Purdue University
Purdue e-Pubs

College of Technology Masters Theses | College of Technology Theses and Projects

12-10-2010

A Field Test of Mobile Phone Shielding Devices

Eric Katz
Purdue University - Main Campus, ekatz@purdue.edu

Follow this and additional works at: http://docs.lib.purdue.edu/techmasters

Katz, Eric, "A Field Test of Mobile Phone Shielding Devices" (2010). *College of Technology Masters Theses.* Paper 33.
http://docs.lib.purdue.edu/techmasters/33

This document has been made available through Purdue e-Pubs, a service of the Purdue University Libraries. Please contact epubs@purdue.edu for additional information.

Graduate School ETD Form 9
(Revised 12/07)

PURDUE UNIVERSITY
GRADUATE SCHOOL
Thesis/Dissertation Acceptance

This is to certify that the thesis/dissertation prepared

By Eric Katz

Entitled
A Field Test of Mobile Phone Shielding Device

For the degree of Master of Science

Is approved by the final examining committee:

Richard Mislan
Chair

Marcus Rogers

Anthony Smith

To the best of my knowledge and as understood by the student in the *Research Integrity and Copyright Disclaimer (Graduate School Form 20)*, this thesis/dissertation adheres to the provisions of Purdue University's "Policy on Integrity in Research" and the use of copyrighted material.

Approved by Major Professor(s): Richard Mislan

Approved by: Gary Bertoline 12/9/2010
Head of the Graduate Program Date

Graduate School Form 20
(Revised 9/10)

PURDUE UNIVERSITY
GRADUATE SCHOOL

Research Integrity and Copyright Disclaimer

Title of Thesis/Dissertation:

A Field Test of Mobile Phone Shielding Devices

For the degree of Master of Science

I certify that in the preparation of this thesis, I have observed the provisions of *Purdue University Executive Memorandum No. C-22,* September 6, 1991, *Policy on Integrity in Research.**

Further, I certify that this work is free of plagiarism and all materials appearing in this thesis/dissertation have been properly quoted and attributed.

I certify that all copyrighted material incorporated into this thesis/dissertation is in compliance with the United States' copyright law and that I have received written permission from the copyright owners for my use of their work, which is beyond the scope of the law. I agree to indemnify and save harmless Purdue University from any and all claims that may be asserted or that may arise from any copyright violation.

Eric Katz

Printed Name and Signature of Candidate

12/9/2010

Date (month/day/year)

*Located at http://www.purdue.edu/policies/pages/teach_res_outreach/c_22.html

A FIELD TEST OF MOBILE PHONE SHIELDING DEVICES

A Thesis

Submitted to the Faculty

of

Purdue University

by

Eric Katz

In Partial Fulfillment of the

Requirements for the Degree

of

Master of Science

December 2010

Purdue University

West Lafayette, Indiana

To my mom and dad who encouraged and supported me through thick and thin. Providing me guidance, wisdom and patience when needed. Please continue to do so as I continue on my path.

ACKNOWLEDGEMENTS

This research would not have been possible without the support and guidance of my committee members: Professor Rick Mislan (chair), Dr. Marc Rogers, and Professor Tony Smith. My research team helping me in the field made these experiments possible. Evan Albersmeyer, Kelly Cole, Kyle Johansen, Matt Schweikert, and Parker Woods, your help was and is greatly appreciated, thank you. Dustin Hillman and Natalie Katz, thank you for peer reviewing and revising my thesis multiple times.

TABLE OF CONTENTS

Page
LIST OF FIGURES vi

LIST OF TABLES ……..viii

ABSTRACT ……..……..x

CHAPTER 1: INTRODUCTION ……...……1

1.1 Statement of the Problem …….……2

1.2 Significance of the Problem ……...……3

1.3 Statement of Purpose ……4

1.4 Definitions …….……..….4

1.5 Assumptions ……..……7

1.6 Delimitations ……..…….……..8

1.7 Limitations ……...…….9

CHAPTER 2: REVIEW OF THE LITERATURE …….……..10

2.1 Significant Evidence ……...10

2.2 The Need for RF Isolation ……..17

2.3 Signal Theory ……..23

2.4 Faraday Cages ……30

2.5 Shielding Issues ……..32

Page

2.6 Preservation Tools ……..35

CHAPTER 3: METHODOLOGY …..……40

3.1 Devices to be Used ……40

3.2 Method ……...……42

3.3 Hypothesis ……..……44

CHAPTER 4: FINDINGS ……..…...…….……..45

4.1 eDEC's Black Hole Bag ……...……..47

4.2 LessEMF High Performance Silver Mesh ……..50

4.3 MWT Materials' Wireless Isolation Bag ……50

4.4 Paraben's StrongHold Bag ……..51

4.5 Ramsey STP1100 ……..……..53

4.6 Ramsey STP360 ….……..……..54

4.7 Distance ……...55

CHAPTER 5: CONCLUSIONS AND DISCUSSION …….……..…….....59

5.1 Call Penetration ……...60

5.2 Legal Implications …...……...61

5.3 Scientific Implications ……...……64

5.4 Improving Shielding Devices ……...……..67

5.5 Closing Remarks ……70

LIST OF REFERENCES ……..……...……72

APPENDIX ……..……77

LIST OF FIGURES

Figure Page
Figure 2.1 Number of Text Messages Sent 12

Figure 2.2 TDMA and CDMA ……...…….…….26

Figure 2.3 Wave Refraction ……...…….……...……..27

Figure 2.4 Wave Reflection ……..……28

Figure 2.5 Wave Scattering ……..…….28

Figure 2.6 Wave Diffraction …...…….…….29

Figure 2.7 Antenna Propagation ……...30

Figure 2.8 How Faraday Cages Work …….……...31

Figure 2.9 Paraben Shielding Effectiveness Chart ..…….36

Figure 2.10 Effectiveness of the Black Hole Bag …..……..…….38

Figure 2.11 BK Forensics' Magic Mesh Effectiveness …….……...39

Figure 4.1 SMS Tests Across all Shielding Devices ……46

Figure 4.2 Voice Call Tests Across all Shielding Devices ……...……46

Figure 4.3 MMS Tests Across all Shielding Devices ……...……...47

Figure 4.4 Black Hole Bag – Combined Results ……..……48

Figure 4.5 Black Hole Bag – Base of the Towers ……...…….49

Figure 4.6 Black Hole Bag – 500' From the Towers ……49

Figure 4.7 LessEMF High Performance Silver Mesh – Combined Results …….50

Figure Page

Figure 4.8 MWT Materials' Wireless Isolation Bag – Combined Results ……...51

Figure 4.9 Paraben's StrongHold Bag – Combined Results ……52

Figure 4.10 Paraben's StrongHold Bag – Base of the Towers ……53

Figure 4.11 Paraben's StrongHold Bag – 500' From the Towers ……53

Figure 4.12 Ramsey STP1100 – Combined Results ……54

Figure 4.13 Total Voice Calls Failed Over All Distances ……56

Figure 4.14 Total MMS Messages Failed Over All Distances ……56

Figure 4.15 Total SMS Messages Failed Over All Distances ……..…57

Figure 5.1 Total Pass Fail Rates ……...60

Figure 5.2 Sprint Tower Near I-65 … ……..62

Figure 5.3 AT&T Tower Near Purdue ….. ……...62

LIST OF TABLES

Table Page
Table 2.1 Ramsey 4500Z Effectiveness ….....37

Table 3.1 Phones Used During the Experiments ……..…41

Table A-1.1 eDEC Black Hole Bag - Base of the Tower ……..……...77

Table A-1.2 eDEC Black Hole Bag- 100' ……..…...78

Table A-1.3 eDEC Black Hole Bag – 150’ ……...79

Table A-1.4 eDEC Black Hole Bag – 200’ ……...80

Table A-1.5 eDEC Black Hole Bag -500’ ……...81

Table A-2.1 LessEMF High Performance Silver Mesh – Base of the Tower ……..82

Table A-2.2 LessEMF High Performance Silver Mesh – 100’ ……..……..83

Table A-2.3 LessEMF High Performance Silver Mesh – 150’ ……....84

Table A-2.4 LessEMF High Performance Silver Mesh – 200’ …….……...85

Table A-2.5 LessEMF High Performance Silver Mesh – 500’ ……...86

Table A-3.1 MWT Material Wireless Isolation Bag – Base of the Tower ……...87

Table A-3.2 MWT Material Wireless Isolation Bag – 100’ …..……...88

Table A-3.3 MWT Material Wireless Isolation Bag – 150’ ..……...89

Table A-3.4 MWT Material Wireless Isolation Bag – 200’ ……..……...90

Table A-3.5 MWT Material Wireless Isolation Bag – 500’ ..……...91

Table page

Table A-4.1 Paraben StrongHold Bag – Base of the Tower ..……...92

Table A-4.2 Paraben StrongHold Bag – 100’ ……...93

Table A-4.3 Paraben StrongHold Bag – 150’ ……...94

Table A-4.4 Paraben StrongHold Bag – 200’ ……...95

Table A-4.5 Paraben StrongHold Bag – 500’ ……...96

Table A-5.1 Ramsey STE3600 – Base of the Tower …….……...97

Table A-5.2 Ramsey STE3600 – 100’ ...……...98

Table A-5.3 Ramsey STE3600 – 150’ ...……...99

Table A-5.4 Ramsey STE3600 – 200’ ……...…….100

Table A-5.5 Ramsey STE3600 – 500’ ..…….……101

Table A-6.1 Ramsey STP1100 – Base of the Tower …….……102

Table A-6.2 Ramsey STP1100 – 100’ …...……103

Table A-6.3 Ramsey STP1100 – 150’ ...……104

Table A-6.4 Ramsey STP1100 – 200’ ……...……105

Table A-6.5 Ramsey STP1100 – 500’ ……...……106

ABSTRACT

Katz, Eric. M.S., Purdue University, December, 2010. A Field Test of Mobile Phone Shielding Devices. Major Professor: Richard P. Mislan.

Mobile phones are increasingly a source of evidence in criminal investigations. The evidence on a phone is volatile and can easily be overwritten or deleted. There are many tools that claim to radio isolate a phone in order to preserve evidence. Unfortunately the wireless preservation devices do not always successfully prevent network communication as promised. The purpose of this study was to identify situations where the devices used to protect evidence on mobile phones can fail. There has been little published research on how well these devices work in the field despite the escalating importance of mobile phone forensics. These shielding devices were tested using mobile phones from three of the largest services providers in the U.S. Calls were made to contact the isolated phones using voice, SMS, and MMS at varying distances from the provider's towers. In the majority of the test cases the phones were not isolated from their networks despite being enclosed in a shielding device. It was found that SMS calls penetrated the shields the most often. Voice calls were the next most likely to penetrate the shields and MMS were the least.

CHAPTER 1: INTRODUCTION

Mobile phones have penetrated our society like few other technologies have. These phones are storing ever-increasing amounts of information about their owners. It is no surprise that mobile phones are now commonly seized as a source of evidence during an investigation. Unfortunately the evidence on a phone is volatile and can easily be overwritten or deleted. Vendors claim that their products can radio isolate a phone in order to preserve the evidence stored on it. Regrettably this may not always be true.

There can be an incredible amount of information stored on a mobile phone. When a crime is committed evidence may often be found on a phone if an investigator can find it. This evidence can take many forms such as call histories, contact lists, text messages, and multimedia. There are also several ways of deleting this data even if the phone has already been seized. Incoming calls and data packets can overwrite stored information and there are even some packets that can cause a phone to delete some or all information stored on it.

To protect evidence on a mobile phone it must be isolated from its network. As long as the signal is attenuated enough, communication will be prevented and the evidence preserved. One of the he most common method of attenuating radio signal is to use a device that will shield the phone from radio waves (Scientific Working Group on Digital Evidence, 2009). These devices function like a Faraday cage but do not truly

block all radio signals. Some signal can still penetrate the shield providing a chance for the shielding device to fail.

The purpose of this research was to test multiple shielding devices in order to points of failure where the phone is not isolated. This testing is necessary because if the devices can fail to protect evidence it needs to be known before being relied upon during an investigation. Phones from three of the largest providers in the United States were tested at varying distances from cellular towers. The results will show where different shields can potentially fail. Proof that the shielding device can fail is the first step to fixing the problem.

1. 1 Statement of the Problem

Wireless preservation devices do not always successfully prevent network communication to a mobile phone as the vendors promised. The purpose of these devices is to protect evidence on a mobile phone from being deleted or changed. When the shields fail, it can mean that valuable evidence can be lost and the remaining evidence admissibility called into question. According to Emil De Toffol, president of LessEMF, a firm that manufactures many of the materials used in wireless preservation equipment, there are three reasons why shielding may fail. They are: (De Toffol, 2009)

- The material doesn't provide enough attenuation
- Leaks or seams in the shield allow signal through
- The conductive shield is too close to the phone and acts like an antenna

If the shielding device can fail then it must be known under what circumstances this can happen. It is important to know what and where the limitations of the equipment are before they are used in the field.

1.2 Significance of the Problem

Within the past 10 years mobile phone use has skyrocketed. From 2005 to 2009, the number of wireless subscribers has jumped from 194.4 million to 276.6 million (CTIA, 2009). In 2006, nearly a billion mobile phones were sold worldwide and the number continues to rise (Jansen, Delaitre, & Moenner, 2008). Mobile phones are so common that in the United States roughly 89% of the population has at least one of them (CTIA, 2009). Mobile phones store more data about their users than ever before and addressing mobile phones as a source of evidence is becoming increasingly important.

Depending on the type of mobile phone, there is a potential wealth of information stored on a mobile phone that can be evidence once a crime has been committed. Information that is most commonly gathered from mobile phones include; the contact list, call history, and text messages. These three items are stored on almost every mobile phone and provide valuable information about the phone's user. Given the personal nature of this information, it is no wonder that acquisition of the evidence can lead and investigator to the next suspect or victim (Mislan, Casey, & Kessler, 2010). Other items of interest include the Location Information (LOCI), Global Positioning System (GPS) data, pictures, videos, Internet browser history, and a myriad of application and personal data (Lesemann & Mahalik, 2008). All of this potential evidence needs to be protected when a phone is seized so that it can be properly analyzed later.

The National Institute for Standards and Technology (NIST) published guidelines for how a mobile phone investigation should be conducted. NIST recommends that phones be isolated from the radio network to keep new traffic from overwriting existing data (Jansen & Ayers, 2007). Interpol and the Association of Chief Police Officers (ACPO) also recommend radio frequency isolation to protect evidence on a mobile phone as part of their first principle of seizing digital evidence (Interpol European Working Party on IT Crime, 2006).

With all the potential evidence available on mobile phones it is no surprise how much importance is placed on isolating mobile phones in order to preserve the evidence found on them. However, all the proper intentions and efforts are for naught if the devices being relied upon have unknown failures that might allow the evidence to be changed. It is for this reason that the tools must be tested and validated.

1.3 Statement of Purpose

There are a myriad of conditions in which shielding devices can be used that will cause them to fail. For this research the devices will be used appropriately and vendor instructions will be followed when applicable. This research tested several of the shielding devices that are currently available to investigators for use with mobile phones. The experiment determined if distance from a tower, the type of information being transmitted, and the network being used effect the isolation capabilities of the shielding devices. The success or failure of the shield to isolate the phone was recorded. This will allow users of the devices to know where they can expect faults to occur. For researchers and manufacturers the results will also provide insight into where and how improvements can be made into RF shielding tools.

1.4 Definitions

BlackBerry Enterprise Server (BES): A software administration suite from RIM that allows an administrator to manage multiple phones

Code Division Multiple Access (CDMA): A method for dividing bandwidth into segments in order to allow multiple signals to be broadcast on a carrier channel. Sprint and Verizon are the largest NSPs in the U.S. that utilizes CDMA.

Decibel (dB): A dimensionless ratio unit used to measure the signal strength in mobile phones from a predetermined reference point.

Exchangeable Image File Format (EXIF): metadata embedded in a photograph when the picture is taken that contains information that can be used to distinguish when, where, and what took the picture.

Faraday Cage: An enclosure developed by scientist Michael Faraday that can be used to spread incoming electrical signals out over its outer shell while signals that originate from the inside are spread across the interior. This in effect electrically isolates any device inside it from the outside world.

Global Positioning System (GPS): A series of computers and satellites designed to determine the latitude and longitude of a receiver on Earth.

Global System for Mobile Communications (GSM): Standard for mobile telephone systems. It originated in Europe and is the most common standard worldwide for mobile phones. GSM makes use of SIM cards to identify devices on the network. AT&T and T-Mobile are the largest NSP providers in the U.S. that operates with GSM.

Isolation: Normally meaning a device is unable to recieve any source of radio communication. When used in this paper it means that a mobile phone has been placed in a shielding device that attenuates RF signal enough to prevent any meaningful communication on the network.

Location Area Information (LAI): A list generated by some mobile phones to store recently used towers in order to increase communication efficiency

Location Information (LOCI): Unique codes that identify which tower a mobile phone was last using. This information is updated as the phone communicates with new towers.

Multimedia Message Service (MMS): A standard way to transmit messages that include multimedia content to and from mobile phones

Multipath Propagation: The combined effects of diffraction, reflection, and scattering causing a mobile phone to receive multiple versions of the same signal at different times which creates noise on the primary channel.

Network Service Provider (NSP): The company that provides communication service to a mobile phone.

Personal Identification Number (PIN): A 4 to 8 digit code that can be user enabled to lock a SIM card and prevent a phone from functioning until entered

Sexting: A recent phenomena where people are sending semi to fully nude pictures of themselves to others via MMS.

Short Message Service (SMS): A protocol used to transmit text messages to and from mobile phones

Shielding device: A tool designed to act as a Faraday cage and isolate a mobile phone from its network

Signal-to-noise Ratio (SNR): The amount of interference in a communication channel compared to the strength of signal. The higher the SNR, the fewer errors will occur.

Time Division Multiple Access (TDMA): A method of dividing bandwidth into time segments to allow for multiple users on the same signal. GSM networks use TDMA

Trophy Photo: A picture that is taken to prove the accomplishment of an action. Often taken during or following the commencement of a crime, these photographs provide valuable evidence towards a case.

1.5 Assumptions

It is assumed that the shielding devices will function as they are specified by their vendors and will block RF signal at the dB levels they specify. This does not mean that the device will block enough RF signal all of the time to successfully isolate a mobile phone.

The towers chosen are another point of assumption. Without expensive equipment to measure the output of the tower's transmission, its exact wattage is unknowable. Macro towers along highways are most likely to have the maximum wattage the Network Service Provider (NSP) will generate. This will give the phones the best reception possible and will be used in the experiment.

1.6 Delimitations

There are several means to preserve evidence on a mobile phone from the network besides using a shielding device. The most common are: radio jamming, enabling airplane mode, and simply turning the phone off. All of these solutions have their own benefits and problems. In many countries, radio-jamming devices are illegal and may interfere with coverage outside of the examination area (Interpol European Working Party on IT Crime, 2006). Not every phone can enter airplane mode and all of them use different methods to enable it. Without previous knowledge of the phone it may be impossible for an officer to properly enable airplane mode. Turning the phone off can enable handset lock codes and Personal Identification Numbers (PIN) locks that prevent any further analysis. A comparison of one of these methods over any of the others was not examined in this experiment.

The 3G capabilities of each phone and the shielding devices' abilities to prevent that type of communication were also not examined in this study. Most of the phones that were tested are capable of utilizing 3G networks and the higher frequencies associated with them to stream data. While it is possible to test the if the shields can isolate a 3G stream, for this research study it was considered more important to examine incoming calls and whether or not they were capable of penetrating the shields. Interrupting a stream during download or upload will still leave evidence of the file on the phone. However, incoming calls can change evidence or even zero out the memory of a phone and are therefore the most destructive communications and have priority for testing. No testing will be done on the current 4G labeled networks either for the same reason. It is also impossible to get the exact transmission level of a tower without specialized and

calibrated equipment. The purchasing of and training for this equipment is beyond the scope of this research.

1.7 Limitations

There are several limitations that must be dealt with when conducting this experiment. There are many devices available that can be used as shielding devices. Some of these devices are more common than others and some are cost prohibitive. Only a few of the shielding devices manufactured today will be examined in this research. These will be chosen based on availability and cost.

There are also many phones with different antennas and capabilities. It is possible that the form factors of the phone itself and of the shielding tool will affect how well the shield can isolate the mobile phone. Form factor such as: candy bar, clamshell, antenna design, and touch screen interface can all alter how well a particular shielding tool will work. The more phones examined the more a particular design difference can be found. The number and type of mobile phones to be examined will be limited by cost and availability. This is due to availability and cost of phones. When possible the same phone models will be used for different carriers. This will show if various signaling or provider differences impact the shielding tool's effectiveness.

There are also too many different forms of information that can be stored on a mobile phone to try them all in one study. For this experiment the information that was examined are incoming phone calls, text messages, and multimedia messages. These are especially important because if the phone receives more calls while it's supposed to be protected inside a shielding tool the call history may be deleted or worse, a remote wipe could be activated.

CHAPTER 2: REVIEW OF THE LITERATURE

The review of literature for this research focused on four different primary areas: types of evidence and their significance, signal theory, how RF isolation functions, and the current tools and market claims. When combined, all of the topics show that mobile phones need to be isolated from the network to protect evidence. Vendors will always claim that their product is the best possible solution and will always work. This is because it affects the vendor's bottom line and they are selling a product to make money. Due diligence requires that the shielding devices used to isolate a phone must be tested to ensure that they work as claimed.

2.1 Significant Evidence

There are several items on a mobile phone that could potentially be used as evidence examples include: call logs, email pictures, documents, and videos (Lesemann & Mahalik, 2008). The gaining popularity of the smart phone is increasing this factor of digital evidence almost exponentially. The types of evidence that will be examined here are considered volatile. This means the evidence can be deleted by remote signals sent to the phone. This section is by no means a comprehensive list of the types of volatile evidence that can be located on a phone nor is it a complete list of evidentiary items that need to be looked for when examining a mobile phone. These are some examples of the

forms of evidence that can be lost if the shielding device used to attenuate the RF signals being sent and received by a phone isn't successfully isolating the phone.

One of the many items of potential evidence considered when investigating a mobile phone is the recent call history and contact list. The call history is a list of all the incoming and outgoing calls the phone has recently received or placed. Depending on the model of phone, the call history can only contain so many items before the older numbers start to be overwritten. Any phone calls that come to a mobile phone after it has been taken into evidence can potentially erase the fact that a number was on the call history list. This is especially true with non-smart phones. Smart phones have more memory available to them and can keep this information longer, but may not display older information to the user without forensic recovery. Knowing who is calling whom can prove or disprove alibis and so the call history must be protected and preserved.

The contact list is also an important feature of a cell phone. The contact list can maintain many names, numbers, physical addresses, and email addresses among other things. These can also be used to determine who the phone's owner knows and how they know them. Often pictures on the phone are associated with names on the list allowing for a visual confirmation of who is being identified. When dealing with multiple suspects and victims the call history and contact lists on mobile phones may be the evidence needed to tie everyone together.

Another widely used function on mobile phones is the Short Message Service (SMS) or text messaging. Text messaging has seen a rapid rise in popularity and the number of text messages has increased to 75 billion per month in the US alone as seen in Figure 2.1 (CellSigns Inc., 2010). People often send text messages that contain

information corresponding to what they have been doing with whom and where they were. For example former Detroit mayor Kwame Kilpatrick resigned because of text messages that were sent to a city owned pager and recovered by the press (Lesemann & Mahalik, 2008). These text messages were used to prove that he was having an affair with one of his aides.

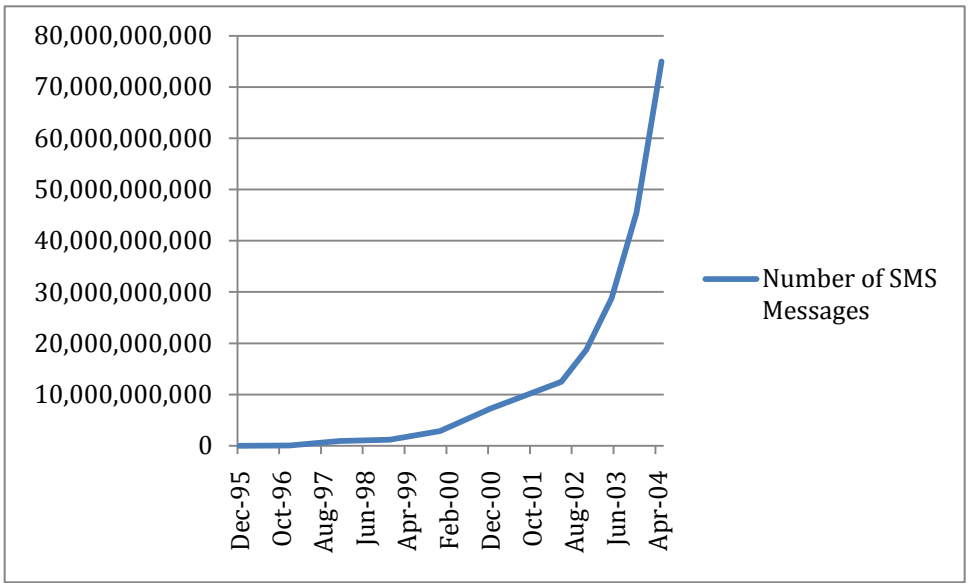


Figure 2.1 Number of Text Messages Sent (Data compiled from CTIA)

Another set of popular functions includes picture phones and the Multimedia Messaging Service (MMS), which is used to send picture mail or other files. Pictures and video taken on camera phones are very useful evidence. As mentioned earlier, it is not uncommon to find photographs of people in the phones contact list on the phone.

It is also not uncommon to see trophy photos and videos on a phone. These trophy shots are often sent to other people as bragging rights or proof that a crime has been committed. An example of a trophy video being used in prosecuting a case is from July of 2007 when a football player from the University of Minnesota was charged with sexual assault after a video was found of him having sex with an unconscious woman

(Lesemann & Mahalik, 2008). Videos of crimes being committed are appearing on web sites, such as YouTube, more and more frequently. In one instance a group of six girls and 2 boys brutally beat another teenager specifically to post the video online (Phillips, 2008).

Another form of MMS that has received a lot of attention in the news media lately is sexting. Sexting is a recent phenomena where people combine sexual text messages and use their camera phones to send nude or semi-nude photos of themselves. Current studies show as many as 20% of teenagers and 33% of young adults in the U.S. have sexted (The National Campaign to Prevent Teen Pregnancy, 2008).

Self-portraits are not the only pictures that can be sent. It is possible for child pornographers to produce, store, and trade their collections via their mobile phones. Any device that can store or send pictures is being used to facilitate the trading and viewing of child pornography. Trophy photos of the victims of violent crimes or suspects posing with the illicit goods are commonly found on mobile phones.

The people and scenes in these videos and photographs can provide more evidence than just who was doing what. They can provide clues as to how crimes were committed, what tools were used, where they were, and Exchangeable Image File Format (EXIF) data. EXIF information is metadata created when a picture is taken that can be used to uniquely identify which camera took the photo (JEITA, 2002). EXIF data can contain information on the model of the camera used to take the picture, the time and date it was taken, GPS data, and more.

GPS has also become a popular feature on mobile phones. Not only is this information recorded when photographs are taken but it is constantly being updated by

the phones that can use it. This means that the mobile phones are recording where their user is carrying them. This information is used for all sorts of purposes including real time directions and geo tagging. Some smart phones allow for this functionality to be toggled on and off by the user and can take advantage of it by providing turn for turn directions and mapping. Because GPS information is constantly being recorded by the phone when it is on it also provides a means of tracking cell phone users as they go about their day. To prevent this, most phones do not allow the user to access to the GPS information directly (Adomatis, 2010). This information can be accessed only emergency services after a 911 call is placed or search warrant issued (Adomatis, 2010).

GPS is just the newest of the Location Information (LOCI) that can be found on a mobile phone. As mobile phones are moved around they continue to adjust and attempt to connect to the tower with the strongest signal. The unique designation of this tower is stored as a database entry on the phone (Lewis, 2009). This information can be very useful in an investigation, however, if the phone is not shielded this information will be updated even as the phone is being transported back to the lab (Dankner & Gupta, 2007). This data is very sensitive and any communication between the phone and a tower will cause it to update before the user even knows the signal is getting through. If the phone is placed in a Faraday shield often this data is zeroed out as the phone fails to find any towers to communicate with (Dankner & Gupta, 2007).

The introduction of the Internet to mobile phones allows for a myriad of new possible evidence to be found on a mobile phone. This includes web browsing, downloads, email, and much more. The browsing history of a user has long been a virtual treasure trove of evidence in traditional computer forensics.

Knowing which websites a user is viewing can go a long way to establishing motive and intent. It can also tie many circumstantial clues together to form a more complete picture. Criminals such as Phillip Markoff, the alleged Craigslist Killer, used online communities to find and arrange to meet his victims (McPhee, Schabner, & Battiste, 2010). Browser history can also show that the user has been searching for websites to provide instructions on how to commit or cover up a crime. Often the browsing history can often include proof that the suspect has recently purchased or sold the tools used to commit a crime. The Lee murder investigation, a case from the Lafayette Police Department (Indiana), made extensive use of the browser history. There were searches for the murder weapon (pistol), maps to the seller's home, and searches for the dB level of the gun, trains, and garbage trucks (Huff, P. personal communication, June 2, 2010). It doesn't take much imagination to see how these tie together. Included with Internet browsing are cache folders and files that contain pictures and other images that have been downloaded automatically. These images often contain contraband or further evidence of the suspect's activities. The iPhone will even take screenshots of what the user was looking at whenever the home button is hit providing images of exactly what the user was seeing (Zdziarski, 2010).

Email has been an important source of digital evidence since its inception. It is estimated that nearly 2.5 trillion emails are exchanged yearly (M. Rogers, 2009). Many people will send information in an email that they never expect anyone else to examine. Emails have been used to prove cases such as the *1999 U.S. v. Microsoft Corporation* and the 2001 Enron scandal. In these cases emails showed that people knowingly took actions that were illegal. Due to the importance of email evidence, Enron's entire

database is now publicly available for research. These same emails can be sent and received from mobile phones and are potentially paramount to proving a case. This can make the phone the only source of evidence available. If these emails are deleted from the mobile phone for any reason it may be impossible to recover them.

Smart phones such as the Android phones, BlackBerry, and iPhones are capable of installing applications that provide new functionality to the phones. Internet access grants users nearly the same capabilities they would have on a PC or laptop. As more programmers and companies design programs and tools for mobile phones, more and more information can become potential evidence that needs to be preserved. Depending on the programs that are installed information the type and amount of information available will vary wildly.

Many of these applications combine previously mentioned functions to create new and useful tools. Programs such as WhosHere combine GPS with social networking and Internet access to identify where users are and notifies them when other users are nearby. Locimobile provides tools for Android and iPhone users that allow them to enter their contact lists and track where the people they know are. Facebook and Foursquare, popular social networking websites now have mobile applications to allow users to check in and post their current locations. It is easy to see where programs such as these can be abused for stalking and child predator incidents. The data stored on the phone can be used to show where the user has been and whom they are finding. Applications like those previously mentioned also may have information stored on the application provider's servers. Subpoena and search warrants will most likely be needed to get this information from the company.

All of these forms of evidence and more can exist available on a mobile phone and are can be at risk as long as the phone can communicate with its network. In order to preserve this evidence for examination and analysis the phone must be isolated from any network it can communicate with. In the United States and many other countries, isolation methods that involve RF jamming are illegal. This makes signal attenuation one of the best methods available for isolating a mobile phone.

2.2 The Need for RF Isolation

The amount of potential evidence stored on mobile phones increases with every generation of phone. According to the Scientific Working Group on Digital Evidence (SWGDE) "new families of mobile phones are typically manufactured every 3 to 6 months (Scientific Working Group on Digital Evidence, 2009)." With every new phone exists the possibility for new evidence. Preserving the data on a mobile phone can be extremely important to solving a case. Once information is deleted from a mobile phone it is difficult if not impossible to recover it by traditional forensic means. Preservation is also needed in order to protect the evidences admissibility in court. Court rulings and published guidelines from Interpol and the Scientific Working Group on Digital Evidence exist that suggest mobile phones should be isolated from the networks in order to protect evidence.

There are a handful of ways to remotely wipe information stored on a mobile phone (Scientific Working Group on Digital Evidence, 2009). Like computers, once the data on a phone has been overwritten or zeroed out it can't be recovered. Unlike traditional computer forensics it is often difficult to acquire a physical image for a mobile phone making data carving and other means of recovering deleted information unlikely.

There is also no standard method of analysis for cell phones (Willassen, 2005). This is why preserving the evidence on a mobile phone is of paramount importance.

In talks with police investigators they have reported instances where a phone known to be in custody has received numerous calls and text messages. Unfortunately many mobile phones will only display a limited number of text messages at any given time. Some of these phones will store a limited number of texts and calls in its logs before they start to overwrite some of the older ones. Smart phones that have access to more memory use databases to store these histories for as long as possible. Placing calls to a smart phone won't necessarily overwrite the previous information in the database but the phone may not display it anymore. If the database can be recovered from the phone it may be possible to see the entire call history for the lifespan of the phone. There are programs such as Textspammer that can be used to flood a phone with SMS messages. Given enough messages a phone's entire SMS history can be overwritten and all the evidence and information in the messages lost.

Research in Motion (RIM) offers a software suite called the BlackBerry Enterprise Server (BES) that can be used to administrate multiple phones and accounts. There is a security tool in the BES that allows the administrator to impose a device lock down or a remote wipe of the phone (Research in Motion, 2010). This tool was designed to protect sensitive or private data from being stolen or lost. Criminals can also use the BES to purge evidence from a phone after it has been seized. Issuing the Erase Data and Disable Handheld command from the BES overwrites, not just deletes, the entire memory area of the phone with zeroes (Punja & Mislan, 2008). Isolating the phone from any incoming signals is the only way to prevent this command from occurring and ruining the

evidence that may be on it. The phone is susceptible to these commands as long as it can communicate with the NSP. The sooner the phone is isolated the more securely stored the evidence on it will be. It is important to note that removing the phone from isolation will allow it to start communicating again and it will receive any commands that have been queued by the NSP, including the remote wipe.

Blackberry smart phones are not the only phones that have remote wiping functionality. A highly advanced smart phone now seen as a status symbol, the iPhone from Apple is gaining in market share. Apple's current catch phrase is "There is an App for that" and they aren't wrong about it from a remote wiping stance. Part of the MobileMe! functionality allows for remotely reformatting the phone. This tool isn't as effective as the BES remote wipe function because it is possible to interrupt it by shutting off the phone and removing the SIM.

Remote deletion is not the only security feature that can be used to halt an investigation. There are also apps such as LockMe and OmaiProtect that can send a signal to a mobile phone to enable the handset lock (Jansen & Ayers, 2007). Once the phone's lock is engaged, the data on the phone cannot be accessed until the code is properly entered. Incorrectly entering these codes can cause the phone to permanently lock, completely deny access, or reformat itself. Another means of crippling an investigation is to intentionally send malformed packets to specific mobile phones. This can cripple the phone much like the "ping of death" was used to disable computers on a network (Leyden, 2001).

Some applications can also be installed on a phone that will zero all the data on the phone out. Jonathan Zdziarski, the developer of one of the most popular iPhone

forensics techniques, had a program called iWipe available on the iPhone app store. This tool was intended as a privacy and security program. According to Zdziarski, he has since removed this program from the app store after hearing that a suspect used it to wipe his iPhone. This is just one example of many different programs that exist to delete information from a phone. While these tools are not intended for use by criminals to hamper an investigation, they can easily be adapted to do so. Once they are used, any evidence that existed is gone and cannot be recovered, proving it is important for preservation tools to work.

Any of these situations could represent a breach in the chain of custody once evidence has been seized. Not only would information be damaged, but it is possible that any remaining evidence would be inadmissible in court. Any new data that the phone receives while in custody may not be within the scope of the original search warrant (Jansen & Ayers, 2007). In order to prevent this and to protect the evidence on a phone many organizations, such as NIST, INTERPOL, and SWGDE all recommend the isolation of the phone from any signals as soon as it is seized.

Several major national and international organizations have published guidelines about how and why mobile phones should be isolated. While not a regulatory agency, organizations like NIST spend a great deal of time researching and developing their recommendations. To prevent data from being overwritten and to prevent add-on programs from remotely locking phones, NIST recommends that a mobile phone be isolated from its radio network (Jansen & Ayers, 2007). The Scientific Working Group on Digital Evidence (SWGDE) also recommends the isolation of a phone from radio networks. Upon seizure SWGDE recommends turning the phone off completely or

isolating the phone while maintaining power (Scientific Working Group on Digital Evidence, 2009). SWGDE also reports that turning off the phone can initiate lock out codes and other security features when the phone is tuned back on. During the examination and analysis of the phone, SWGDE also recommends maintaining radio isolation the entire time. Similarly Interpol also recommends using radio isolation to protect evidence on a mobile phone. All of these major organizations have independently come to the conclusion that phones must maintain radio isolation while in custody.

There are still numerous undecided issues facing the court system in the United States when dealing with proper search and seizure of mobile phones. The U.S. Supreme Court has made very few rulings when dealing with mobile phones and their search and seizure. Depending on the state or even the county an investigation is occurring in, there are different requirements for being able to search a phone.

U.S. v. Parada (2003) concluded that because exigent circumstances exist, such as the possible destruction of evidence, mobile phones can be examined incident to arrest (Marcinkoski, 2008). This is one of the first cases that recognized the importance of protecting evidence found on a mobile phone. Once the officer has reason to believe that the phone contains evidence, proper measures should be used to ensure that no changes to the phone occur. The phone can then be brought back to the lab for a more thorough examination. In *United States v. Finley* (2007) it was determined that mobile phones can be searched incident to an arrest because an officer is allowed to look for evidence of a crime (Marcinkoski, 2008). Most law enforcement officers today do not have the proper training to forensically examine a mobile phone on scene. This means the evidence on the phone needs to be preserved so it can be taken to a lab for proper examination.

In *U.S. v. Windrix* (2005) it was determined a search warrant allowing the police to look for evidence of drug distribution also included searching mobile phones of the suspect (Marcinkoski, 2008). The *U.S. v. Gamboa* (2006) stated that a mobile phone itself can be contraband because it can contain records used in the purchase and selling of controlled substances (Marcinkoski, 2008). The *U.S. v. Diaz* (2007) said the search and seizure of mobile phones is allowed when consent to search a house is given and evidence related to the crime could be found on the phone (Marcinkoski, 2008). The *U.S. v. Santillan* (2008) determined the phones could be contraband and fall under the plain view doctrine because they are known tools for drug dealers (Marcinkoski, 2008). When a phone is found during the execution of a search warrant it is better to shield the phone from communication and preserve its current state than to manually examine it. Unless the officer is trained at on-scene mobile phone forensics, data that may prove to be important can be changed or lost.

Recently, the Ohio Supreme Court ruled that officers must have a warrant to analyze a suspect's phone, unless the officers' safety is in danger (Majors, 2009). This means that phones found incident to arrest or in plain view during a search warrant may not be admissible. Until the U.S. Supreme Court makes a ruling there will be questions as to when and how a mobile phone can be searched. This means there is always the potential that evidence found without a warrant could be thrown out. Unfortunately warrants can take time and this time may allow the evidence on a phone to be deleted. For this reason it is best to isolate a phone whenever it is seized to preserve the information in case it needs be searched later. Just like DNA, fingerprint, and other

volatile forms of evidence, evidence on mobile phones needs to be protected and preserved in order to maintain permissibility in court.

2.3 Signal Theory

To understand how to protect evidence on a mobile phone it is important to understand how the phone communicates and how data can change. Mobile phones operate by using radio frequencies to communicate with towers and vice versa. Knowing how these signals propagate through the air is the only way to truly understand how radio isolation works. Signal attenuation is what is really occurring when a shielding device is used to isolate a mobile phone. It is how much a signal is attenuated that determines if the phone can still communicate with its network.

Signal strength for a mobile phone is measured in a unit called a decibel (dB). Decibels are logarithmic dimensionless units. This is because a dB is the ratio of the same type of unit, which causes the units to cancel out. Despite this, a dB is a useful number because it provides a measurement from a known reference value. Decibels have long been used in electronics as a unit of measurement. Mobile phones, "measure absolute strength in in dBμV/m, or decibel-microvolts per meter (O'Brien, 2008). When examining the signal strength for a mobile phone it is a negative number. That is because the signal the phone is receiving is less powerful than the reference value for which it was set.

Decibels are determined by the equation 10 log (P2/P1) dB. P1 is the power output of the original source and P2 is the power of the second source. "If the second produces twice as much power as the first the, the difference in dB is: 10 log (P2/P1)= 10 log 2=3 dB (Wolfe, 1998)". This means that a 3 dB increase represents double the power

of the first. Attenuation is the opposite effect, when P2 is less than the P1. The same equation still holds true but for every -3dB in the reading, the signal is reduced to half strength. When dealing with cell phones more often than not, one will see a negative reading.

Most people are not used to reading and understanding measurements in dB. In order to have people understand what is going on cellular providers created the bars. The more bars the phone has the better its reception is supposed to be. "The problem with measuring cell reception is that there is no industry standard for measuring signal strength (O'Brien, 2008)." Therefore these bars can represent different strengths depending on the manufacturer of the phone and the Network Service Provider (NSP). They are good for knowing approximately how well the phone is receiving and sending transmissions. The bars do not tell how strong the signal actually is nor how much noise is occurring. Many phones can be set to show the exact dB level they are maintaining. Settings like these can be found in the manufacturers guides.

The strength of the signal isn't the only thing that matters when conducting RF communications. The signal to noise ratio (SNR) is also important. "Noise is unwanted electrical or electromagnetic energy that degrades the quality of signals and data (TechTarget, 2008)." No matter the signal strength, if there is too much noise a call will not go through (TechTarget, 2010). When noise is strong enough it can cause a bit to change from a 1 to a 0 or dropped altogether. This can be a large part of the reason calls are lost, dropped, or have static despite having bars displayed on the phone. If the SNR is high enough it also means a phone with no bars displayed is still capable of communicating with the network successfully.

The Shannon Capacity formula describes how much information can be sent through noisy channels. The formula for SNR is often written in dB for convenience and states that $SNR_{dB} = 10 \log_{10}$ (signal power/noise power) (Stallings, 2005). Claude Shannon, considered the father of information theory, used SNR to conclude that the maximum capacity for any given channel is $C = B \log_2 (1+SNR)$ where C is the capacity and B is the bandwidth measured in Hertz (Hz) (Stallings, 2005). This is a theoretical maximum transmission capacity because it doesn't include many sources of additional noise. In practice there are many other sources of noise in a channel. These sources can include: other RF signals being broadcast, free-space path loss, diffraction, reflection, refraction, and scattering.

A major component of noise in mobile phone communication is other RF broadcasts being made in the same band of the RF spectrum. This is the reason radio stations have to be several MHz apart from one another. In order to use the limited bandwidth allowed for mobile phone networks, NSPs use multiple towers to create zones known as cells; each cell allows the for the full use of the RF spectrum in its area. There are multiple standards used for communication but in the United States the most commonly used standards are GSM and CDMA. A GSM mobile phone in the United States operates at 900 and 1900 MHz. It is split into 200 kHz carriers for both uplink and a corresponding downlink channels (Smith & Collins, 2007). GSM uses Time Division Multiple Access (TDMA) in order to allow more users to connect to the same tower. Code division multiple access (CDMA) networks also operate at 800 MHz and 1900 MHz frequencies but it utilizes the bandwidth differently. In CDMA the bandwidth is divided into two parts to allow full duplex communication. The forward channel is used

to send information from the tower to the phone and the reverse channel is used to send from the phone to the tower (Stallings, 2005). CDMA has many advantages and disadvantages when compared to TDMA. One advantage is that CDMA is more resistant to several forms of noise including multipath propagation (Stallings, 2005). However, CDMA doesn't handle transitions from tower to tower as easily and can suffer from attenuation problems due to distance from the tower (Stallings, 2005). Figure 2.2 shows how these methods utilize the frequency range they are allocated.

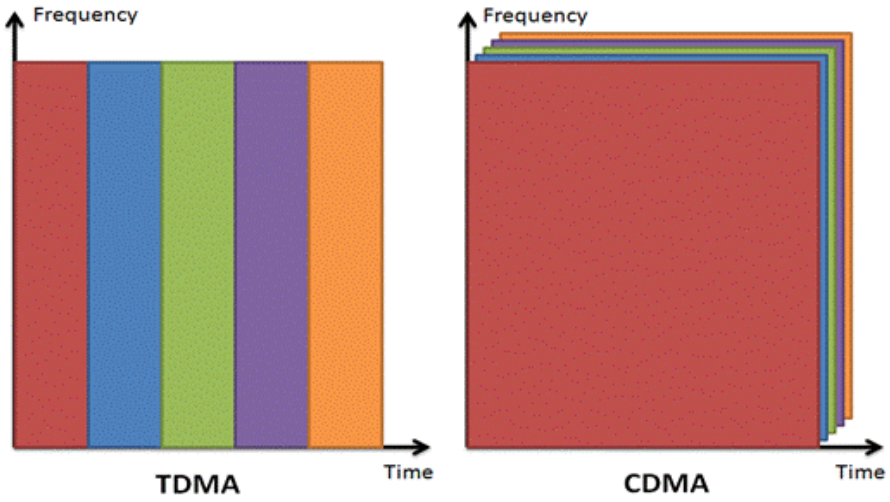


Figure 2.2 TDMA and CDMA (National Instruments, 2009)

The development of the cellular system itself is an attempt to allow the maximum number of customers to make use of the limited bandwidth allowed for mobile phone communication. Each cell, or zone of coverage, has a limited number of connections that it can allow. After the saturation point has been reached, the cell zone starts to have bleed through where calls interfere with or terminate other communications. Increasing the number of cells allows for the same frequencies to be reused by neighboring cells. Other strong sources of electromagnetic radiation can also be a source of noise when using mobile phones. Signals from radio towers, satellites, and microwave antennas are

examples of electro magnetic radiation that may interfere with communication. Bleed through from other cellular signals can also interfere with communication. Strong signals can override or alter bits as they are being transmitted and cause mobile telecommunication services to fail.

Free-space path loss is the amount of signal that is lost as a radio wave travels through air. As the radio wave travels it naturally attenuates and dissipates. There are many different models that can be used to predict path loss, but they are all based on the general equation of $L_f = 32.4 + 20 \log(R) + 20 \log(f)$ where *R* is the range in kilometers and *f* is in megahertz (Smith & Collins, 2007). This is important when designing a mobile phone system because the phones will be at variable distances from the towers. The further a mobile phone is from the tower the more difficult communication becomes because of free-space path loss.

Refraction is the gradual bending of a radio wave as they travel through the atmosphere. These changes occur due to differences in atmospheric conditions, altitude, speed or other spatial changes (Stallings, 2005). This usually causes radio waves to bend downwards instead of traveling in a direct path.

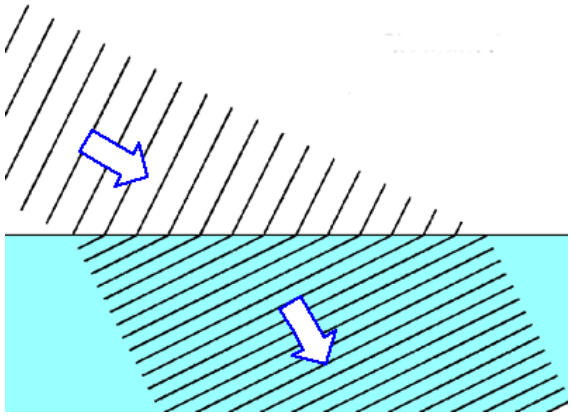


Figure 2.3 Wave Refraction (Kurtis, 2008)

Reflection occurs when a radio wave strikes an object that is large when compared with the wavelength (G. Rogers & Edwards, 2003).This causes the radio wave to bounce back from the object at a different angle. Reflection can be useful for propagating waves, but there is always some signal lost to absorption by the object (Dankner & Gupta, 2007).

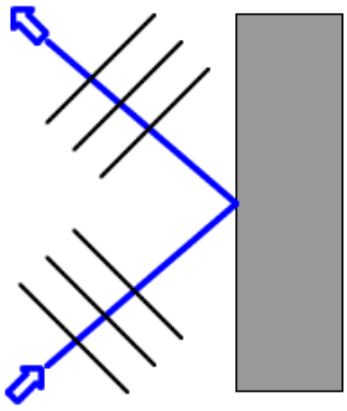


Figure 2.4 Wave Reflection (Kurtis, 2008)

Scattering is caused when a radio wave strikes an object and is sent back out in multiple weaker signals (Stallings, 2005). It is almost impossible to predict all of the scattering effects because there are too many factors that come into play (Dankner & Gupta, 2007). Any object such as a building, car, or lamppost can cause scattering. When used in conjunction with reflection and refraction these explain a significant amount of signal degradation and noise in the channel.

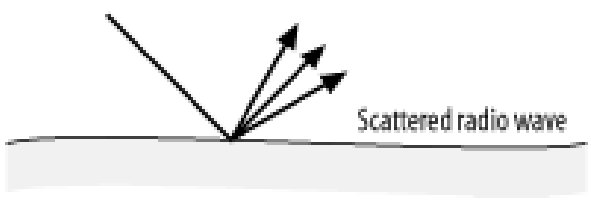


Figure 2.5 Wave Scattering (eTutorials.org, 2010)

Another major form of noise that can be introduced into a RF communication is diffraction. Diffraction occurs when a signal hits a blocking object. Some of the signal will be lost to scattering. The rest of the wave will travel around this object in order to fill the void created by the object (Dankner & Gupta, 2007). This is an important feature of RF because it allows mobile phones to communicate with towers despite being behind a building or some other obscuring object. It also means signals are no longer traveling in line of sight and their viability as a communication path attenuates.

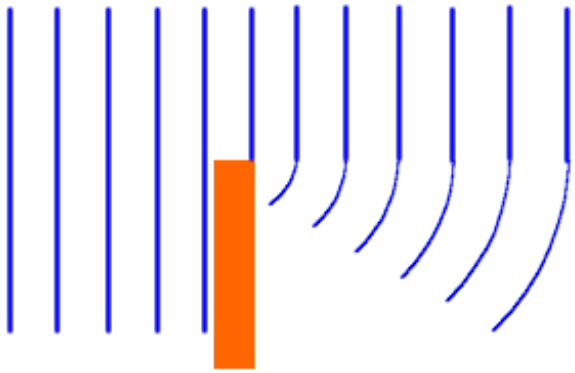


Figure 2.6 Wave Diffraction (Kurtis, 2008)

When all of these sources of noise are combined, there is a significant portion of signal lost. Known as multipath propagation, three of mechanisms (diffraction, reflection, and scattering) can cause a mobile phone to receive multiple copies of the same signal. These delayed signals can interfere with the phone's ability to recover the original information (Stallings, 2005). Often a "dead zone" occurs because of a combination of these items.

Despite these difficulties, mobile phones continue to function better every year by developing more powerful antennas. Network service providers are also building more towers and installing signal regenerators throughout their service zones. All of this means

that mobile phones are able to maintain better signal longer and that more data is transmittable. It also means that it is very difficult to tell how far a mobile phone is from the source of a signal at any given point in time. Even if one does know where all the towers are it can be near impossible to tell how strong the signal is at any given location. Antennas are designed to send the strongest signal possible in a particular direction. However, radio waves do not propagate in straight lines and in fact develop nodes as they travel where the signal can be stronger. Figure 2.7 shows how waves can propagate from a tower in both the horizontal and vertical axis.

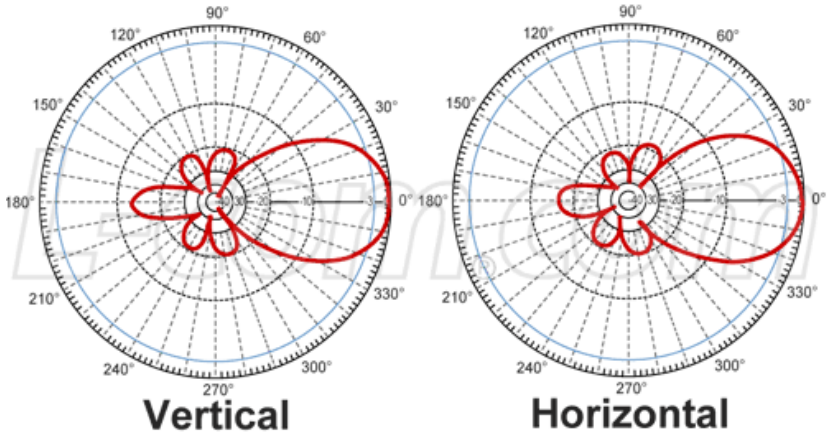


Figure 2.7 Antenna Propagation (L-com, 2010) Used by Permission From L-Com

Every antenna can have a unique propagation pattern where signal strength will vary. Without the ability to know when or where a mobile phone can successfully transmit to the network, it becomes important to use a tool that can isolate the phone from the NSP in order to preserve the evidence on the phone.

2.4 Faraday Cages

There are many different tools and devices that can be used to prevent a mobile phone from communicating with its network. One of the most common types is a Faraday cage or shield. Named after Michael Faraday, the scientist who discovered them in the

1830s, Faraday cages are devices that spread incoming electrical signals across the exterior of the cage (Murphy, 2010). Similarly signals generated inside the cage are also wrapped around the interior of the shield. This effectively electromagnetically isolates any device placed inside the cage.

A Faraday cage requires layers of different metals, such as: aluminum, copper, nickel, and silver, in order to block the entire electro-magnetic spectrum (Murphy, 2010).

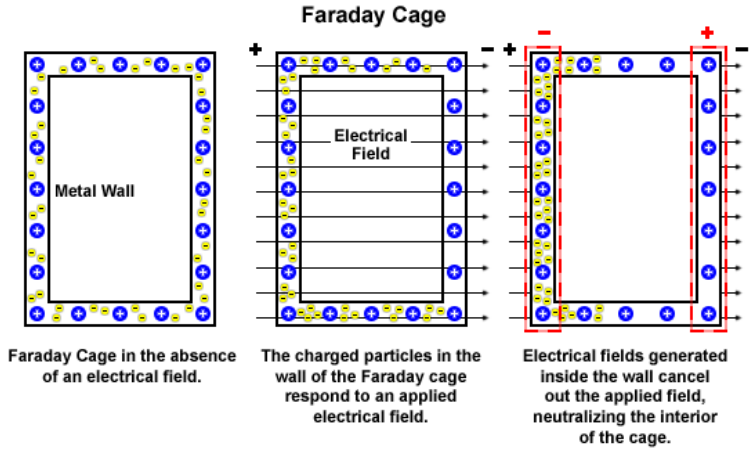


Figure 2.7 How Faraday Cages Work (Murphy, 2010)

Many of the shielding tools available in the mobile forensics market have only one thin layer of mixed metal fibers designed to attenuate signal between 800MHz and 1900MHz bands, which is where mobile phones in the United States operate (Kessler, 2009). This means that many of the devices sold as Faraday containers are not really Faraday devices. They do block signal in a similar manner, but not as effectively allowing some signal to get through. The shielding tool can still function properly as long as its RF attenuation is greater than 50dB (Hill, personall communication, April 6, 2007). This number was determined from practical measurements that Hill conducted showing that the typical mobile phone does not have a 50dB margin of operation (Hill, 2010).

According to Disklabs, a vendor for mobile phone shielding devices, 17dB attenuation through their bag is enough to isolate a mobile phone (Disklabs, 2008). This shows that there is little consistency for determining how much attenuation is needed to isolate a phone. The inability to attenuate all signals is where the errors from this experiment are expected come from.

Faraday or Faraday-like products on the market range from true Faraday rooms to simple cloth like meshes that are wrapped around mobile phones. Faraday chests and bags exist in all sorts of sizes; there are even tents and wallpapers that are available. Waveguide beyond cutoff is the method that is also used to attenuate signal by mesh like devices. It is the same principle that allows microwave ovens to have transparent doors and not leak microwave radiation. The metal substrates in the material reflect the signal preventing it from passing through the shield. The effectiveness of this is based on several factors including depth, geometry, and the shape of the aperture in the metal (Intel Coporation, 2001). Other commonly used tools are arson cans, heavy aluminum foil, and even potato chip bags (Kubasiak & Morrissey, 2009). Each of these tools has advantages and disadvantages. The most portable and likely to be used on scene are bags, boxes, and meshes that create a shield around the phone.

2.5 Shielding Issues

There are some problems inherent with these portable shields. Most of these devices are not perfect Faraday cages and allow some signal to enter and escape. Other devices utilize waveguide beyond cutoff to attenuate the signal instead of the Faraday effect.

All of these shields, no matter their design, operate by attenuating, or weakening the signal enough that the phone should not be capable of communicating with the NSP. Another problem is that if there is a gap anywhere in the shield, the phone will be able to acquire a signal. This problem is apparent in tools such as the various meshes and bags available from many companies. This does not mean that they do not work; just that care must be taken to properly ensure there are no openings. Not only do the seams and edges need to be secured, but care should be taken with them to prevent a tear in the material. Other products such as boxes and other cases must be closed completely and arson cans need to have their lids sealed shut in order to function correctly.

Another problem inherent in all wireless preservation systems is that cutting off the cell phones signal causes them to increase the strength of the signal broadcast from their antennae (Interpol European Working Party on IT Crime, 2006). If the equipment being used isn't capable of attenuating the more powerful signal then it has failed.

Increased strength also means increased power drain. The longer the phone is isolated from its network the quicker the battery will drain. This can create multiple problems. There has never been a standard power connection for the mobile phone industry. An investigator may not have access to the appropriate charger to provide power to keep the phone charged. A phone that loses power may be subject to keypad and/or PIN lock upon restarting. Lock codes are the main reason it is not recommended to power off the phone in the first place. Once enabled these locks may prevent any information from being extracted from the phone. If the investigator does have the proper power cable for the phone there is another danger they must be aware of. Plugging a phone in after it has been placed in a RF shielding tool not only breaks the seal but the

phone can also use its power cord as an antennae. RF signals are capable of following the cable into the shield allowing communication to occur. There are shielding chests that have filtered power feeds that can be safely used to charge a mobile phone such as the Ramsey 4500Z. These chests are usually significantly more expensive than their non-powered counterparts and may be cost prohibitive in many situations. They also are not as transportable as a bag or mesh tool.

Another means to create antennae out of the preservation material is to put it directly against the phone. Metal mesh in direct connection to the phone can turn the entire mesh into an antenna and cause the exact opposite of the desired effect. Instead of attenuating the signal of the cell phone and preventing reception, inadvertently the shield has increased the reception of the phone. To ensure that this doesn't happen the phone should be set in a nonconductive material before being placed within the shield.

One of the largest problems with shielding devices is that in order to examine the phone, most of the time it must be removed from the shielding device. This gives the phone an opportunity to communicate with the tower and update itself automatically. The phone will receive all the information that the NSP has queued up to transmit to the phone. This of course will change the LOCI information and may contain new SMS, MMS, and possibly even the packets for remote wiping. To prevent this, the phone should only be removed after a trained expert has disabled radio communications or when the phone has been brought to a laboratory environment that functions as a Faraday cage and truly blocks all incoming signal.

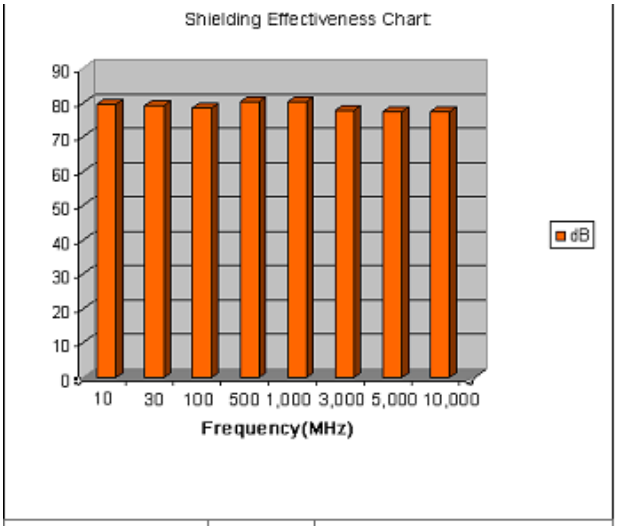
2.6 Preservation Tools

The vendors themselves publish most of the data about the performance capabilities of the various tools. They often use charts, graphs, and tables in or to showcase their product. Due to the fact that the vendor wants to sell their products, some of this information can become misleading. Due to mobile phones being a relatively new source of evidence and a lack of training and equipment, law enforcement officers have tried several tools that were never intended to be to be wireless preservation devices. Items such as arson cans, Taco Bell wrappers, and potato chip bags were never intended to be used as such but have been by necessity. These tools have not been scientifically determined to function as a proper shield to preserve evidence nor is there documentation concerning their attenuation capabilities.

There are dozens of tools available to investigators for wireless preservation; the following are just a select few of them. Comparing the websites of vendors will reveal similar findings as to what is shown below. This is not an endorsement of products nor is it intended to disparage them.

Paraben has a convenient chart on their website to show the effective attenuation of its StrongHold Bag. The StrongHold Bag is just one example of many Faraday bags that are available. Figure 4 shows the amount of attenuation at each frequency. Beside that is a percentage rating of effectiveness. This is where a lot of confusion has occurred. Misreading the chart can cause the belief that the bag is 99% effective. The vendor actually is claiming to attenuate between 77-80 dB. Theoretically that is more than enough attenuation to work properly. Phones have also gotten better at maintaining signal at lower power. This means it's not uncommon for a phone to still get clear reception at

-100dB or more. If a phones starting signal is powerful enough, cutting off 80dB will not attenuate the signal enough to isolate the phone. What is being stated is that 99.99999% of the time the bag attenuates the signal of anything placed inside of it by 77-80dB. Not that 99% of the time it isolates the phone and can preserve the evidence located on it. This is important because it explains how phones placed securely in the StrongHold Bag may still receive calls and texts.



Frequency(MHz)	dB	Effectiveness (%)
10	79.7	99.99999
30	79.2	99.99999
100	78.6	99.99999
500	80.5	99.99999
1,000	80.4	99.99999
3,000	77.9	99.99998
5,000	77.5	99.99931
10,000	773	99.99732

Figure 2.8 Paraben Shielding Effectiveness Chart (Paraben Corporation, 2007)

Teel Technologies is a distributor of many mobile phone forensic tools and software. Included in the products available are various chests such as the Ramsey 4500Z mentioned previously. Describing the chest is a simple list stating the attenuation rate of the box at different frequencies. Like the table in figure 2.8 this table is not

reporting that the Ramsey 4500Z will successfully isolate a mobile phone all the time. It shows that the box will attenuate 90dB from RF at the listed frequencies

Table 2.1: Ramsey 4500Z Effectiveness (TEELtechnologies, 2010)

dB	Frequency
-90	1 GHz
-90	3GHz
-80	6GHz

LessEMF manufactures a High Performance Silver Mesh that has a shielding effectiveness that is greater than 50dB for frequencies ranging from 30 MHz to 3 GHZ. Mobile phones operate between 900 MHz and 1800 MHz placing it within the 50dB attenuation range provided by the mesh. These means that any phone wrapped in the mesh will lose 50dB of signal. This does not mean that a phone is automatically isolated being wrapped in the mesh. If the signal strength is strong enough the phone will continue to send and receive transmissions including any signals that could potentially damage evidence.

eDEC has recently released its Black Hole bag. This bag like many others is made of a metal mesh. Unlike many other shielding bags the Black Hole has a transparent window that allows an investigator to see that status of the phone and even allows for some manipulation of the phone while it is isolated. This window was incorporated into the bag from the beginning so that it doesn't cause any loss of the bag's attenuation capabilities. According to eDEC the Black Hole bag effectively attenuates signal by 30 to 50dB. This may or may not be enough attenuation to completely RF isolate a mobile phone.

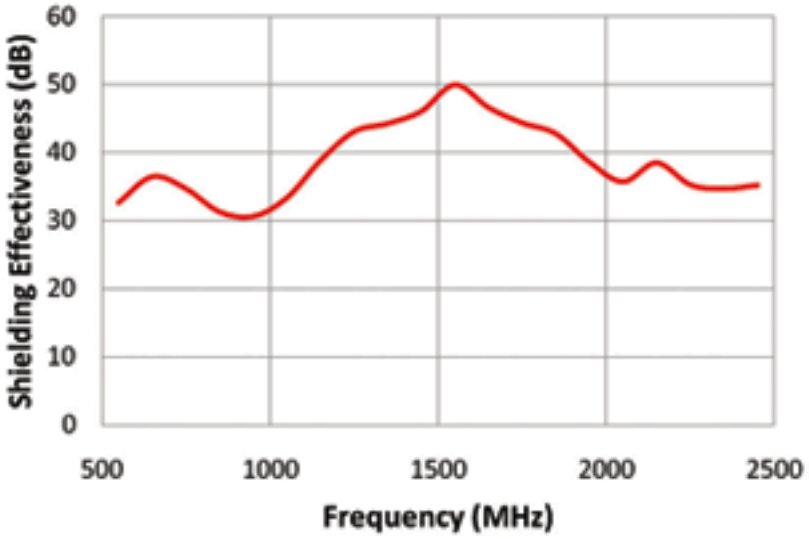
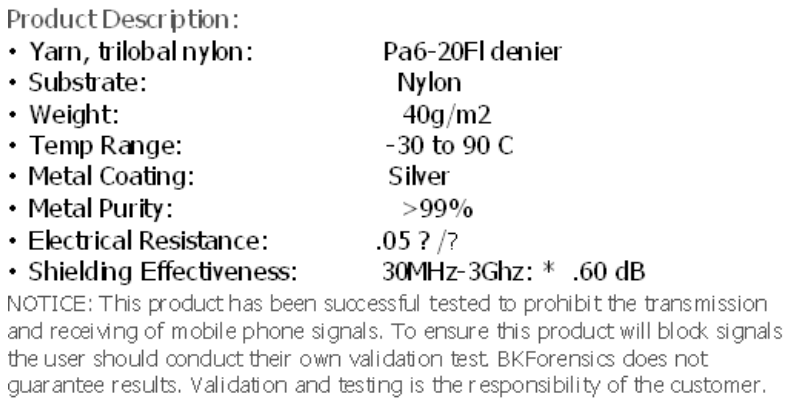


Figure 2.9: Effectiveness of the Black Hole Bag (eDEC & Ryan Security Technologies, 2009)

BKForensics is another company that specializes in mobile phone forensics. On their website is another mesh cloth that is supposed to isolate a mobile. The table they have for their mesh is very informative. An equation is given to describe the amount of attenuation provided by their mesh. At 900 MHz the mesh should attenuate signal by 540MHz dB and at 1900 by 1140MHZ dB according to the equation. This is an impossible attenuation rate. When asked about the equation the company responded stating that it was given to them by them by the testing agency that worked on the material and they did not know what it meant. Shortly after emailing BKForensics they changed the effectiveness to simply state 30MHz – 3GHz. Perhaps the most important item however is the notice that is at the bottom of the table. The reason this notice is so important is that BK is willing to admit that results are not guaranteed and that validation testing is the customer's responsibility.


Product Description:

- Yarn, trilobal nylon: Pa6-20Fl denier
- Substrate: Nylon
- Weight: 40g/m2
- Temp Range: -30 to 90 C
- Metal Coating: Silver
- Metal Purity: >99%
- Electrical Resistance: .05 ? /?
- Shielding Effectiveness: 30MHz-3Ghz: * .60 dB

NOTICE: This product has been successful tested to prohibit the transmission and receiving of mobile phone signals. To ensure this product will block signals the user should conduct their own validation test. BKForensics does not guarantee results. Validation and testing is the responsibility of the customer.

Figure 2.10 BK Forensics' Magic Mesh Effectiveness (BKForensics, 2010)

CHAPTER 3:METHODOLOGY

"Validation and testing is the responsibility of the customer (BKForensics, 2010)". It is a simple statement that needs to be followed and is what this experiment was about. Before going into the field and potentially risking evidence, a tool should be properly and thoroughly tested. If there is a chance that a tool will fail, an investigator must know when, where, and how it happens in order to stand up to the rigors of court. This section describes the mobile phones that were used and the preservation tools tested. It also lays out the method by which the research was conducted and how the results were recorded.

3.1 Devices Used

There are many models of phones, too numerous to test them all. There are also too many shielding devices available to do an exhaustive and comprehensive study on them. Any device that is not commercially available specifically as a wireless preservation tool will be excluded in this study. Availability, cost, and scale were the main factors that prevented any specific device from being used.

Every phone has a different antenna configuration and strength. The more phones that are tested for each NSP the more comprehensive the test results. The phones used during this experiment were limited to what is available in the Purdue Cyber Forensics lab. This impacts the studies ability to generalize the shielding devices' performance across all phones. Using more models and form factors will create a more comprehensive

study. There are too many models of mobile phones in existence to try them all, but this study provides some ability to predict if a model of phone is more likely to maintain signal despite being secured in a shielding device. Similar model phones were used from multiple providers to see if difference in GSM and CDMA networks affected the shielding device's performance. Due to the cost of acquiring phones T-Mobile was excluded from this experiment. The phones used in this study were:

Table 3.1 Phones Used During the Experiments

AT&T	
	Apple iPhone 3Gs
	BlackBerry Curve 9300
	Palm Pixi Plus
Sprint	
	BlackBerry Curve 8330
	HTC Hero 2
	Motorola Clutch i465
	Palm Pixi
	Samsung Galaxy S
Verizon	
	Casio G'Zone Ravine
	HTC Droid Eris
	HTC Imagio
	HTC Droid 2

These shielding devices were chosen because they are commercially available tools marketed specifically for isolating mobile phones. Most of them were designed for use by law enforcement as a forensic device to protect evidence on mobile phones. These devices are also some of the most commonly used ones by law enforcement agencies and made testing them all the more important. The shielding devices used are:

- eDEC Black Hole Bag
- LessEMF High Performance Silver Mesh Fabric

- MWT Materials' Wireless Isolation Bag
- Paraben Stronghold Bag
- Ramsey STE3600 - Chest
- Ramsey STP1100 - Bag

3.2 Method

Three towers were located, one for AT&T, Sprint, and Verizon. The towers were outside of major city limits in order to keep away from any alternative sources of signal the phones can use such as a signal repeater. Where possible, towers near highways were chosen because it was believed they would have the highest power output.

A voice, MMS, and SMS call was placed to each phone before being placed in a shield to insure that all the needed features worked. This was done at every distance repeated at every distance in order to establish a baseline and confirm that the phone still received the calls at that location. The ringer volume for the mobile phones was turned to maximum. This alerted the researcher as to which call penetrated the shield because many of the shields do not allow any other interaction with the phone.

At the base of each tower a phone from the appropriate company was then placed in each shielding device. The shielded phone was then called with another mobile phone. It was then noted if the shielded phone received the call. Next SMS and MMS messages were also sent to the shielded phone. The results of each test were recorded.

This experiment was repeated with each phone from a distance of 100, 150, 200, and 500 feet from the towers. These distances are the same used in Dankner and Gupta's research in 2007 and provided an opportunity to see how much distance altered performance of the shields. A Bushnell Yardage Pro Sport 450 laser range finder was

used to determine the proper distances. It is often impossible to tell how far one is from a tower or signal regenerator. Testing from multiple distances better simulates possible conditions that an officer in the field might encounter while transporting a mobile phone back to a forensics lab.

The goal was to find out at what distances, if any, the shielding instruments failed to successfully isolate the mobile phone. Results are P for passed representing blocked calls and F for failure representing calls where the shield was penetrated. If for some reason a test couldn't be performed or measured the result was N/A. In this research the N/A results were caused when a phone did not have a data plan that permitted MMS calls.

When a mobile phone detects that it has lost signal to the network it increases power to its antennae in an attempt to reestablish the connection. To make sure that each of the tested shields could handle the ramped up power output each phone was called at 15-second intervals after being placed into a shielding device. The intervals were chosen because they provided an even distribution over one minute and would provide clues as to how time effected isolation. After each test call the phone was allowed to reestablish its connection and then shielded once more. If the phone is not isolated after 1 minute the shielding device was considered to be faulty at the current distance.

The failure of any shielding device to isolate a phone and protect the evidence on it is very important by itself. Analyzing all of the results from these tests provided interesting findings. Other results such as the average time needed for a shielding device to isolate a phone and the optimal distance from a tower were also determined.

Comparing the dB attenuation rate of the shielding devices to their performances also provided insight into if a design or materials are more efficient than others.

3.3 Hypothesis

The main hypothesis of this research is that the shielding devices do not fully protect a mobile phone once it is placed inside the shield. The most likely place for these devices to fail, if they will, is when they are close to the NSP towers. Due to the nature of radio waves, the signals to and from the mobile phones are stronger at this point and better attenuation is needed to isolate the phone. This means that not only do the devices have to attenuate the radio signal but that the level of attenuation must actually be capable of isolating the phone. If the attenuation capabilities of the tools are appropriate then there should be no failures.

The second hypothesis is that communications that don't require a high SNR value are more likely to penetrate the shielding devices. SMS requires the least signal quality and will therefore be more likely to penetrate the shield. MMS will be the next most likely to bypass the shields as voice call require a constant and steady connection.

There was limited statistical analysis of the results, as each shield was tested pass-fail. The results of the pass-fail tests were compared across shield and distance. Time was another factor and was tested repeatedly allowing some analysis to be done regarding how time affected the shields performance.

CHAPTER 4: FINDINGS

This was a pilot experiment to determine if mobile phone shielding devices could fail to protect evidence on a mobile phone. Each shielding device was tested at multiple distances with multiple phones. For each distance there were 360 tests for SMS and Voice calls and 300 tests for MMS. MMS had fewer possible tests because the iPhone 3Gs and the HTC Imagio that were tested did not have data plans that allowed for MMS messages. The overall rate of failure for all of the shields was 53.08%. That means over half of all the test cases resulted in the shields not isolating the phone.

The hypothesis that SMS messages were the most likely to penetrate the shields held true. SMS messages were only blocked 778 out of the 1,800 tests that were run. This is a 56.78% failure rate for blocking SMS messages. Figure 4.1 shows the overall results of the SMS tests across all of the shields.

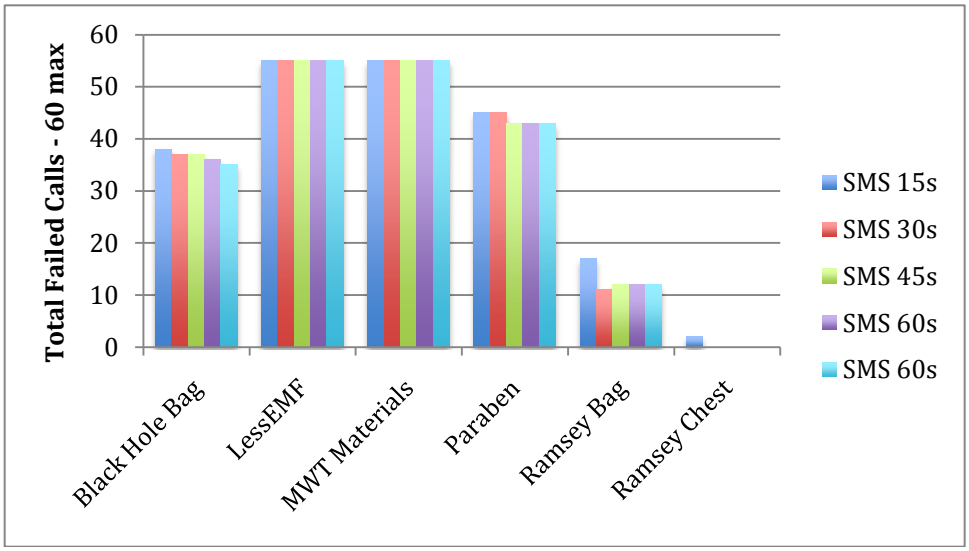


Figure 4.1 SMS Tests Failed Across all Shielding Devices

Voice calls were the next most likely call type to penetrate the all of the shields. In total the shields failed to block 968 calls out of 1,800 or 53.78%. Any one of these calls will change the call history resulting in the potential loss of evidence.

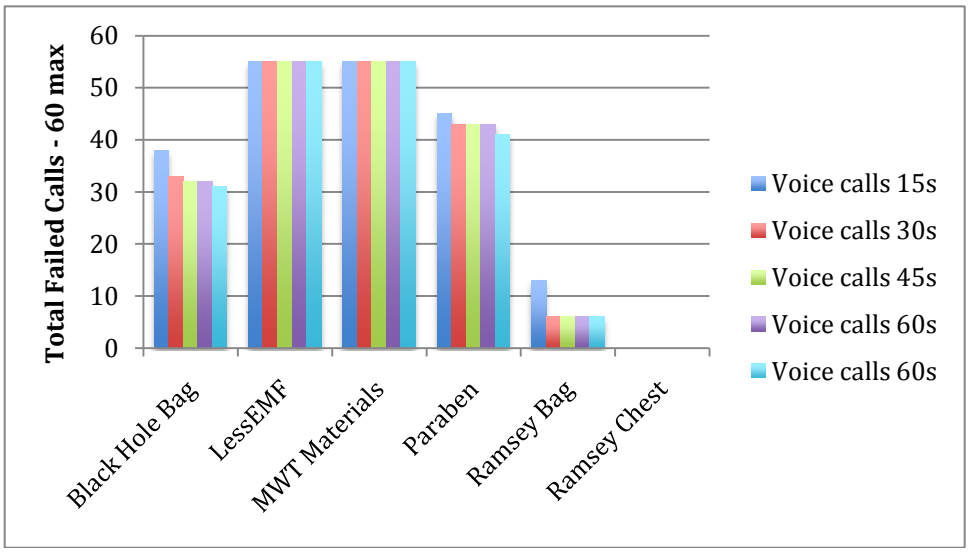


Figure 4.2 Voice Call Tests Failed Across all Shielding Devices

MMS messages were the most commonly blocked call type, only penetrating the shields in 721 out of 1,500 tests or 48.07%. Figure 4.3 shows how the shields worked with MMS messages. A nearly 50% failure in even the best-blocked call type proves that

the shielding devices cannot handle the increased power output of towers and mobile phones.

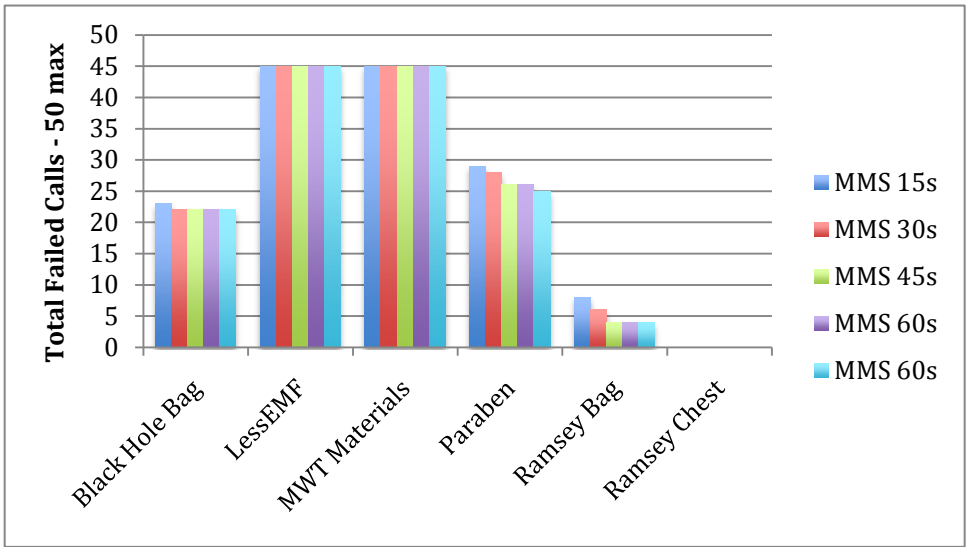


Figure 4.3 MMS Tests Failed Across all Shielding Devices

An ANOVA test was used to explore the results of the data between the various shields. It was found that the distribution of the data was not normal when the Test of Homogeneity of Variances (Levene's Test) results were significant. This violates one of the assumptions of ANOVAs and will result in an uncontrolled type 1 error rate. While it means using an ANOVA is not effective for analyzing this data set, it does not mean the data is useless. These results provide important real world information regarding the functionality of RF shielding devices in the field. The results of the experiments are broken down and explained in the following subsections. Specific data for each shielding device can be found in the tables within the Appendix.

4.1 eDEC's Black Hole Bag

The Black Hole Bag from eDEC and Ryan Security Technologies is the only shield with a built in view screen that was tested. This screen allowed the investigator to see the phone while it was in isolation and permitted limited interaction with phone.

Figure 4.4 below shows the combined results of all the tests conducted with the Black Hole Bag. For specific information about each phone and how well the Black Hole Bag isolated them see tables A-1.1 through A-1.5 in the Appendix.

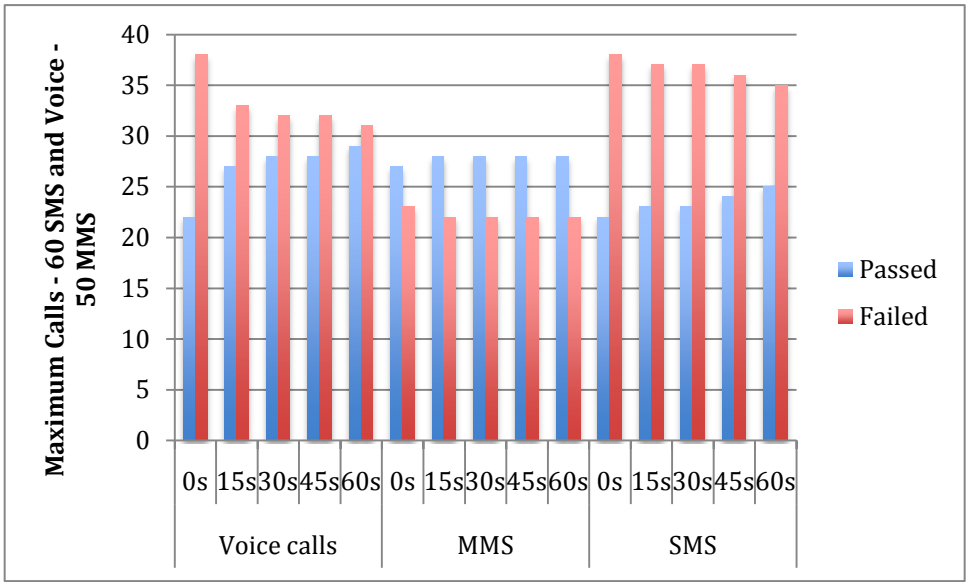


Figure 4.4 Black Hole Bag – Combined Results

In this graph it is clear to see that the Black Hole Bag fails to isolate most of the mobile phones during the tests. It is evident that SMS messages are the least isolated of the call types. Voice calls started out penetrating this shield as often as SMS but were more affected by time. This is most likely explained by the increase in noise in the communication channel that being placed inside the RF shield causes. As the SNR decreases the phones have a harder time communicating with the tower despite still receiving some signal. This supports the hypothesis that SMS messages require less SNR than the other call types.

Overall the Black Hole Bag had a 54.12% failure rate during these tests. One hypothesis predicted the further from the towers the shield was the better it performed. This was mostly true and figures 4.5 and 4.6 show the performance results of the Black Hole Bag at the base of and 500’ from the towers. At the base of the towers the Black

Hole Bag failed 79.41% of the tests, at 500’ away the failure percentage was reduced to 24.12%. This was not always the case as the results at 200’ were worse than those at 100’. The reason for this is due to how radio waves propagate and is discussed in a later section.

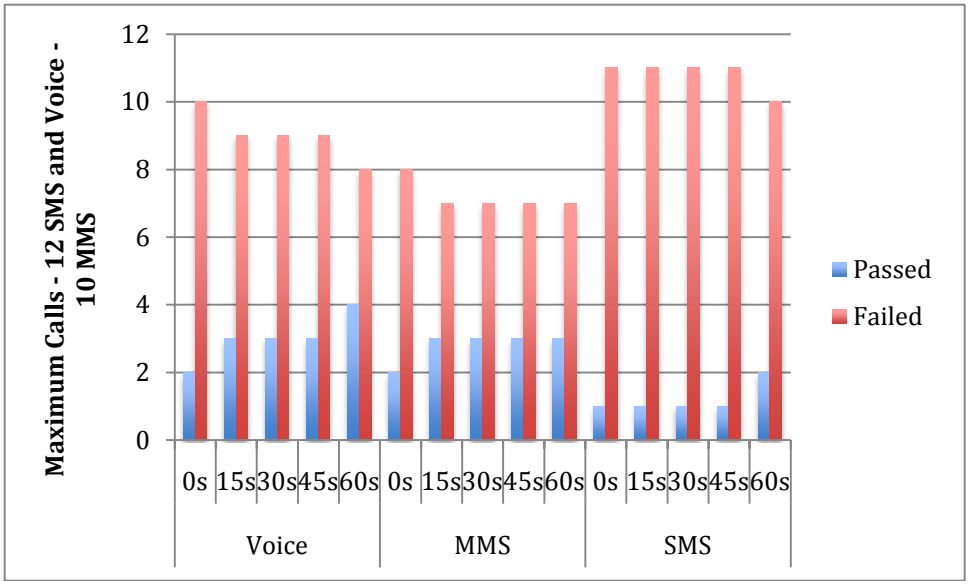


Figure 4.5 Black Hole Bag – Base of the Towers

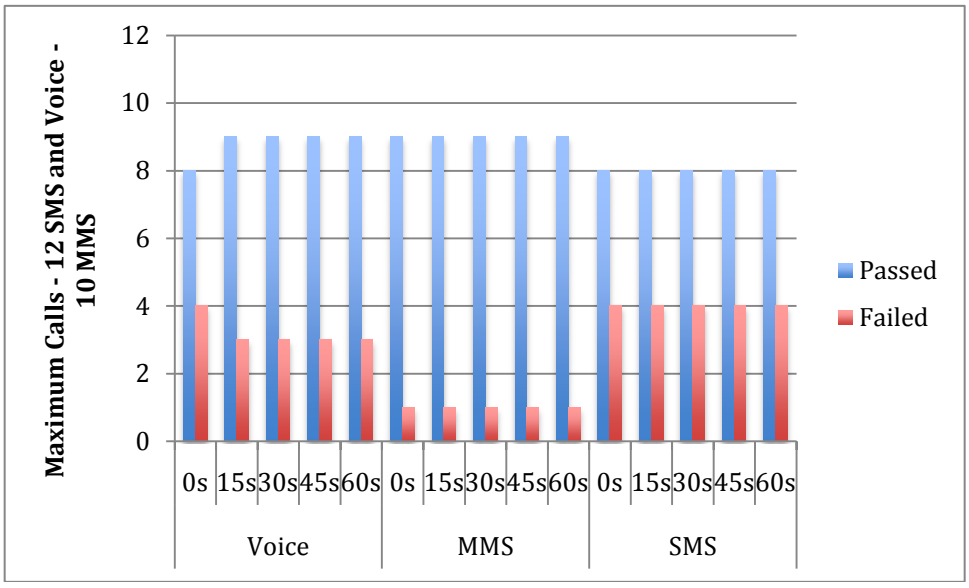


Figure 4.6 Black Hole Bag – 500’ From the Towers

4.2 LessEMF High Performance Silver Mesh

LessEMF's High Performance Silver Mesh tied for the least effective of the RF shielding devices. Throughout all of the tests it was able to isolate only one of the phones. That phone is the Motorola Clutch i465. It was able to isolate every call type at every distance with this phone. Below, Figure 4.7 displays the combined results for this shield. These tests were conducted using only one layer of the mesh over the phone. As consecutive layers were added the mesh did have improved performance. When similar devices are sold as a tool for law enforcement, such as BKForensic's Magic Mesh, the device is roughly a square foot in size. This prevents the layering technique from being used and is why the tests were conducted with only one full wrapping of the mesh. Distance and time did not appear to make a difference in this shields performance. Specific test results can be found in tables A-2.1 through A-2.5.

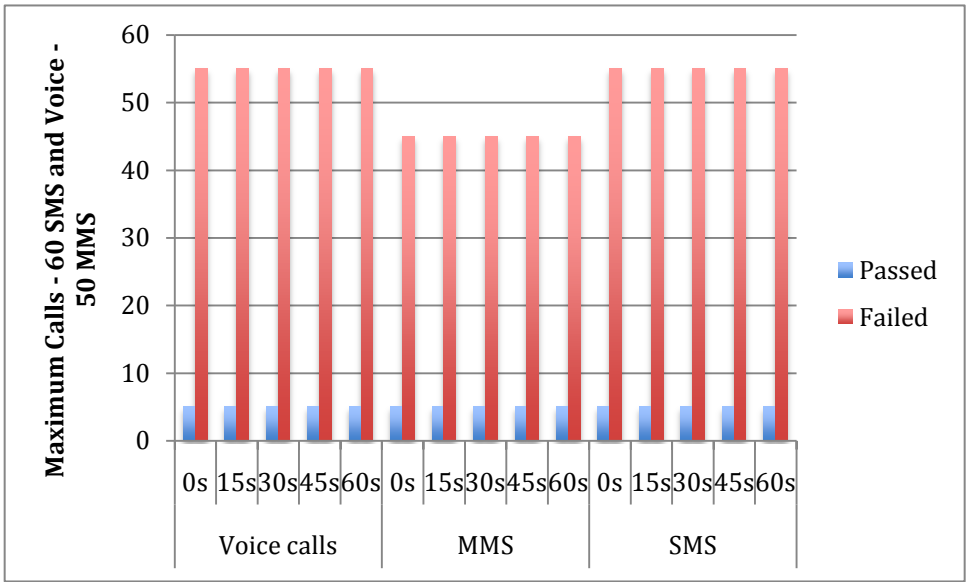


Figure 4.7 LessEMF High Performance Silver Mesh – Combined Results

4.3 MWT Materials' Wireless Isolation Bag

This is the other device that tied for least effective shield. Its' performance was identical to that of the LessEMF High Performance Shield as seen in Figure 4.8. It too

only blocked the Motorola Clutch i465 from receiving signal. As with the mesh shield time and distance did not play a factor in how this shield performed during these tests. Specific test results for MWT Materials' Wireless Isolation Bag can be found in tables A-3.1 through A-3.5.

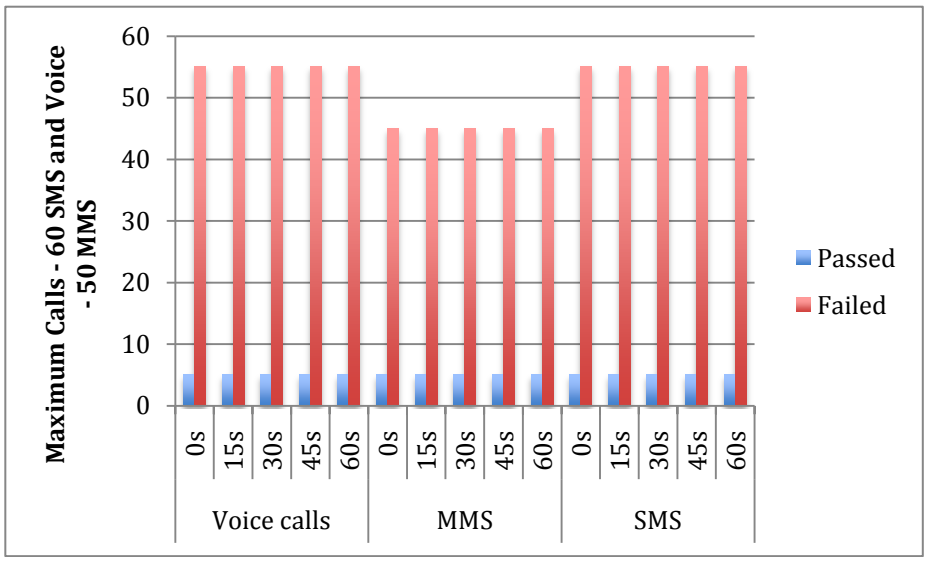


Figure 4.8 MWT Materials' Wireless Isolation Bag – Combined Results

4.4 Paraben's StrongHold Bag

The Strong Hold Bag had a 66.82% failure rate. Figure 4.9 shows the combined test results for the StrongHold Bag. As with the Black Hole Bag SMS messages penetrated the most often closely followed by voice calls. 73% of all the SMS calls made it through but only 71.67% of the voice calls. MMS was the most easily blocked only penetrating the shield in 53.6% of the tests.

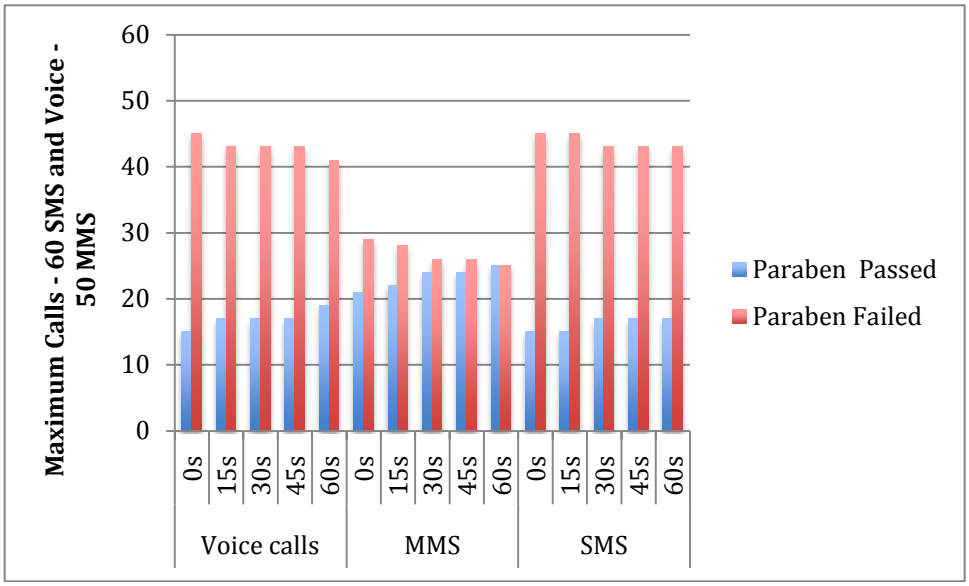


Figure 4.9 Paraben's StrongHold Bag – Combined Results

As the time interval increased, the StrongHold Bag was able to block more calls. However, this only resulted in a few more calls being blocked showing that the attenuation and noise caused by the StrongHold Bag wasn't sufficient to isolate the phones being used. Distance did play more of a factor in this shield's ability to isolate a phone. At the base of the towers, calls penetrated the shield 70% of the time. Repeating the tests at 500' from the towers reduced overall call penetration ratio to 52.94%. This confirms that free space path loss does reduce the signal strength of mobile phones quickly and that the farther from a tower a RF shield is the more effective it will be. Figures 4.10 and 4.11 graph the results of the tests at the base of the towers and 500 feet from them. Specific test information regarding the StrongHold Bag can be found in the appendix on tables A-4.1 through A-4.5.

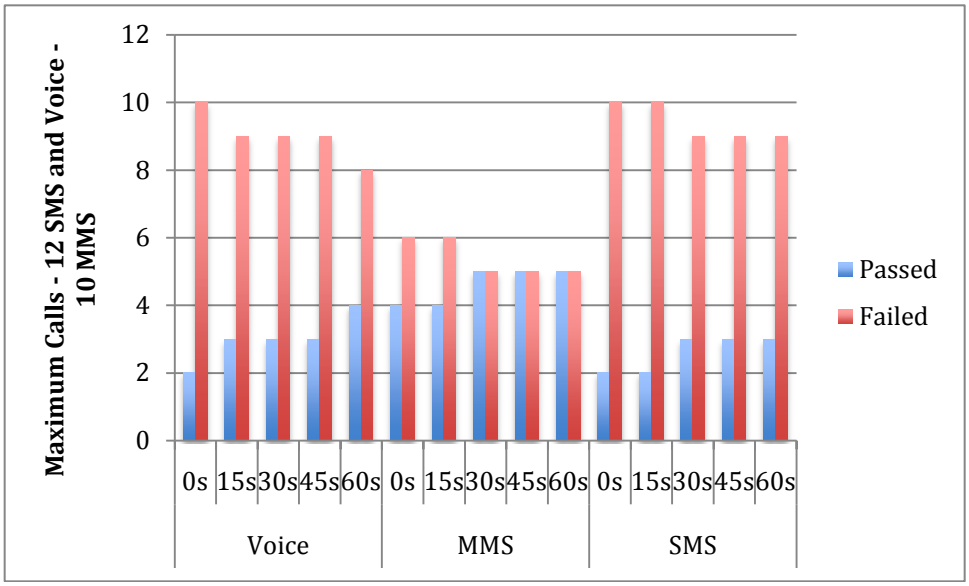


Figure 4.10 Paraben's StrongHold Bag – Base of the Towers

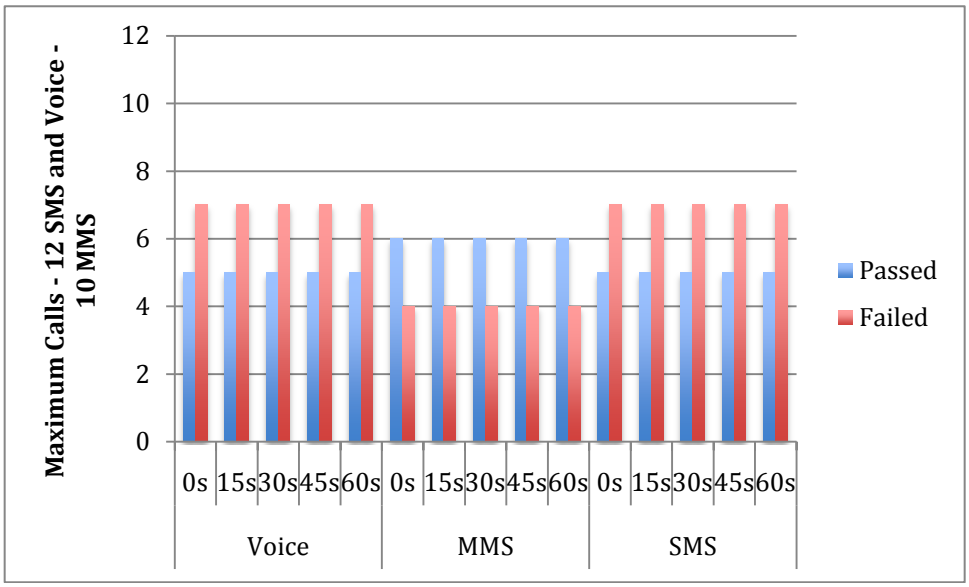


Figure 4.11 Paraben's StrongHold Bag – 500' From the Towers

4.5 Ramsey STP100

The Ramsey STP1100 was the best performing of the bag style RF shields that were tested. It is also the only one tested that used two separate layers of shielding material to create its walls. This double layering is likely responsible for it having an overall failure rate of only 15.4%. It failed to block 22.67% of the SMS messages. Following the trend, voice calls were the next most likely to penetrate the STP1100 at

12.33%. MMS messages penetrated this bag 10.4% of the time. Figure 4.12 shows the combined results for the Ramsey STP1100 tests. At 500 feet from the tower the STP1100 only failed to block 1 0s SMS and voice test on the Palm Pixi Plus. It successfully isolated all the phones after that. Appendix tables A-5.1 through A-5.5 contain all of the test results for the STP1100.

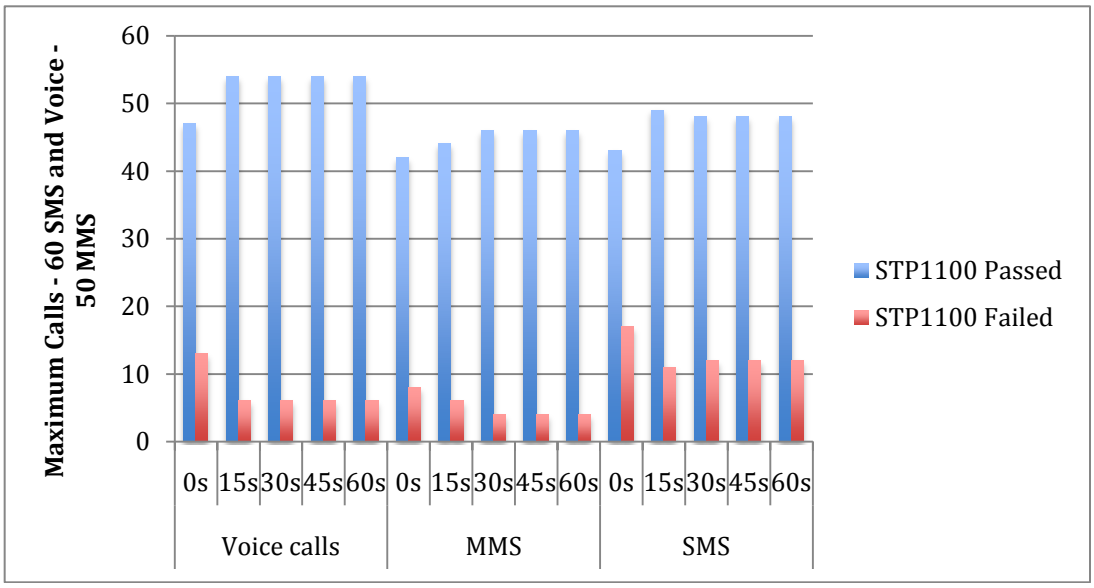


Figure 4.12 Ramsey STP1100 – Combined Results

4.6 Ramsey STE3600

The Ramsey STE3600 was the only chest type RF shield that was tested in this experiment. It also was the best performing shielding device out of all of them. It only failed to block 2 SMS messages in all of the recorded tests. It is important to note that some phones, such as the iPhone 4G and BlackBerry Curve 8350, could not be fully tested and therefore not included in these results. They were able to receive SMS and voice calls from inside the chest at multiple distances. Specific test results from this experiment can be found in tables A-6.1 through A-6.5 in the appendix.

4.7 Distance

Another hypothesis that was tested is that the further away a shield is from the tower, the better it will isolate a mobile phone. This proved to be partially true when moving from the base of the tower to 500 feet away from it. Most of the shields did in fact perform better at 500 feet than they did from the base of the tower. LessEMF and MWT Materials products performed the same throughout all of the tests. At 200 feet, several of the shields performed worse allowing more calls to penetrate them than had at 150 feet. 500 feet from the tower the over all performance of the shields was always at its best.

Figure 4.13 displays the voice calls made over all the distances. Examining it reveals interesting behavior in the shields isolation capabilities. From 100 to 150 feet there was a slight decrease in the number of calls blocked. More 0s tests were passed but fewer of the 30, 45, and 60s tests passed. At 200 feet the same number of 0s tests passed as they did at 100 feet but all the other tests were reduced. The overall failure rate increased from 53.89% at 100 feet to 57.5% at 200. When taken out to 500 feet the shields once again performed as predicted and voice calls penetrated only 45% of the time.

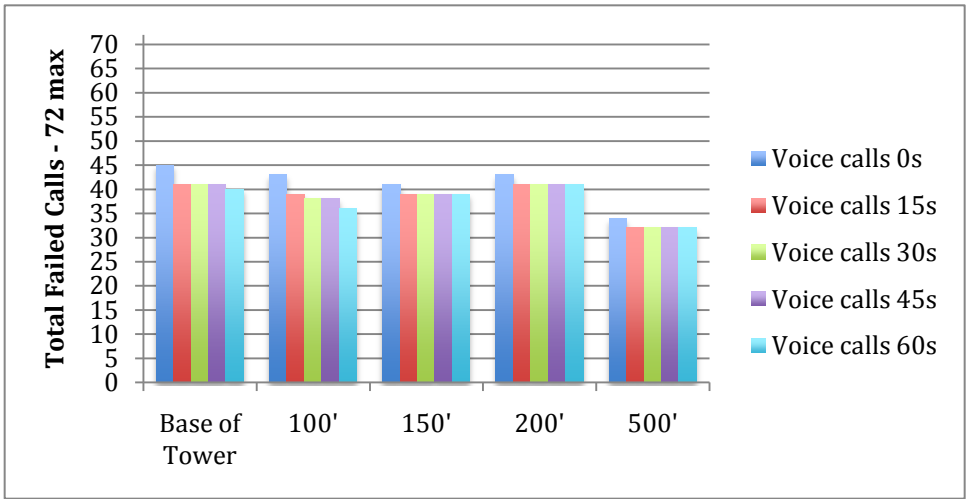


Figure 4.13 Total Voice Calls Failed Over All Distances

MMS messages followed the same pattern as voice calls. On a whole as distance from the tower increased the number of calls the shields blocked increased. However, there were more failures at 200 feet than at 100 or 150 feet. Figure 4.14 illustrates the overall behavior of MMS messages across the distances tested.

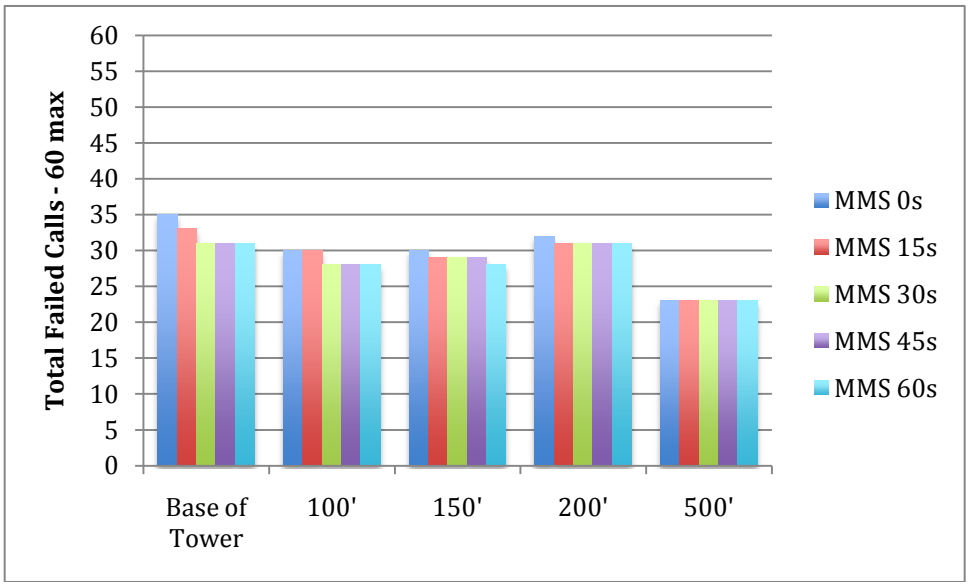


Figure 4.14 Total MMS Messages Failed Over All Distances

As would be expected from the previous results, SMS messaged followed the same pattern as Voice and MMS calls. The shields were more effective in isolating mobile phones at 500 feet than they were at any of the closer distances. As with the

previous call types SMS messages penetrated the shields more often at 200 feet than they did at 100 and 150 feet from the towers. SMS messages were the only one where the move from 100 to 150 feet resulted in increased isolation at all the time intervals. At 200 feet though the overall performance of the shields again decreased. The only time the shields were able to block more SMS messages than penetrated them was at 500 feet. Figure 4.15 shows the SMS call results over all the distances.

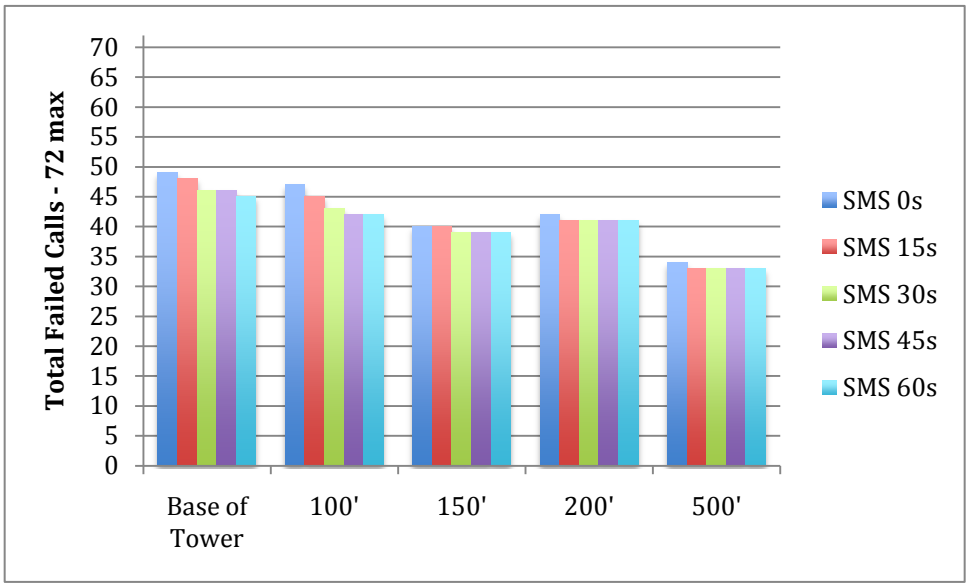


Figure 4.15 Total SMS Messages Failed Over All Distances

There are a few possible reasons the performance of the shields to decrease at 200 feet instead of increasing. The most probable reason is based on antennae design and how radio waves propagate. The tower antennas are sectored and designed to broadcast radio waves in specific directions. However, radio waves do no propagate in straight lines. As discussed in section 2.3, they often develop horizontal and vertical lobes where signal is stronger. At 200' from the towers where the experiments were conducted it is likely there was a lobe where stronger signal existed. At 500 feet the effectiveness of the shields increased as the hypothesis predicted. Without equipment that can measure the specific

wattage of the signal at each distance it is difficult to confirm that this is indeed what happened.

CHAPTER 5: CONCLUSIONS AND DISCUSSION

Many of the tested shielding devices are marketed as forensics tools, which implies that they should be forensically sound and accomplish their intended task. The vendors of these products state that they are 99.99% effective at blocking up to 90dB or that they can effectively block that many dB for signals between 3 and 30MHz. All of this is to increase marketability by implying that once a mobile phone is enclosed in their shielding device it will be isolated.

This study did not confirm or even test vendor claims on the dB that their products blocked. It did test the real world effectiveness of the RF shields. The purpose of this research was to find out if RF shielding devices would fail and what distance from a tower they fail at. Attempts were made to isolate as many variables as possible in order to eliminate extraneous factors that could influence the experiments results. This research isolated distance from a tower and time as factors on the effectiveness of RF shields.

It is evident that the shields do not always isolate the mobile phones. None of the RF shields tested were able to successfully isolate the phones 100% of the time. At the very least the call history on the phones will have been changed by the incoming calls. Worst case, any one of these failures could also potentially represent the complete loss of all evidence contained on the mobile phone due to a remote wipe command. Evidence on mobile phones can be too important to investigations to allow it to be contaminated or

erased by not being properly protected. This is why there are recommendations from scientific and law enforcement communities, such as Interpol, NIST, and SWGDE, dictating that mobile phones should be isolated when they are seized. The following subsections discuss the research results and their implications as well as what should be done in future testing of these and similar devices.

5.1 Call Penetration

One hypothesis of this research was that SMS messages were the most likely to successfully penetrate the shields. This turned out to be true. SMS messages were able to successfully penetrate the shields 56.5% of the time. The same hypothesis predicted that MMS messages would be the next most successful at penetrating the RF shields. This was not supported by the data. Results show that MMS was the most likely to be blocked by the RF shields, penetrating in 48.2% of the tests. Voice calls turned out to be the second most likely to penetrate the RF shields and did so in 53.78% of the tests. Any one of these failures represents a potential opportunity that evidence could be altered or deleted. Figure 5.1 is display of the total pass and fail results for the call types against all of the shields. There were 1,800 voice and SMS test in total and 1,500 MMS tests.

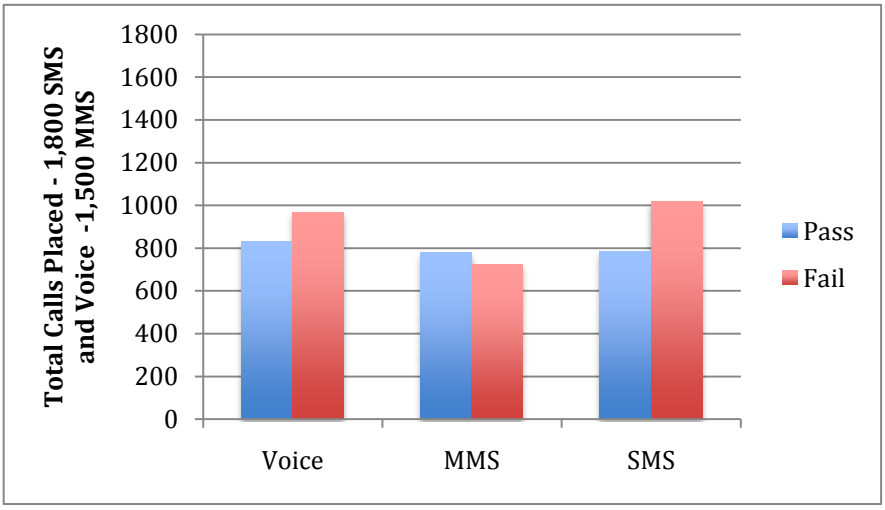


Figure 5.1 Total Pass Fail Rates

5.2 Legal Implications

Law enforcement officers know that mobile phones can contain valuable evidence. This is causing phones to be seized more often. As law enforcement departments establish policies detailing how mobile phones should be treated, it is likely they will follow the guidelines established by organizations such as INTERPOL and SWGDE. Standard operating procedure will be to isolate mobile phones after taking them as evidence. RF isolation shields such as the ones tested will become the equipment used to accomplish this. Unfortunately, the shields that were tested in this study couldn't isolate the mobile phones with absolute certainty. Law enforcement relying upon them to protect evidence may experience problems in the future because of this.

No matter where a phone is seized, it will have to come back to the police station to be examined and stored. If the phone is not near a tower when it is seized there is a decent chance it will pass near one on the way back to the station. For example, the Sprint tower used in this experiment is located next to I-65. The 500' test range that was used in this experiment easily crosses both lanes of the highway. Figure 5.2 shows the tower as a green marker and the red marker is positioned 500 feet away. Any phone being transported along this road would attempt to connect to this tower even if only for a few seconds. Those seconds of activity are all that are needed for a remote wipe command to be sent to the phone and have all the evidence on it zero out.

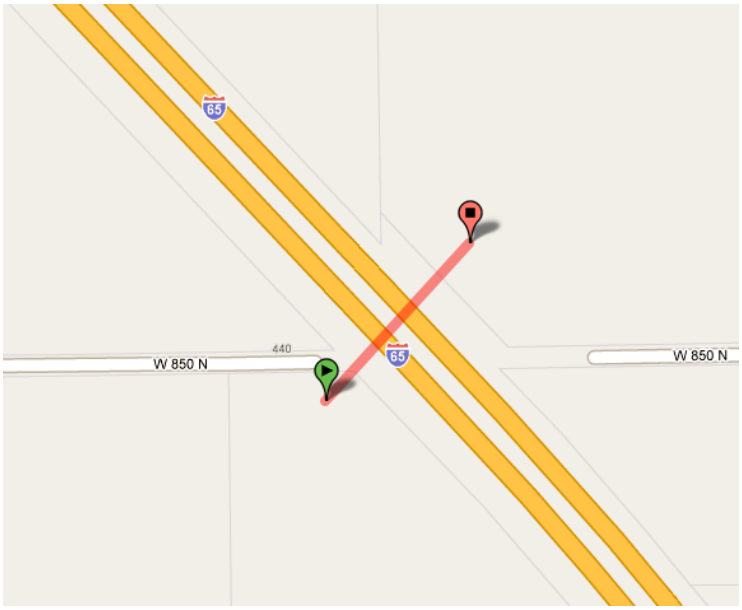


Figure 5.2 Sprint Tower Next to I-65

In a city, such as West Lafayette towers are located to provide optimum coverage for the NSP's customers. The urban environment can make it difficult for an officer to know where they are in relation to a tower. In Figure 5.3 an AT&T tower is located near Purdue University's main campus and is represented by a green marker. Within a 500' range are several important roads, shopping centers, a parking garage, library, and a church.

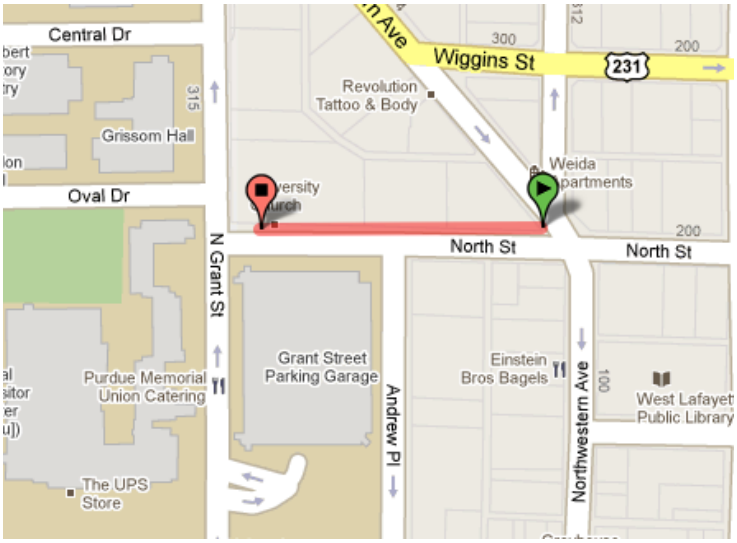


Figure 5.3 AT&T Tower Near Purdue

These are high traffic areas where the seizure of a cell phone incident to an arrest would not be uncommon. Just as with towers used for this research, mobile phones will attempt to maintain their connection to this tower. Without testing the shields with this tower it can't be said for certain if they are capable of isolating phones connected to this tower. Based on the results of this research though, the closer the phone is to the tower the less likely it will work. This goes to show how close people can be to a network tower and not even realize it. The denser the city population, the more towers will be present to allow the NSP to reuse bandwidth allowing them to have more subscribers. Future testing should cover more distance from the tower and measure the signal strength so more generalities can be made about the performance of the shields.

The results of this study show that there can be reason to suspect the integrity of any evidence taken from a shielded mobile phone. If this change occurs after the phone has been seized, there is a chance that any evidence later found on the phone can be called into question. The term "fruit of the poisoned tree" means that no matter how condemning evidence might be; once it is contaminated it is no longer reliable. This applies to evidence mobile phones as well as any other form of evidence. That is part of the reason protecting evidence on phones is so important. There are enough difficulties acquiring evidence from a mobile phone without having to worry if the evidence will change while the phone is in storage.

Defense attorneys could use this information to their advantage. As attorneys become more acquainted with evidence on mobile phones they will look for more ways to have it dismissed. It is not unreasonable to believe that an attorney could have evidence from an improperly protected phone dismissed from court entirely. Even if that

evidence is not dismissed, there is now the problem of explaining to a jury why evidence has potentially changed. The results of this pilot study prove that more testing needs to be done and that shielding devices need to be improved in order truly protect evidence on mobile phones so it can be presented in court.

5.3 Scientific Implications

This was a pilot study into the field effectiveness of mobile phone shielding devices. It proved that the tested mobile phone shielding devices could potentially fail to isolate phones when used in a field environment. Knowing the rate of failure of these devices is one of the criteria that are required to pass a Daubert examination. The American Academy of Science recently berated the entire forensic science community for not following scientific procedure and a lack of failure rates is one of the problems they addressed. More research needs to be done to determine the exact point and frequency of these failures, but this study is a good start. One of the major contributions of this study besides the results is the methodology that was used to conduct it. Determining what, where, and how to test the devices was a major part of this research. This methodology will be very useful for developing future studies and methods for investigating the effectiveness of mobile phone shielding devices.

The first thing that had to be determined was exactly what was to be tested. For this research MMS, SMS, and voice calls were determined to be the most important items to test. This is because they can quickly alter some of the most commonly used and important items of forensic evidence found on a mobile phone. Due to the threat these calls represent, the ability of the shields to isolate phones from these calls is of the utmost importance. The binary pass-fail tests conducted during this research were appropriate for

the functionality the shields are meant to provide. When preserving evidence in a forensically sound manner, there is no room for partial protection. Evidence is either preserved or it isn't and that can make or break a trial. For scientists analyzing shielding devices, pass-fail tests conducting over a set time intervals and distances provides detailed knowledge of what is occurring without over complicating the information being collected. This is also a means to determine the expected rate of failure of these devices.

There are other means to transmit data to and from a mobile phone besides these calls. 3G and 4G capabilities were intentionally left out of this research, as it was a pilot study. Future research should include these features when possible. A simple test would be to start streaming a video to the phone and then seeing how long it takes a shield to interrupt this stream. Another test that would be appropriate to include in future studies is sending the remote wipe commands to phones that can utilize them. This test would examine how well these signals can penetrate shields and if they behave more like SMS or MMS messages. Other signals that could also be tested in future studies include GPS and Bluetooth. As mobile phones integrate with more technology it becomes important to make sure that they are isolated not only from their towers but also from anything else that they could potentially connect to.

The next problem addressed when developing this methodology was where should these tests be conducted. One goal of this test was to find out if the shields could in fact fail to isolate a phone and how far from a tower do they need to be to work. For this reason the towers chosen were outside of city limits. These towers have less population per square mile and broadcast at a higher wattage in order to provide coverage to larger areas (Stallings, 2005). One advantage of conducting these tests outside of city

limits is that there was a clear line of sight to the tower. That meant factors such as alternative networks and multipath propagation were reduced and less likely to interfere with the results of the study allowing the strongest signal possible to reach the phones.

Tests were originally to be done at the base of the tower, 50', 100', 150', 200', and 500' from the towers. The reason for the 50' increments was to examine how much distance was necessary to provide different results. The 500' distance was set to determine if the longer distance would have a more significant effect. As this was a pilot study there were no prior test results to use to determine what the best distances would be. One of the difficulties presented when testing began was that the towers had safety enclosures that pushed testing back 30' to 50' away. This is the reason the 50' testing point was removed from the methodology.

There was often little difference in the results when increasing the distance at 50-foot intervals. Future research would benefit by conducting the same experiments but setting the distance intervals to 100-foot distances and testing back to 1,000 feet or more from the tower. This will provide a better sense of how distance affects the shields performance. It will also more accurately demonstrate how shields can be expected to behave as phones are transported from one location.

More precise tests could be run using equipment that can read the output wattage of the towers. This would allow for exact signal strength to be recorded instead of distance. Eliminating distance in favor of wattage would not only be more accurate but also would allow for testing inside city conditions and not require the experiment to be done in isolated environments. Measuring signal strength's biggest advantage is that once a shield is tested against a known signal strength a generalized formula can be determined

to predict the shields failure rate at any given distance and time. This would be tremendously useful to digital forensic science. It would provide known rates of failure for equipment used in evidence gathering. It would also allow law enforcement departments to defend the integrity of evidence collected in their jurisdictions when cases come to trial. The current results of this test provide a rate of failure for the shields but the power output of the towers is unknown. This makes determining a correct formula unfeasible at this point but does demonstrate that it can be done.

Using signal strength would also allow for a direct strength comparison to determine if there is a difference in CDMA or GSM networks. From the data collected during this research it would appear that Sprint has the weakest signal strength of all the NSPs. This could be true, but it could also be that the power output of the tower is lower than that of the AT&T and Verizon towers that were also tested. Sprint and Verizon are both CDMA networks but had drastically different responses. If the power of the signal from the tower was accounted for it is probable that this difference could be explained. At the time of this research equipment of this nature was unavailable.

Mobile phones automatically increase their power output when they lose connection to their network. To guarantee that the shields can continue to isolate the phone despite this ramped up power, time was a tested factor for this research. The results of this study show that over the course of a minute a phone was more likely to be isolated. Unknown factors in this test are how long does it take for a mobile phone to start increasing its power output and how long before it reaches maximum power. It is possible that one minute was not a long enough time interval to fully test this. Future

research should include a longer time interval or find other means to determine the amount of time needed to test a fully powered phone antenna.

Another unknown factor in this study is the receiver sensitivity and transmitter output of each of the phones that was tested. This data is not located in the user manuals for phones nor is it published on the vendor websites. The reason this is important is that it is possible that the phones used in the study have higher output and receive capabilities than the average phone currently available. This would cause the shields to appear to have a higher failure rate than an average phone would generate. Finding or determining these values would also help in creating an exact formula for determining the rate of failure for RF shielding devices.

The methodology designed for this research accomplished its goals and successfully tested the hypotheses. Future research will benefit greatly from following this model of testing. Repeating this study will allow for more generalizations to be made about the effectiveness of shielding devices to protect evidence on mobile phones. Improvements can be made to this methodology and are suggested. With the right equipment and time it should be possible to determine a formula to predict each shields performance based on distance from the tower and strength of the signal.

5.4 Improving Shields Devices

A side benefit to this study is that highlights the fact that shielding devices need to be improved. In the past few years touch screen phones have become more popular. The nature of materials used to make the shielding device causes them to be conductive. Most of the shields that were tested in this research are made from some form of copper, nickel, and silver mesh. When put into direct contact with touch screen phones the shields

would often activate buttons at random. This resulted in all sorts of activity on the phones and in a couple of cases caused the phones to dial out. This is just as problematic as the shield not isolating the phone. Now the device being used to protect evidence is altering it, and altering it in an uncontrolled unspecified manner. This too will allow attorneys to question the integrity of any evidence found on a phone.

The Black Hole Bag was the only shield tested that was designed with a clear window to allow the user to interact with the phone while it is enclosed, but it too would activate buttons without user interaction. Placing a non-conductive material between the walls of the shields may prevent accidental button activation in future shielding devices. For the Black Hole Bag or any shield intending to allow user interaction, placing a bumper between the phone and the shield will allow users to manipulate the phone while preventing accidental activations. Future tests should include using foam rubber, bubble wrap, or similar non-conductive material insert to hold the phone away from the shield walls. This will prevent the shield from accidently activating buttons on touch screen phones. It may also increase performance of the shields as there is a chance the walls of the shield can become an antennae they make direct contact with the phone's antennae.

The STP1100 was the best performing of the bag style shields used in this study. This is because it used two separate layers to make each of its walls. This allowed it to act more like a true Faraday cage. The inner layer wrapped the signal being sent out by the phones around the inside of the shield. The outer layer spread the signal from the tower across the outside of the shield. Any signal that penetrated past the first layer still had waveguide beyond cutoff point of the second layer to pass through as well. As long as the holes in the two layers are not perfectly aligned this will make it more difficult for

a radio wave to penetrate the shield. Some of the phones were still able to penetrate the STP1100 despite the advantages of its design. This may be because the two layers of the shield are in direct connection with each other. If possible, a double walled shield should be designed and tested with a nonconductive padding placed between the walls to see if it improves the performance of the shield. It is also likely the shield's walls are too thin to completely isolate the phones. This would mean that performance could be improved by increasing the depth of the wall.

5.5 Closing Remarks

As the number of mobile phones taken into custody increases, more standard operating procedures will be developed dictating that phones be isolated to protect and preserve the evidence found on them. RF isolation shields, such as the ones tested, will likely be what are used to protect evidence on a mobile phone. There are limitations to this technology and improvements are needed. It is important for anyone using these shielding devices to know what can happen and not blindly rely upon them. As things currently stand, the shields that were tested cannot be guaranteed to block all signals coming to or from the mobile phones. These experiments were intentionally conducted near high power towers where nothing could interfere with the signal. The likelihood of having a high power tower near where a phone is being seized is unknown, but it is quite possible. Future tests following an improved version of this methodology should be able to develop a formula that can accurately predict any tested shield's rate of failure. This will allow for users to determine what they can expect from their products and hopefully prevent complications from arising in court. Vendors can use this study to find where

improvements to their product can be made. Though this was a pilot study, it proves that RF shielding devices need to be verified before relying on them to preserve evidence.

LIST OF REFERENCES

LIST OF REFERENCES

Adomatis, D. (2010, Apr, 15). Using the gps for people tracking Retrieved May, 29, 2010, from http://www.travelbygps.com/articles/tracking.php

BKForensics. (2010). Solutions Retrieved Feb 5, 2010, from http://www.bkforensics.com/Mesh.html

CTIA. (2009). Wireless quick facts. *CTIA The Wireless Association* Retrieved Feb 10, 2010, from http://www.ctia.org/media/industry_info/index.cfm/AID/10323

Dankner, S., & Gupta, M. (2007). *Evidence preservation: RF signal blocking fffficiency & effect of lack of signal on a sim card*. Term Paper.

De Toffol, E. (2009). [Re: Wireless preservation].

Disklabs. (2008). FaradayBag Retrieved Sep. 6, 2010, from http://www.faradaybag.com/faraday_bag_testing.html

eDEC, & Ryan Security Technologies. (2009). Faraday-Bags.com Retrieved Aug, 28, 2010, from http://www.faraday-bags.com/index.php?option=com_content&view=article&id=2&Itemid=2

eTutorials.org. (2010). Understanding radio waves Retrieved May 30, 2010, from http://etutorials.org/Microsoft+Products/windows+xp+unwired/Chapter+1.+Wireless+Networking+Fundamentals/1.2+Understanding+Radio+Waves/

Hill, L. (2007). An inexpensive method to shield wireless devices during hardware forensic investigations in a labrotory setting. [Research Report]. *ACM*, 6.

Intel Coporation. (2001). EMI waveguide apertures. 33. Retrieved from http://www.formfactors.org/developer%5Cspecs%5Cwg_overview_098.pdf

Interpol European Working Party on IT Crime. (2006). *Good Practice Guide for Mobile Phone Seizure and Examination*.

Jansen, W., & Ayers, R. (2007). *Guidelines on cell phone forensics*.

Jansen, W., Delaitre, A., & Moenner, L. (2008). *Overcomming impediments to cell Phone forensics*.

JEITA. (2002). Exif2-2.pdf *4.6.4 TIFF Rev. 6.0 Attribute Information* (pp. 148). exif.org: JEITA.

Kessler, G. (2009). *Cell phone analysis: technology, tools, and processes*. Paper presented at the Mobile Forensics World 2009, Chicago. http://msdim.champlain.edu/PD/public/CellPhone_200905_ICAC-sanitized.pdf

Kubasiak, R., & Morrissey, S. (Eds.). (2009). *Mac os x, ipod, and iphone forensic analysis dvd toolkit* (551 ed.). Burlington: Syngress Publishing Inc.

Kurtis, R. (2008, Jan. 5th, 2008). Waves and obstacles Retrieved May, 30, 2010, from http://www.schoolforchampions.com/science/waves_obstacle.htm

L-com, I. (2010). 2.4ghz dbi dual diversity antenna. *L-Com Global Cnnectivity* Retrieved Dec. 1, 2010, from http://www.l-com.com/item.aspx?ID=20308

Lesemann, D., & Mahalik, H. (2008). Dialing up and drilling down: Forensic preservation of handheld devices. [Journal]. *Information Security Systems Association Journal*.

Lewis, D. (2009). Examing cellular phones and handheld devices. *Forensic Magazine*(August/September 2009), 4.

Leyden, J. (2001). How to crash a phone by sms. *The Register*. Retrieved from http://www.theregister.co.uk/2001/11/28/how_to_crash_a_phone/

Majors, S. (2009). Ohio justices: Cell phone searches require warrant. *The New York Times*. Retrieved from NYTimes.com

Marcinkoski, J. (2008, 10/01/08). [Re: Cell phones and the fourth amendment].

McPhee, M., Schabner, D., & Battiste, N. (2010). 'Craigslist killer' philip markoff commits suicide Retrieved Sep 6, 2010, from http://abcnews.go.com/US/craigslist-killer-phillip-markoff-commits-suicide/story?id=11405484

Mislan, R., Casey, E., & Kessler, G. (2010). *The growing need for on-scene triage of mobile devices*, 6(3-4), 112-124 Retreived from 4YXKFT5-2&_user=10&_coverDate=05%2F31%2F2010&_rdoc=1&_fmt=high&_orig=search&_origin=search&_sort=d&_docanchor=&view=c&_acct=C000050221&_version=1&_urlVersion=0&_userid=10&md5=d5c013c0b1c4380e14e5baac7f0b3f28&searchtype=a

Murphy, T. (2010). Faraday cage. *Magnet Lab* Retrieved Feb 5, 2010, from http://www.magnet.fsu.edu/education/tutorials/tools/faradaycage.html

National Instruments Corporation. (200(). Is-95 (cdma) and gsm (tdma). *NI Developer Zone* Retrieved Dec 6, 2010, from http://sone.ni.com/devzone/cda/tut/p/id/7107

O'Brien, T. (2008). What do cell phone signal bars really, really mean Retrieved Sep. 9, 2009, from http://www.switched.com/2008/01/15/what-do-cell-phone-signal-bars-really-really-mean/

Paraben Corporation. (2007). Paraben's wireless stronghold bag. *Paraben Forensic Tools* Retrieved Feb 5, 2010, from http://www.paraben.com/catalog/product_info.php?products_id=173

Phillips, R. (2008). Suspects in video beating could get life in prison. *CNN.com*. Retrieved from http://www.cnn.com/2008/CRIME/04/10/girl.fights/

Punja, S., & Mislan, R. (2008). Mobile device analysis. *Small Scale Digital Device Forensics Journal, 2*(1). Retrieved from http://www.ssddfj.org/papers/SSDDFJ_V2_1_Punja_Mislan.pdf

Research in Motion. (2010). Blackberry enterprise server express features Retrieved Feb. 2, 2010, from http://na.blackberry.com/eng/services/business/server/express/features.jsp#tab_tab_security

Rogers, G., & Edwards, J. (2003). *An introduction to wireless technology* (1st ed.). Upper Saddle River: Prentice Hall.

Rogers, M. (2009). Digital evidence triage: Financial services training series (pp. 386). West Lafayette: Purdue University Cyber Foreniscs.

Scientific Working Group on Digital Evidence. (2009). *Best practices for mobile phone examinations*. SWGDE Retrieved from http://www.swgde.org/documents/swgde2009/Best%20Practices%20for%20Mobile%20Phone%20Examinations%20v1.0.pdf.

Smith, C., & Collins, D. (2007). *3g wireless networks* (Second ed.). New York: McGraw-Hill.

Stallings, W. (2005). *Wireless communications & networks* (2nd ed.). Upper Saddle River: Pearson: Prentice Hall.

TechTarget. (2008, May 07, 2008). Whatis?com. *noise* Retrieved Sep 6, 2010, from http://WhatIs.techtarget.com/definition/0,,sid9_gci212667,00.html

TechTarget. (2010, Aug 3, 2009). Whatis?com. *signal-to-noise ratio* Retrieved Sep 6, 2010, from http://searchnetworking.techtarget.com/sDefinition/0,,sid7_gci213018,00.html

TEELtechnologies. (2010). Ramsey 4500 z Retrieved Feb 2, 2010, from http://www.teeltech.com/tt3/ramsey_ste-zrt.asp

The National Campaign to Prevent Teen Pregnancy. (2008). Sex and tech: Results from a nationally represenative survey of teens and young adults (pp. 19): The National Campaign to Prevent Teen Pregnancy.

Willassen, S. (2005). Forensic analysis of mobile phone internal memory. 23. Retrieved from

Wolfe, J. (1998). dB: What is a decibel? Retrieved Sep 9, 2009, from http://www.phys.unsw.edu.au/jw/dB.html

Zdziarski, J. (2010). *Forensic investigative methods for the iphone, iphone 3g, and iphone 3g[s]*. Technical Review Draft.

APPENDIX

APPENDIX

Table A-1.1 eDEC Black Hole Bag - Base of the Tower

Black Hole	**Voice Calls**					**MMS**					**SMS**				
	0s	15s	30s	45s	60s	0s	15s	30s	45s	60s	0s	15s	30s	45s	60s
AT&T															
Apple iPhone 3Gs	F	F	F	F	F	NA	NA	NA	NA	NA	F	F	F	F	F
BlackBerry Curve 9300	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
Palm Pixi Plus	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
Sprint															
BlackBerry Curve 8330	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
HTC Hero 2	F	P	P	P	P	F	P	P	P	P	F	F	F	F	P
Motorola Clutch i465	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
Palm Pixi	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
Samsung Galaxy S	F	F	F	F	P	P	P	P	P	P	F	F	F	F	F
Verizon															
Casio G'zOne Ravine	P	P	P	P	P	F	F	F	F	F	F	F	F	F	F
HTC Droid Eris	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
HTC Imagio	F	F	F	F	F	NA	NA	NA	NA	NA	F	F	F	F	F
HTC Droid 2	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F

Table A-1.2 eDEC Black Hole Bag- 100'

Black Hole 100ft	Voice Calls					MMS					SMS				
	0s	15s	30s	45s	60s	0s	15s	30s	45s	60s	0s	15s	30s	45s	60s
AT&T															
Apple iPhone 3Gs	F	F	F	F	F	NA	NA	NA	NA	NA	F	F	F	F	F
BlackBerry Curve 9300	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
Palm Pixi Plus	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
Sprint															
BlackBerry Curve 8330	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
HTC Hero 2	P	P	P	P	P	P	P	P	P	P	F	P	P	P	P
Motorola Clutch i465	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
Palm Pixi	F	F	P	P	P	P	P	P	P	P	F	F	F	P	P
Samsung Galaxy S	F	P	P	P	P	P	P	P	P	P	F	F	F	F	F
Verizon															
Casio G'zOne Ravine	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
HTC Droid Eris	F	F	F	F	P	F	F	F	F	F	F	F	F	F	F
HTC Imagio	F	F	F	F	F	NA	NA	NA	NA	NA	F	F	F	F	F
HTC Droid 2	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F

Table A-1.3 eDEC Black Hole Bag - 150'

Black Hole 150ft	**Voice Calls**					**MMS**					**SMS**				
	0s	15s	30s	45s	60s	0s	15s	30s	45s	60s	0s	15s	30s	45s	60s
AT&T															
Apple iPhone 3Gs	F	F	F	F	F	NA	NA	NA	NA	NA	F	F	F	F	F
BlackBerry Curve 9300	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
Palm Pixi Plus	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
Sprint															
BlackBerry Curve 8330	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
HTC Hero 2	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
Motorola Clutch i465	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
Palm Pixi	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
Samsung Galaxy S	F	P	P	P	P	P	P	P	P	P	P	P	P	P	P
Verizon															
Casio G'zOne Ravine	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
HTC Droid Eris	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
HTC Imagio	F	F	F	F	F	NA	NA	NA	NA	NA	F	F	F	F	F
HTC Droid 2	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F

Table A-1.4 eDEC Black Hole Bag - 200'

Black Hole 200ft	**Voice Calls**					**MMS**					**SMS**				
	0s	15s	30s	45s	60s	0s	15s	30s	45s	60s	0s	15s	30s	45s	60s
AT&T															
Apple iPhone 3Gs	F	F	F	F	F	NA	NA	NA	NA	NA	F	F	F	F	F
BlackBerry Curve 9300	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
Palm Pixi Plus	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
Sprint															
BlackBerry Curve 8330	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
HTC Hero 2	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
Motorola Clutch i465	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
Palm Pixi	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
Samsung Galaxy S	F	P	P	P	P	P	P	P	P	P	P	P	P	P	P
Verizon															
Casio G'zOne Ravine	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
HTC Droid Eris	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
HTC Imagio	F	F	F	F	F	NA	NA	NA	NA	NA	F	F	F	F	F
HTC Droid 2	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F

Table A-1.5 eDEC Black Hole Bag - 500'

Black Hole 500ft	**Voice Calls**					**MMS**					**SMS**				
	0s	15s	30s	45s	60s	0s	15s	30s	45s	60s	0s	15s	30s	45s	60s
AT&T															
Apple iPhone 3Gs	P	P	P	P	P	NA	NA	NA	NA	NA	P	P	P	P	P
BlackBerry Curve 9300	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
Palm Pixi Plus	F	F	F	F	F	P	P	P	P	P	F	F	F	F	F
Sprint															
BlackBerry Curve 8330	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
HTC Hero 2	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
Motorola Clutch i465	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
Palm Pixi	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
Samsung Galaxy S	F	P	P	P	P	P	P	P	P	P	P	P	P	P	P
Verizon															
Casio G'zOne Ravine	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
HTC Droid Eris	F	F	F	F	F	P	P	P	P	P	F	F	F	F	F
HTC Imagio	P	P	P	P	P	P	NA	NA	NA	NA	F	F	F	F	F
HTC Droid 2	F	F	F	F	F	P	F	F	F	F	F	F	F	F	F

Table A-2.1 LessEMF High Performance Silver Mesh - Base of the Tower

LessEMF	Voice Calls					MMS					SMS				
	0s	15s	30s	45s	60s	0s	15s	30s	45s	60s	0s	15s	30s	45s	60s
AT&T															
Apple iPhone 3Gs	F	F	F	F	F	NA	NA	NA	NA	NA	F	F	F	F	F
BlackBerry Curve 9300	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
Palm Pixi Plus	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
Sprint															
BlackBerry Curve 8330	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
HTC Hero 2	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
Motorola Clutch i465	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
Palm Pixi	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
Samsung Galaxy S	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
Verizon															
Casio G'zOne Ravine	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
HTC Droid Eris	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
HTC Imagio	F	F	F	F	F	NA	NA	NA	NA	NA	F	F	F	F	F
HTC Droid 2	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F

Table A-2.2 LessEMF High Performance Silver Mesh - 100'

LessEMF 100ft	**Voice Calls**					**MMS**					**SMS**				
	0s	15s	30s	45s	60s	0s	15s	30s	45s	60s	0s	15s	30s	45s	60s
AT&T															
Apple iPhone 3Gs	F	F	F	F	F	NA	NA	NA	NA	NA	F	F	F	F	F
BlackBerry Curve 9300	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
Palm Pixi Plus	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
Sprint															
BlackBerry Curve 8330	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
HTC Hero 2	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
Motorola Clutch i465	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
Palm Pixi	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
Samsung Galaxy S	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
Verizon															
Casio G'zOne Ravine	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
HTC Droid Eris	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
HTC Imagio	F	F	F	F	F	NA	NA	NA	NA	NA	F	F	F	F	F
HTC Droid 2	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F

Table A-2.3 LessEMF High Performance Silver Mesh - 150'

LessEMF 150ft	Voice Calls					MMS					SMS				
	0s	15s	30s	45s	60s	0s	15s	30s	45s	60s	0s	15s	30s	45s	60s
AT&T															
Apple iPhone 3Gs	F	F	F	F	F	NA	NA	NA	NA	NA	F	F	F	F	F
BlackBerry Curve 9300	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
Palm Pixi Plus	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
Sprint															
BlackBerry Curve 8330	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
HTC Hero 2	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
Motorola Clutch i465	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
Palm Pixi	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
Samsung Galaxy S	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
Verizon															
Casio G'zOne Ravine	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
HTC Droid Eris	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
HTC Imagio	F	F	F	F	F	NA	NA	NA	NA	NA	F	F	F	F	F
HTC Droid 2	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F

Table A-2.4 LessEMF High Performance Silver Mesh - 200'

Less EMF 200ft	**Voice Calls**					**MMS**					**SMS**				
	0s	15s	30s	45s	60s	0s	15s	30s	45s	60s	0s	15s	30s	45s	60s
AT&T															
Apple iPhone 3Gs	F	F	F	F	F	NA	NA	NA	NA	NA	F	F	F	F	F
BlackBerry Curve 9300	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
Palm Pixi Plus	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
Sprint															
BlackBerry Curve 8330	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
HTC Hero 2	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
Motorola Clutch i465	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
Palm Pixi	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
Samsung Galaxy S	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
Verizon															
Casio G'zOne Ravine	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
HTC Droid Eris	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
HTC Imagio	F	F	F	F	F	NA	NA	NA	NA	NA	F	F	F	F	F
HTC Droid 2	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F

Table A-2.5 LessEMF High Performance Silver Mesh - 500'

LessEMF 500ft	**Voice Calls**					**MMS**					**SMS**				
	0s	15s	30s	45s	60s	0s	15s	30s	45s	60s	0s	15s	30s	45s	60s
AT&T															
Apple iPhone 3Gs	F	F	F	F	F	NA	NA	NA	NA	NA	F	F	F	F	F
BlackBerry Curve 9300	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
Palm Pixi Plus	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
Sprint															
BlackBerry Curve 8330	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
HTC Hero 2	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
Motorola Clutch i465	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
Palm Pixi	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
Samsung Galaxy S	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
Verizon															
Casio G'zOne Ravine	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
HTC Droid Eris	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
HTC Imagio	F	F	F	F	F	NA	NA	NA	NA	NA	F	F	F	F	F
HTC Droid 2	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F

Table A-3.1 MWT Material Wireless Isolation Bag - the Base of the Tower

MWT	Voice Calls					MMS					SMS				
	0s	15s	30s	45s	60s	0s	15s	30s	45s	60s	0s	15s	30s	45s	60s
AT&T															
Apple iPhone 3Gs	F	F	F	F	F	NA	NA	NA	NA	NA	F	F	F	F	F
BlackBerry Curve 9300	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
Palm Pixi Plus	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
Sprint															
BlackBerry Curve 8330	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
HTC Hero 2	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
Motorola Clutch i465	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
Palm Pixi	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
Samsung Galaxy S	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
Verizon															
Casio G'zOne Ravine	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
HTC Droid Eris	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
HTC Imagio	F	F	F	F	F	NA	NA	NA	NA	NA	F	F	F	F	F
HTC Droid 2	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F

Table A-3.2 MWT Material Wireless Isolation Bag - 100'

MWT 100ft	Voice Calls					MMS					SMS				
	0s	15s	30s	45s	60s	0s	15s	30s	45s	60s	0s	15s	30s	45s	60s
AT&T															
Apple iPhone 3Gs	F	F	F	F	F	NA	NA	NA	NA	NA	F	F	F	F	F
BlackBerry Curve 9300	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
Palm Pixi Plus	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
Sprint															
BlackBerry Curve 8330	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
HTC Hero 2	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
Motorola Clutch i465	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
Palm Pixi	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
Samsung Galaxy S	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
Verizon															
Casio G'zOne Ravine	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
HTC Droid Eris	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
HTC Imagio	F	F	F	F	F	NA	NA	NA	NA	NA	F	F	F	F	F
HTC Droid 2	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F

Table A-3.2 MWT Material Wireless Isolation Bag - 150'

MWT 150ft	Voice Calls					MMS					SMS				
	0s	15s	30s	45s	60s	0s	15s	30s	45s	60s	0s	15s	30s	45s	60s
AT&T															
Apple iPhone 3Gs	F	F	F	F	F	NA	NA	NA	NA	NA	F	F	F	F	F
BlackBerry Curve 9300	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
Palm Pixi Plus	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
Sprint															
BlackBerry Curve 8330	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
HTC Hero 2	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
Motorola Clutch i465	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
Palm Pixi	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
Samsung Galaxy S	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
Verizon															
Casio G'zOne Ravine	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
HTC Droid Eris	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
HTC Imagio	F	F	F	F	F	NA	NA	NA	NA	NA	F	F	F	F	F
HTC Droid 2	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F

Table A-3.4 MWT Material Wireless Isolation Bag - 200'

MWT 200ft	Voice Calls					MMS					SMS				
	0s	15s	30s	45s	60s	0s	15s	30s	45s	60s	0s	15s	30s	45s	60s
AT&T															
Apple iPhone 3Gs	F	F	F	F	F	NA	NA	NA	NA	NA	F	F	F	F	F
BlackBerry Curve 9300	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
Palm Pixi Plus	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
Sprint															
BlackBerry Curve 8330	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
HTC Hero 2	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
Motorola Clutch i465	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
Palm Pixi	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
Samsung Galaxy S	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
Verizon															
Casio G'zOne Ravine	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
HTC Droid Eris	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
HTC Imagio	F	F	F	F	F	NA	NA	NA	NA	NA	F	F	F	F	F
HTC Droid 2	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F

Table A-3.5 MWT Material Wireless Isolation Bag - 500'

MWT 500ft	Voice Calls					MMS					SMS				
	0s	15s	30s	45s	60s	0s	15s	30s	45s	60s	0s	15s	30s	45s	60s
AT&T															
Apple iPhone 3Gs	F	F	F	F	F	NA	NA	NA	NA	NA	F	F	F	F	F
BlackBerry Curve 9300	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
Palm Pixi Plus	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
Sprint															
BlackBerry Curve 8330	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
HTC Hero 2	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
Motorola Clutch i465	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
Palm Pixi	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
Samsung Galaxy S	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
Verizon															
Casio G'zOne Ravine	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
HTC Droid Eris	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
HTC Imagio	F	F	F	F	F	NA	NA	NA	NA	NA	F	F	F	F	F
HTC Droid 2	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F

Table A-4.1 Paraben StrongHold Bag - Base of the Tower

Paraben	Voice Calls					MMS					SMS				
	0s	15s	30s	45s	60s	0s	15s	30s	45s	60s	0s	15s	30s	45s	60s
AT&T															
Apple iPhone 3Gs	F	F	F	F	F	NA	NA	NA	NA	NA	F	F	F	F	F
BlackBerry Curve 9300	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
Palm Pixi Plus	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
Sprint															
BlackBerry Curve 8330	F	P	P	P	P	P	P	P	P	P	P	P	P	P	P
HTC Hero 2	F	F	F	F	P	F	F	P	P	P	F	F	F	F	F
Motorola Clutch i465	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
Palm Pixi	F	F	F	F	F	P	P	P	P	P	F	F	F	F	F
Samsung Galaxy S	P	P	P	P	P	P	P	P	P	P	P	F	P	P	P
Verizon															
Casio G'zOne Ravine	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
HTC Droid Eris	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
HTC Imagio	F	F	F	F	F	NA	NA	NA	NA	NA	F	F	F	F	F
HTC Droid 2	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F

Table A-4.2 Paraben StrongHold Bag- 100'

Paraben 100ft	Voice Calls					MMS					SMS				
	0s	15s	30s	45s	60s	0s	15s	30s	45s	60s	0s	15s	30s	45s	60s
AT&T															
Apple iPhone 3Gs	F	F	F	F	F	NA	NA	NA	NA	NA	F	F	F	F	F
BlackBerry Curve 9300	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
Palm Pixi Plus	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
Sprint															
BlackBerry Curve 8330	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
HTC Hero 2	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
Motorola Clutch i465	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
Palm Pixi	F	F	F	F	F	P	P	P	P	P	F	F	F	F	F
Samsung Galaxy S	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
Verizon															
Casio G'zOne Ravine	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
HTC Droid Eris	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
HTC Imagio	F	F	F	F	F	NA	NA	NA	NA	NA	F	F	F	F	F
HTC Droid 2	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F

Table A-4.3 Paraben StrongHold Bag – 150’

Paraben 150ft	Voice Calls					MMS					SMS				
	0s	15s	30s	45s	60s	0s	15s	30s	45s	60s	0s	15s	30s	45s	60s
AT&T															
Apple iPhone 3Gs	F	F	F	F	F	NA	NA	NA	NA	NA	F	F	F	F	F
BlackBerry Curve 9300	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
Palm Pixi Plus	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
Sprint															
BlackBerry Curve 8330	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
HTC Hero 2	F	F	F	F	F	F	F	F	F	P	F	F	F	F	F
Motorola Clutch i465	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
Palm Pixi	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
Samsung Galaxy S	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
Verizon															
Casio G'zOne Ravine	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
HTC Droid Eris	F	F	F	F	F	P	P	P	P	P	F	F	F	F	F
HTC Imagio	F	F	F	F	F	NA	NA	NA	NA	NA	F	F	F	F	F
HTC Droid 2	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F

Table A-4.4 Paraben StrongHold Bag - 200'

Paraben 200ft	Voice Calls					MMS					SMS				
	0s	15s	30s	45s	60s	0s	15s	30s	45s	60s	0s	15s	30s	45s	60s
AT&T															
Apple iPhone 3Gs	F	F	F	F	F	NA	NA	NA	NA	NA	F	F	F	F	F
BlackBerry Curve 9300	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
Palm Pixi Plus	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
Sprint															
BlackBerry Curve 8330	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
HTC Hero 2	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
Motorola Clutch i465	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
Palm Pixi	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
Samsung Galaxy S	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
Verizon															
Casio G'zOne Ravine	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
HTC Droid Eris	F	F	F	F	F	P	P	P	P	P	F	F	F	F	F
HTC Imagio	F	F	F	F	F	NA	NA	NA	NA	NA	F	F	F	F	F
HTC Droid 2	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F

Table A-4.5 Paraben StrongHold Bag - 500'

Paraben 500ft	Voice Calls					MMS					SMS				
	0s	15s	30s	45s	60s	0s	15s	30s	45s	60s	0s	15s	30s	45s	60s
AT&T															
Apple iPhone 3Gs	F	F	F	F	F	NA	NA	NA	NA	NA	F	F	F	F	F
BlackBerry Curve 9300	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
Palm Pixi Plus	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
Sprint															
BlackBerry Curve 8330	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
HTC Hero 2	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
Motorola Clutch i465	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
Palm Pixi	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
Samsung Galaxy S	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
Verizon															
Casio G'zOne Ravine	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
HTC Droid Eris	F	F	F	F	F	P	P	P	P	P	F	F	F	F	F
HTC Imagio	F	F	F	F	F	NA	NA	NA	NA	NA	F	F	F	F	F
HTC Droid 2	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F

Table A-5.1 Ramsey STE3600 - Base of the Tower

Box	Voice Calls					MMS					SMS				
	0s	15s	30s	45s	60s	0s	15s	30s	45s	60s	0s	15s	30s	45s	60s
AT&T															
Apple iPhone 3Gs	P	P	P	P	P	NA	NA	NA	NA	NA	P	P	P	P	P
BlackBerry Curve 9300	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
Palm Pixi Plus	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
Sprint															
BlackBerry Curve 8330	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
HTC Hero 2	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
Motorola Clutch i465	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
Palm Pixi	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
Samsung Galaxy S	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
Verizon															
Casio G'zOne Ravine	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
HTC Droid Eris	P	P	P	P	P	P	P	P	P	P	F	P	P	P	P
HTC Imagio	P	P	P	P	P	NA	NA	NA	NA	NA	P	P	P	P	P
HTC Droid 2	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P

Table A-5.2 Ramsey STE3600 – 100’

Box 100ft	Voice Calls					MMS					SMS				
	0s	15s	30s	45s	60s	0s	15s	30s	45s	60s	0s	15s	30s	45s	60s
AT&T															
Apple iPhone 3Gs	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
BlackBerry Curve 9300	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
Palm Pixi Plus	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
Sprint															
BlackBerry Curve 8330	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
HTC Hero 2	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
Motorola Clutch i465	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
Palm Pixi	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
Samsung Galaxy S	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
Verizon															
Casio G'zOne Ravine	F	F	F	F	F	P	P	P	P	P	P	P	P	P	P
HTC Droid Eris	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
HTC Imagio	P	P	P	P	P	NA	NA	NA	NA	NA	P	P	P	P	P
HTC Droid 2	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P

Table A-5.3 Ramsey STE3600 - 150'

Box 150ft	Voice Calls					MMS					SMS				
	0s	15s	30s	45s	60s	0s	15s	30s	45s	60s	0s	15s	30s	45s	60s
AT&T															
Apple iPhone 3Gs	P	P	P	P	P	NA	NA	NA	NA	NA	P	P	P	P	P
BlackBerry Curve 9300	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
Palm Pixi Plus	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
Sprint															
BlackBerry Curve 8330	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
HTC Hero 2	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
Motorola Clutch i465	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
Palm Pixi	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
Samsung Galaxy S	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
Verizon															
Casio G'zOne Ravine	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
HTC Droid Eris	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
HTC Imagio	P	P	P	P	P	NA	NA	NA	NA	NA	P	P	P	P	P
HTC Droid 2	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P

Table A-5.4 Ramsey STE3600 - 200'

Box 200ft	Voice Calls					MMS					SMS				
	0s	15s	30s	45s	60s	0s	15s	30s	45s	60s	0s	15s	30s	45s	60s
AT&T															
Apple iPhone 3Gs	P	P	P	P	P	NA	NA	NA	NA	NA	P	P	P	P	P
BlackBerry Curve 9300	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
Palm Pixi Plus	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
Sprint															
BlackBerry Curve 8330	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
HTC Hero 2	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
Motorola Clutch i465	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
Palm Pixi	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
Samsung Galaxy S	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
Verizon															
Casio G'zOne Ravine	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
HTC Droid Eris	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
HTC Imagio	P	P	P	P	P	NA	NA	NA	NA	NA	P	P	P	P	P
HTC Droid 2	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P

Table A-5.5 Ramsey STE3600 -

Box 500ft	Voice Calls					MMS					SMS				
	0s	15s	30s	45s	60s	0s	15s	30s	45s	60s	0s	15s	30s	45s	60s
AT&T															
Apple iPhone 3Gs	P	P	P	P	P	NA	NA	NA	NA	NA	P	P	P	P	P
BlackBerry Curve 9300	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
Palm Pixi Plus	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
Sprint															
BlackBerry Curve 8330	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
HTC Hero 2	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
Motorola Clutch i465	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
Palm Pixi	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
Samsung Galaxy S	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
Verizon															
Casio G'zOne Ravine	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
HTC Droid Eris	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
HTC Imagio	P	P	P	P	P	NA	NA	NA	NA	NA	P	P	P	P	P
HTC Droid 2	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P

Table A-6.1 Ramsey STP1100 - Base of the Tower

Ramsey Bag	Voice Calls					MMS					SMS				
	0s	15s	30s	45s	60s	0s	15s	30s	45s	60s	0s	15s	30s	45s	60s
AT&T															
Apple iPhone 3Gs	P	P	P	P	P	NA	NA	NA	NA	NA	P	P	P	P	P
BlackBerry Curve 9300	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
Palm Pixi Plus	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
Sprint															
BlackBerry Curve 8330	F	P	P	P	P	P	P	P	P	P	F	F	F	F	F
HTC Hero 2	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
Motorola Clutch i465	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
Palm Pixi	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
Samsung Galaxy S	F	P	P	P	P	F	F	P	P	P	F	F	P	P	P
Verizon															
Casio G'zOne Ravine	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
HTC Droid Eris	P	P	P	P	P	P	P	P	P	P	F	F	F	F	F
HTC Imagio	P	P	P	P	P	NA	NA	NA	NA	NA	F	F	F	F	F
HTC Droid 2	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P

Table A-6.2 Ramsey STP1100- 100'

Ramsey Bag 100ft	**Voice Calls**					**MMS**					**SMS**				
	0s	15s	30s	45s	60s	0s	15s	30s	45s	60s	0s	15s	30s	45s	60s
AT&T															
Apple iPhone 3Gs	P	P	P	P	P	NA	NA	NA	NA	NA	P	P	P	P	P
BlackBerry Curve 9300	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
Palm Pixi Plus	F	F	F	F	F	P	P	P	P	P	F	F	F	F	F
Sprint															
BlackBerry Curve 8330	F	P	P	P	P	P	P	P	P	P	F	P	P	P	P
HTC Hero 2	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
Motorola Clutch i465	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
Palm Pixi	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
Samsung Galaxy S	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
Verizon															
Casio G'zOne Ravine	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
HTC Droid Eris	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
HTC Imagio	P	P	P	P	P	NA	NA	NA	NA	NA	P	P	P	P	P
HTC Droid 2	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P

Table A-6.3 Ramsey STP1100 – 150’

Ramsey Bag 150ft	**Voice Calls**					**MMS**					**SMS**				
	0s	15s	30s	45s	60s	0s	15s	30s	45s	60s	0s	15s	30s	45s	60s
AT&T															
Apple iPhone 3Gs	P	P	P	P	P	NA	NA	NA	NA	NA	P	P	P	P	P
PlackPerry Curve	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
Palm Pixi Plus	F	F	F	F	F	P	P	P	P	P	F	F	F	F	F
Sprint															
BlackBerry Curve 8330	F	P	P	P	P	F	P	P	P	P	F	F	P	P	P
HTC Hero 2	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
Motorola Clutch i465	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
Palm Pixi	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
Samsung Galaxy S	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
Verizon															
Casio G'zOne Ravine	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
HTC Droid Eris	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
HTC Imagio	P	P	P	P	P	NA	NA	NA	NA	NA	P	P	P	P	P
HTC Droid 2	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P

Table A-6.4 Ramsey STP1100 - 200'

Ramsey Bag 200ft	**Voice Calls**					**MMS**					**SMS**				
	0s	15s	30s	45s	60s	0s	15s	30s	45s	60s	0s	15s	30s	45s	60s
AT&T															
Apple iPhone 3Gs	P	P	P	P	P	NA	NA	NA	NA	NA	P	P	P	P	P
BlackBerry Curve 9300	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
Palm Pixi Plus	F	F	F	F	F	P	P	P	P	P	F	F	F	F	F
Sprint															
BlackBerry Curve 8330	F	P	P	P	P	F	P	P	P	P	F	P	P	P	P
HTC Hero 2	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
Motorola Clutch i465	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
Palm Pixi	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
Samsung Galaxy S	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
Verizon															
Casio G'zOne Ravine	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
HTC Droid Eris	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
HTC Imagio	P	P	P	P	P	NA	NA	NA	NA	NA	P	P	P	P	P
HTC Droid 2	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P

Table A-6.5 Ramsey STP1100 - 500'

Ramsey Bag 500ft	**Voice Calls**					**MMS**					**SMS**				
	0s	15s	30s	45s	60s	0s	15s	30s	45s	60s	0s	15s	30s	45s	60s
AT&T															
Apple iPhone 3Gs	P	P	P	P	P	NA	NA	NA	NA	NA	P	P	P	P	P
BlackBerry Curve 9300	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
Palm Pixi Plus	F	P	P	P	P	P	P	P	P	P	F	P	P	P	P
Sprint															
BlackBerry Curve 8330	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
HTC Hero 2	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
Motorola Clutch i465	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
Palm Pixi	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
Samsung Galaxy S	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
Verizon															
Casio G'zOne Ravine	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
HTC Droid Eris	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
HTC Imagio	P	P	P	P	P	NA	NA	NA	NA	NA	P	P	P	P	P
HTC Droid 2	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P