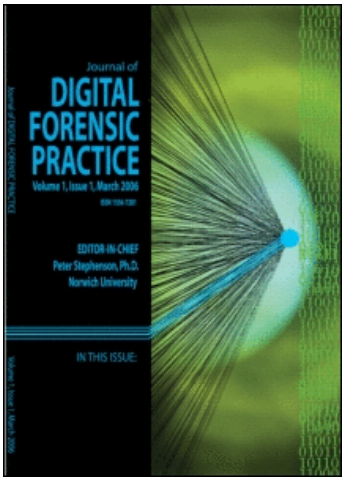

Journal of Digital Forensic Practice

Publication details, including instructions for authors and subscription information:
http://www.informaworld.com/smpp/title~content=t716100764

Prevalence, Use, and Evidentiary Issues of Digital Evidence of Cellular Telephone Consumer and Small-Scale Digital Devices

Michael Losavio [a]; Deborah Wilson [a]; Adel Elmaghraby [b]
[a] Department of Justice Administration, Brigman Hall, University of Louisville, Louisville, Kentucky, USA [b] Computer Engineering and Computer Science, J.B. Speed School of Engineering, J.B. Speed Building, Room 123, University of Louisville, Louisville, Kentucky, USA

Online Publication Date: 01 December 2006

To cite this Article Losavio, Michael, Wilson, Deborah and Elmaghraby, Adel(2006)'Prevalence, Use, and Evidentiary Issues of Digital Evidence of Cellular Telephone Consumer and Small-Scale Digital Devices',Journal of Digital Forensic Practice,1:4,291 — 296

To link to this Article: DOI: 10.1080/15567280701418080

URL: http://dx.doi.org/10.1080/15567280701418080

Journal of Digital Forensic Practice, 1:291–296, 2006

ISSN: 1556-7281 print / 1556-7346 online
DOI: 10.1080/15567280701418080

Taylor & Francis
Taylor & Francis Group

ARTICLE

Prevalence, Use, and Evidentiary Issues of Digital Evidence of Cellular Telephone Consumer and Small-Scale Digital Devices

Michael Losavio and Dr. Deborah Wilson
Department of Justice Administration, Brigman Hall, University of Louisville, Louisville, Kentucky 40292, USA

Dr. Adel Elmaghraby
Computer Engineering and Computer Science, J.B. Speed School of Engineering, J.B. Speed Building, Room 123, University of Louisville, Louisville, Kentucky 40292, USA

ABSTRACT Digital systems are found in a number of casual consumer tools, including cellular telephones. Their prevalence in society is matched by a growing presence as evidence in civil and criminal court cases. The current survey research suggests that cell phones and their potential evidence may be found in over half of all violent crime and even more substantially in drug crimes in some jurisdiction. The police commander respondents to this survey reported that cell phones had been used as evidence via lay testimony and expert analysis in their jurisdictions. Such evidence may face increasing judicial challenges in the future as the specialized nature of the analysis, even with commercially available, easy-to-use practices, goes "well beyond that of the average layperson." Digital forensics analysts must be prepared to provide both proper lay testimony on cell phones as well as details and justifications for their own tools, techniques, and qualifications as required by *Daubert* and Federal Rule of Evidence 702.

KEYWORDS cell, cellular, phone, telephone, evidence, prevalence, small-scale, digital, *Daubert*, Federal Rule; 702

INTRODUCTION

There are an estimated 232 million cell phone/wireless users in the United States alone.[1] Consumer and small-scale digital devices such as cell phones, personal data assistants ("PDA"), and iPods contain vast amounts

Dr. Deborah Wilson is Professor and Chair of the Department of Justice Administration of the University of Louisville and responsible for oversight of the Southern Police Institute and the Institute for Community Security and Public Safety. She is currently completing a project with $2.9 million in federal funding that has resulted in the creation of a Regional Computer Forensics Laboratory in partnership with the FBI on the University's Shelby Campus.

Dr. Adel Elmaghraby is Professor and Chair of the Department of Computer Engineering and Computer Science of the University of Louisville. His research focus is in distributed and interactive simulation, multimedia systems and digital forensics.

Michael Losavio, an attorney, is a lecturer in the Departments of Computer Engineering and Computer Science and Justice Administration of the University of Louisville. His research interest is in digital forensics and judicial process.

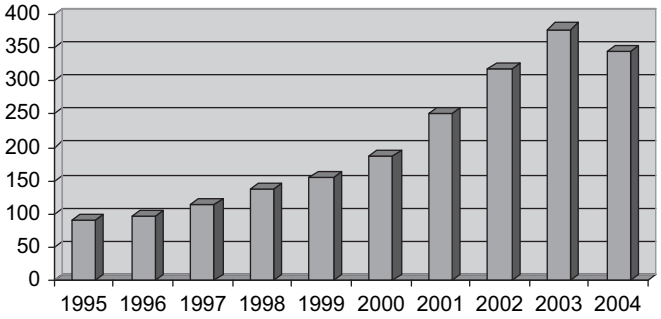

FIGURE 1 **Analysis of U.S. District case opinions for involvement of cell phones 1995 through 2004.**

of data stored primarily in digital media. This data may, in some instances, be relevant to criminal and civil proceedings.[2,3] Applying the Computer Fraud and Abuse Act (U.S.)[4] one court said, "Every cell phone and cell tower is a 'computer' under this statute's definition; so is every iPod, every wireless base station in the corner coffee shop, and many another gadget."[5] In that case, disruption of the Madison, Wisconsin, police telecommunications SmartNet II system via computer and radio was a computer crime under that statute. The same application of the rules of evidence to general purpose computers holds for cell phones and other small-scale digital devices.

A search of "cell or cellular w/3 telephone or phone" within reported United States District Court opinions over a ten-year period shows dramatic growth in the number of cases in which these devices were considered to be relevant to legal proceedings This is detailed in Figure 1.

These cases represent both criminal and civil matters with cellular telephone references for conversations, possession, use, and stored data. A sequential examination of the first one hundred such cases from May 1, 2004, to May 1, 2005, found that approximately one third were related to criminal actions. A similar search of federal appellate decisions found 219 cases over the same time period with similar references; of these, only one addressed a challenge to the admissibility of the cell phone evidence.

CRIMINAL ACTIVITY AND CELL PHONES

Cell phones are used in crimes of violence, such as an assassination directed by a corrupt police officer or extortion by a mob boss, and drug crimes.[6,7] Purposes include storing cell phone numbers,[8] as a means for "… co-conspirators … to communicate with each other to further facilitate their drug trafficking activities."[9] and as other evidence linking someone to a drug conspiracy.[10]

During January of 2007, fifty-nine law enforcement executives (individuals at the rank of sergeant or above) from agencies throughout the United States who were attending a police executive leadership course were asked to respond to a written survey concerning the involvement of cell phones and crime in their jurisdictions. Specifically, they were asked whether or not a cell phone was present at the scene of the crime or in the possession or vicinity of a suspect or witness in (a) violent crimes and (b) drug crimes.[11] Figures 2 and 3 contain the responses to these questions.

As shown in Figure 2, these police executives reported frequent involvement of cell phones in violent crimes. A majority of the respondents (90 percent) reported knowing of some involvement. The minority reported "uncertainty" and could not respond to the question. However, as shown in Figure 2, of those who responded to the question, a clear majority (49 percent) reported they believed cell

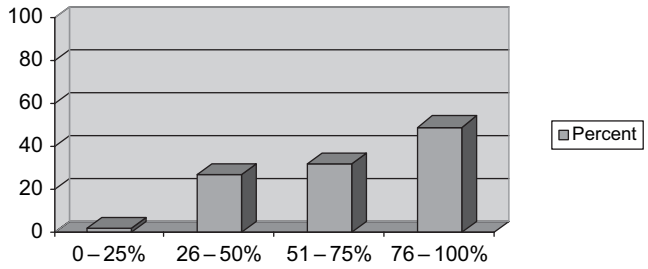

FIGURE 2 **Reported involvement of cell phones in violent crimes.**

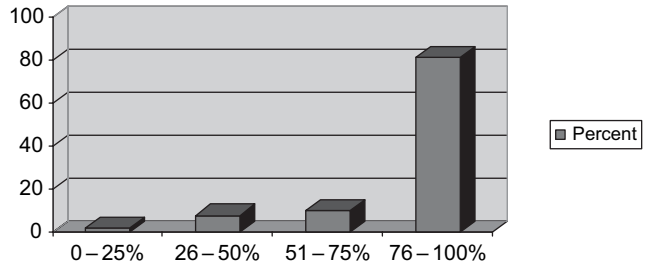

FIGURE 3 **Reported involvement of cell phones in drug crimes.**

phones were involved in 76 to 100 percent of all violent crimes. A total of 81 percent of the sample responded they believed cell phones were involved in 50 percent or more of violent crimes. The observations of these police commanders show the clear and repeated involvement of cell phones on violent crimes.

As with the responses to the question concerning violent crimes, approximately 4 percent of the commanders did not feel they could respond to the question. However, among those who responded, Figure 3 clearly shows their observations concerning the involvement of cell phones in drug crimes. Specifically, 81 percent reported they believed cell phones were involved in 76 to 100 percent of drug crimes. A total of 92 percent reported they believed cell phones were in involved in 51 percent or more of all drug crimes. As with the responses to questions of involvement of cell phones in violent crimes, these police commanders report an extremely high involvement of cell phones in drug crimes within their respective jurisdictions. The findings also show a higher rate of cell phone involvement in drug compared to violent crimes.[11]

Ironically, at least one drug defendant has argued the absence of cell phones showed he was innocent; he was unsuccessful.[12]

The police commanders were additionally asked whether or not the cell phones they identified as involved in drug and violent crimes contained evidence related to the crime. The findings for this question are contained in Figure 4. In those cases where cell phones were involved with violent or drug crimes, they usually contained evidence relating to the offense. Figure 4 displays the frequency such evidence was found on these cellular telephones.

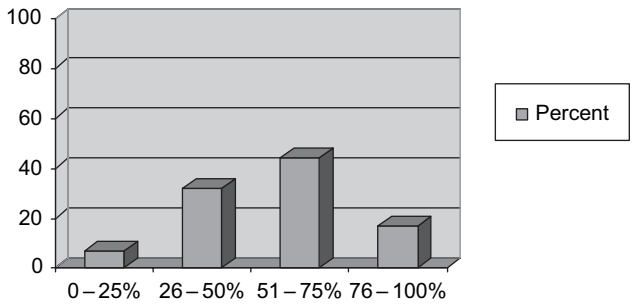

FIGURE 4 **Frequency of criminal evidence found in cell phones violent and drug crimes.**

A total of 23 percent of the police commanders responding to the survey did not feel they could respond to this question. The findings from those who felt they could respond are contained in Figure 4. As shown in this figure, a majority of the respondents (44 percent) believed the cell phones involved in violent and drug crimes contained evidence in 51 to 75 percent of the crimes. An additional 17 percent believed the cell phones contained evidence in 76 percent or more of the crimes. Only 7 percent believed these cell phones contained evidence 0 to 25 percent of the time. In sum, a total of 93 percent of the police commanders reported they believed the cell phones contained evidence of a crime in more than 25 percent of the crimes.

LAY TESTIMONY AND CELL PHONE EVIDENCE

Cell phone evidence may be used without the expert foundation of reliability required by U.S. Federal Rule of Evidence 702. "Every case involving equipment–whether it be computers, camera, or speed guns–does not automatically require a *Daubert* hearing regarding the physics behind the operation of the machine."[13] For example, a court may permit a witness to read telephone numbers from pager or cell phone memory for the jury.[14]

As one court of appeals observed:

> [Defendant] contends that the district judge committed error in allowing [the officer] to testify that [the officer]'s cell phone registered the number of one of [defendant]'s cell phones as a previously-dialed number, and that yet another cell phone recovered from the defendant indicated that someone using that second phone had placed a call to [the officer] at the same time the officer received a call from [defendant] regarding plans for a drug sale on April 12, 2004. The defendant contends that admission of such evidence was improper because [the officer] was not qualified as an expert in cell phone technology and should not, therefore, have been allowed to offer his opinion regarding the origin and destination of particular telephone calls. In the absence of a contemporary objection at trial, we review this issue for plain error only.
>
> A review of the record indicates that [the officer]'s testimony did not involve the offering of any expert opinion. *See* Fed. Rule Of Evid. 702. Instead, the witness merely recounted information retrieved from various cell phones in a procedure used and relied upon not by experts in telephonic technology, but by literally millions of cell phone users. Simply relating to a jury the information gained from a function performed, known, and understood by most members of modern society did not render [his] testimony improper.[15]

UNITED STATES v. GANIER, 468 F.3D 920 (6TH CIR. 2006) AND THE BOUNDARIES BETWEEN LAY WITNESS AND EXPERT TESTIMONY

At some point cell phone evidence testimony becomes expert evidence under F.R.E. 702 and must meet its requirements. In *United States v. Ganier*, the Court of Appeals for the Sixth Circuit described boundaries for digital forensics in this area.[16]

In *Ganier* the defendant was accused of obstruction of justice for destruction of certain e-mails. The government wished to present evidence developed from forensic software by "running commercially-available software, obtaining results, and reciting them." It argued this testimony did not fall under Rule 702 as it was of the same type as "facts … that could be observed by any person reasonably proficient in the use of commonly used computer software, such as Microsoft Word and Microsoft Outlook" and was not based on "scientific, technical, or other specialized knowledge." The court noted one example of the type of reported information produced by the forensic software:

Registry - Al Ganier Desktop

Software Microsoft Internet Explorer Explorer Bars C4EE31F3–4768–11D2-BE5C- 00A0C9A83DA1 FilesNamedMRU

Last Written Time 12/09/02 08:34:57

Name	Type	Data
000	REG_SZ	al ...
001	REG_SZ	sony ...
002	REG_SZ	RFP ...
003	REG_SZ	sundquist ...
004	REG_SZ	ARC ...
005	REG_SZ	roadmap to evenue ...
006	REG_SZ	road ...
007	REG_SZ	roadmap ...

Ganier Digital Forensic Report.

The court found interpretation of the reports to show different kinds and times of searches required application of special knowledge of computers and the forensic software used "well beyond that of the average layperson." This brought the testimony into the realm of "scientific, technical or other specialized knowledge" of Rule 702.

The court noted categorization of computer-related testimony is a relatively new question and made comparisons with other areas of expertise:

> Software programs such as Microsoft Word and Outlook may be as commonly used as home medical thermometers, but the forensic tests [here] are more akin to specialized medical tests run by physicians. … The average layperson today may be able to interpret the outputs of popular software programs as easily as he or she interprets everyday vernacular, but the interpretation [the government's examiner] needed to apply to make sense of the software reports is more similar to the specialized knowledge police officers use to interpret slang and code words used by drug dealers.

Ganier indicates when testimony on electronic evidence must be prepared to meet a *Daubert* challenge under Federal Rule of Evidence 702.

CELL PHONE EXPERT TESTIMONY POST-GANIER

When the *Daubert*/702 threshold is crossed by observations "well beyond that of the average layperson," testimony as to cell phone operations and data readouts of that digital information may be required to demonstrate:

1. witness qualifications, including sufficient technical knowledge of cell phone operations and data recordation, to do so and
2. the soundness of the examination methods to assure authenticity of the results.[17–20]

In particular, the examiner must show (a) the testimony is based upon sufficient facts or data, (b) the testimony is the product of reliable principles and methods, and (c) the witness has applied the principles and methods reliably to the facts of the case. Key *Daubert* factors include whether a technique has been tested; whether evaluation results have been peer-reviewed and published; with respect to a particular technique, the "known or potential rate of error"; and whether there are "standards controlling the technique's operation" that have been applied and maintained. These analytical considerations map to factors that increase the difficulty and cost for digital forensic analysis, which include:

1. extensive use of propriety operating systems by each manufacturer,

2. multiple device designs,
3. need for multiple toolkits to analyze this diversity,
4. short product release cycles for new cell phone technologies, and
5. lagging support by forensic tool makers for new technologies.[21]

These factors may increase the difficulty of meeting *Daubert*/702 considerations for the testing, error rates, peer review, and standards applicable to cell phone forensic techniques. This effect will be magnified as more and newer digital devices are introduced and the distributed aspects of data increase. The sheer newness and rapidity of innovation in cell phone development and deployment makes testing and review difficult. Once such evaluation is done, the technology may have moved on to the next level of innovation.

IMPLICATIONS

Given its prevalence and consumer use, the proper scope of lay analysis versus expert analysis of cell phone evidence acquisition, analysis, and presentation needs an even more rigorous delineation than that for general-purpose computing devices. The prevalence, ease of use, and defined feature set of Windows-based personal computers make some lay analysis of those devices more likely to be accepted in court. But the sheer diversity of cellular handset technology and the prevalence in crime scenes might overwhelm any police department that required technical forensic analysis of each and every cell phone.

The survey conducted among the police commanders asked them to respond to a question asking if officers/personnel in their departments had ever been unable to search for evidence of a crime from cellular telephones because of a lack of timely access to forensic examiners and/or a lack of forensic skills among department personnel. The findings in response to this question are contained in Figure 5.[3]

As shown in Figure 5, a majority (60 percent) of the commanders responded that "yes," officers or other personnel within their department had been unable to search for evidence of a crime from cellular telephones because of a lack of timely access to forensic examiners and a lack of forensic skills among their personnel. While other evidence is most certainly present, it is significant that a readily available possible source of evidence was reported as potentially not being examined simply due to a lack of the availability of personnel with forensic skills or forensic examiners within these jurisdictions.

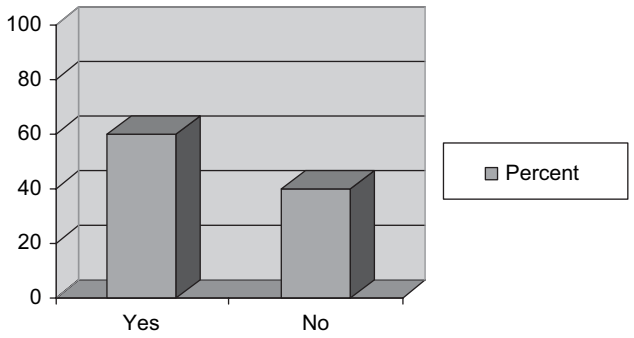

FIGURE 5 **Reported inability to search for cell phone evidence due to timely access to forensic examiners and lack of forensic skills.**

CONCLUSIONS AND RECOMMENDATIONS

Use of lay witness skills with cell phone evidence will continue to be important, yet the expansion of feature sets away from a limited appliance to a general-purpose computing device may lead to concern about lay testimony. This compounds the problems of forensic specialists of propriety operating systems, rapid product innovation, and multiple technologies, among other issues. As analysis moves toward knowledge well beyond that of the average layperson, these problems may converge.

Strategies for addressing these begin with establishing best practices and standards relating to both lay observation and expert analysis, with that expert analysis being available to support the reliability of lay observation where needed and serve as a training resource for potential lay witnesses. Even basic knowledge regarding such matters as cloned cell phones can be of value to a lay witness challenged over the reliability of his observations.[22–24] The delineation of boundaries between testimony qualifying as lay or expert will continue to evolve in this new and largely untested area.

Ultimately, particularly regarding cell phone technologies, a review of government regulatory power to mandate manufacturers themselves to set standards or

observe protocols that permit rapid testing and validation of data extraction from their systems and otherwise support forensic efforts may be needed.

Prevalence and ease of use do not automatically equate to reliability. But the ubiquity of the cell phone in modern life, whether at the crime scene or part of a pre-divorce dalliance, assures its evidentiary place in legal matters. Proper understanding and use of lay investigative techniques for cell phones will aid in their efficient use for evidence while permitting the digital forensic expert to focus on appropriate matters needing her attention. The boundary between proper lay and expert testimony must be watched closely. This assures that the examiner is appropriate and prepared for the digital evidence task. Forensic examiners must be prepared to defend not only their analysis but, where appropriate, that of a challenged lay witness.

NOTES

1. Cellular Telecommunications & Internet Association, [cited 28 February 2007]. Available from http://www.ctia.org/
2. Peter Lyman and Hal R. Vavian, "How Much Information? 2003" School of Information Management and Systems, University of California, Berkeley. www.sims.berkeley.edu/how-much-info-2003. Visited May 22, 2007.
3. J. Seward, "The Debtor's Digital Reckonings," *International Journal of Digital Evidence*, Vol. 2, Issue 2. (fall 2003).
4. *Computer Fraud and Abuse Act* (U.S.), 18 U.S.C. §1030.
5. *United States v. Mitra*, 405 F3d 492 (7th Cir. 2005); 2005 U.S. App. LEXIS 6717.
6. *United States v. Davis*, 380 F3d 821 (5th Cir. 2004).
7. *United States v. Gotti*, 459 F3d 296 (2nd Cir. 2006); 2006 U.S. App. LEXIS 17430.
8. *United States v. Francis,* 367 F3d 805 (8th Cir. 2004).
9. *United States v. Lazu-Rivera*, United States District Court for the District of Puerto Rico, 2004 U.S. Dist. LEXIS 27002, December 29, 2004, Decided, Adopted by, Motion denied by United States v. Lazu-Rivera, 2005 U.S. Dist. LEXIS 5028 (D.P.R., Mar. 23, 2005).
10. *United States v. Stuckey*, 325 F. Supp. 2d 793 (ED Michigan 2004).
11. "Southern Police Institute Survey of Administrative Police Officers." (February 27, 2007). Losavio, Michael.
12. *United States v. Johnson*, No. 03–4573, United States Court of Appeals for the Fourth Circuit, 110 Fed. Appx. 319; 2004 U.S. App. LEXIS 20453 (unpublished opinion).
13. *United States v. Lauder*, 409 F3d 1254, 1265 (10th Cir. 2005).
14. *United States v. Wells*, 347 F3d 280, 289 (8th Cir. Cert denied, 541 U.S. 1081, 124 S. Ct. 2435, 158 L.Ed. 2d 996 2004).
15. *United States v. Barnes*, 83 Fed. Appx. 526; 2006 U.S. App. LEXIS 13216, (6th Cir. 2006) (unpublished opinion).
16. *United States v. Ganier*, 468 F3d 920 (6th Cir. 2006).
17. *Daubert v. Merrill-Dow Pharmaceuticals, Inc.*, 509 US 579 (1993).
18. Federal Rule of Evidence 701 (U.S.).
19. Federal Rule of Evidence 702 (U.S.).
20. *Kumho Tires Co. Ltd. v. Carmichael*, 526 US 137 (1999).
21. Rick Ayers and Wayne Jansen, "Guidelines on Cell Phone Forensics: Recommendations of the National Institute of Standards and Technology," draft, Special Publication 800-101, National Institute of Standards and Technology, August 2006. http://CSRC.nist.gov/publications/drafts/Draft-SP800-101.pdf
22. *United States v. Kyser*, Nos. 02–2998, 02–3265, & 02–4221, United States Court of Appeals for the Seventh Circuit 102 Fed. Appx. 51; 2004 U.S. App. LEXIS 13268 (unpublished opinion).
23. *United States v. Cabrera*, 172 F3d 1287, 1289 n.1 (11th Cir. 1999).
24. *United States v. Staves*, 383 F3d 977 (9th Cir. 2004) ; 2004 U.S. App. LEXIS 18991 Note 3.