The latest mobile library applications make it possible for mobile users to not only view and edit documents from anywhere, but also to share these rapidly changing documents with other mobile users. Today's mobile library applications are able to interface with online storage services such as Dropbox and Google Docs. This allows users to not only easily exchange documents between a computer system and a mobile device, but also directly with other mobile peers, taking the traditional computer system out of the loop. This type of cloud collaboration on mobile devices is allowing users to keep up with the fast paced information dissemination and collaboration needed in today's digital world.

Several library related products and applications include:

- iBooks® from Apple: When Steve Jobs announced to the world iBooks® for the iPad®, the future of eBooks changed. Even though Kindle has been available for several years, the market muscle of Apple combined with over seven million iPads® in circulation has changed the landscape and possibilities. In addition, the prospect of creating applications that deliver timely and relevant content to these devices is considerable. The iBook application is just one of many offerings that provide access to books on the iPad® and other mobile devices. The iBook library can store not only books, but articles, presentations and other documents.



Commission's final deficit report preserves controversial spending...
The leaders of President Obama's fiscal commission released a final report Wednesd...
Wed 1 Dec 2010

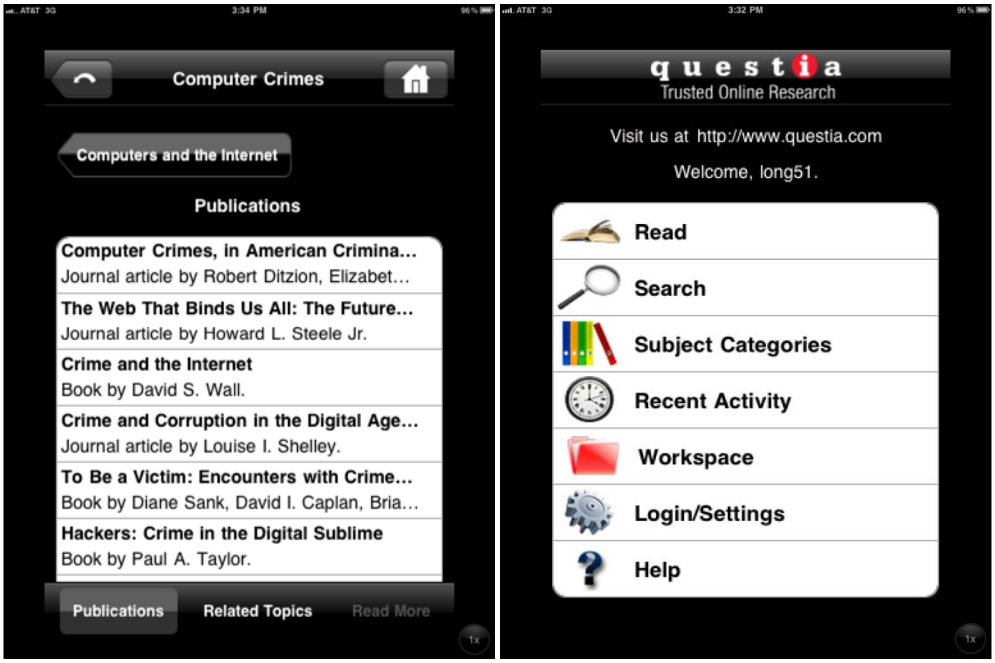
Putin warns of arms buildup if New START isn't ratified
The Russian prime minister says his country will have to renew and expand its nuclear ars...
Wed 1 Dec 2010

George W. Bush: Former president on America's global fight against...

Figure 2: Post App

- Other applications, such as the Washington Post App, delivers news content based upon user filters directly to the device (Figure 2). Note that this is not a just a web page rendering of the post, but rather an application that identifies specific content when it becomes available.
- The Questia application (Figure 3) provides access to over three million journal, magazine and news articles. This application may fundamentally change the way research is done.

Mobile based library applications are becoming enormously popular and widespread and are widely available on iPhone®, Android™, and Windows Mobile™ devices. Leveraging mobile technology for the purpose of retrieving information offers many advantages. Perhaps the biggest advantage is the ability to filter incoming information. Rather than manually navigating through information in a database, mobile users can choose to have specific categories of information automatically streamed to their mobile devices without user interaction. This is not only more efficient than traditional library systems, but also ensures that the user has access to



Computer Crimes, in American Crimina...
Journal article by Robert Ditzion, Elizabet...

The Web That Binds Us All: The Future...
Journal article by Howard L. Steele Jr.

Crime and the Internet
Book by David S. Wall.

Crime and Corruption in the Digital Age...
Journal article by Louise I. Shelley.

To Be a Victim: Encounters with Crime...
Book by Diane Sank, David I. Caplan, Bria...

Hackers: Crime in the Digital Sublime
Book by Paul A. Taylor.

Visit us at http://www.questia.com
Welcome, long51.

Figure 3: Questia

all of the latest information on a subject as soon as it is available. If a user still wishes to search for information on a subject manually, this can be done from any location where there is mobile data service. As a result, information is disseminated when users need it the most. Table 3 is a representation of the library apps that are in existence today for mobile devices.

Platform	Application Name	Manufacturer	Description
iPhone®	Documents To Go	DataViz	Allows users to view and edit Microsoft Word, Excel & PowerPoint, PDF, Apple iWork and other files and attachments, and easily share documents utilizing Google Docs, Box.net, Dropbox, iDisk and SugarSync.
iPhone®	Questia	Questia	Provides access to a collection of over 76,000 books and over 3 million magazine and newspaper articles.
iPhone®	Delicious Library 2	Delicious Monster Software, LLC	Allows users to photograph the barcode on CDs, DVDs, games, documents, and books, then reads the UPC and downloads all pertinent information about the scanned item.
iPhone®	Soonr	LetsGoMobile	A cloud based document collaboration solution. All documents are automatically stored and updated to the cloud and can be viewed and edited simultaneously by multiple users.
iPhone®	ReaddleDocs	Readdle	A file management application to distribute and receive documents from Windows, Mac or Linux computers, various web sites, email attachments, MobileMe iDisk and other online file storages and other iPhone®s.
iPhone®/IPad®	IStorage	ARAT	Allows users to view, edit, and receive documents from PC or Mac computers, websites, FTP, WebDAV, iDisk, and other online storage locations. Documents can also be shared between iPhone®s.

Table 3: Examples of Mobile Library Applications

5.0 Mobile Information Collection and Dissemination

When considering how to architect a mobile information collection and dissemination system assurances must be made that information can be delivered (pushed or pulled) to mobile devices in a trustworthy manner, specifically:

- What is the most effective means of making people aware of what information is available to assist them?
- Is it better to disseminate partial information (i.e., is timeliness more important that completeness)?
- How is information controlled and protected, and is this different in a crisis vs. normal operations?
- How can we be sure that information is available in multiple formats? What are these formats?
- Should the information be pushed, pulled, delivered via the web, or via custom applications?
- Should the tools used during a mission or emergency be the same as those used every day by those involved?
- What role does presence play in the dissemination of information (in other words, how can I be sure that the right people get the right information)?
- How long do users wait for a response before engaging others who could carry out orders or respond?

Digital devices, both mobile and traditional, running intelligent applications could play a key role in answering these questions. These devices would manage the complete information collection and dissemination process providing instantaneous decisions on how information should be distributed, secured, and stored.

5.1 Information Dissemination

Today’s mobile devices are able to disseminate information in many ways. Each of these dissemination technologies offers distinct advantages and disadvantages depending on the mode of operation. Currently, there are five widely adopted methods of information dissemination for the mobile user, including podcasts, V CASTs, custom mobile applications, traditional websites, and wikipedias.

5.1.1 Podcasts

A podcast is a non-streamed webcast. It consists of a series of digital media files that are released by episode and downloaded from the Internet. The method of delivery for content distributors is different than that of traditional downloads over the Internet. A list of the podcast files associated with a given series is usually kept on the distributor's server as a web feed. The client uses special software to access the web feed, check it for updates, and download any new files in the series. This process can be automated so that new episodes or files can be downloaded without user interaction. After acquisition, the podcast files are stored locally on the user's computer or mobile device ready for offline use. Podcasts, in many ways, are closer to traditional publishing models associated with books and magazines than other web content [POD].

Podcasts are already being utilized by the DoD. The Pentagon Channel uses podcasts to distribute the military news and information to personnel stationed around the globe [DOD]. Podcasts are also utilized as a training and informational tool. Soldiers can view podcasts on virtually any subject, anywhere on a mobile device. For example, if a military unit came upon an explosive device and needed to disarm it, a podcast could be played that walks the soldiers through the proper technique of disarming the explosive device.

The major benefit of information dissemination via a podcast is its portability. Because the podcast is downloaded in its entirety before viewing, no active connection is needed when watching the podcast. A user is only limited by the storage space on the device. Connectivity issues are completely eliminated.

5.1.2 V CAST

V CAST is a 3G Evolution-Data Optimized (EV-DO) network created by Verizon Wireless to deliver audio, video, and entertainment content to mobile devices. V CAST provides downloads of music, streaming video clips, and games which can be saved to the phone or a removable memory card. However, they cannot be read by other phones or computers because they are protected by Digital Rights Management software. Video playback and menu navigation in V

CAST requires EV-DO coverage to function. Without coverage, video playback is blocked [VCAST].

V CAST would be useful in a DoD environment where connectivity is not going to be a problem. Due to the streaming nature of this technology, information could be updated and distributed real-time to soldiers in the field on their mobile devices. This feature makes V CAST especially useful for dynamic information that will be constantly changing and evolving.

The real benefit of the V CAST network is its ability to adapt to rapidly changing information content and disseminate this information in real time. However, without a connection to an EV-DO network, information cannot be disseminated or viewed. An active connection to a mobile network is not always possible during a military operation due to factors such as geography and interference. During these times, V CAST technology will be unable to function to its fullest and will provide only limited value.

5.1.3 Custom Applications

Custom applications for mobile devices are third party developed software programs designed specifically for mobile usage. These applications can be downloaded to the mobile device and used immediately. They also allow for added control on how information is disseminated to mobile devices and what type of information is sent and received.

Custom mobile applications are already widely used in DoD environments. As seen in Table 1, the usage ranges from field intelligence, to training regimens, to map and terrain information. Preferences about when to receive information updates, what types of information to receive automatically, and connectivity settings can all be customized by the user allowing applications to be tailored to the environment they need to function in.

Because many custom applications are targeted to a specific brand of hardware, they are often not cross-compatible. In cases where multiple types of mobile devices are being used, this issue must be considered when implementing custom applications.

5.1.4 Traditional Web

The Internet, or traditional web, is still the most widely used source of informational content distribution today. Web information can be accessed by traditional computer systems and mobile devices via web browsers. With its widespread usage, virtually any type of information can be located and retrieved from the web.

Almost all government and DoD agencies have a web presence. They maintain websites to disseminate information to the public and also maintain more secure portions of web sites for employees and other insiders to view more sensitive information. The advantage of this type of information dissemination is it can be handled by most any web browser on any device. The major drawback is that an active Internet connection is necessary. Without an active connection, traditional web sites cannot be viewed and utilized.

To help support traditional web information dissemination to mobile devices, the Wireless Application Protocol (WAP) was created. By defining a communications protocol and an application environment, WAP was able to standardize information that is disseminated to mobile devices. Compatible with most major cellular signal types including GSM, CDMA, and 3G, the advantage of WAP is that it optimizes traditional web information for viewing on devices with low amounts of bandwidth, memory, and display capabilities. With support from companies such as Microsoft, Oracle, IBM, and Intel, WAP standards are rapidly being adopted [WAP].

5.1.5 Wiki

A wiki is a website that allows the creation and editing of interconnected web pages from a web browser using a customized markup language. Wikis are most often used in a collaborative environment with multiple sources able to contribute to the content of the site. Many wikis have user management capabilities providing different users with different levels of access. For example, a user with editing rights would be allowed to change, add or remove material. A user with only viewing rights could not alter any of the contents of the wiki and could only view the material. This feature is useful in maintaining the integrity of the information.

Wikis are an excellent method for information dissemination and collection. Because of their collaborative nature, the variety and quantity of information available in a wiki is unmatched by any other type of information dissemination medium. This method of information dissemination would be very useful for military personnel spread around the globe. Users can contribute and view information from any computer. Because wikis are collaboratively managed and updated, new information can be instantly disseminated as it becomes available.

Similar to traditional web technology, access to wiki pages require Internet connectivity. Therefore, the latest up-to-date information could not be viewed in areas where there was limited or no connectivity. Wikis offer a powerful information tool when connectivity is present.

5.2 Information Collection

Modern mobile devices have a number of different technologies to collect information, such as standard interconnections. This is best illustrated by the new Motorola Atrix™ 4G smartphone which can be docked and subsequently viewed from a laptop called the Motorola Lapdock™ [ATRIX].

Mobile device architectures usually have several components that communicate for data collection, transmission, storage and retrieval. Information collection is typically composed of three main components: the data collection application, the data transfer system, and the server-side components to receive and store the data. Figure 4 illustrates how these three components interrelate with each other [DATA].

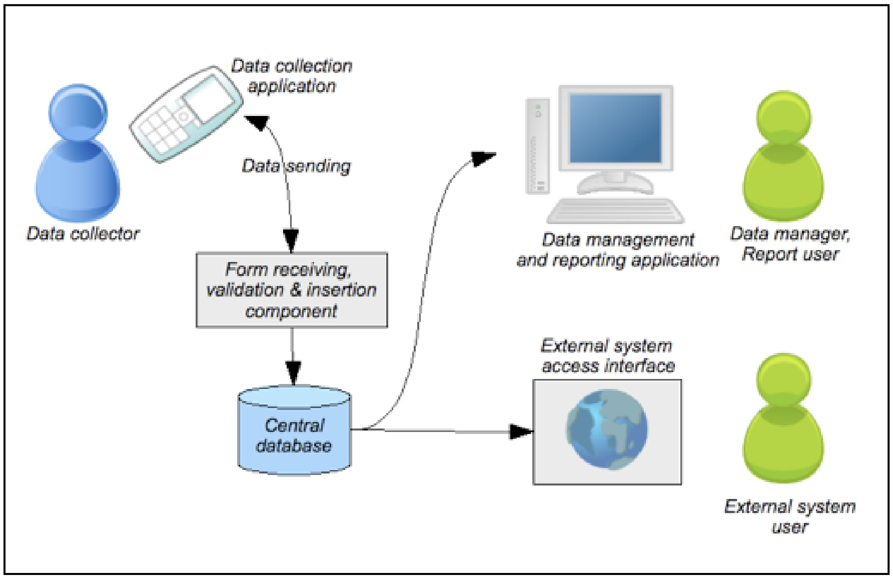

Data collection application
Data sending
Data collector
Form receiving, validation & insertion component
Central database
Data management and reporting application
Data manager, Report user
External system access interface
External system user

Figure 4: Mobile Device Collection Architectures

5.2.1 Data Collection Application

The data collection application is the interface the user interacts with for data collection and transmission. There are six popular types of data collection applications [DATA].

- **Fixed Format Short Messaging Server (SMS)** utilizes the mobile device's existing SMS capabilities to collect information. Using this type of data collection, the user provides answers to successive questions in a predefined format.
- **Java Micro Edition Platform** is an application written in the Java programming language. It is loaded onto the mobile device where the user navigates through questions in the application which collects the answers and submits the completed form to a server.
- **Web-based Forms** are forms published in an optimized format for mobile browsers. An online form is filled out utilizing a mobile web browser and then saved on the mobile device.
- **Voice-Data Collection** is when a user dials a number and chooses options from a menu.
- **Wireless Internet Gateway Menus** uses the Wireless Markup Language to create data collection menus.
- **Unstructured Supplementary Service Data** in which the mobile user starts a session and is able to interact with the remote server by selecting number based menu options.

5.2.2 Data Transfer Method

The data transfer method controls how collected information on a mobile device is transmitted to a central server for storage and future retrieval. Most mobile devices utilize the Global System for Mobile Communications (GSM) network for data transfer, specifically utilizing SMS or the General Packet Radio Service (GPRS). There are some important differences between SMS and GPRS technology. SMS is more widespread and is available on almost all mobile devices. GPRS is a higher-end technology that is not yet available on many mobile devices. However, GPRS offers advantages in cost and size. SMS is limited to 160 characters of data for each message. GPRS has virtually no character limit. Also, for the cost of one 160-character SMS message, many times that amount of data can be sent for the same cost using GPRS [DATA].

5.2.3 Server Side Components

There are three basic components to an information collection server side system [DATA]:

- A component that verifies the collected information and either rejects the information and notifies the information collector or accepts the data and inserts it into the database.
- A database to store collected information.
- A reporting system that can be accessed by both humans and external software systems.

6.0 Mobile Technology Architectures in Use by the Government

Much can be learned by understanding how existing mobile technology users are building or enhancing system architectures to support new capabilities.

6.1 US Army Common Operating Environment Architecture

The Common Operating Environment (COE) as depicted in Figures 5 and 6 is an approved set of computing technologies and standards that will enable secure and interoperable applications to be developed rapidly and executed across a variety of computing environments, including servers, clients, mobile devices, sensors and platforms. Each computing environment has a minimum standard configuration that supports the Army's ability to produce and deploy quickly high-quality applications, applications, and to reduce the complexities of configuration, support and training. The Army intends to establish a mobile deployment framework similar to industry best practices. Mobile applications will be designed, developed, and deployed on a common computing environment to allow the user to download what is needed. COE does not apply to embedded, real-time or safety-critical vetronics[2] and avionics systems. [COE].

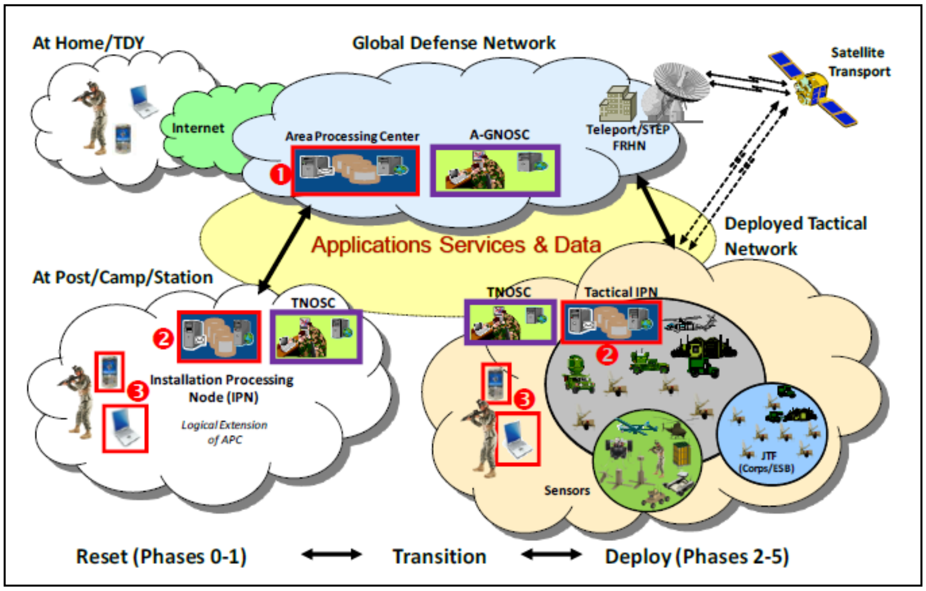


Figure 5: Common Operation Environment Network & Systems Diversity

[2] Vetronics is a portmanteau of the words vehicle and electronics, used extensively in the military domain

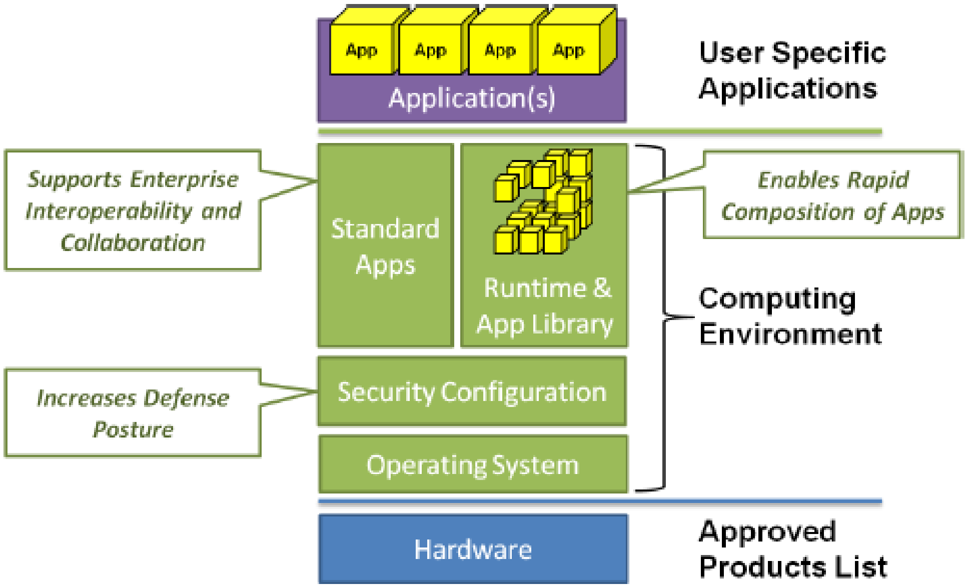


Figure 6: Mobile COE Computing Environments

6.2 DHS Homeland Security Information Network

Two of the primary objectives of the Department of Homeland Security (DHS) are to protect the country from potential terrorist attacks and to respond to natural disasters. To meet these objectives, rapid and efficient information sharing is needed. As a result, one of the core missions of DHS is to "create the technological and organizational infrastructure necessary to promote the sharing of information" [DHS ISS]. To facilitate this, DHS developed the Homeland Security Information Network (HSIN), a national web portal that allows information sharing and collaboration between local, state, and federal agencies [GSN]. The HSIN provides collaboration tools such as instant messengers, discussion boards, and document libraries making it possible for agencies across the country to work together. The HSIN, coupled with mobile technology, will allow rapid communication in the field during a disaster. While the current version of the HSIN is not set up for mobile technology, upgrade plans are in place that will require the HSIN to support the Wireless Application Protocol (WAP), the purpose of which is to standardize wireless data so it can be easily viewed on mobile devices [WAP2]. Once the HSIN is fully WAP compliant, DHS agents across the country will be able to rapidly access information via any data enabled mobile device. The following are some examples of technologies present in the HSIN [DHS]:

- Document Libraries
- Instant-messaging tool
- Web conferencing
- Incident reporting
- Common Operational Picture (COP) providing situational awareness and analysis
- Integrated Common Analytical Viewer
- Discussion Boards
- Online training materials

Figure 7 represents a small subsection of how information is currently collected and disseminated within the DHS network [HSA].

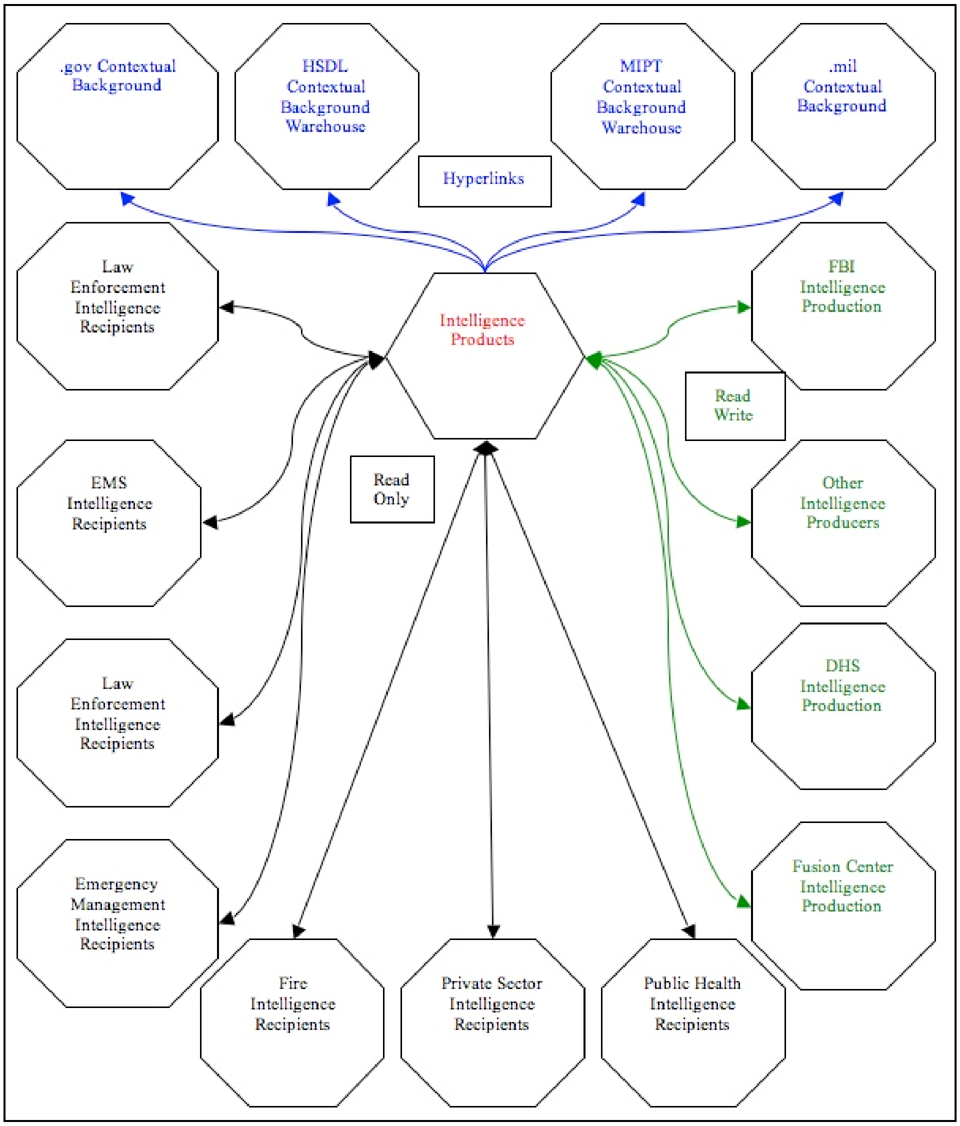

.gov Contextual Background
HSDL Contextual Background Warehouse
Hyperlinks
MIPT Contextual Background Warehouse
.mil Contextual Background
Law Enforcement Intelligence Recipients
Intelligence Products
FBI Intelligence Production
Read Write
EMS Intelligence Recipients
Read Only
Other Intelligence Producers
Law Enforcement Intelligence Recipients
DHS Intelligence Production
Emergency Management Intelligence Recipients
Fusion Center Intelligence Production
Fire Intelligence Recipients
Private Sector Intelligence Recipients
Public Health Intelligence Recipients

Figure 7: Homeland Information Security Network

6.3 Navy Next Generation Enterprise Network

The Next Generation Enterprise Network, or NGEN, is the latest advancement of the Department of the Navy's enterprise networks (Figure 8). According to the Navy's requirements document, "NGEN will provide a secure and reliable enterprise-wide voice, video, and data networking environment that meets the warfighter's needs, enabling command and control (C2) in conjunction with Consolidated Afloat Networks and Enterprise Services (CANES) and will provide a capability to access data, services, and applications anywhere worldwide." The network will also have the ability to interface with secure mobile devices. Information will be disseminated to these devices via secure voice, text, and paging services [NGEN].

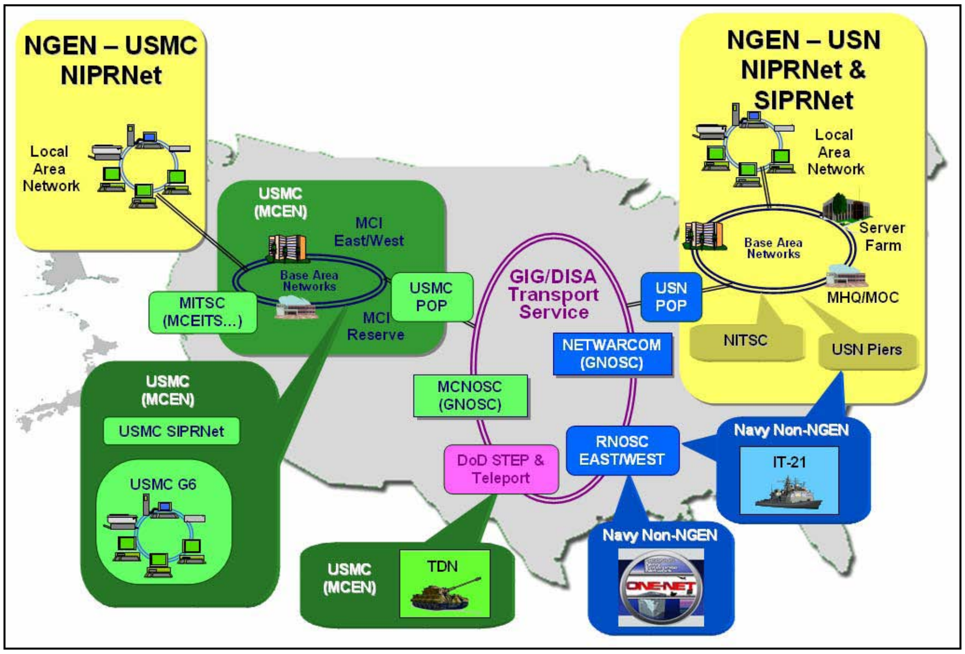


Figure 8: Navy Next Generation Enterprise Network

7.0 Current Mobile Device Technology

There has been much advancement in mobile technology recently. With the advent of open architectures for mobile devices, new applications and technologies are rapidly being developed.

7.1 iPad® and iPhone® Architecture

The iPad® is a tablet computer developed by Apple® Inc. The iPhone® is Apple's smartphone. Both iPhone® and iPad® run on iOS 4.X which provides a platform for developing multi-touch user applications. Applications for the iPad® and iPhone® are written in Objective-C and can be developed using Xcode, a fully featured Integrated Development Environment (IDE) aiding design, source code development and management. With the advent of iOS Software Developer's Kit (SDK), Xcode along with the Cocoa and Cocoa Touch frameworks provide a tightly coupled environment for application development. Cocoa is one of Apple's native object oriented programming interface for Mac OS X operating system and provides APIs for iPhone® and iPad® applications.

To work on the graphical components Apple provides an easy to use graphical editor, Interface Builder (IB), which stores the interface design of the application in one or more resources files as a set of objects together with the relationships between the objects. The code managing the implementation of the classes developed in Xcode using Objective-C can be synchronized with changes made to the interface using IB. Objective-C is the programming language of choice for developing iPad® applications. This object oriented language with its dynamic class system is built as a superset of the standard C language.

Applications developed for iPad® can make use of the following components:

- Accelerometers
- Core Location
- Maps (using the MapKit framework)
- Preferences (either in the app or presented from the Settings application).
- Address Book contacts
- External hardware accessories
- Peer-to-peer Bluetooth connectivity (using the Game Kit framework)

All iPad® and iPhone® applications use multi-touch technology. The screen receives one or more touch events that are translated into actions for manipulating the contents of the application. iOS also provides support for detecting gestures. Gesture recognizers simplify the interface for detecting swipe, pinch, and rotation gestures, among others, and use those gestures to trigger additional behavior. Users can also extend the basic set of gesture recognizer classes to add support for the custom gestures of the application.

All applications at the system level follow certain core principles:

- Only one application runs at a time, and an application's window fills the entire screen.
- Applications are expected to launch and exit quickly.
- For security purposes, each application executes inside a sandbox environment. The sandbox includes space for application-specific files and preferences, which can be backed up to the user's computer. Interactions with other applications on a device are through system-provided interfaces only.
- Each application runs in its own virtual memory space but the amount of usable virtual memory is constrained by the amount of physical memory. In other words, memory is not paged to and from the disk.
- Custom plug-ins and frameworks are not supported.

The key components of an iPad® and iPhone® application are shown in Figure 9.

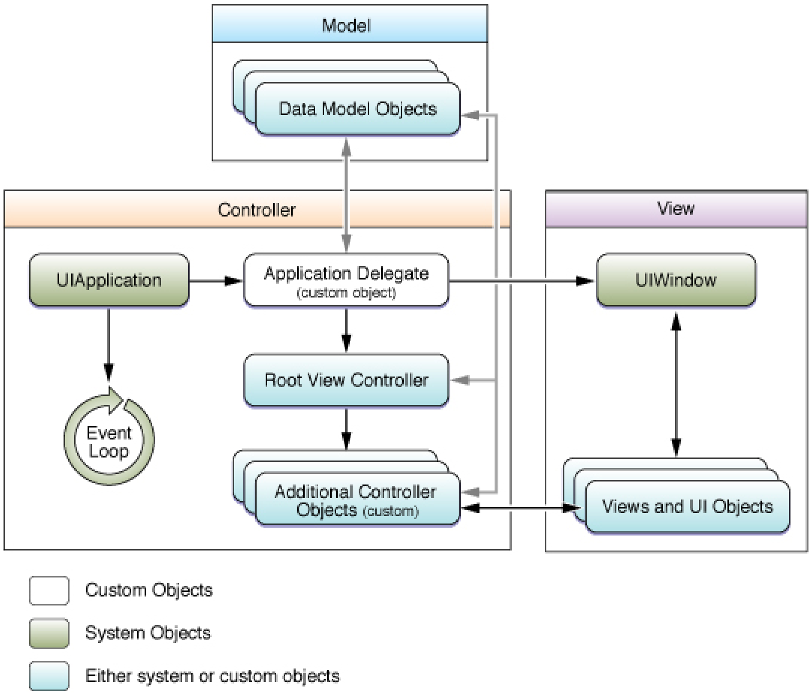


Figure 9: Apple's iPad® and iPhone® Architecture

7.2 Android™ Architecture

Android™ is a mobile operating system developed by Google® Inc. Android™ runs on an open-source Linux kernel that offers hardware access to all applications through a series of API libraries. Android™ uses the Dalvik Virtual Machine, a custom virtual machine that ensures multiple instances run efficiently on a single device. Applications for Android™ are developed using Java or C++. Android™ is an application-neutral platform, meaning that native and third-party applications are written with the same APIs and executed on the same run time environment. Eclipse provides a fully featured IDE aiding design and code management. With the advent of Android™'s SDK plugin, Eclipse now provides a tightly coupled environment for application development. Google freely provides the Android™ SDK including APIs, Android™ Virtual Device Manager and Emulator, sample code, full documentation, and online support for Android™ applications [MEIER].

"All Android™ hardware and system service access is managed using Dalvik as a middle tier. By using a virtual machine to host application execution, developers have an abstraction layer that ensures they never have to worry about a particlular hardware implementation. The Dalvik Virtual Machine executes Dalvik excutable files, a format optimized to ensure minimal memory footprint. Developers create .dex files by using the tools supplied within the SDK" [MEIER].

Applications developed for the Android™ can make use of the following components:

- Hardware-accelerated graphics (including 3D graphics using Open GL ES 2.0)
- GPS Location
- Maps
- InterProcess Communication (IPC) message passing
- Address Book contacts
- External hardware accessories
- Peer-to-peer Bluetooth connectivity
- Wi-Fi hardware access
- GSM, EDGE, 3G networks for telephony or data transfer
- Full multimedia hardware control, including playback and recording with the camera and microphone
- SQLite Database for data storage and retrieval
- Home-screen, Widgets, Live Folders, Live Wallpaper
- HTML5 WebKit-based browser

All Android™ applications use multi-touch technology. Gesture recognizers work as in the iPad® and iPhone® for detecting swipe, pinch, and rotation gestures, among others, using those gestures to trigger additional behavior. Users can also add support for custom gestures.

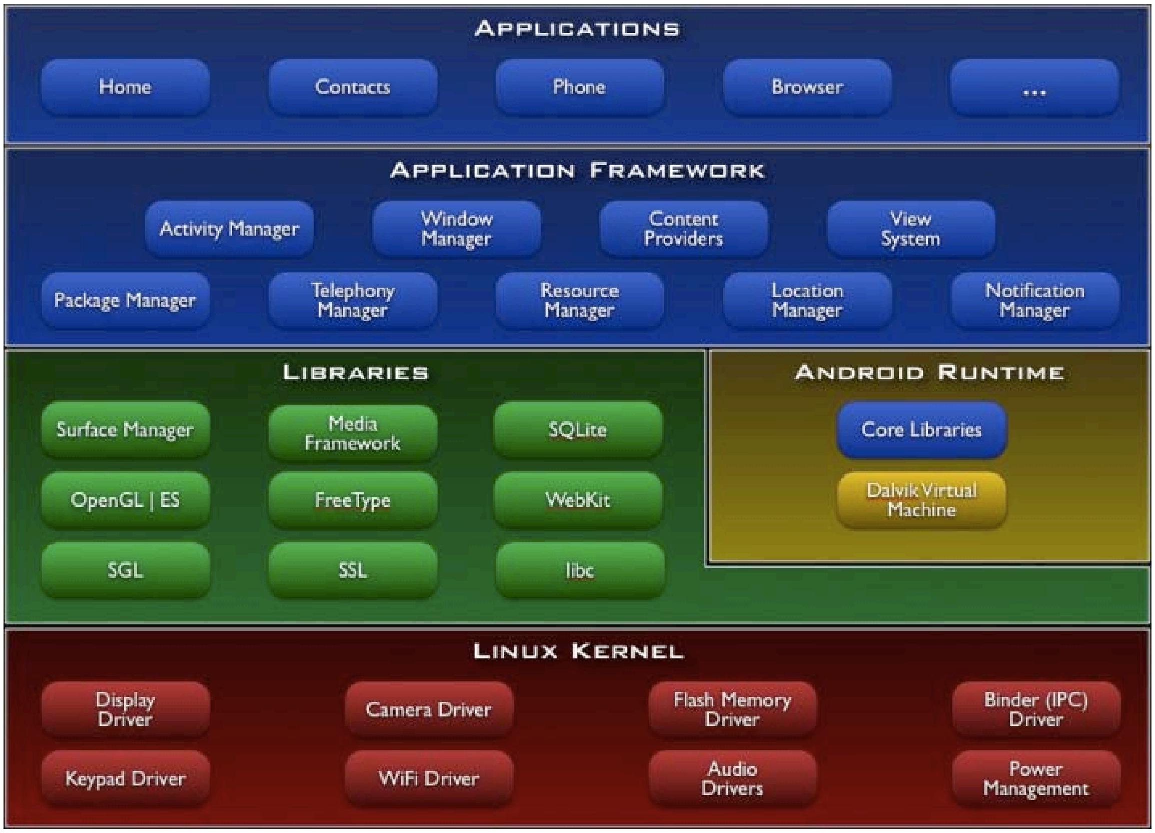


Figure 10: Android™ Architecture

Figure 10 shows the major components of the Android™ operating system.

7.3 Windows Mobile™ Architecture

Windows Mobile™ is an operating system developed by Microsoft for use in mobile devices. The OS features a suite of applications which were developed using the Microsoft API. The OS was recently rebranded from Windows Mobile™ to Windows Phone 7. As the successor to the Windows Mobile™ platform, Windows Phone 7 is aimed at individual consumers rather than the enterprise market like its predecessor.

Applications and games for Windows Phone 7 devices must be based in XNA, Silverlight, or the .NET Compact Framework 4 only. Developers can obtain Visual Studio Express and Expression Blend for Windows Phone to create mobile applications free of charge. Additional APIs are scheduled to be released for Windows Phone 7 to give developers more access to the hardware [PHONE 7]. Windows Phone 7 devices will make use of the Microsoft Unified File System for user files. This means that applications will not be able to distinguish between files on internal storage and main memory. Therefore, if the user removes the memory card, the phone will be able to do nothing but make emergency calls [SURUR].

Strict new hardware requirements have been released for Windows Phone 7 device manufacturers. They are as follows [PHONE 7]:

- Capacitive, 4-point multi-touch screen with WVGA (800x480) resolution
- 1 GHz ARM v7 "Cortex/Scorpion" or better processor
- DirectX9 rendering-capable GPU
- 256 MB of RAM with at least 8 GB of Flash memory
- Accelerometer with compass, ambient light sensor, proximity sensor and Assisted GPS
- 5-megapixel camera with an LED flash
- FM radio tuner
- 6 dedicated hardware buttons - back, Start, search, camera, power/sleep and Volume Up and Down
- External hardware accessories (via a USB connector)

Many new features have been added into the Windows Phone 7 operating system [PHONE 7]:

- The user interface consists of tiles. Tiles are links to applications, features, functions, and individual items such as contacts. The user has the ability to add, remove, or rearrange tiles. The tiles are also dynamic. They update in real time to provide information back to the user.
- User input is handled by an on-screen virtual keyboard.
- The web browser is Internet Explorer Mobile. Its rendering engine is halfway between the capabilities of Internet Explorer 7 and Internet Explorer 8.
- The new Windows Phone 7 hardware requirements state that every Windows phone must have a dedicated Search button on the front of the device. This button can be used to conduct searches across the phone or within currently open applications. The Bing search engine is the default built into all Windows Phone 7 devices.

- Updates to Windows Mobile™ devices will now be delivered via Microsoft Updates. Microsoft will directly update the phones rather t
- han via wireless carriers [SURUR].

Figure 11 illustrates the application framework in Windows Phone 7 [WIN7].

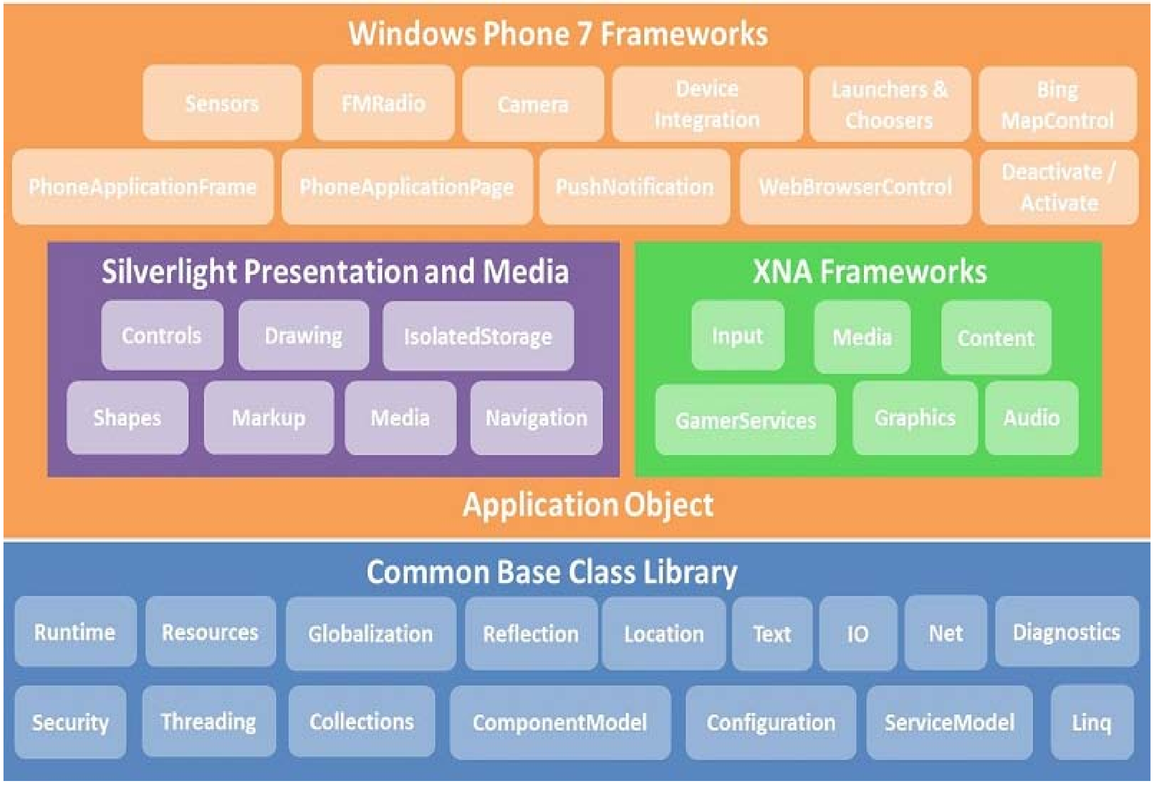


Figure 11: Windows Phone 7 Application Frameworks

7.4 Mobile Architecture Expandability

The mobile architectures discussed above are the basis for information collection and dissemination on any mobile device. It is important to understand how the different mobile architectures function not only for a better understanding of how mobile applications work, but also to develop new applications that expand upon the existing architectures for mobile information collection and dissemination.

As noted in the iPad® and iPhone® Architecture section, development on iOS based devices is accomplished with a combination of Xcode tools and the iOS SDK. Xcode is closely integrated with the Cocoa Touch frameworks which drive user interaction in the iOS operating system.

Cocoa Touch provides developers access to the device hardware including the camera, GPS sensor, and accelerometer. It is this access to the hardware that will lead future advancements in applications for information collection and dissemination. Because the Xcode tools and iOS SDK are both available free of charge from the Apple web site once a user is registered [APPLE], anybody can develop new technologies for both the iPhone® and iPad®. This will increase the number of new applications developed for these devices and bring new ideas on how to utilize the iOS architecture, likely initiating development of new methods of information collection and dissemination.

Much like the iPhone® and iPad®, Android™-based devices also offer a free downloadable SDK from their website. The latest Android™ SDK gives developers access to hardware components including GPS sensors, near-field communications hardware, Bluetooth, speech recognition hardware, displays, and accelerometers. Unlike Apple, which approves all applications before they are published to the application store, Android™ developers are able to publish applications to the Android™ Market simply by registering as an Android™ developer. As a result, applications are being added to the Android™ Market at a much greater rate than the iPhone® application store. However there is greater opportunity for bugs in Android™ applications as they are not as thoroughly vetted as iOS applications [ANDR]. Despite this, the opportunity for technology advancements and expandability on Android™ based hardware is greater due to the open nature of the architecture.

Windows Mobile™ devices also have similar development tools. Microsoft has developed an "APP HUB", a developer's resource for creating applications on Windows Phone 7 based devices. Included on the APP HUB web site is a free SDK and tutorials that walk developers through Windows Phone 7 programming. Included in the tutorials is a section detailing how to interact with the device's hardware features, specifically the GPS sensor, accelerometer, and camera [APP HUB]. All of these hardware devices can be utilized by future developers to expand the capabilities of Windows Phone 7 based devices to both collect and disseminate information.

7.5 Best Practices for Mobile Web Software Development

When moving to mobile technology it is important to understand how to best develop application software, taking into account the unique and limiting features of the devices. The Mobile Web Best Practices Working Group of the World Wide Web Consortium (W3C)[3] has developed a proposed recommendation of *Mobile Web Application Best Practices* (see http://www.w3.org/TR/mwabp/) "to aid the development of rich and dynamic mobile Web applications. It collects the most relevant engineering practices, promoting those that enable a better user experience and warning against those that are considered harmful."

As noted in the document, the line between mobile and non-mobile is blurred, and thus the document focuses on aspects of web development that are non-trivial concerns associated with the mobile context. It addresses limitations (e.g., screen size) and unique features of mobile devices. Most of the best practices are targeted for mid- to upper-end devices which support XHTML, JavaScript[4], and Cascading Style Sheets (CSS) capabilities.

The software development best practice recommendations fall into seven broad categories:

- Appropriate technologies and techniques to use for managing a web application's data
- Security and privacy considerations – use trusted information and protect personal information. Most desktop related security advice (e.g., OWASP) is applicable to mobile devices.
- User Awareness and Control – allow the user to control application behavior
- Conserve use of device resources – minimize use of device memory, power, bandwidth, etc.
- User experience considerations
- Handling variation in the delivery context (i.e., device capabilities)
- Other Considerations – these are not best practices, but advisory notes

[3] The W3C is the where most developers look for new Web standards.

[4] JavaScript is a popular dialect of the ECMAScript, widely used for client-side scripting

These best practices, summarized in Table 4, organized into the seven categories, recognize the following realities of mobile technology:

- Mobile devices are resource constrained in memory, screen size, battery life, etc.
- Mobile networks are not as reliable and fast as other networks
- Mobile devices are not uniform, so a single solution for an application may not be possible
- Mobile technology has the same security issues as other technology

Category	Best Practice	Explanation
1. Web Application Data	1. *Use Cookies Sparingly*	Applications should remain functional even if cookies are unavailable (e.g., if disabled). Cookies are a way to store small amounts of state data on the device, such as user identity for automatic sign-in. Information in cookies is sent to server for every request, which may impact performance.
	2. *Use Appropriate Client-Side Storage Technologies for Local Data*	Applications should continue to be able to run, even with unreliable network signal. Use for storing larger amounts of data other than cookies. When application is started, application data can be displayed immediately, reducing start-up latency. Make updates locally first, then replicate changes to server in the background when connectivity is available.
	3. *Replicate Local Data to a Server if Necessary*	Send data back to a server in order to provide a consistent view across devices and make data recovery possible in the event of a lost device.
2. Security Considerations[5]	1. *Do not Execute Unescaped or Untrusted JSON (JavaScript Object Notation) data*	A common technique is to use JSON to transfer data to the device and then use a JavaScript function [eval()] to

[5] The document does not provide an exhaustive set of security issues, but only identifies the one that is specific to mobile devices

Category	Best Practice	Explanation
		parse it. However this represents a security risk and should be avoided. Malicious JavaScript on a mobile device may expose personal information.
3. User Awareness and Control	1. *Ensure the User is Informed About Use of Personal and Device Information*	Provide enough information so the user can judge whether to allow application access to their data. Provide notice on first access by the web application, or when first access to the information occurs.
	2. *Enable Automatic Sign-In*	Prompt the user for username and password within the application, but provide the option to automatically sign-in on next session. Provide a sign-out link.
4. Conservative Use of Device Resources	1. *Use Transfer Compression*	Use HTTP 1.1 compression. Configure web servers to serve compression responses.
	2. *Minimize Application and Data Size*	Given constrained devices, smaller applications are more reliable.
	3. *Avoid Redirects*	Delays by redirects are much higher in mobile networks.
	4. *Optimize Network Requests*	Establishing connections on a mobile network may take a long time. It is better to make fewer, but larger requests.
	5. *Minimize External Resources*	Web applications require many resources, such as style sheets, images, etc., so fewer and larger requests are preferred.
	6. *Aggregate Static Images into a Single Composite Resource (Sprites)*	Icons, buttons, etc. depend on images. Each image may result in an individual request, so it is better to combine images and transmit as a single request.
	7. *Include Background Images Inline in CSS Style Sheets*	To avoid additional network requests, include images and gradients in CSS.
	8. *Cache Resources by Fingerprinting Resource References*	Browsers do not have to check resource headers to validate cache by identifying them with a URI that includes a hash of the resource content.

Category	Best Practice	Explanation
	9. *Cache AJAX (Asynchronous JavaScript) Data*	Data to be accessed by AJAX requests should be cached.
	10. *Do Not Send Cookie Information Unnecessarily*	Static resources do not need cookie information.
	11. *Keep DOM (Document Object Model) Size Reasonable*	Complex pages may exceed DOM size limits.
5. User Experience	1. *Optimize for Application Start-up Time*	Follow techniques that minimize application start up time.
	2. *Minimize Perceived Latency*	Usability is improved when perceived latency is optimized
	3. *Design for Multiple Interaction Methods*	Due to variation across devices, use Focus Based, Pointer Based, and Touch Based interaction methods.
	4. *Preserve Focus on Dynamic Page Updates*	Avoid unexpected page focus changes.
	5. *Use Fragment IDs to Drive Application View*	Enable deep links and browser history to improve usability.
	6. *Make Telephone Numbers "Click-to-Call"*	Use standard URI schemes for common device functions.
	7. *Ensure Paragraph Text Flows*	Make sure flow doesn't require horizontal scrolling.
	8. *Ensure Consistency of State Between Devices*	User credentials, preferences, and data from one device should be valid and available on other devices. Store device independent data on server.
	9. *Consider Mobile Specific Technologies for Initiating Web Applications*	Use content "push" methods for updates and notifications.
	10*. Use Meta Viewport Element to Identify Desired Screen Size*	Always render pages at 100%. Do not use browser based scaling.
6. Handling Variation in the Delivery Context (e.g., device capabilities)	1. *Prefer Server-Side Detection Where Possible*	Server should determine the properties of the context and adapt responses to client before transfer.
	2*. Use Client-Side Capability Detection Where Necessary*	Client may have to adapt content from server if server cannot adapt.
	3. *Use Device Classification to Simplify Content Adaption*	Build a single application variant for each class of device, resulting in a manageable code base.
	4*. Support a non-JavaScript Variant if Appropriate*	If broadest device support is desirable, provide a variant of an application that uses FORM posts rather than XML Http Requests; particularly in low-

Category	Best Practice	Explanation
		bandwidth settings.
	5. *Offer Users a Choice of Interfaces*	If multiple versions of an application are available, allow user to select version to use.
7. Further Considerations (not Best Practices, but Advisory Notes)	1. *Consider Use of Canvas Element*[6] *or SVG*[7] *for Dynamic Graphics*	Support for these technologies varies across devices.
	2*. Inform the User About Automatic Network Access*	Network traffic uses battery life
	3. *Provide Sufficient Means to Control Automatic Network Access*	Provide a means for the user to disable network access.

Table 4: Mobile Software Development Best Practices Summary

[6] Canvas element specifies a display region for JavaScript

[7] SVG – Scalable Vector Graphics XML Language

8.0 Key Aspects of Mobile Information Management

The following subsections examine mobile-specific technical considerations when deciding whether to implement mobile technology.

8.1 Dynamic Information Dissemination

Mobile based software primarily works on a user controlled model to retrieve information. The user initiates an event where information is exchanged between the client and server. In a mobile computing environment where information changes frequently, having to always initiate the information exchange can be impractical. As a result, an information-push model (where delivery of information is initiated by the server rather than the user) is more efficient and potentially more useful.

The information-push model has many advantages for mobile devices:

- Users can view previously fetched information much more quickly than if it is downloaded on demand.
- The information-push model is a natural fit for hands free interfaces on mobile devices. This model can allow mobile devices to be set to receive specific types of data. Once set, streams of information, or channels, would flow to the device with no user input necessary.
- Asynchronous user notifications are more easily modeled in mission-critical applications when information-push based communication is available.

Dynamic information dissemination allows users to react and adapt to new operating conditions quickly. The information pushed to devices could automatically adjust based on the location of the device. [DYNAMIC]

Lockheed Martin and DARPA have implemented this principle into the prototype application shown in Figure 12. The goal was to rapidly push information gathered by soldiers to other units so it could be acted upon quickly. To achieve the dynamic nature of the information disseminated a series of intelligent agents were built into the architecture of the application. An analysis agent was used in this application to determine when a member of the squad needed information pushed to their mobile device, based primarily on location. As a soldier approached a location where data or intelligence was available or critical, the data would be automatically sent to their mobile device. This enabled relevant information about threats, terrain, and field equipment to be rapidly and automatically disseminated to the correct soldiers at the correct time. This dynamic push of only relevant data to the soldiers minimized bandwidth loads over the mobile network. A separate delivery agent handled receiving information for the soldier. If there was a connection failure, the agent would retry to push the data at regular intervals without user interaction [AGENTS]. Figure 13 shows a sample screen of this application.

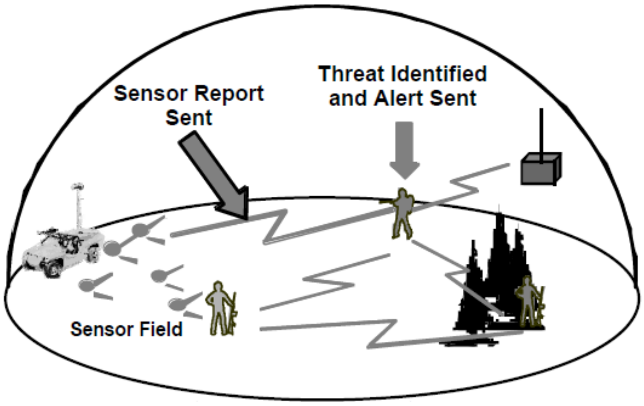


Figure 12: Intelligent Mobile Agents

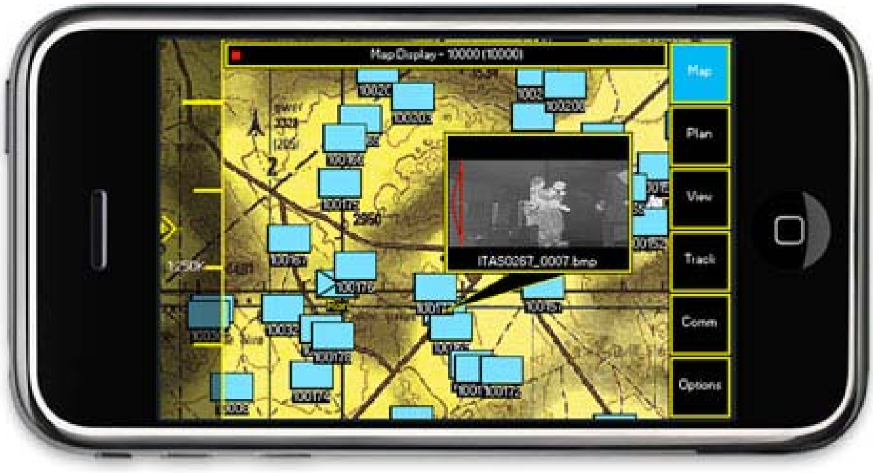


Figure 13: Intelligent Mobile Agents Screenshot

8.2 Security Considerations

As the use of mobile devices continues to increase, the amount of data being transmitted will continue to rise. This data can be sensitive or classified and must be kept secure. Certain unique security considerations must be examined when using mobile devices.

8.2.1 Electronic Tracking

One of the most widely used mobile features is the Global Positioning System (GPS). While this feature is beneficial and valuable in a mobile device, it can also be exploited. Cellular phone carriers have long had the ability to track the location of mobile devices using either the GPS or cellular communication towers, and other companies are now beginning to develop products and provide services to track mobile devices. Many of these tracking services run covertly to the mobile device's user, sending no messages or indications that the device is being tracked [NIST]. Also, photographs taken with mobile devices can be geotagged by the unit's GPS without the user's knowledge. This data can then be extracted from the photograph by a potential adversary to determine where the photograph was taken [GEO]. Another danger of mobile device tracking services is an attacker can secretly register a mobile device for tracking without having actual possession of the mobile device [NIST]. This can ultimately help an attacker track a mobile device and its owner. This becomes especially problematic in a military setting where confidentiality of location is crucial to mission success.

8.2.2 Mobile Device Cloning

Another security issue is mobile device cloning. Each device has unique identifiers programmed into it to help identify it. For example, the signal produced by a mobile device contains both a unique Electronic Serial Number (ESN) and Mobile Identification Number (MIN). If an adversary was able to intercept the signal and extract these two pieces of data, a cloned mobile device could be created that was able to both send and receive data posing as the original device. This type of attack presents both confidentiality and integrity concerns. First, with a cloned mobile device, an attacker could intercept sensitive and confidential information. Secondly, the attacker could also send out false information which would appear to be valid [NIST]. For warfighters this could be catastrophic as an adversary could both intercept mission plans and send out new falsified mission plans to units. Many of today's mobile devices have begun encrypting signals to ensure that neither the ESN nor the MIN can be captured. However, a how-to-guide was recently released detailing how to crack the A5/1 stream cipher used to encrypt GSM networks [INFO].

8.2.3 Denial of Service

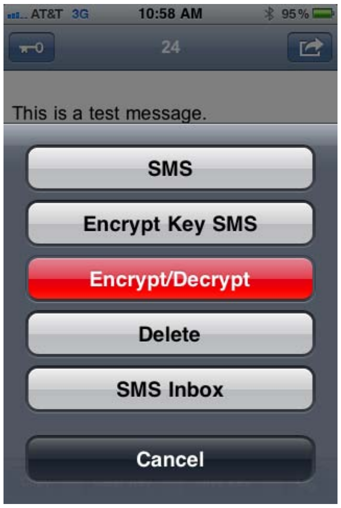
A crucial component to any mobile device is the availability of data and communication networks. One of the main objectives of information warfare is to deny adversaries access to information systems, cutting off the ability to effectively send and receive anything. There are a number of methods to disrupt communication services. The simplest is a jamming device. Devices available on the market today can jam mobile devices in localized areas, leaving the user unable to receive a signal. The downfall to this type of attack is only a limited number of users are affected; only those in range of the jamming device will lose service. Software based approaches to denial of service can have much wider reaching effects. An example of a denial of service attack would be Short Message Service (SMS) texting. If a mobile network was spammed with enough SMS messages, all services, from voice calls to data, would be rendered unusable in that network. A more advanced denial of service attack may attack the mobile device itself, using SMS injection to crash connectivity [INFO]. With respect to jamming, friendly forces use that tactic as well. In 2006, the Pentagon spent around $1.4 billion on jamming devices. Users need to determine what effect jamming equipment will have on their own mobile based information communication assets and adjust accordingly.

8.2.4 Mobile Malware

With the increasing popularity of mobile devices new forms of malware, which specifically target mobile devices, are emerging. Malware can be delivered to a mobile device through Multimedia Messaging Services (MMS), email, Bluetooth connections, or internet downloads. Just as on a traditional computer system, users can download malware from the internet disguised as a game, patch, application, or any other benign piece of software. Using Bluetooth, the malware engages the connectivity services that Bluetooth offers to connect to a mobile device and deliver the malware. Once the mobile device is infected it is susceptible to attacks including data theft, spoofing, backdoor access, data interception, service abuse, and device availability [NIST].

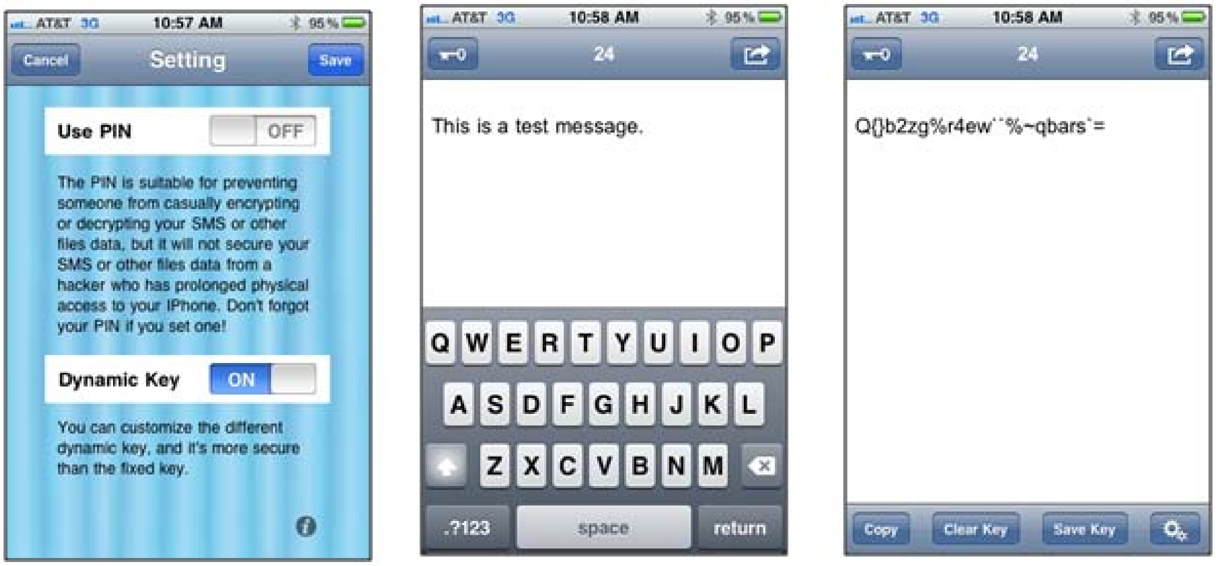
8.2.5 Secure Messaging

Based upon the above security considerations, one of the major areas of research in mobile devices today is the ability to securely send and receive messages. An application, **SecureSMS Pro**, for the iPhone® was recently released that addresses this problem (Figures 14 & 15). This application allows the user to encrypt SMS messages before sending. This can be done by utilizing either a user defined PIN, which is less secure but quicker, or a dynamically generated key which is the most secure method of transmitting messages offered by this application. The application can also encrypt the content of an email message before transmission as well.



This is a test message.

Figure 14: SMS Menu



Use PIN OFF

The PIN is suitable for preventing someone from casually encrypting or decrypting your SMS or other files data, but it will not secure your SMS or other files data from a hacker who has prolonged physical access to your IPhone. Don't forgot your PIN if you set one!

Dynamic Key ON

You can customize the different dynamic key, and it's more secure than the fixed key.

This is a test message.

Q{}b2zg%r4ew``%~qbars`=

Figure 15: SMS Screenshots

8.2.6 Trusted Applications

When using a mobile device to deal with sensitive, high-assurance information, it is critical to utilize only trusted applications. As stated above, there are multiple methods to deliver malware to a mobile device. One method of combating this is to only use trusted applications. DoD has developed a trusted application store known as "DoD Storefront." Designed to be used only by military personnel, this store contains trusted applications designed for smartphones. Because the DoD Storefront utilizes preapproved software development toolkits and automates submission, testing, and certification, applications are able to get to the field more quickly and efficiently. Access to the store is only available through the use of a DoD Common Access Card (CAC). Also available to users of the DoD Storefront will be collaboration tools. Through a comment and rating system, developers and end-users will be able to work together to deliver the types of applications that are really needed in the field. An online testing environment will also be available for end users to test beta versions and offer feedback. As development continues on the DoD Storefront, individual sub-stores will be developed for different branches. An example of this is the U.S. Army Marketplace which is already in the preliminary stages of use. This will allow for increased specialization in the types of apps developed for each branch of the military, increasing both the effectiveness and the efficiency of applications developed for use in DoD [ARCH].

Another approach to ensuring only trusted applications are used on a mobile device is whitelisting. Whitelisting is a process by which only known and trusted applications are allowed to be installed on a system. The iPhone® currently operates on this principle. When a user wants a program to run on the iPhone®, he or she must get it approved by Apple and put in the iPhone® store (unless the phone is tampered with or what is commonly referred to as iOS jailbreaking). The whitelisting process used by Apple is not a perfect solution for trusted applications, but whitelisting in general is gaining momentum as a way to gain trust in the applications we depend upon. [WHITE].

8.3 Mobile Device Usage Considerations

Usage considerations include hardware limitations and environmental variables which can have a major impact on how devices perform in the field. Knowledge of these limitations is vital prior to widespread deployment.

8.3.1 Touch Screen

Many of today’s advanced mobile devices have a touch screen for typing or selecting options. In a harsh environment, this can create problems. Most touch screens react to touch through the natural bioelectricity in the skin. Small amounts of moisture, salts, and oils on the skin create the

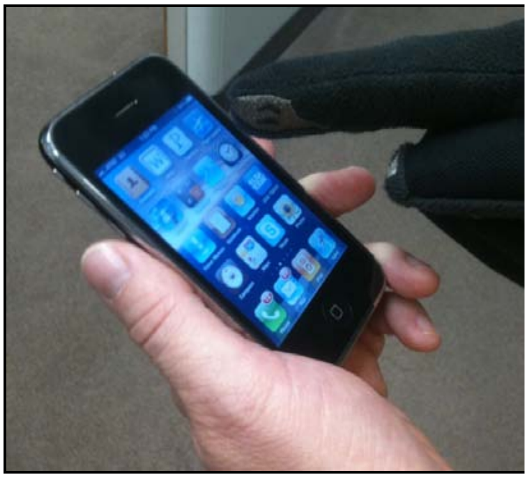
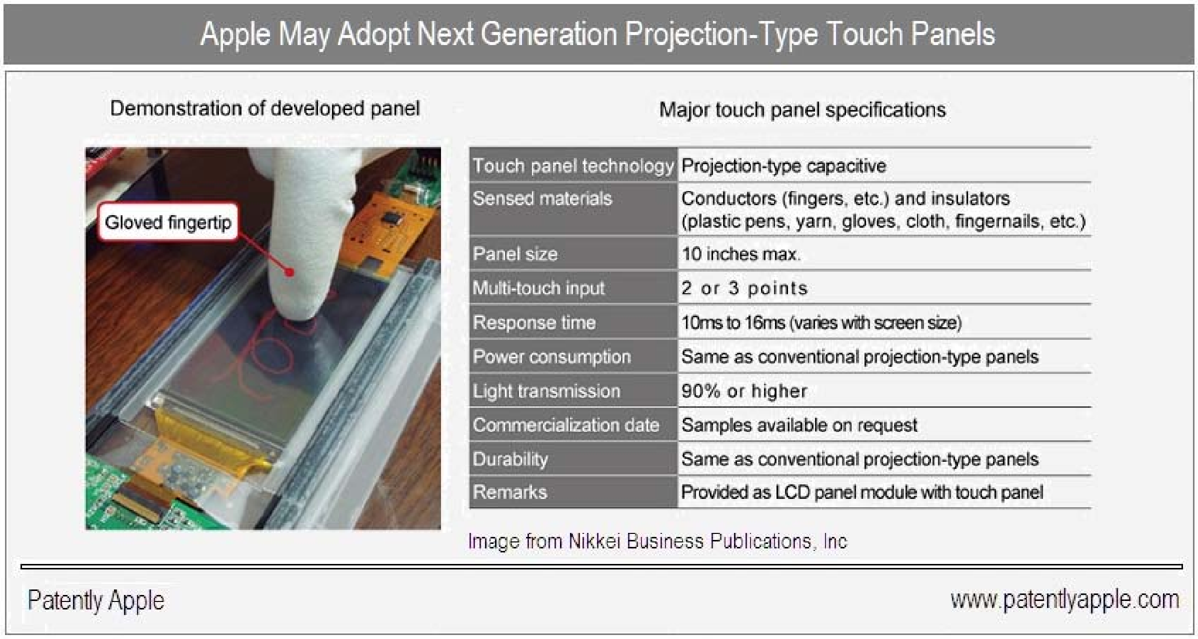


Figure 16: Touchscreen Glove

necessary conductivity. Many soldiers, during operations and exercises, wear protective gloves which prevent the conductivity. As a result, soldiers must remove their gloves whenever they want to input or select data. This can be time consuming and often impractical. To combat this problem some technological advances have been made. Companies have started producing gloves made from highly conductive elements, such as silver, which allows the user to use a touch screen while wearing the gloves (Figure 16) [GLV].

Apple is also looking into a solution for this problem on its next generation of iPhone®. Apple has been working with Japan's Hitachi Displays who has developed a projection-type touch panel capable of detecting insulators such as plastic and cloth. With this new display, users can select icons with the tip of a gloved finger or input handwriting with a plastic pen. Figure 17 shows the technical specifications for the new projection-type capacitive screen [TCH].



Apple May Adopt Next Generation Projection-Type Touch Panels

Demonstration of developed panel

Gloved fingertip

Major touch panel specifications

Touch panel technology	Projection-type capacitive
Sensed materials	Conductors (fingers, etc.) and insulators (plastic pens, yarn, gloves, cloth, fingernails, etc.)
Panel size	10 inches max.
Multi-touch input	2 or 3 points
Response time	10ms to 16ms (varies with screen size)
Power consumption	Same as conventional projection-type panels
Light transmission	90% or higher
Commercialization date	Samples available on request
Durability	Same as conventional projection-type panels
Remarks	Provided as LCD panel module with touch panel

Image from Nikkei Business Publications, Inc

Patently Apple www.patentlyapple.com

Figure 17: Next Generation Touch Screens

8.3.2 Display

Another consideration in the deployment of mobile devices is how the display screen reacts to direct sunlight. Most displays currently in use are Active-Matrix Organic Light-Emitting Diode (AMOLED). These often become extremely washed out and difficult to read in direct sunlight. Anti-glare screen protectors have been introduced over the years to help combat this problem with little or no success. One technology, Super AMOLED, is showing promise. Traditional touch screens consist of two layers, a separate display and touch layer. These two layers can create a reflective glare when exposed to sun.

Super AMOLED screens have only one layer, eliminating the air gap that causes this glare. The result is a much easier to read display in direct sunlight. Super AMOLED screens also offer a 180 degree viewing angle and a 20% brighter and are noticeably clearer than a typical AMOLED screen. Color reproduction is also 30% better than LCD screen technology. This technology is already available on some smart phones such as the Galaxy S from Samsung [SAM].

8.3.3 Environmental Variables

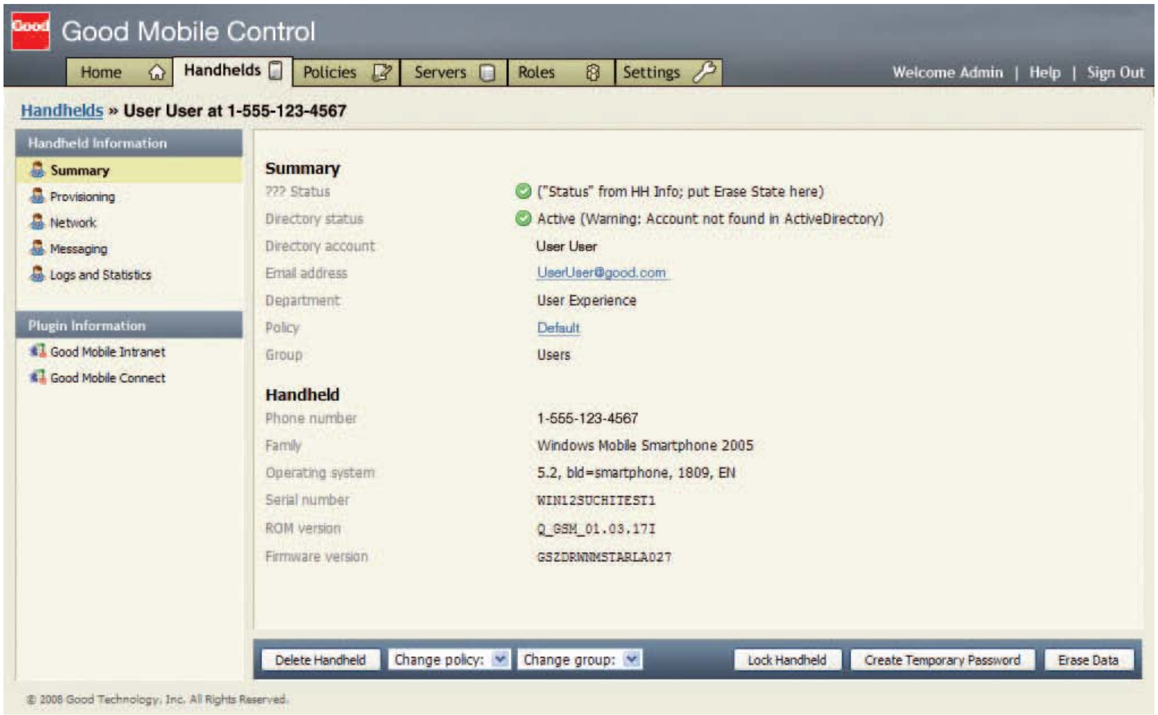
When used in military operations, mobile devices can be exposed to some harsh environmental conditions. It is important to understand the limits of mobile hardware before exposing it to these conditions. The following operating requirements are specified for the iPhone®:

- Operating temperature: 32° to 95° F (0° C to 35° C)
- Nonoperating temperature: -4° to 113° F (-20° C to 45° C)
- Relative humidity: 5% to 95% noncondensing
- Maximum operating altitude: 10,000 feet (3000 m)

The operating requirements for the iPhone® are representative of the limits in environmental conditions that most mobile devices can work in. These can become significant when operating in mountainous regions, extreme hot or cold areas, or areas with very high humidity [SPECS].

8.3.4 Secure Information Removal

A major concern with mobile devices is how to securely delete sensitive information if a device is lost or stolen. To help accomplish this, many DoD agencies are adopting a suite of tools known as Good for Government. Good for Government is defined as “productivity and mobile device management tools for agencies requiring the highest level of end-to end security." Some of the features of this tool suite include: locking down device functionality such as the camera, infrared port, Wi-Fi, and Bluetooth features; controlling which applications are allowed to exist on the device; dictating which apps must be running before allowing a secure connection; and remotely wiping a lost or stolen unit. The remote wiping feature allows mission commanders to initiate a secure and unrecoverable data wipe sequence if a mobile device is compromised (Figure 18) [GFG].



Handhelds » User User at 1-555-123-4567

Summary

??? Status	✓ ("Status" from HH Info; put Erase State here)
Directory status	✓ Active (Warning: Account not found in ActiveDirectory)
Directory account	User User
Email address	UserUser@good.com
Department	User Experience
Policy	Default
Group	Users

Handheld

Phone number	1-555-123-4567
Family	Windows Mobile Smartphone 2005
Operating system	5.2, bld=smartphone, 1809, EN
Serial number	WIN12SUCHITEST1
ROM version	Q_GSM_01.03.17I
Firmware version	GSZDRWNMSTARLA027

© 2008 Good Technology, Inc. All Rights Reserved.

Figure 18: Mobile Device Security Example

9.0 Mobile Device Trends

With the increasing use of mobile devices for information collection and dissemination some distinct trends are developing for their applications, hardware and how they are used. These are already having an impact on future development directions for these devices.

9.1 Mobile Applications

Mobile network carriers are rapidly losing their dominance in providing consumer applications to mobile devices. Internet players, application stores, and cross-industry services are quickly replacing mobile carriers as the primary applications providers. These groups are competing to control the overall mobile device experience for users. A recent study published by Gartner [TOP2012], a leading IT research and advisory company, predicted the top ten consumer mobile applications for 2012. Six of the predicted top ten application categories for 2012 are specifically designed for information collection and dissemination. The first of these is location-based services, which are applications that are context-aware, meaning they collect information about the device's location and provide relevant information based on this location. Gartner predicts that the number of users for location-based services will grow globally from 96 million in 2009 to more than 526 million in 2012.

Mobile web browsing is also expected to grow significantly. Currently, web browsing is available on more than 60% of mobile devices. This number is expected to rise to around 80% by 2013. The mobile web will be a key component of most corporate business-to-consumer information distribution strategies in the future.

Another category of application predicted to be very prevalent in 2012 is near-field communication (NFC) services. This allows information transfer between compatible devices by placing them close to each other, usually within 10 centimetres, providing the capability to collect information for such things as retail purchases, transportation, personal identification and retail loyalty cards.

Though not necessarily applicable to government applications, mobile advertising is also on the rise. Despite the recent economic downturn, the distribution of information via mobile advertising has continued to grow over the last several years. The total money spent on mobile advertising in 2008 was $530.2 million and is expected to grow to $7.5 billion by 2012.

9.2 Hardware

The main catalyst for developments and trends in mobile device hardware is the continued need to improve performance, reduce costs, and promote continued miniaturization. Five hardware trends expected to occur in the next year are dual-core processors, 3D displays, NFC wireless technology, dual SIM cards, and advanced video recording and playback capabilities. All of these hardware trends are not only relevant to information dissemination and collection, but will change how information is exchanged.

The first advancement, dual core processors, will offer users of mobile devices better video performance, faster and smoother web browsing, and multitasking with virtually no screen lag. This translates to viewing and retrieving information quicker, easier, and more efficiently.

3D displays will enhance how information is viewed. Imagine a soldier who can view the terrain of a battlefield in 3 dimensions.

NFC wireless technology will also change the way the information is collected and disseminated. Version 2.3 of the Android™ operating system includes NFC technology and Google is taking advantage of this in the commercial world by equipping businesses with NFC-compatible window stickers that allow users to touch their phones to the sticker and learn more about the business.

Finally, video recording and playback hardware is expected to advance significantly. Video playback and recording is expected to move from 720P resolution to 1080P resolution. Many devices supporting this will also offer an HDMI out feature that will allow video playback to be output to an external display [INFOWORLD].

9.3 Cloud Computing

Information collection, dissemination, and processing on mobile devices are all moving towards cloud based storage. This is due largely to faster, cheaper, and more reliable data networks available on mobile devices. Cloud based computing is where information is stored or processed on networked online servers rather than local computer systems. Cloud based storage offers mobile users virtually limitless information storage capacity which can also be made available to any mobile user with access to that storage location. Information processing is being performed on cloud based servers as well. Another cloud based development for both mobile devices and computers in general is SaaS, or software as a service. This allows mobile users to use applications from the web rather than having them locally installed, eliminating the need to constantly download updates for applications. Cloud based computing for mobile devices increases the amount of information that can be stored, disseminated and processed [PC].

10.0 Conclusions

Mobile technology is changing the way information can be collected and disseminated. Not limited by geographic location, mobile users have unprecedented access to information. Fueled by immense popularity and government funded initiatives to advance the technology, mobile usage is rising exponentially.

Three primary types of mobile devices currently dominate the mobile information market, iPhone®/iPad®, Android™, and Windows Mobile™. These devices offer tremendous promise if applications are well designed and take advantage of the technology these devices have to offer to the fullest. Future applications should be heterogeneous, operating on a variety of mobile platforms. The open architectures and sophisticated hardware on these devices create ideal conditions for rapid application development and advancement. As a result, new applications are being delivered to users at an increasing rate. The danger in this rapid development is that applications will be developed which do not fully utilize the unique capabilities of mobile devices, making them more traditionally web-like and unable to operate autonomously from the web.

The advancements in mobile technology have attracted many government agencies to integrate mobile technology into their standard operating procedures. Along with adoption of mobile technology, certain considerations must be taken into account, including the use of mobile devices in harsh environments, security of the information collected and disseminated from these devices, and the availability of networks necessary for many mobile applications to function. Innovation needs to create security mechanisms that will protect the unique capabilities of these devices.

With hardware trending toward smaller, faster, more reliable, and longer lasting mobile devices, the migration of information collection and dissemination to mobile technology does not appear to be at risk of slowing down. Instead, the use of mobile technology will continue to grow and change the way in which information is collected, disseminated and processed.

11.0 References

[AGENTS] Susan McGrath, Daria Chacon, Kenneth Whitebread. “Intelligent Mobile Agents in the Military Domain” http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.64.9788

[ANDR] “Android™ Developer Guide” http://developer.Android™.com/guide/index.html

[APP HUB] “App Hub” http://create.msdn.com/en-us/education/quickstarts

[APPLE] “Developer Tools Technology Overview”http://developer.apple.com/technologies/tools/features.html

[ARCH] “Architecture Community” http://architecture.army.mil/technical-view/applications/applications.html

[ARMY] “Connecting Soldiers to Digital Applications”http://www.army.mil/standto/archive/2010/07/15/

[ARMY APPS] “Apps for the Army to Shape Future Software Acquisition”http://www.army.mil/-news/2010/08/05/43293-apps-for-army-to-shape-future-software-acquisition/

[ATRIX] “AT&T” http://www.att.com/

[C4ISR] “Year of the Smart Phone” http://www.c4isrjournal.com/story.php?F=4733634

[COE] “Common Operating Environment” http://ciog6.army.mil/ArmyEnterpriseNetworkVision/tabid/79/Default.aspx

[COIN] “New Smartphone App Provides Data for Counter-Insurgency Intelligence Collection” http://www.mitre.org/news/digest/defense_intelligence/06_10/app.html

[DATA] “Mobile Phones for Data Collection” http://mobileactive.org/howtos/mobile-phones-data-collection

[DHS] “Homeland Security Information Network” http://www.dhs.gov/files/programs/gc_1156888108137.shtm

[DHS ISS] “Department of Homeland Security Information Sharing Strategy http://www.dhs.gov/xlibrary/assets/dhs_information_sharing_strategy.pdf

[DOD] “Pentagon Channel Adds Video Podcasting to Production Line” http://www.defense.gov/releases/release.aspx?releaseid=9441

[DYNAMIC] Ana Paula Afonso, Mario J. Silva. “Dynamic Information Dissemination to Mobile Users” http://www.springerlink.com/content/ggm8783nr7887356/fulltext.pdf

[GARTNER] “Gartner Identifies the Top 10 Consumer Mobile Applications for 2012”http://www.gartner.com/it/page.jsp?id=1230413

[GEO] “Geotagging”
http://en.wikipedia.org/wiki/Geotagging

[GLV] “Glove Science”
http://www.agloves.com/pages/Glove-Science.html

[GFG] “Good for Government”
http://www.good.com/media/pdf/government/Good_for_Govt_Brochure.pdf

[GSN] “DHS information sharing needs streamlining”
http://www.gsnmagazine.com/article/21528/dhs_information_sharing_needs_streamlining

[HSA] “Homeland Security Affairs”
http://www.hsaj.org/?fullarticle=4.1.3

[INFO] Brett van Niekerk and Manoj Maharaj. “Information Security from an Information Warfare Perspective”

[INFOWORLD] “Five Smartphone Hardware Trends in 2011”http://www.infoworld.com/d/mobilize/five-smartphone-hardware-trends-in-2011-196?page=0,1

[M-GOVT] Rain Rannu, Siim Saksing, Triin Mahlakoiv. “Mobile Government: 2010 and Beyond”
http://www.mobisolutions.com/files/Mobile%20Government%202010%20and%20Beyond%20v100.pdf

[MEIER] “Professional Android™ 2 application development”. Indianapolis: Wiley Publishing, Inc.

[NASA] “NASA and DHS Demonstrate Air Sniffing Mobile Phones”
http://www.geek.com/articles/mobile/nasa-and-dhs-demonstrate-air-sniffing-mobile-phones-20091030

[NGEN] “Department of the Navy Next Generation Enterprise Network Requirements Document”
http://www.public.navy.mil/spawar/PEOEIS/NGEN/Documents/NGEN_Requirements_v2_Signing_Draft_4_040808_rel.pdf

[NIST] “Guidelines on Cell Phone and PDA Security”
http://csrc.nist.gov/publications/nistpubs/800-124/SP800-124.pdf

[PC] “6 Noteworthy Mobile Trends: Mobility is Resphaping our Notion of Today’s Worker” http://bestbuybusinessdistrict.com/knowlege-center/91-6-noteworthy-mobile-trends-mobility-is-reshaping-our-notion-of-today%27s-worker

[PHONE 7] “Windows Mobile™” http://en.wikipedia.org/wiki/Windows_Mobile

[PIA] “Privacy Impact Assessment for MyTSA Mobile Application” http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_tsa_mytsa.pdf

[POD] “Podcast” http://en.wikipedia.org/wiki/Podcast

[SAM] “Galaxy S: A New Era in AMOLED Technology” http://www.samsung.com/us/article/galaxy-s-a-new-era-in-amoled-technology

[SCADA] “ScadaMobile User Manual” http://www.sweetwilliamsl.com/sites/default/files/ScadaMobile%20Manual.pdf

[SENS] “A Miniature Chemical Sensor for Mobile Phone Has Been Developed in USA” http://www.articlesbase.com/cell-phones-articles/a-miniature-chemical-sensor-for-mobile-phone-has-been-developed-in-usa-2606295.html

[SPECS] “iPhone® 4 Technical Specifications” http://www.apple.com/iPhone®/specs.html

[SURUR] “Architecture Guide for Windows Phone OS 7.0” http://wmpoweruser.com/leaked-windows-phone-7-architecture-guide-reveal-more-os-info/

[TCH] “Next-Gen iPhone® Displays May Support Touch with Gloves On” http://www.patentlyapple.com/patently-apple/2010/11/next-gen-iPhone®-displays-may-support-touch-with-gloves-on.html

[TOP2012] "Mobile Insight: Ten Consumer Mobile Applications to Watch in 2012," http://www.gartner.com/resId=1471813.

[VCAST] “V Cast” http://en.wikipedia.org/wiki/V_Cast

[WAP] “Introduction to the Wireless Application Protocol” http://www.wirelessdevnet.com/channels/wap/training/wapoverview.html

[WAP2] “Wireless Application Protocol” http://en.wikipedia.org/wiki/Wireless_Application_Protocol

[WHITE] Steve Mansfield-Devine “The promise of whitelisting”, Network Security Volume 2009, Issue 7, July 2009, Pages 4-6

[WIKI] “M-government”
http://en.wikipedia.org/wiki/M-government

[WIN7] Application Platform Overview for Windows Phone
http://msdn.microsoft.com/en-us/library/ff402531(VS.92).aspx

[WTC2004] Sharon S. Dawes, Thomas Birkland, Giri Kumar Tayi, Carrie A. Schneider
“Information, Technology, and Coordination: Lessons from the World Trade Center Response” 2004

Appendix A
Glossary of Terms

AJAX

Stands for Asynchronous JavaScript and XML and is a group of interrelated web development methods used on the client-side to create interactive web applications.

API

A set of rules and specifications that a software program can follow to access and utilize the services and resources provided by another software program

Android™

A mobile operating system originally development Android™, Inc. subsequently purchased by Google. Android™ capabilities ride on a modified version of the Linux operating system.

Capacitive Screen

Consists of an insulator such as glass, coated with a transparent conductor

Cloud Computing

Computation, software, data access, and storage services that do not require user knowledge of the physical location and configuration of the system that delivers the services.

Cookies

A piece of text stored on a user's computer by their web browser used for authentication, storing site preferences, shopping cart contents, the identifier for a server-based session, or anything else that can be accomplished through storing text data

Dalkvic Virtual Machine

Provides a platform-independent programming environment that takes away details of the underlying hardware or operating system and allows a program to execute in the same way on any platform.

Geotagging

The process of adding geographical identification metadata to various media sources such as photographs, video, websites, or SMS messages.

GRPS

A packet-based mobile data service on the 2G and 3G cellular communication systems

GSM

The world’s most widely used cellular network.

HDMI	A compact audio and video interface for transmitting uncompressed digital data.
iOS	Apple's mobile operating system for devices such as the iPhone®, iPad®, and Apple TV.
Jailbreaking	A process that allows devices running Apple's operating to gain root access to unlock all features of the operating system, removing limitations imposed by Apple.
Near-Field Communication	A set of short-range wireless technologies which allow devices to exchange information when in close proximity
SDK	A set of development tools that allows for the creation of applications for a certain software package.
Short Message Service	The text communication component of a phone using standardized communications protocols that allow the exchange of short text messages between mobile devices.
Stream Cipher	A symmetric key cipher where plaintext bits are combined with a pseudorandom cipher bit stream (keystream).
Windows Phone 7	A mobile operating system developed by Microsoft and the successor to the Windows Mobile™ platform.

Appendix B
List of Acronyms

AJAX	Asynchronous JavaScript
AMOLED	Active-Matrix Organic Light-Emitting Diode
API	Application Programming Interface
ARCIC	Army Capabilities Integration Center
ARM	A British Semiconductor Intellectual Property Supply Company
CAC	Common Access Card
CANES	Consolidated Afloat Networks and Enterprise Services
CIO	Chief Information Officer
COE	Common Operating Environment
COIN	Counter-Insurgency Intelligence Collection
COP	Common Operating Picture
CPR	Cardiopulmonary Resuscitation
CSDA	Connecting Soldiers to Digital Applications
CSS	Cascading Style Sheets
DARPA	Defense Advanced Research Agency
DHS	Department of Homeland Security
DMS	Degree-Minute-Second (Map Format)
DoD	Department of Defense
DOM	Document Object Model
DUI	Driving Under the Influence
EDGE	Enhanced Data rates for GSM Evolution
ESN	Electronic Serial Number
FAA	Federal Aviation Administration
FASTCOM	Forward Airborne Secure Transmissions and Communications
FBI	Federal Bureau of Investigation
FM	Frequency Modulation
GB	GigaByte
GL ES	Graphics Library for Embedded Systems
GNOSC	Global Network Operations and Security Center
GPRS	General Packet Radio Service
GPS	Global Positioning System

GPU	Graphical Processing Unit
GSM	Global System for Mobile Communications
HSIN	Homeland Security Information Network
HTTP	Hypertext Transfer Protocol
IB	Interface Builder
IDE	Integrated Development Environment
IPC	InterProcess Communication
JSON	JavaScript Object Notation
LCD	Liquid Crystal Display
LED	Light Emitting Diode
MB	MegaByte
MCEITS	Marine Corps Enterprise Information Technology Services
MCEN	Marine Corps Enterprise Network
MCNOSC	Marine Corps Network Operations and Security Center
MGRS	Military Grid Reference System
MHQ/MOC	Maritime Headquarters with Maritime Operations Center
MIN	Mobile Identification Number
MITSC	Marine Air Ground Task Force (MAGTF) Information Technology Support Center
MMS	Multimedia Messaging Service
NETWARCOM	Naval Network Warfare Command
NFC	Near Field Communication
NGEN	Next Generation Enterprise Network
NIPRNet	Non-classified Internet Protocol Router Network
NITSC	Navy Information Technology Support Center
OS	Operating System
OWASP	Open Web Application Security Project
PDA	Personal Data Assistant
PDF	Portable Document Format
PIN	Personal Identification Number
RAM	Random Access Memory
RATS	Raytheon Android™ Tactical System
RNOSC	Regional Network Operations and Security Center
SDK	Software Development Kit
SIM	Subscriber Identity Module
SIPRNet	Secret Internet Protocol Router Network

SMS	Short Message Service
STEP	Standardized Tactical Entry Point
SVG	Scalable Vector Graphics
TRADOC	Training and Doctrine Command
TSA	Transportation Security Administration
UPC	Universal Product Code
URI	Uniform Resource Identifier
USB	Universal Serial Bus
USMC	United States Marine Corp
USN	United States Navy
VIN	Vehicle Identification Number
WAP	Wireless Application Protocol
WebDAV	Web-based Distributed Authoring and Versioning
WVGA	Wide Video Graphics Array
XHMTL	eXtensible HyperText Markup Language
XML	eXtensible Markup Language
XNA	Xbox New Architecture

Appendix C
Additional Resources

Android™ Developers
http://developer.Android™.com/index.html

Army Mobile
http://www.army.mil/mobile/

Consumer Guide to Wireless Device Security
http://spotlight.getnetwise.org/wireless/wirelessguide.pdf

Device Independence Principles
http://www.w3.org/TR/2003/NOTE-di-princ-20030901/

Delivery Context Overview for Device Independence
http://www.w3.org/TR/di-dco/

DoD Mobile
http://www.defense.gov/mobile/

Gartner
http://www.gartner.com/technology/home.jsp

Government Mobile Apps
http://apps.usa.gov/

Information Dissemination in Mobile Ad-Hoc Geosensor Networks
http://www.geosensor.net/papers/giscience04.pdf

iOS Dev Center
http://developer.apple.com/devcenter/ios/index.action

Navy Mobile Apps
http://www.public.navy.mil/ia/Pages/mobile.aspx

Mobile Device Technology and Trends
http://www.idc.com/research/viewfactsheet.jsp?containerId=IDC_P1600&sectionId=null&elementId=null&pageType=SYNOPSIS

Mobile GIS for Homeland Security
http://www.esri.com/library/whitepapers/pdfs/mobile-gis-for-hls.pdf

The Open Web Application Security Project (OWASP)
http://www.owasp.org/index.php/Main_Page

Widget Packaging and Configuration
http://www.w3.org/TR/widgets/

Windows Phone 7 App Hub
http://create.msdn.com/en-US