Admissibility of Small Scale Digital Devices in U.S. Civil Litigation

Rebecca Hendricks

***Abstract*—Amendments to The Federal Rules of Civil Procedure which went into effect on December 1, 2006 clearly address Electronically Stored Information ("ESI") and that includes ESI found on small scale digital devices, such as cell phones and Personal Digital Assistants (PDAs). Failure to address ESI on small scale digital devices can lead to spoliation claims when these devices may contain relevant ESI.**

***Index Terms*—small scale digital devices, digital forensics, electronically stored information, FRCP, Federal Rules of Civil Procedure, cell phone, mobile device, mobile phone**

I. Technology is Prevalent

TECHNOLOGY-BASED tools aid in the way humans communicate. The components of technology-based communication, such as the message content, message recipient, message sender, and transport mechanism, as well as all other components, can be stored electronically. As a result of being electronically stored, the information can be preserved and reviewed for authenticity. Within the realm of the United States judicial system, the authentication of electronically stored information ("ESI") becomes critical when pursuing the truth in resolving civil disagreements.

A variety of technological tools are available to aid in communication. While electronic mail may first come to mind, the use of small scale digital devices, such as cell phones, is quickly dominating the United States. "The penetration rate for cell phones in the U.S. is a lofty 81.5%, according to market researcher iSuppli Corp." [10].

Electronic mail, names and addresses, calendar items, notes, and journal entries are just a few of the electronic data types which can be stored on a small scale device. On December 1, 2006, the Federal Rules of Civil Procedure (FRCP) were amended to specifically address electronically stored information [11]. The definition of electronically stored information must be "flexible enough to encompass future changes and developments" in technology [12]. Given that information is electronically stored on cell phones and other small scale digital devices, the ESI contained on those devices is subject to the rules of discovery in legal matters. In Craig Ball's 2006 article titled *Hitting the High Points of the New EDD Rules*, he writes, the upshot of the new Rules is that:

- ESI is discoverable
- Litigants must preserve and produce ESI
- Lawyers must understand how to request, protect, review and produce ESI
- The courts have the tools to rectify abusive or obstructive electronic discovery

In particular, Rule 16 of the Federal Rules of Civil Procedure requires that parties, at the outset of litigation, address ESI issues [11]. Parties are to "meet and confer" to discuss ESI and are to address ESI in their initial disclosures. The rules clearly indicate ESI must be identified, including ESI on cell phones and other small scale digital devices, such as Personal Digital Assistants (PDAs). ESI should be cataloged and disclosed to the other party. Quite often, parties are struggling to catalog ESI found in traditional locations, such as desktops, laptops, and network servers. It can be common to overlook ESI found on small scale digital devices, which includes cell phones and PDAs. That oversight can prove costly. Overlooking ESI, relevant to the litigation matter, on any device, including small scale digital devices, can lead to evidentiary spoliation claims. When ESI is not properly preserved, the continued use of any devices which contain the ESI will lead to the modification, alteration or deletion of potentially relevant ESI.

II. Admissibility Standards Exist

There are two basic evidentiary tests used in the United States legal system, The Frye Test [7] and The Daubert Test [5]. In the last fifty years, courts have been faced with the admissibility of more sophisticated scientific evidence. The standard test for admissibility of expert witness testimony and its accompanying lab data used by both federal and state courts from 1923 until 1993 was based on Frye v. United States, 293 F. 1013 (D.C. Cir. 1923). The court announced that a novel scientific technique "must be sufficiently established to have gained general acceptance in the particular field in which it belongs" (p. 1014). This conservative approach was the principal legal test for evidentiary admissibility through 1975 when the "Federal Rules of Evidence" were adopted. Federal judges were granted more discretion in determining the admissibility of evidence.

- Rule 104(a) assigns judges the responsibility of making a preliminary determination on allowing an expert to testify.
- Rule 702 requires the judge to determine whether the admission of such testimony will assist the trier of fact to understand evidence or determine a fact at issue.
- Rule 403 allows the judge to exclude evidence if it's likely prejudicial effect outweighs its probative value.

The Frye test survived until 1993 when the Supreme Court issued a new opinion. This new opinion was considered more liberal and became the new standard for testing admissibility of evidence in the Federal Judicial system. Since it was

Fig. 1. Geographical Map of Frye Versus Daubert States /citeChengal2005

announced by the Supreme Court in 1993, *Daubert v. Merrell Dow Pharmaceuticals*, Inc. has become the foundational opinion in the modern law of scientific evidence [4].

In *Daubert v. Merrell Dow Pharmaceuticals*, 509 U.S. 579 (1993), the Court suggested the following four factors to be considered in assessing the reliability of expert testimony:

1) Whether a "theory or technique ... can be (and has been) tested";
2) Whether the theory or technique "has been subjected to peer review and publication";
3) Whether, in respect to a particular technique, there is a high "known or potential rate of error" and whether there are "standards controlling the technique's operation"; and
4) Whether the theory or technique enjoys "general acceptance" within a "relevant scientific community."

In Federal court, The Daubert Test is used. State courts have their own discretion on admissibility tests. Some state courts have accepted The Daubert Test, some have continued to use The Frye Test and other states have adopted their own tests for determining the legal admissibility of evidence. While some exceptions do apply, Figure 1 generally represents which admissibility tests are accepted by the United States state courts.

The Federal Rules of Civil Procedure, which were amended on December 1, 2006, require that electronically stored information be addressed in litigation matters. Both federal and state courts have well established precedents for how evidence should be handled and admissibility rules for the evidence and subsequent testimony of experts. The very rules which apply to admissibility of *evidence* also, apply to the admissibility of evidence harvested from small scale digital devices.

When admissibility in court is the ultimate goal for the electronic evidence, steps should be taken to ensure the evidentiary collection, examination, analysis and production methods can withstand a challenge under the Rules of Evidence. In particular, a civil matter in Federal court should be able to withstand the scrutiny of the Daubert Test. Some investigative instances will occur in which court admissibility is not the objective. The term "mobile phone exploitation," coined by Richard Mislan at the Purdue University Cyber Forensics Lab, can be used to describe the intended deviation from methods which can withstand admissibility tests such as Frye or Daubert.

III. Small Scale Digital Devices are Challenging

There are many challenges facing the forensic examination of a small scale digital device. In 2007, the Scientific Working Group on Digital Evidence (SWGDE) published *Special Considerations When Dealing With Cellular Telephones* which included the following limitations:

- **Cables** - access cables are often unique to a particular device.
- **Passwords** - passwords can restrict access to a device. Traditional password cracking methods can lead to permanent inaccessibility of data.
- **SIM (Subscriber Identity Module) Cards** - easily passed between cellular handsets, the amount and type of data that is located on a SIM card varies by manufacturer and carrier.
- **Lack of Training** - as a result of vendor specific technology, there is not a standardized method of extracting data from these devices.
- **Dynamic Nature of the Data** - most embedded devices do not have a non-intrusive method to access stored data. Specifically, the system data on cellular telephones is constantly changing regardless of conventional write blocking methods.
- **Block Incoming and Outgoing Signals** - attempts should be made to block incoming and outgoing signals of a wireless device. Common methods include portable Faraday bags and RF enclosures. However, these methods can be quite expensive and not always successful or practical.
- **Legal Issues** - unopened emails, unread text messages, and incoming phone calls of seized devices present non-consensual eavesdropping issues, especially if the examination is not conducted in a timely manner.
- **Condition of the Evidence** - cell phones and similar devices are subject to be damaged or contaminated. Damaged / destroyed handsets present a unique challenge in that the current methodologies suggest interaction with an operable device.
- **Loss of Power** - many of these devices lose data or initiate additional security measures once discharged or shut down.
- **Unallocated Data** - most of the forensic tools available do not address storages areas in cellular telephones that may contain deleted information.

The process and tools used to preserve ESI, including ESI harvested from small scale digital devices, must withstand the scrutiny of the United States judicial system as well as the supporting scientific community.

Unfortunately, many of the methods, processes and tools to preserve ESI are still in their infancy when compared to many other types of physical evidence. In particular, many of the tools used to preserve ESI harvested from small scale digital devices are less than a decade old. Many of the tools that investigators use to extract evidence are not designed to be forensically sound [3]. Because the tools were not designed with court admissibility as their objective, gaps can be found then exploited by opposing counsel and their experts.

Commonly, a software tool will be used to collect ESI from small scale digital devices. The software is simply installed on a desktop or laptop computer. The small scale digital device is then connected to the computer, most typically through a USB connection, Bluetooth, or Infrared Data Association (IrDA). The ESI collection is then made by the software tool. These tools differ in their approach of the data collection and a common standard for collection of ESI from small scale digital devices has not developed.

A key digital forensics principal is the collection process should not introduce change to the original evidence. When an examiner is collecting ESI from more traditional devices, such as a hard drive, the examiner will typically use a write-blocker to ensure the original media is not being changed during the collection process. In some cases, the software tool attempting to connect to the small scale digital device will need to have read/write access to the device. There are times when an attempt to use a USB write blocker in acquiring data from a small scale digital device will negatively impact the computer's ability to connect to the small scale digital device. In those instances, the write-blocker must be removed and the ability to testify that no changes have been made during the acquisition process becomes very circumstance. Opposing counsel with good experts on their team should carefully review the collection method of small scale digital devices when key evidence is harvested from these devices.

An examiner conducting an ESI collection on small scale digital devices will want to ensure they are using read-only cables. Read-only cables ensure that accidental writes to the small scale device cannot occur. Every step of each ESI process must be conducted in a manner to withstand challenges. Wise practitioners will always ensure their methods can withstand the scrutiny of another expert. While situations do exist where such a scrutiny is not necessary, it is important for examiners to clearly communicate up the chain of command when methods are being employed which may not withstand a challenge. In civil litigation matters, an attorney or other officer of the court may discern that deviation from a traditional evidentiary method is acceptable and when the risk is too great to consider such deviations.

ESI can be stored in numerous locations in relation to a small scale digital device. ESI can be found on the SIM card found in the small scale digital device, the device's embedded memory and on any removable media. Additionally, ESI can be stored by the service provider [14]. Finally, ESI can exist in multiple locations as a result of synchronization. Many small scale digital device users desire to have all communications flow to their device and some may employ the services of a synchronization tool to ensure that data from a multitude of sources can flow seamlessly to their small scale digital devices. Often, synchronization service providers will house ESI on their servers to provide that service. More commonly, synchronization can occur with a host computer to ensure data is backed up and accessible should the small scale digital device fail or become lost. The host computer will contain ESI which may or may not still exist on the small scale digital device.

A significant amount of work needs to be completed to determine if the tools really exist to collect the ESI found in small scale digital devices in a forensically sound manner. As researchers are finding, "these applications do not directly access the memory; rather, they use commands provided by the phone's software and/or hardware interfaces, and as such are placing a significant amount of trust in the phone software" [9].

The very nature of small scale digital devices with their remote connectivity features leave them susceptible to individuals with malicious intent. Keith Thomas stated, "the real problem for investigators will begin – when courts start to realize that evidence from cell phones isn't any more foolproof than what's found on computers" [3].

There are two schools of thought on how to handle the small scale digital device when taking possession of it for an ESI collection. When new data is transmitted to the small scale digital device it can potentially corrupt existing ESI. Therefore, a reasonable approach would be to disable the device from its ability to receive new ESI. There are three common methods for disabling a small scale device from receiving new ESI. First, the device can be turned off. Taking this approach, while it seems to be the easiest method, is sometimes the most difficult from an overall project perspective. When turning the device back on to make the ESI collection, password protected authentication may engage; making collection of the ESI much more complicated. Second, the device can be placed in a shielded container designed to block radio signals which would allow the small scale digital device to receive or transmit ESI. The containers have yet to prove they can completely eliminate the radio signal and sealing the container improperly is always a risk [8]. Third, if the small scale digital devices has the capability, "airplane" mode can be set on the device to restrict the radio transmission of new ESI to the device. All approaches to disable the transmission of new ESI to the device have various levels of risk associated with them.

However, disabling transmission of new ESI to a small scale digital device is not always desired. In field investigations, key evidence may be found in that next transmission of ESI to the small scale digital device. In those situations, cell phone exploitation may be warranted. As the small scale digital device community matures, the ability to exploit new ESI to follow clues in an ongoing investigation may need to be substantiated by evidence which is court admissible and defensible. The continued demand of locating evidence in ESI as well as the demand for defensible methods and processes will continue to push researchers and software developers to create tools which meet all needs.

Personal Digital Assistants (PDAs) also fall under the umbrella of small scale digital devices. "PDAs require specialized forensic tools and procedures distinct from those tools used for single PC systems and network servers" [1]. The tools to collect and examine evidence on small scale digital devices is clearly different from the tools commonly used for more traditional ESI collections, such as hard drives and server storage. This will continue to place challenges on examiners and researchers. While there is an evolving scientific community which addresses only small scale digital devices such

as cell phones and PDAs, these devices have typically been included as part of the digital forensics community. Over time there may be the evolution of many supporting scientific communities under the broader ESI umbrella. Communities which specialize in computers, small scale digital devices, telephone systems could easily develop when the distinctions and complexities of each scientific community are considered. While many communities may evolve, each community should have a foundation grounded in the evidentiary principles which are cornerstones in our nation's legal system. The Frye Test, the Rules of Evidence, The Daubert Test and the Rules of Civil Procedure all contribute to the admissibility of evidence and supporting expert witness testimony.

IV. Evidence Must Withstand the Tests

All ESI, including ESI harvested from small scale digital devices, must be preserved in a manner which protects and preserves the original evidence. The methods used to examine and analyze any ESI must be well documented, tested and reliable. The tools used must be generally accepted by the supporting scientific community. The results derived must be reproducible.

Practitioners who refuse to consider cell phones and other small scale digital devices when addressing ESI in litigation matters are potentially opening themselves and their organizations to malpractice claims. The Federal Rules of Civil Procedure clearly use the broad term of electronically stored information to cover digital data which can be harvested from any electronic device. Given the proliferation of small scale digital devices, their mobility and their increased capacity it is very likely that relevant ESI can be harvested from these devices. The standards for admissibility of any electronic evidence exist in The Frye Test, the Rules of Evidence, The Daubert Test and the Rules of Civil Procedure. As a result, the procedures used in the preservation, collection, examination and production of evidence from small scale digital devices must withstand these tests.

References

[1] Ayres, Rick and Jansen, Wayne. (August 2004). *PDA Forensic Tools: An Overview and Analysis.* National Institute of Standards and Technology. U.S. Department of Commerce.

[2] Ball, Craig. (December 28, 2006). *Hitting the High Points of the New EDD Rules.* Available at http://www.law.com/jsp/ihc/PubArticleFriendlyIHC.jsp?id=1167214011463.

[3] Cell Phone Evidence Used to Convict, Called into Question. *Courts Cast Wary Eye on Evidence Gleaned From Cell Phones*. Wired (May 10, 2007). Available at http://www.surety.com/solutions/article/cell_phone_evidence_used_to_convict_called_in to_question/.

[4] Cheng, Edward, K. and Yoon, Albert H. (April, 2005). *Does Frye or Daubert Matter? A Study of Scientific Admissibility Standards*. Virginia Law Review, Vol. 91, No. 2.

[5] *Daubert v. Merrell Dow Pharmaceuticals*, 509 U.S. 579 (1993).

[6] Federal Rules of Evidence. Available at http://www.law.cornell.edu/rules/fre/.

[7] *Frye v. United States*, 293 F. 1013 (D.C. Cir. 1923).

[8] Jansen, Wayne and Ayres, Rick. (May 2007). *Guidelines on Cell Phone Foresnics.* Recommendations of the National Institute of Standards and Technology. U.S. Department of Commerce.

[9] McCarthy, Paul. (October 2005). *Forensic Analysis of Mobile Phones*. University of South Australia.

[10] Schenker, Jennifer. (October 15, 2007). *The Rise of the Affinity Cell Phone*. Business Week, Issue 4054, page 84.

[11] Amendments Approved by the Supreme Court - Submitted to Congress (April 2006). (Effective December 1, 2006). Available at http://www.uscourts.gov/rules/congress0406.html

[12] Report of the Judicial Conference Committee on Rules of Practice and Procedure (Judicial Conference Committee) to the Chief Justice of the United States and Members of the Judicial Conference of the United States. (September 2005). Judicial Conference Committee Report. Available at http://www.uscourts.gov/rules/Reports/ST09-2005.pdf

[13] *Special Considerations When Dealing With Cellular Telephones. Scientific Working Group on Digital Evidence*. (April 5, 2007). Available at http://68.156.151.124/documents/swgde2007/SpecialConsiderationsWhenDealingwithCellularTelephones-040507.pdf

[14] Willassen, Svein Yngvar. (Spring 2003). *Forensics and the GSM mobile telephone system.* International Journal of Digital Evidence Spring 2003, Volume 2, Issue 1 Available at http://www.utica.edu/academic/institutes/ecii/publications/articles/A0658858-BFF6- C537-7CF86A78D6DE746D.pdf

Rebecca Hendricks Rebecca Hendricks is the President of Mirror Consulting, Inc. a Midwestern-based electronic discovery and digital forensics firm. Ms. Hendricks is currently working on her Ph.D. in CyberForensics at Purdue University and can be reached at rebecca.hendricks@mirrorconsulting.com.