SLEEPING GATE-KEEPERS: CHALLENGING THE ADMISSIBILITY OF CELL PHONE FORENSIC EVIDENCE UNDER DAUBERT

Andrew McQuilkin*

Cite as 11. J. HIGH TECH. L. 365 (2011)

"Any sufficiently advanced technology is indistinguishable from magic."
ARTHUR C. CLARK[1]

I. Introduction

Cell phones hold a wealth of evidence for investigators.[2] They contain call logs, text messages, calendars, phone books, media files, and the location of the last cell tower connection.[3] In addition, 87% of U.S. residents currently own a cell phone, and that phone is likely to be carried with them at all times.[4] This

* J.D. Candidate, Suffolk University Law School, 2011.

1. ARTHUR C. CLARK, PROFILES OF THE FUTURE 21 n.1 (Rev. ed. 1973).

2. *See* Noah Shachtman, *Fighting Crime With Cellphones' Clues*, N.Y. TIMES, May 3, 2006, *archived at* http://www.webcitation.org/5vysin4ZB (describing cell phone evidence as a "gold mine of information . . . ."). *See also* Don Kohtz & Matt Churchill, *Cell Phone Forensics: The New Evidentiary Gold Mine*, 34-SEP MONT. LAW. 5, 6 (2009) (noting wealth of multimedia evidence on cell phones).

3. *See* Wayne Jansen, Aurélien Delaitre & Ludovic Moenner, *Overcoming Impediments to Cell Phone Forensics*, PROCEEDINGS OF THE 41ST ANNUAL HAWAII INTERNATIONAL CONFERENCE ON SYSTEM SCIENCES 4 (2008), *archived at* http://www.webcitation.org/5vyu2jaFA (listing potential evidentiary sources in cell phones). *See also* Rebecca Kanable, *The New Frontier in Digital Forensics*, L. ENFORCEMENT TECH., July 1, 2007, at 16, 16 (acknowledging cell phones are used for more than talking); Kohtz & Churchill, *supra* note 2, at 6 (explaining type of evidence left on cell phones); Shachtman, *supra* note 2 (stating that cell phones "do more than dial numbers.").

4. *See Cell Phone Nation*, MARIST POLL, June 12, 2009, *archived at* http://www.webcitation.org/5oiy2kziw (providing cell phone use statistics); Kohtz & Churchill, *supra* note 2, at 5 (describing that most Americans take their cell phone everywhere).

 ISSN 1536-7983.

means that in most cases, there will be cell phone evidence, and it will be particular to a single person.[5]

Despite the great utility of this evidence, the scientific methods used to retrieve it have several serious problems.[6] There are several major cell phone operating systems, all with different, proprietary methods of storing data.[7] This fact, coupled with the rapid release of new phones and the various types of cell networks, make it nearly impossible for forensic tool developers to adequately test their product on every model.[8] Also, unlike traditional computer forensics, there is no way to ensure that the data on the phone has not been altered during the course of the investigation through write-blocking or hash values.[9]

Despite these problems, the evidence has entered the courtroom largely unchallenged.[10] The Supreme Court has directed judges to act as gate-keepers to prevent the jury from considering assertions or inferences that are not based on

5. *See* Kanable, *supra* note 3 (observing that typically cell phones are only used by one person).

6. *See* Kanable, *supra* note 3, at 19-21 (listing problems discovered using the current methods of evidence extraction).

7. *See* Prince McLean, *Canalys: iPhone Outsold All Windows Mobile Phones in Q2 2009*, APPLEINSIDER, Aug. 21, 2009, *archived at* http://www.webcitation.org/5lmAftr5i (listing the various phone operating systems). *See also Best Practices for Mobile Phone Examinations Version 1.0* 3 (SCIENTIFIC WORKING GROUP ON DIGITAL EVIDENCE, 2009), *archived at* http://www.webcitation.org/5lgBUfACZ [hereinafter *Best Practices*] (highlighting closed operating systems and proprietary data connections as alternatives); Jansen et al., *supra* note 3, at 1 (explaining growth and development of storage and technical capacity of cell phones); Kohtz & Churchill, *supra* note 2 (noting that data storage is unique to each manufacturer and model); Paul McCarthy, Forensic Analysis of Mobile Phones 14 (Oct. 2005) (unpublished B.S. thesis, University of South Australia), *archived at* http://www.webcitation.org/5lgAylTQD (discussing the issues with different network technologies).

8. *See* Jansen et al., *supra* note 3, at 1 (detailing the issues with tool validation because of the large variety of phones).

9. *See Best Practices*, *supra* note 7 (listing as limitations the fact that phone data is constantly changing, resulting in inconsistent hash values).

10. Gary Craig Kessler, Judges' Awareness, Understanding, and Application of Digital Evidence 89 (Sept. 2010) (unpublished dissertation, Nova Southeastern University), *archived at* http://www.webcitation.org/61BgrjWsu (presenting findings on frequency of *Frye* and *Daubert* challenges).

"scientific knowledge."[11] With regard to mobile forensic evidence, the courts have failed at this task by not demanding testing and transparency from the scientists in the mobile forensics field.

This Note contends that judges should no longer admit cell phone forensic evidence until formal testing methods and standards are adopted because it fails to meet any of the factors of the *Daubert v. Merrell Dow Pharmaceuticals, Inc.* test. Part II examines this test, and the history leading up to its inception. Part III explains how computer and mobile forensics work and their limitations. Part IV applies the *Daubert* factors to the technology. Part V looks at the cases where courts have admitted mobile forensic evidence. In Part VI, the Note examines how the courts have judged other types of scientific evidence under *Daubert*, and applies their reasoning to cell phone forensics. Part VII proposes solutions to the problems that render the technology inadmissible.

II. Standard for Admissibility of Scientific Evidence

Prior to 1923, courts treated scientific evidence the same as any other type, and it only needed to be relevant to be admitted.[12] To show that the evidence made a proposition more or less probable, the proponent had to demonstrate that the results of the scientific technique were accurate.[13] Thus, a reliability standard was created with judges acting as gate-keepers.[14] Although the judges did not typically have a background in the applicable field of science, this decision forced

11. *See* Daubert v. Merrell Dow Pharm., Inc., 509 U.S. 579, 590 (1993) (ensuring that reliable evidence reaches the jury).

12. *See* PAUL R. RICE, ELECTRONIC EVIDENCE 464-65 (2nd ed. 2008) (explaining that scientific and technological evidence was treated the same as all evidence, creating controversy with regards to relevance).

13. *See* RICE, *supra* note 12 (illustrating that unlike other evidence, relevance of scientific evidence could not be established "by simply identifying underlying premises that intuitively connected a fact to a proposition.").

14. *See* RICE, *supra* note 12, at 464 (employing judges as "gate-keepers" of evidence due to the potential influence expert testimony could have on jurors).

judges to look into the scientific methods and appraise their accuracy.[15]

This issue led the Court of Appeals for the District of Columbia to create a new standard in *Frye v. United States*, 293 F. 1013 (1923).[16] The scientific principle at issue was a lie detector test based on blood pressure.[17] The court ruled that the scientific evidence offered "must be sufficiently established to have gained general acceptance in the particular field in which it belongs."[18] Since the lie detector test did not have adequate "standing and scientific recognition among physiological and psychological authorities," it was held inadmissible.[19]

Frye only required an expert witness to be qualified and testify that the scientific principle has gained general acceptance in the particular field.[20] Courts widely adopted the standard because it allowed judges to shift the burden of determining reliability to experts.[21] However, it was widely criticized as being vague and both too lenient and too strict.[22] Critics also attacked the presumption that the newness of a scientific theory necessarily correlates with unreliability.[23] The criticism rose to a

15. *See* RICE, *supra* note 12, at 465 (raising concerns about the effectiveness of a judge in determining the reliability of scientific evidence).

16. *See* Frye v. United States, 293 F. 1013, 1014 (1923) (establishing the general acceptance standard for scientific evidence).

17. *See id.* at 1013. The theory behind the test is that it takes a conscious effort to lie, but not to tell the truth, and therefore, a person's blood pressure will rise when lying. *See id.* at 1014.

18. *Id.* at 1014 (setting out admissibility standards).

19. *Id.* Initially *Frye* was only used for novel scientific principles, but was later expanded to include novel methodologies and applications of accepted principles. *See* RICE, *supra* note 12, at 466.

20. *See* RICE, *supra* note 12, at 466 (recognizing the continuing role of judges as gate-keepers). A judge must still determine what the particular field is. *Id.* at 465. In some cases, admissibility may hinge on how broadly or narrowly the field is defined. *Id.* at 466.

21. *See* RICE, *supra* note 12, at 465 (allowing judges to "avoid the determination of reliability" by passing the role to those knowledgeable in the field).

22. *See* CHRISTOPHER B. MUELLER & LAIRD C. KIRKPATRICK, FEDERAL EVIDENCE § 7:10 (3d ed. 2010) (explaining contradicting range of criticism of the *Frye* test).

23. *See* Harvey Brown, *Eight Gates for Expert Witnesses*, 36 HOUS. L. REV. 743, 779 (1999). Brown argues that *Frye* creates unnecessary delays in the

new level in the late 1980s when the standard began to be applied to toxic tort cases, where courts would frequently admit scientific testimony from fringe scientists, or "junk science."[24]

To address these problems, in 1993, the Supreme Court created a new test in *Daubert v. Merrell Dow Pharmaceuticals., Inc.*, 509 U.S. 579 (1993).[25] The Court ruled that Rule 702 of the Federal Rules of Evidence superseded *Frye*, reasoning that the "rigid 'general acceptance'" test went against the "liberal thrust" of the Federal Rules.[26] The decision reaffirmed the role of judges to act as "gatekeepers," as they could not longer simply defer to experts.[27] It directed the courts to ensure that all scientific evidence was both reliable and correctly applied to the facts.[28] The ruling also extended judicial review to cover all scientific

admission of novel scientific evidence. *See id.* The decision was criticized as too vague because it did not define "general acceptance" or "particular field." S*ee* David E. Bernstein, *Frye Frye Again: The Past, Present, and Future of the General Acceptance Test*, 41 JURIMETRICS J. 385, 390 (2001) (listing the criticisms of *Frye* by various commentators).

24. *See* RICE, *supra* note 12, at 466-67 (pointing to several factors building up to the expansion of the *Frye* test); Bernstein, *supra* note 23, at 391-93 (tracing history of *Frye* decision). *See, e.g.*, PETER HUBER, GALILEO'S REVENGE: JUNK SCIENCE IN THE COURTROOM 141 (1991) (portraying the way attorneys abuse science illiteracy through employing professional "expert" witnesses to further unsupported claims).

25. *See Daubert*, 509 U.S. at 589. Parents of two minor children sued a drug company for over drug, Benedictin, which allegedly caused birth defects. *See id.* at 582. The company introduced over thirty studies that all showed the drug did not cause birth defect. *See id*. In response, the plaintiffs had eight well-qualified experts who testified based on reanalysis and structural similarity with drugs known to cause birth defects. *See id.* at 583. The defendant objected to the testimony on reliability grounds. *See id.*

26. *See id.* at 588 (elucidating the Court's reasoning behind replacing the *Frye* test). At the time of the decision, Rule 702 read: "[i]f scientific, technical, or other specialized knowledge will assist the trier of fact to understand the evidence or to determine a fact in issue, a witness qualified as an expert by knowledge, skill, experience, training, or education, may testify thereto in the form of an opinion or otherwise . . . ." FED. R. EVID. 702.

27. *See Daubert*, 509 U.S. at 589 (revising the standard for the admissibility of scientific evidence); RICE, *supra* note 12, at 468 (maintaining the judge's role as gate-keeper).

28. *See Daubert*, 509 U.S. at 589. The Court interpreted Rule 702's "scientific knowledge" to require that the knowledge be based on reliable scientific principles. *See id.* at 589-98. The language, "to assist the trier of fact," goes to relevance, or the degree of fitness the evidence has to the present case. *See id.* at 591.

evidence, not just novel principles.[29] In 2000, an amendment to Rule 702 codified *Daubert v. Merrell Dow Pharmaceuticals, Inc.*, 509 U.S. 579 (1993) and its progeny.[30]

To determine the reliability of the evidence, the Supreme Court listed a series of factors for court to consider.[31] These include whether the method has been tested, its potential rate of error, the existence of standards governing the method, and if the theory has been subjected to publication and peer review.[32] The Court also included the *Frye* general acceptance test as one of its factors, but it is no longer the exclusive measure.[33] The standard is meant to be "flexible," and deal only with the method of acquiring scientific evidence, not the evidence itself.[34]

Currently, twenty-five states, and the federal courts apply the *Daubert* standard, whereas thirteen states continue to use the *Frye* test.[35] Since *Daubert* was handed down, judges have been scrutinizing scientific evidence more closely.[36] However, it does

29. *See Daubert*, 509 U.S. at 593 n.11 (justifying the expansion of what qualifies as scientific evidence). In *Gen. Electric v. Joiner*, the Court ruled that admissibility of expert testimony can only be examined under an "abuse of discretion review." 522 U.S. 136, 143 (1997).

30. *See* RICE, *supra* note 12, at 469 (noting that in 2000 *Daubert* and *Kumho Tire* were codified in Rule 702). The following was added to the end of Rule 702: "[i]f (1) the testimony is based upon sufficient facts or data, (2) the testimony is the product of reliable principles and methods, and (3) the witness has applied the principles and methods reliably to the facts of the case." FED. R. EVID. 702.

31. *See Daubert*, 509 U.S. at 593-94 (compiling factors trial judges must consider in admitting expert scientific testimony).

32. *See id* (specifying judicial considerations for the admissibility of scientific evidence).

33. *See id.* at 594 (permitting the use of general acceptance as a consideration, but noting it is by no means required in determining reliability).

34. *See id.* at 594-95 (stating intended application of new factors).

35. *See* Edward K. Cheng & Albert H. Yoon, *Does* Frye *or* Daubert *Matter? A Study of Scientific Admissibility Standards*, 91 VA. L. REV. 471, 473 (2005). This includes some states that have adopted the standard in all but name, and states that adopted *Daubert* but not the subsequent, related Supreme Court cases. *See id.* at 473-74 n.8.

36. *See* Joseph Sanders, Shari S. Diamond & Neil Vidmar, *Legal Perceptions of Science and Expert Knowledge*, 8 PSYCHOL. PUB. POL'Y & L. 139, 141 n.13 (2002) (recounting efforts of both plaintiffs and defendants to construe *Daubert* in their favor). *See also* LLOYD DIXON & BRIAN GILL, CHANGES IN THE STANDARDS FOR ADMITTING EXPERT EVIDENCE IN FEDERAL CIVIL CASES SINCE THE

not seem to matter whether the *Daubert* or *Frye* standard is applied.[37] A 2001 study showed that in federal court opinions the general acceptance part of the *Daubert* standard was the most important factor in determining admissibility.[38] Studies of state courts have found that judges find the general acceptance prong the most useful, and give it the most consideration in their opinions.[39] Another study examined removal rates to see if litigators were attempting to forum shop for one standard over another.[40] It found no statistically significant difference.[41] These results indicate that the *Daubert* decision did not change the test for admissibility from *Frye's* "general acceptance" test, but rather increased judicial awareness of the problems of unreliable scientific evidence.[42]

DAUBERT DECISION xiii, xv (2001) (studying 399 federal district court opinions, and determining judges now apply more scrutiny to scientific evidence); Carol Krafka et al., *Judge and Attorney Experiences, Practices, and Concerns Regarding Expert Testimony in Federal Civil Trials*, 8 PSYCHOL. PUB. POL'Y & L. 309, 330 (2002) (surveying attorneys and judges, and finding more stringent standards for scientific evidence).

37. *See* Cheng & Yoon, *supra* note 35, at 511 (giving an overview of Connecticut, New York, and national studies on *Frye* and *Daubert*).

38. *See* DIXON & GILL, *supra* note 36, at 41 (summarizing the role of the general acceptance standard).

39. *See* Sophia I. Gatowski et al., *Asking the Gatekeepers: A National Survey of Judges on Judging Expert Evidence in a Post-*Daubert *World*, 25 LAW & HUM. BEHAV. 433, 447, 453 (2001) (reporting that ninety-three percent of judges in a survey found the general acceptance prong to be the most useful criterion in determining the admissibility of scientific evidence). *See also* Jennifer L. Groscup et al., *The Effects of* Daubert *on the Admissibility of Expert Testimony in State and Federal Criminal Cases*, 8 PSYCHOL. PUB. POL'Y & L. 339, 365-66 (2002). The study found that judges now discussed reliability more thoroughly, but relied heavily on the general acceptance prong of *Daubert*, and barely discussed the other factors. *See id.* Pamela Jensen, in her Note, highlighted a study which analyzed thirty-two appellate decisions on three types of scientific evidence, and found no difference between the rate of admissibility when *Daubert* or *Frye* were used. *See* Pamela J. Jensen, Frye *Versus* Daubert*: Practically the Same?*, 87 MINN. L. REV. 1579, 1611-12 (2003).

40. *See* Cheng & Yoon, *supra* note 35, at 482-84 (describing methods of study).

41. *See* Cheng & Yoon, *supra* note 35, at 503 (proffering that no practical difference exists in admissibility rates between the *Frye* and *Daubert* standards).

42. *See* Cheng & Yoon, *supra* note 35, at 474, 503 (drawing conclusions from study's findings).

This conclusion should not be surprising given how both tests rely solely on the scientific community. In determining if the scientific method has been sufficiently tested, the judge has no personal knowledge of the standards in a given field, so he or she must defer to the expert.[43] The same is true in determining whether the error rate is acceptable.[44] Furthermore, the peer review factor is essentially stating that others in the field must have reviewed the method and approved of it.[45] This is essentially the same as the general acceptance prong.[46] Even after *Daubert*, judges still do not have the technical expertise to make a determination of reliability on their own and must rely almost exclusively on the opinion of expert witnesses.[47]

III. Digital Forensics

A. Computer Forensics

Since modern cell phones are essentially small, low-powered computers, the study of mobile phone forensics emerged as a branch of computer forensics.[48] Thus, an overview of computer forensic procedures is helpful in understanding the techniques for cell phones.

When dealing with a computer investigation, an investigator arriving on the scene adheres to the most important rule in evidence collection: "Change nothing."[49] In practical

43. *See* RICE, *supra* note 12, at 471 n.20 (pointing out the difficulty judges face when considering admissibility of scientific evidence under any standard).

44. *See* RICE, *supra* note 12, at 472 n.20 (discussing the difficulty of determining what an acceptable rate of error is for a given industry).

45. *See* RICE, *supra* note 12, at 471 n.20 (comparing peer review discussions in *Daubert* and *Frye*).

46. *See* RICE, *supra* note 12, at 472 n.20 (requiring the judge to return to the expertise of the given scientific community).

47. *See* RICE, *supra* note 12, at 471 n.20 (noting the lack of scientific expertise among most judges).

48. *See* Shafik G. Punja & Richard P. Mislan, *Mobile Device Analysis*, 2 SMALL SCALE DIGITAL DEVICE FORENSICS J. 1, 1 (2008) (describing the growth of digital forensics in the twenty-first century).

49. *See* MICHAEL SHEETZ, COMPUTER FORENSICS: AN ESSENTIAL GUIDE FOR ACCOUNTANTS, LAWYERS, AND MANAGERS 29 (2007) (highlighting the importance of the "Change nothing" rule); Rebecca Hendricks, *Admissibility of Small Scale*

situations, however, small alterations are inevitable.[50] Presented with a powered-on computer, the forensic expert must make a decision on how to proceed based on the facts of the case.[51] Even simply moving the mouse changes the state of the computer, because the operating system shifts memory to re-position the cursor on the screen.[52] Turning off the computer causes many more alterations to the evidence as files are closed, and the system performs standard "housekeeping" operations.[53] Powering off the machine also erases any data stored in RAM, the fast-access memory which stores the current state of the system.[54]

Despite the impracticality of flawless preservation, there are a number of ways to ensure that only minor changes occur.[55] The investigator will meticulously record every detail of the collection process so that he or she can testify as to what changed within the system during the investigation.[56] Because there are only a few major operating systems, and their function is well-known, an examiner can describe exactly what system processes were running and what memory was changed during the collection process.[57]

Once a computer is turned off, a forensic specialist can ensure that no data on the hard drive will change from that point

Digital Devices in U.S. Civil Litigation, 2 SMALL SCALE DIGITAL DEVICE FORENSICS J. 1, 3 (2008) (explaining the importance of not altering electronic evidence).

50. *See* SHEETZ, *supra* note 49, at 28-29 (contrasting forensics in theory with forensics in practice).

51. *See* SHEETZ, *supra* note 49, at 28 (listing the items a forensic examiner must review during his or her investigation).

52. *See* SHEETZ, *supra* note 49, at 28-29 (highlighting the difficulties of following the "change nothing" rule).

53. *See* SHEETZ, *supra* note 49, at 27-28 (weighing factors examiner must consider when faced with a powered-on computer).

54. *See* SHEETZ, *supra* note 49, at 30 (asserting additional considerations for computer forensic acquisition).

55. *See* SHEETZ, *supra* note 49, at 31 (stressing importance of complying with standards to minimize alteration to data).

56. *See* SHEETZ, *supra* note 49 (presenting the best practices for an examiner regarding the collection of digital evidence).

57. *See* Shachtman, *supra* note 2 (noting difficulties in cell phone forensics as compared to computer forensics).

forward.[58] This process is accomplished in two ways.[59] First, the hard drive is connected to the forensic workstation using a write blocking device.[60] This device captures all the commands from the workstation computer to the drive and filters out any commands that would change data.[61] Next, the settings in a part of the computer called the BIOS are changed so the operating system cannot be loaded from the hard drive.[62] The BIOS contains the initial instructions to the computer on how to start up.[63] By changing the settings, the processor never accesses the hard drive, and instead reads the operating system from an entirely separate source.[64]

Once the forensic specialist has gained access without altering the disk, he or she will then acquire an exact, bit-for-bit copy of the drive.[65] As an alternative, the investigator could simply copy each individual file from the hard drive, but this is not the accepted method, as file-by-file duplication may miss critical evidence and will not recover deleted data.[66]

58. *See* SHEETZ, *supra* note 49, at 30, 32 (explaining that when computer is off data is saved and preserved).

59. *See* SHEETZ, *supra* note 49, at 33 (outlining two methods of preservation).

60. *See* SHEETZ, *supra* note 49, at 33 (listing initial steps in a forensic examination). *See also* KEITH J. JONES ET AL., REAL DIGITAL FORENSICS 171-74 (2006) (providing step-by-step instructions for digital forensic analysis).

61. *See* SHEETZ, *supra* note 49, at 117-18 (explaining how "write blocker" works). Write blockers can also be software that runs in the background of the forensic tools which prevent write commands from going to the disk. *See id.* at 117-18. However, some forensic investigators prefer physical write-blocking devices that attach to the cable connecting the computer to the drive. *See id.* at 117.

62. *See* SHEETZ, *supra* note 49, at 32 (continuing to the next step in the analysis process under BIOS method).

63. *See* SHEETZ, *supra* note 49, at 32 (defining "BIOS"). BIOS stands for "basic input output system or basic integrated operating system . . . ." *Id.*

64. *See* SHEETZ, *supra* note 49, at 32 (outlining how BIOS preserves the integrity of the existing operating system). Forensics investigators can boot the hard drive from a CD, floppy disk, or a different computer. *See id.* at 33.

65. *See* SHEETZ, *supra* note 49, at 34 (stating results of a successful acquisition).

66. *See* SHEETZ, *supra* note 49, at 33-34 (noting that a complete hard drive backup does not copy all files). When a file is deleted, its contents are not changed, but instead it is simply flagged as deleted. *See* FORENSIC COMPUTER CRIME INVESTIGATION 104 (Thomas A. Johnson ed., 2006). This indicates that the particular memory used to store the file is free to be overwritten should it ever

After the disk has been copied, the forensic investigator can prove that no data has been altered by computing the hash value of the copy to that of the original.[67] A hash is a mathematical algorithm that takes in the value of every bit on the drive and computes a fixed-size, unique identifier.[68] If even a single bit is changed, the hash value will be substantially different.[69] If using the popular MD5 hashing algorithm, the chances of two files computing to the same hashing is about one in 3.4×10^{38}.[70] Therefore, if the forensic examiner computes the hash of the acquired drive before and after copying, he or she can prove to a mathematical certainty that no data has changed.[71] Also, the hash of the copy can be compared to that of the original to prove that it is in fact an exact copy.[72]

B. Cell Phone Forensics

be needed. *Id.* Thus, the data will remain until it is overwritten, and even once it is overwritten, parts of the original file can still be recovered. *Id.*

67. *See* SHEETZ, *supra* note 49, at 118-19 (advocating for reliability of hash values).

68. *See* Shira Danker, Rick Ayers & Richard P. Mislan, *Hashing Techniques for Mobile Device Forensics*, 3 SMALL SCALE DIGITAL DEVICE FORENSICS J. 1, 1 (2009) (defining "secure hash" as "[a] mathematical algorithm that takes an arbitrary block of data and returns a fixed-size bit string, the hash value, such that any change to the data will modify the hash value.").

69. *See* ACCESSDATA, MD5 COLLISIONS: THE EFFECT ON COMPUTER FORENSICS 3 (2006) (highlighting effectiveness of hash values with MD5 algorithm); FORENSIC COMPUTER CRIME INVESTIGATION, *supra* note 66, at 105 (describing features of hashing such as matching known violations); SHEETZ, *supra* note 49, at 113 (comparing hash values to digital fingerprint). To illustrate, compare the MD5 hashes of the following words:

Words	MD5 Hash Value
cell tower	654bb73b6ee0288e1518103d2bd45274
bell tower	53496f39032693e28610561192e54342

See MD5 HASH GENERATOR, Feb. 1, 2011, *archived at* http://www.webcitation.org/5wB5E3My7 (allowing users to enter string to create MD5 hash values).

70. *See* ACCESSDATA, *supra* note 69, at 3 (calculating the effectiveness of a MD5 hash in ensuring uniqueness).

71. *See* SHEETZ, *supra* note 49, at 118-19 (highlighting overall purpose of hashing).

72. *See* SHEETZ, *supra* note 49, at 118-19 (explaining importance of hash value).

Since both cell phones and computers store information electronically, once removed from their respective devices, evidence acquired from either is stored and handled in the same way.[73] The difference between the two forensic processes is the method for retrieving the data from the device.[74] Computer hard drives store information in a few widely-known formats and thus computer forensic tools know exactly where to look, and how to access the data.[75] Cell phones store data in a large variety of different formats, and the manufacturers traditionally have not released the storage specifications.[76] This means that no mobile forensic tool is able to simply make an exact copy of everything stored on the device, forcing mobile forensic investigators to come up with other techniques.[77]

The most obvious way to access the phone is to simply press its buttons and navigate through the information the same way its user would.[78] This method, however, is widely disfavored in the mobile forensic community as it will change the data on the phone, and pressing the wrong key could destroy vital evidence.[79] Despite its problems, companies sell products which allow investigators to easily take pictures of cell phone screens as

73. *Compare* DUMMIES.COM, *RAM, ROM, and Flash Memory, archived at* http://www.webcitation.org/5wB6w8Dg1 (listing and describing various kinds of computer memory) *with* USB4EVER, *Types of Cell Phone Memory, archived at* http://www.webcitation.org/5wB6pf15n (listing types of cell phone memory).

74. *Compare* Jansen et al., *supra* note 3, at 1 (explaining cell phone memory retrieval), *with* TYLER MOORE, THE ECONOMICS OF DIGITAL FORENSICS 2 (2006) (explaining computer memory retrieval).

75. *See* MOORE, *supra* note 74, at 2 (comparing forensic effectiveness of open versus closed systems). NTFS and FAT are the most common formats for computer data storage. *Id.*

76. *See* Jansen et al., *supra* note 3, at 1 (explaining that "mobile phone manufacturers employ many different proprietary operating systems and storage structures.").

77. *See* Jansen et al., *supra* note 3, at 2 (pointing to creative steps forensic specialists must take when new phones are released).

78. *See* McCarthy, *supra* note 7, at 22 (illustrating a possible technique for navigating a cell phone).

79. *See* McCarthy, *supra* note 7, at 22 (highlighting issues with the manual extraction technique). *See also Best Practices*, *supra* note 7, at 6 (listing manual acquisition as the least recommended method); Svein Yngvar Willassen, *Forensics and the GSM Mobile Telephone System,* 2 INT'L J. OF DIGITAL EVIDENCE 1, 11 (2003) (criticizing the method as "cumbersome").

they browse through the phone using the keypad.[80] In at least one instance, a court admitted evidence acquired in this manner.[81]

The way that most forensic specialists acquire data is using phone interface commands.[82] A command is sent to the phone, which processes it and replies with the information requested.[83] Different commands must be used based on a phone's model and manufacturer.[84] With new phones released every three to six months, it is almost impossible for forensic tools to keep pace.[85] As a result, there is no universal software program that works with every phone.[86]

Some cell phone manufacturers offer "phone manager" software which allow for data acquisition from their own brand of phone, but these programs are not designed to be forensically sound and thus, likely alter the data during acquisition.[87] The

80. *See* PROJECT-A-PHONE, *archived at* http://www.webcitation.org/5wB9zBiKT (selling product that takes pictures of cell phone screens).

81. *See* Dickens v. State, 927 A.2d 32, 36 (Md. Ct. Spec. App. 2007). A mother, scrolling through her daughter's cell phone after the girl was murdered, found five incriminating text messages. *Id.* She alerted the police and an officer came to her house and took photos of the cell phone screen displaying the text messages. *Id.* These photos were admitted into evidence. *Id.* The defense objected on authentication grounds, but it is not clear whether there was ever a reliability challenge. *Id.*

82. *See* WAYNE JANSEN & RICK AYERS, NAT'L INST. OF STANDARDS AND TECH., SPECIAL PUB. 800-101, GUIDELINES ON CELL PHONE FORENSICS 45 (2007) [hereinafter NIST GUIDELINES] (stating that phone interface commands are "the prevailing technique used by present day forensic tools").

83. *See* McCarthy, *supra* note 7, at 34 (stating conclusions from study of AT commands). For example, some GSM phones, if sent the command "AT+CGSN," will respond with the IMEI, which is the phone's unique identification number. *See id.*

84. *See* McCarthy, *supra* note 7, at 33 (explaining how command-based mobile forensics works).

85. *See* Ibrahim M. Baggili et al., *Mobile Phone Forensics Tool Testing: A Database Driven Approach*, 6 INT'L J. OF DIGITAL EVIDENCE 1, 4-5 (2007) (acknowledging the need to constantly re-evaluate error rates in forensic tools as technology quickly advances to avoid being outpaced).

86. *See* McCarthy, *supra* note 7, at 14-15 (describing the impossibility of the creation of a software application that works with all phones).

87. *See* Jansen et al., *supra* note 3, at 2. Because the technology is not forensically sound, it allows for data to be changed on the phone. *See id.* In one incident, a forensic examiner accidentally put data from his own personal phone onto a suspect's phone he was examining. *See id.*

alternative is a group of third party forensic software, covering only a select number of phones.[88] Even if a phone is supported, the command-based acquisition technique the software uses still cannot retrieve deleted data.[89] This is because the phone is being accessed at the operating system level, which can no longer access deleted data.[90]

To further complicate matters, how the phone internally processes the commands has traditionally been a closely-guarded secret of the phone manufacturer.[91] Forensic specialists must reverse engineer the phone to discover what works.[92] Each new phone a manufacturer issued must be individually "cracked" to determine which commands work.[93] At the end of the process, the examiner only knows the command and its output, but not what happened in between.[94] Thus, there is no way to tell for certain if a tool properly acquired the data without changing anything else.[95] In fact, just by sending a command, it is necessarily causing at least some change in data by making the phone process it.[96]

88. *See* McCarthy, *supra* note 7, at 14-15 (explaining the impossibility of a universal software application).

89. *See* MOORE, *supra* note 74, at 3 (observing that deleted data cannot be retrieved by means of the phone's interface software); McCarthy, *supra* note 7, at 23 (noting that deleted information is inaccessible).

90. *See* MOORE, *supra* note 74, at 3 (listing limitations of cell phone forensic technology).

91. *See* MOORE, *supra* note 74, at 3 (contrasting landscape of computer and mobile forensics). Recently several mobile operating systems have been made open-source, most notably Google's Android OS.91.*See* Clint Boulton, *Google Open-Sources Android on Eve of G1 Launch*, EWEEK.COM, Oct. 21, 2008, *archived at* http://www.webcitation.org/61CvHUYsD (announcing Google's release of the full source code for Android)

92. *See* MOORE, *supra* note 74, at 3 (describing various challenges for examiners). *See, e.g.*, McCarthy, *supra* note 7, at 28 (stating that the only publicly-available information for Nokia's FBUS protocol is from monitoring and reverse engineering).

93. *See* Hilary Hylton, *What Your Cell Knows About You*, TIME, Aug. 15, 2007, *archived at* http://www.webcitation.org/5wEDqgUtF (describing the progress made in the field of mobile forensics in the last twenty years). The top mobile forensics companies can crack a new phone's operating system in about a week. *See* Shachtman, *supra* note 2.

94. *See* McCarthy, *supra* note 7, at 33 (drawing attention to limitations of command-based forensics).

95. *See* McCarthy, *supra* note 7, at 33 (providing an overview of methods of mobile forensic acquisition).

96. *See* McCarthy, *supra* note 7, at 33 (highlighting issues with scientific

To illustrate these problems, take the example of the Sony Ericsson f500i. For this phone, the command to retrieve a text message is "AT+CMGR=10, /r."[97] The examiner sends this command from a computer to the phone, and will receive back "+CMGR; 0,,35, /r/n," then the text of the message.[98] The zero in the return message indicates that the text is unread.[99] If the same command is sent again, the phone will return the same message, except with a one instead of a zero, indicating the text has been read.[100] This example highlights two major problems with command-based cell phone forensics.[101] First, the examiner changed the data on the phone by making a text message change status from "unread" to "read."[102] This violates the most important principle of evidence collection by altering the evidence.[103] Second, the only thing that is known about the process is the command entered and the result.[104] The examiner cannot know how the phone processed the command and returned the text message.[105]

This basic example highlights the shortcomings at the core of command-based acquisition.[106] In actual practice, the situation

validity of results).

97. *See* McCarthy, *supra* note 7, at 36 (providing example of where command-based forensics alters data within the phone).

98. *See* McCarthy, *supra* note 7, at 36 (demonstrating the beginning stage of the AT command retrieval process).

99. *See* McCarthy, *supra* note 7, at 36 (deciphering the meaning of the text message code).

100. *See* McCarthy, *supra* note 7, at 36 (instructing how to discern whether a text has been read or not).

101. *See* McCarthy, *supra* note 7, at 36 (observing that entering the same code twice yields inconsistent outcomes).

102. *See* McCarthy, *supra* note 7, at 36 (verifying that when the examiner reads the message he alters the command to retrieve it).

103. *See* NIST GUIDELINES, *supra* note 82 (reiterating first evidentiary principle: "actions taken should not modify data contained on the device . . . ."). *See also* SHEETZ, *supra* note 49, at 29 (stating that the most important rule is "change nothing").

104. *See* McCarthy, *supra* note 7, at 34 (observing that the result does not indicate whether there was an alteration to the data).

105. *See* McCarthy, *supra* note 7, at 33 (demonstrating a limitation of command-based mobile forensics).

106. *See* McCarthy, *supra* note 7, at 36 (summarizing the limitations of the AT command retrieval system).

is even murkier.[107] The everyday examiner does not interact with the phone at a command level, but instead uses software tools.[108] Instead of typing each individual command, clicking the software's "acquire" button will simply retrieve all the data it can from the phone.[109] While some open-source tools exist, much of this software used today is itself proprietary.[110] This means that in addition to not knowing how the phone is processing the commands, the examiner also does not even know what commands the tool is sending.[111] Despite all these issues, mobile forensic experts commonly use this type of acquisition.[112]

A new technology called "flashing" claims to fix all the problems of command-based acquisition.[113] Rather than interfacing with the operating system, this method goes straight to where the memory is stored and retrieves it.[114] This bypasses any password protection, does not require the phone to be on, and can acquire much more information than other techniques, including deleted data.[115] Much like traditional computer forensics, flashing acquires an image of the phone's memory,

107. *See* NIST GUIDELINES, *supra* note 82 (noting the care a technician should take to avoid altering data stored on a phone).

108. *See* NIST GUIDELINES, *supra* note 82 (connecting to a forensic work station allows software to acquire data from the cell phone).

109. *See* NIST GUIDELINES, *supra* note 82 (demonstrating the use of software-based acquisition versus manual command-based acquisition); One such open source forensics tool is the Open Source Android Project. Open Source Android Project, VIAFORENSICS.COM, http://www.webcitation.org/61BiPkm5l.

110. *See* McCarthy, *supra* note 7, at 33 (stating that "the internal workings of a mobile phone
are proprietary information . . . .").

111. *See* McCarthy, *supra* note 7, at 33 (conceding that the first evidentiary principle of not changing data cannot be strictly complied with).

112. *See* NIST GUIDELINES, *supra* note 82 (employing the use of software-based acquisition).

113. *See* Michael Harrington, *Hex Dumping Primer*, MOBILE DEVICE FORENSICS 1, 1, Apr. 5, 2007, *archived* at http://www.webcitation.org/5lmBUbE3U (describing the purpose of flashing). The purpose is "to get as close to the forensic image which is the bread and butter of conventional electronic evidence forensics and thereby have a best evidence exhibit as defined by legal courts." *Id.*

114. *See* Lars Wolleschensky, *Cell Phone Forensics* 11 (Ruhr-Universität Bochum, Working Paper, 2007) (realizing the potential of the flashing technique).

115. *See* Harrington, *supra* note 113, at 1-2 (extolling the advantages of flashing).

called a "hex dump."[116] This is a bit-for-bit snapshot of the physical memory.[117]

Flashing, however, is not without problems.[118] Because the software is proprietary, it is not known exactly how the technology works.[119] It was not developed for forensics, but rather to bypass manufacturer restrictions.[120]

None of the current techniques have the safeguards for reliability available for traditional computer forensics.[121] There are no write blocking devices to prevent inadvertent tampering.[122] It allows a user to change the phone settings so that it could be used with a different cell service provider.[123] The tools were developed originally by the hacker community to break into phones and reprogram them.[124] Furthermore, repeated acquisitions from the same phone will yield varying hash values.[125] Research has shown that hash values of some

116. *See* Harrington, *supra* note 113, at 1 (stating that flashing will be closer to traditional computer forensics than other methods).
117. *See* Harrington, *supra* note 113, at 1 (providing the outcome of the flashing process).
118. *See* Harrington, *supra* note 113, at 2 (explaining the caveats of hex dumping).
119. *See* Harrington, *supra* note 113, at 2 (noting the flasher "boxes and software used are not 'officially' sanctioned by the handset manufacturers"). *See also* Wolleschensky, *supra* note 114, at 11-12. "Nothing is officially known about the Flasher Boxes and there workings because they were developed in the black hat community. . . ." *Id.* at 12.
120. *See* Harrington, *supra* note 113, at 2 (listing "caveats" to flashing). *See also* Wolleschensky, *supra* note 114, at 11-12. "The problem is that with very few exceptions these tools were developed by the Black hat community to flash phones, break pin locks and alter operating systems". *Id.* at 11-12
121. *See* McCarthy, *supra* note 7, at 59 (observing that new methods are not as forensically sound as traditional ones).
122. *See Best Practices*, *supra* note 7 (listing limitations of mobile forensics); MARWAN AL-ZAROUNI, INTRODUCTION TO MOBILE PHONE FLASHER DEVICES AND CONSIDERATION FOR THEIR USE IN MOBILE PHONE FORENSICS 151 (Dr. Craig Valli and Dr. Andrew Woodward eds., 2007), *archived at* http://www.webcitation.org/5wq93qrs6 (opining on the necessity of changing data when using command based forensic tools).
123. *See* Harrington, *supra* note 113, at 2 (explaining the original intended use of flasher boxes).
124. *See* Wolleschensky, *supra* note 114, at 11-12 (recounting the history of the development of flashing).
125. *See Best Practices*, *supra* note 7 (describing limitations of the

individual data files, such as pictures and text messages, are consistent in back-to-back acquisitions, but this is not the case with all types of file, and could vary by phone.[126]

IV. Analyzing Cell Phone Forensics Under the *Daubert* Factors

A. Testing

In the field of mobile forensics, the tools used for data extraction have never been fully tested independently and no error rates have been published.[127] In 2005, the National Institute of Standards and Technology attempted to remedy this, conducting an analysis on the major tools on the market at the time.[128] The study, however, only analyzed seventeen phones, and merely intended to demonstrate the tools' capabilities, not ensure their accuracy.[129] The study explicitly differentiates itself from the Computer Forensic Tool Testing (CFFT) project, an effort to ensure the accuracy of *computer* forensic tools.[130] To date, there has not been a similar accuracy test for cell phone forensic tools.[131]

One of the reasons for the lack of testing is that manufacturers release phones too fast for the tools to keep up,

technology). The variable hash values may be because of operating system optimization. *See id.*

126. *See Best Practices*, *supra* note 7 (listing limitations of cell phone forensics). Generally, graphics, audio, and video files will be consistent, but not MMS messages, or system files. *See id.* *See also* Danker et al., *supra* note 68, at 3 (noting that hash values for MMS messages were inconsistent between mobile device families).

127. *See* Baggili, *supra* note 85, at 1 (introducing the idea that a database driven approach to acquisition could address the problem of the lack of error rates based on the proprietary nature of cell phones).

128. *See* RICH AYERS ET AL., NAT'L INST. OF STANDARDS AND TECH., NISTIR 7250, CELL PHONE FORENSIC TOOLS: AN OVERVIEW AND ANALYSIS iv (2005) [hereinafter NIST TESTING] (testing several forensics tools for accuracy).

129. *See* NIST TESTING, *supra* note 128, at v (clarifying the project's objective); Baggili, *supra* note 85, at 1-2 (characterizing the reports of the NIST as far from complete).

130. *See* NIST TESTING, *supra* note 128, at v (stating the purpose of the tests is to provide accurate results for computer forensics investigations).

131. *See* Baggili, *supra* note 85, at 1 (highlighting the need testing the accuracy of mobile forensic tools).

leaving the burden of validation to the experts themselves.[132] There are several standards for tool validation.[133] They require the technician to put test data on a phone, use a tool to acquire it, and then determine if it was extracted accurately.[134] In preparation for trial and prior to extracting data, a mobile forensic expert will test his or her equipment on a phone of the same model as the suspect's.[135]

Under the current state of affairs, the only testing a cell phone expert in a *Daubert* hearing can point to is his own.[136] Courts have rejected this sort of self-verification in the past.[137] In *People v. Young*, 391 N.W.2d 270 (1986), the court stated: "The scientific tradition expects independent verification of new procedures. When other scientists analyze and repeat the tests, they counteract the dangers of biased reporting. It is scientists not responsible for the original research that confirm its validity."[138] The tools of cell phone forensics have yet to undergo legally sufficient testing and therefore, fail the testing prong of *Daubert*.[139]

B. Error Rates

132. *See* Baggili, *supra* note 85, at 4-5 (admitting it is a difficult task to keep up with advancing cell phone technology); Hylton, *supra* note 93 (explaining that forensics are constantly struggling to keep up with cell phone production rates).

133. *See* John J. Barbara, *Appropriate Standards and Controls in Computer Forensics*, FORENSIC MAGAZINE, Oct./Nov. 2007, at 6 (discussing the various tools for validation of cell phone forensics testing). *See also Best Practices*, *supra* note 7, at 5-6 (listing levels of forensic soundness for tools).

134. *See Best Practices*, *supra* note 7, at 7 (enumerating steps for validation).

135. *See* Barbara, *supra* note 133 (examining steps experts will take before bringing evidence to trial).

136. *See* Baggili, *supra* note 85, at 1-2 (pointing to the lack of error rate statistics available for forensic cell phone testing methods).

137. *See* People v. Young, 391 N.W.2d 270, 272 (1986) (proffering that scientists would be biased when verifying their own work); People v. Seda, 139 Misc.2d 834, 846 (N.Y.Sup. 1988) (rejecting the notion that a "relevant scientific community" is comprised almost entirely of law enforcement officials).

138. *Young*, 391 N.W.2d at 283.

139. *See id*. (determining that there is insufficient independent scientific testing for these new procedures).

As noted in the previous section, the field of cell phone forensics has fully tested its tools, and therefore, there are no known error rates.[140] That is not to say, however, that there are no known errors.[141] On the contrary, the existing literature on the technology is replete with instances where the tools have failed to produce accurate results.[142] In the NIST analysis, many tools missed graphics files, e-mails, address books, web content, and contacts.[143] This is especially problematic because an examiner on a real case would not know whether the missing files never existed or were simply just not acquired.[144] The literature also lists the technical limitations of the technology, including: "data can be indirectly altered, when using AT commands," "important data may be omitted from the phone's response," "some data will never be accessible over a software interface," and "overall case file hashes of system files will typically not be consistent."[145] In the current state of cell phone forensics, the error rate is unknown, but it is known that several serious errors can occur.[146]

C. Standards

Several sets of standards exist for cell phone forensics.[147] The Scientific Working Group on Digital Evidence's (SWGDE) has produced *Best Practices for Mobile Phone Examinations*, and the

140. *See* Baggili, *supra* note 85, at 1-2 (stating the need for centralized testing to develop error rates that could be used to validate or invalidate acquisition tools).

141. *See, e.g.*, NIST TESTING, *supra* note 128 (testing major forensic tools and listing the errors produced).

142. *See* NIST TESTING, *supra* note 128, 120-55 (describing conclusions of the study for the various devices tested).

143. *See* NIST TESTING, *supra* note 128, 120-55 (detailing the results of the tests using a Forensic Recovery of Evidence Device).

144. *See* McCarthy, *supra* note 7, at 53 (noting important data may be omitted from results).

145. McCarthy, *supra* note 7, at 53. *See also Best Practices*, *supra* note 7 (introducing systemic problems with software-based acquisition).

146. *See* McCarthy, *supra* note 7, at 53 (outlining four possible substantial flaws).

147. *See Best Practices*, *supra* note 7, at 4 (providing guidelines investigating officers must adhere to when seizing cell phone evidence); NIST GUIDELINES, *supra* note 82, at 82-92 (outlining the various choices a technician has available to him through each step of the acquisition process).

NIST published *Guidelines on Cell Phone Forensics*.[148] Both provide complete guides on how to properly isolate the phone, secure the scene, and later conduct the examination.[149] However, they are lacking when it comes to actual acquisition of evidence.[150] The NIST Guidelines simply describe the steps of using the software.[151] The standards of the SWGDE offer even less guidance; they only list the various ways to acquire the data and instruct the examiner to use the most forensically sound first.[152] Since the standards do not truly cover the acquisition of cell phone evidence, no standards exist concerning the practice. Therefore, the technique fails to meet the standards prong of *Daubert*.

D. Peer-reviewed Articles

While many articles on the topic of cell phone forensics exist, most are concerned with providing instruction for performing the technique rather than an analysis of its reliability.[153] Of the articles that do address admissibility, serveral directly state that mobile evidence in its current state fails the *Daubert* factors. According to one paper, "when [digital forensic]

148. *See Best Practices*, *supra* note 7, at 2 (noting the purpose of *Best Practices* is to "describe the best practices for mobile phone examinations."); NIST GUIDELINES, *supra* note 82 (producing recommendations to the U.S. Departments of Commerce and Homeland Security).

149. *See, e.g.*, *Best Practices*, *supra* note 7, at 2 (describing the step-by-step process for seizing cell phone information); NIST GUIDELINES, *supra* note 82, 82-92 (demonstrating the acquisition method using screen shots from a computer).

150. *See* NIST GUIDELINES, *supra* note 82 (recommending acquiring all information in a single acquisition to avoid problems in the future).

151. *See* NIST GUIDELINES, *supra* note 82 (highlighting the steps of acquisition accounted for in Appendix C of the report). The steps are "selecting a connection, identifying the device to be acquired, identifying the data to be recovered, and viewing the recovered data." *Id.*

152. *See Best Practices*, *supra* note 7, at 5-6. Its rankings for most forensically-sound methods are: 1) MicroRead, 2) Chip-Off, 3) Hex dump, 4) Logical, 5) Manual. *Id.*

153. *See, e.g.*, Danker et al., *supra* note 68 (comparing mobile device memory hash values with other values for data found on cell phones); Rebecca Kanable, *supra* note 3 (summarizing the types of evidence found on cell phones used in criminal investigations); Kohtz & Churchill, *supra* note 2 (stating the usefulness of information stored on cell phones for civil or criminal investigations).

scientists examine the above procedures, it is obvious that the science is deficient in the areas specified by the *Daubert* process."[154] Another article states,

> "The only argument which could be used to confirm the correct operation of these methods is that they are in common use, and are regularly relied upon to acquire data, forensically or otherwise. This argument is insufficient for these methods to be scientifically acceptable, however."[155]

Furthermore, due to the largely proprietary nature of the tools in this field, there are no articles that detail exactly how the process works.[156] *Daubert* requires that the "theory or technique" be subjected to peer-review and publication.[157] The unreliable "technique" in cell phone forensics is data acquisition.[158] Exactly how this technique works has not been published, and therefore, it fails this prong of *Daubert*.

E. General Acceptance

The most important prong of *Daubert* is the "general acceptance of the relevant scientific community."[159] As noted in the previous section, some published peer-reviewed articled

154. *See* Baggili, *supra* note 85, at 3 (advocating the need for better standards and testing).
155. *See* McCarthy, *supra*, note 7, at 33 (discussing the limitations of current forensic techniques).
156. *See* MOORE, *supra* note 74, at 3 (contrasting cell phone and computer forensics); McCarthy, *supra* note 7, at 33 (acknowledging that the proprietary nature of cell phone information makes it impossible to determine whether data retrieval is consistently successful).
157. *See Daubert*, 509 U.S. at 593 (concluding that peer review and publication will be helpful in determining relevance, but not dispositive of determining validity).
158. *See* McCarthy, *supra*, note 7, at 33 (arguing that data retrieval methods may be insufficient as scientifically acceptable under *Daubert*). *See also Daubert*, 509 U.S. at 593 (explaining that the technique needs to be tested to be admissible).
159. *See* RICE, *supra* note 12, at 468 (noting that general acceptance is a key factor in determining admissibility under *Daubert*).

have called the forensic-soundness of such techniques into question.[160] On the other hand, many professionals have used and relied upon the technology, demonstrating an acceptance of its reliability.[161] When presented as evidence, the outcome of the general acceptance prong will depend on how the court determines who is included in the "relevant scientific community."[162]

If the court were to define the community as mobile forensic experts, then clearly the methods they employ everyday in their work would be generally accepted.[163] The fact that the technology is used by law enforcement nationwide would also demonstrate acceptance.[164] On the other hand, should the court expand the community to all digital forensics experts, this would include computer forensics experts.[165] As discussed previously, cell phone forensics lack write-blocking devices, consistent hash values, well-known file systems, and the ability to acquire bit-for-bit copies.[166] These techniques are the cornerstones of traditional computer forensics, and failure to use them is not generally accepted.[167] Thus, the definition of the relevant field is crucial in the analysis.

There are clear problems with defining the relevant scientific community as "mobile forensic experts."[168] Their job depends on the evidence being admissible, giving them personal

160. *See* part IV, D *infra*.
161.
162. *See Daubert*, 509 U.S. at 593 (premising general acceptance on the degree of acceptance in the "relevant scientific community . . .").
163. *See* NIST TESTING, *supra* note 128, at v (identifying the users of cell phone forensics technology as a cohesive group).
164. *See* Shachtman, *supra* note 2 (giving examples of how law enforcement has used cell phone evidence nationwide).
165. *See* MOORE, *supra* note 74, at 3 (comparing multiple types of digital forensics).
166. *See* Harrington, *supra* note 113, at 2 (noting the shortcomings of forensic technology). *See also* McCarthy, *supra* note 7, at 59 (observing that cell phone forensics have not been proven to be scientifically consistent).
167. *See* SHEETZ, *supra* note 49, at 28-34 (demonstrating forensically-accepted techniques for computer digital forensics).
168. *See* NIST TESTING, *supra* note 128, at v (explaining to whom cell phone forensic tools are useful).

and financial incentive to accept the methodology, as opposed to a scientific one.[169] According to the Michigan Supreme Court, a scientific community comprised only of those with an interest in the case, "would be too small for a fair sampling of scientific opinion."[170] Likewise, the Supreme Court of California cited two forensic technician's "identification with law enforcement, their career interest in acceptance of the tests" as reasons for rejecting their claim of general acceptance.[171] In *People v. Seda*, 139 Misc.2d 834 (N.Y.Sup. 1988), the court refused to admit testimony of a methodology that had "not been sufficiently appraised by *unbiased* scientists."[172] Mobile forensics experts hold a professional and financial interest in courts finding the evidence they produce to be admissible.[173] Thus, the scientific community should expand to include those who do not stand to gain.

The courts have also had issues with experts being "technicians" as opposed to "scientists."[174] The *Young* court held that the "relevant scientific community" consists of "scientists not technicians," reasoning that "a theoretical understanding is essential."[175] According to *People v. Brown*, 40 Cal.3d 512 (1985), "the witness must have academic and professional credentials which equip him to understand both the scientific principles

169. *See* "*General Acceptance" Looks for a Relevant Scientific Community*, 3 NO. 2 CRIM. PRAC. GUIDE 11, 11 (2002) [hereinafter *General Acceptance*] (referring to the personal and financial interest of fingerprint experts); David Johnston & Andrew C. Revkin, *Report Finds F.B.I. Lab Slipping From Pinnacle of Crime Fighting*, N.Y. TIMES, Jan. 29, 2007, *archived at* http://www.webcitation.org/5wLlTVgP9 (noting that scientists felt stifled by agents with little scientific knowledge who regularly altered reports to help prosecutors).

170. *Young*, 391 N.W.2d at 271. The court reasoned that "the number of scientists not working for a police agency" on electorphoresis of dried bloodstains is too small. *Id.*

171. *See* People v. Brown, 40 Cal.3d 512, 533 (1985) (concluding that the scientists' personal interest in admissibility of the tests made them unqualified as "impartial scientists").

172. *Seda*, 139 Misc.2d at 848 (emphasis added).

173. *See General Acceptance*, *supra* note 169 (noting inherent bias due to financial and professional interests).

174. *See Brown*, 40 Cal.3d at 533 (distinguishing scientists from technicians).

175. *See Young*, 391 N.W.2d at 274-75 (explaining that the ideal community would be scientists with practical experience).

involved and any differences of view on their reliability."[176] The court in *Brown* held that technicians' "lack of formal training and background in the applicable scientific disciplines made them unqualified to state the view of the relevant community of *impartial scientists*."[177]

While many cell phone forensic experts have strong scientific background, it is not a prerequisite for the job.[178] By defining the relevant scientific community as "mobile forensic experts," a court would include those without science backgrounds.[179] Furthermore, because of proprietary software and lack of scientific research, the experts have no access to information about how the tools work.[180] Without such a background, an expert would not meet the *Daubert* requirement that the testimony be true "scientific knowledge."[181]

V. Current State of Admissibility

To date, the courts have not directly addressed the reliability of cell phone forensic evidence in a published opinion. It has, however, been used in numerous cases but not challenged.[182] One such case is *Southeastern Mechanical Services v. Brody*, 657 F. Supp. 2d 1293 (2009), where the defendant stood accused of spoliation of evidence by wiping his Blackberry.[183] A cell phone forensic expert, Jon Kessler, examined the phone using

176. *Brown*, 40 Cal.3d at 530 (laying out precedent for determining a "qualified expert").
177. *Id.* at 533 (excluding evidence from two forensic technicians).
178. *See* NIST GUIDELINES, *supra* note 82, at 24 (noting that no national standards or certification exists for technicians and forensic examiners).
179. *See Brown*, 40 Cal.3d at 533 (explaining technicians' lack of scientific education).
180. *See* Baggili, *supra* note 85, at 3 (citing market-driven nature of the mobile forensics field as reason for lack of scientific understanding).
181. *See Daubert*, 509 U.S. at 590 (requiring stricter standards for expert witnesses).
182. *See* Baggili, *supra* note 85, at 1 (stating that "[I]n the past five years, dozens of murderers have been convicted partly as a result of evidence about their mobile phones or those of their victims.").
183. *See* Se. Mech. Services v. Brody, 657 F. Supp. 2d 1293, 1295 (2009) (alleging that plaintiff wiped crucial data from his phone and computer that he had a duty to preserve).

Paraben Device Seizure software.[184] He extracted from the phones: "lists of telephone calls, text messages, calendar items, e-mails, contact lists, memos, applications, and deleted items."[185] He testified that the software "ensured that the data on the BlackBerries was not contaminated or altered."[186] It is not clear how the expert determined this, but most likely he depended on a claim of reliability by the Paraben company.[187] Since it is a proprietary tool, working on a proprietary phone, Mr. Kessler has no real knowledge regarding whether data was in fact altered.[188] Still, the defense did not contest the reliability of this statement, and no *Daubert* hearing was held.[189]

VI. *Daubert* Analysis of Other Types of Evidence

Since no court has directly addressed the issue, to determine whether cell phone evidence will be able to stand up to *Daubert* scrutiny, one must analogize to other forms of similar forensic evidence which have recently been tested under the new standard.

A. Firearm Identification

Firearm (or Ballistic) Identification is the science of identifying the particular gun that a recovered bullet, or cartridge case came from.[190] It is based on the principle that no firearm is built exactly the same, and therefore, its unique imperfections

184. *See id.* at 1298 n.7 (testifying to contents of the phone's data).
185. *See id.* (recalling expert witness testimony). The fact that the device recovered deleted items means that it used "flashing" technology. *See* Harrington, *supra* note 113, at 1.
186. Se. Mech Services, 657 F. Supp. 2d at 1298 n.7.
187. *Device Seizure Product Details*, PARABEN CORP., Feb. 8, 2011, *archived at* http://www.webcitation.org/5wLuxEosO (guaranteeing that "[d]evice Seizure does not allow data to be changed on the device.").
188. *See* MOORE, *supra* note 74, at 3 (observing that "relevant data like call histories are stored in proprietary formats. . . ."); McCarthy, *supra* note 7, at 33 (listing limitations of mobile forensics).
189. *See, e.g.*, *Se. Mech. Services*, 657 F. Supp. 2d 1293 (failing to make *Daubert* a consideration in their analysis).
190. *See* MARIA JOSEPHI, FEDERAL BUREAU OF INVESTIGATION, HANDBOOK OF FORENSIC SCIENCE 57 (1994) (defining "firearm identification").

will leave different marks on the ammunition and casings when fired.[191] The forensic examiner fires the suspect weapon and then compares the spent bullet and cartridge case with those found at the crime scene.[192] He must then determine if there is a match based on his experience in the field.[193] This practice has been used as evidence in the courtroom since the 1920s, but it has faced recent challenges under the new *Daubert* standard.[194]

In *United States v. Green*, 405 F. Supp. 2d 104 (2005), an officer from the Boston Police Department testified that .380 caliber shell casings found at two separate crime scenes matched a pistol recovered over a year later.[195] He concluded that the match was so exact that it could be made "to the exclusion of every other firearm in the world."[196] As a result of this conclusion, the two defendants linked to the gun faced serious charges that could lead to the death penalty.[197]

The court was highly skeptical of the firearm identification testimony.[198] The officer had no certification in the science by any professional organization and had never been formally tested.[199] Furthermore, he took no pictures or notes during his investigation and based his entire conclusion on subjective

191. *See* Paul C. Giannelli, Daubert *Challenges to Firearms ("Ballistics") Identifications*, 43 NO. 4 CRIM. L. BULL. 548, 558 (2007) (outlining factors considered by ballistic expert).
192. *See* Giannelli, *supra* note 191, at 559 (listing steps an examiner will take).
193. *See* Giannelli, *supra* note 191, at 559 (calling interpretation of the marks "subjective in nature").
194. *See* Giannelli, *supra* note 191, at 562-63 (giving history of firearm and tool mark identification evidence).
195. *See* United States v. Green, 405 F. Supp. 2d 104, 107-09 (D. Mass. 2005) (reviewing the facts of the case, and holding that despite lack of testing, documentation, evidence or proficiency, firearm evidence could be introduced due to precedent).
196. *Id*. at 107.
197. *See id.* at 106 n.1 (finding that as a result of the ballistics evidence, the defendants could be sentenced to death).
198. *See id.* at 107 (communicating unease for the police officer's lack of ballistics certification).
199. *See id.* (expressing concern with the police officer's lack of actual ballistics qualifications).

judgment.[200] As for the field itself, the court noted that the prosecution produced no evidence of error rates or national standards.[201]

Despite these reservations, the court admitted the evidence stating:

> I reluctantly come to the above conclusion because of my confidence that any other decision will be rejected by appellate courts, in light of precedents across the country, regardless of the findings I have made. While I recognize that the *Daubert-Kumho* standard does not require the illusory perfection of a television show (CSI, this wasn't), when liberty hangs in the balance—and, in the case of the defendants facing the death penalty, life itself—the standards should be higher than were met in this case, and than have been imposed across the country. The more courts admit this type of toolmark evidence without requiring documentation, proficiency testing, or evidence of reliability, the more sloppy practices will endure; we should require more.[202]

The precedent the court refers to includes *United States v. Hicks*, 389 F.3d 514 (2004), *United States v. Foster*, 300 F. Supp. 2d 375 (D. Md. 2004), and *State v. Brewer*, No. X01CR02307016, 2005 WL 1023238 (Conn. Super. Ct. Mar. 9, 2005). These cases all validate ballistic evidence based on its widespread use for decades.[203]

200. *See id.* (listing the police officer's deficient organizational skills in his investigation).
201. *See Green*, 405 F. Supp. 2d at 121-22 (commenting that without error rates, a jury would "have no accurate way of evaluating the testimony.").
202. *Id.* at 109.
203. *See Green*, 405 F. Supp. 2d at 122-23 (outlining the longstanding judicial tradition of recognizing ballistic evidence).

Despite its misgivings, the court admitted the ballistic evidence, but only allowed the expert to point out the markings to the jury.[204] He could not testify that the marks uniquely identified the suspect's gun.[205] This is similar to the approach taken in *Commonwealth v. Meeks*, 2006 WL 2819423 (Mass. Super. Ct. Sept. 28, 2006). The court found ballistic evidence admissible, but required the expert to give a detailed explanation regarding how he reached his conclusion.[206] Likewise, in *United States v. Monteiro*, 407 F. Supp. 2d 351 (D. Mass. 2006), the defense expert could only testify that the match was "more likely than not," but not that it was an absolutely certain.[207] Essentially, these cases only allowed the expert to lay out the facts for the jury, but not make the conclusion for them.

Looking at the challenges to firearm identification sheds some light on how the courts may view cell phone forensics once its reliability is challenged. The courts have been deeply troubled by the lack of empirical testing, or error rates in the ballistics field.[208] The court in *Green* summarized the need for accuracy:

> the question is: "When people in your field offer opinions regarding this task, how accurate are they?" If the expert could not give an informative answer to such question based on sound and adequate data—that is, if the expert's honest answer would have to be "I don't know"—then the testimony is not helpful to the jury and is vulnerable to exclusion.[209]

204. *See id.* at 124 (preventing officer from testifying regarding the conclusions of his ballistics investigation because it provided an improper basis for a jury verdict).
205. *See id.* (illustrating the limitations of officer's testimony).
206. *See* Commonwealth v. Meeks, 2006 WL 2819423, at *50 (Mass. Super. Ct. Sept. 28, 2006) (requiring appropriate documentation with the testimony).
207. *See* United States v. Monteiro, 407 F. Supp. 2d 351, 372 (D. Mass. 2006) (providing that the expert's testimony was limited to asserting likelihood, and not absolute certainty).
208. *See Green*, 405 F. Supp. 2d at 121-22 (criticizing the accuracy of current test methods).
209. *Id.* at 121 n.31 (citing Michael J. Saks, *The Legal and Scientific Evaluation of Forensic Science (Especially Fingerprint Expert Testimony*), 33 SETON HALL L.

A cell phone forensic expert on the stand faces the same scrutiny.[210] When questioned about accuracy, he has no national standards or testing to point to.[211] He could have conducted his own tests on the same model phone, but these would likely not be true science.[212] Thus, an expert has no direct way to demonstrate the accuracy of his findings.

The reputation of ballistic evidence has been its savior in many cases.[213] It has been used and admitted in court for decades, and even post-*Daubert*, judges have allowed it because of this.[214] As a newer technology, cell phone forensics does not enjoy the same lineage: however, it could be associated with computer forensics, which has been consistently admitted for over a decade.[215] Despite their basic similarities, the way the two technologies actually work are very different, and direct analogy is not appropriate.[216] Therefore, because the technology is so new, the courts should not admit cell phone evidence on past admissibility alone.

REV. 1167, 1170 (2003)).

210. *See* Baggili, *supra* note 85, at 2-3 (applying the *Daubert* test to cell phone forensics demonstrates the shortcomings in testing cell phone forensic methods).

211. *See* Baggili, *supra* note 85, at 2-3 (reviewing NIST Testing and concluding that its lack of concreteness causes it to fall short of *Daubert* standards).

212. *See Young*, 391 N.W.2d at 283 (holding that lack of independent verification of testing leads to biased personal interest in the evidence's admissibility).

213. *See Green*, 405 F. Supp. 2d at 108 (acknowledging that "*every single court* post-*Daubert* has admitted this testimony . . . .").

214. *See id.* at 109 (admitting testimony because of precedent despite serious concerns about its accuracy); United States v. Hicks, 389 F.3d 514, 524 (5th Cir. 2004) (relying solely on expert's long experience in the field without consideration of the field itself); United States v. Foster, 300 F. Supp. 2d 375, 377 n.1 (D. Md. 2004) (stating "ballistics evidence has been accepted for many years," and pointing out the first comprehensive textbook was published in 1935); State v. Brewer, No. X01CR02307016, 2005 WL 1023238, at *1 (calling firearms and ballistic evidence "neither new nor innovative . . . .").

215. *See* John Patzakis, *EnCase Legal Journal*, GUIDANCE SOFTWARE, at 45 (2001) (listing "notable" cases rejecting legal challenges to EnCase computer forensic software).

216. *Compare* Jansen et al., *supra* note 3, at 1 (explaining cell phone memory forensics), *with* MOORE, *supra* note 74, at 2 (explaining computer memory forensics).

The main difference separating ballistic from mobile forensic evidence is the subjective nature of its results.[217] In the end, the firearms expert must make a judgment, based mainly on experience, as to whether a match exists.[218] In contrast, the cell phone expert does not need to explain the significance of the evidence he or she found to the jury.[219] The subjective nature of ballistics is a major concern of the courts, and thus, the definite results mobile forensics produce, bolster its likelihood of admissibility.

On the other hand, many courts have required that firearms experts to explain exactly how they arrived at their conclusion, with many even excluding the conclusion itself.[220] Cell phone experts can only explain up to a point: they can describe the tools they used, and the process they went through, but the exact details of how the technology works remains a mystery to them.[221] They cannot testify as to what commands were sent to the phone, how those commands work, what data is changed on the phone, or what data the tool was not able to recover.[222] Whereas in ballistic evidence it is clear which markings the conclusions came from, a cell phone examiner can

217. *See* Giannelli, *supra* note 191, at 555 (concluding that ballistics expert's determination is a judgment call and "is more of an art than a science").

218. *See* Giannelli, *supra* note 191, at 555 (introducing ballistic identification techniques).

219. *See* SHEETZ, *supra* note 49, at 118-119 (noting the general acceptance of computer forensics admissibility).

220. *See Green*, 405 F. Supp. 2d at 124 (preventing expert from claiming a unique match to suspect's gun). *See also Monteiro*, 407 F. Supp. 2d at 372 (limiting expert to facts, not conclusion); *Meeks*, 2006 WL 2819423, at *50 (requiring witness to explain process in detail and provide proper documentation).

221. *See* McCarthy, *supra* note 7, at 33 (stating that mobile forensics has many inherent limitations); Harrington, *supra* note 113, at 1 (highlighting advantages of flashing); Hylton, *supra* note 93 (detailing the intricacies involved in cell phone forensics and the constant evolution of the field).

222. *See* McCarthy, *supra* note 7, at 33 (listing issues of proprietary phone systems); Harrington, *supra* note 113, at 1 (demonstrating purpose of using flasher boxes); Hylton, *supra* note 93 (stating that law enforcement does not typically have access to more sophisticated methods of cell phone information extraction).

only fully explain part of their data extraction technique.[223] Many courts only allow ballistics experts to testify about the process but not their results because of the many problems of that type of evidence.[224] Cell phone forensic experts cannot even fully explain their process, and therefore, applying the same logic, the evidence would be inadmissible altogether.

Firearms identification is an excellent example of where post-*Daubert* courts have struggled with a field that lacks empirical testing and standards.[225] Courts have been severely critical, but the evidence has remained admissible because of its long standing tradition and the power to prevent the expert from giving a definite conclusion.[226] Cell phone forensics shares the problems of ballistics, with no standards or error rates, but lacks its redeeming attributes.[227] There is no long-standing admissibility, and its proprietary tools do not allow the expert to truly explain the technique.[228] Therefore, under the reasoning of the recent firearms identification cases, cell phone forensic evidence is inadmissible.

B. Handwriting Analysis

223. *See* McCarthy, *supra* note 7, at 33 (expressing that investigators cannot completely account for all of the information contained in a phone's operating system); Harrington, *supra* note 113, at 1 (offering a solution to traditional cell phone forensics problems); Hylton, *supra* note 93 (observing current dilemma of law enforcement).

224. *See Green*, 405 F. Supp. 2d at 124 (excluding expert's testimony of a unique shell casing match). *See also Monteiro*, 407 F. Supp. 2d at 372(preventing expert from testifying about conclusions reached); *Meeks*, 2006 WL 2819423, at *50 (allowing witness to testify only if accompanied by sufficient documentation).

225. *See Green*, 405 F. Supp. 2d at 121 (expressing concerns about expert's ability to testify on the subject).

226. *See id.* at 109 (allowing only observations of firearms, not conclusion drawn from them); *Brewer*, 2005 WL 1023238, at *1 (stating that "because the scientific principles of ballistics and firearm analysis are so well established that they can be admitted on a mere showing of relevance.").

227. *See* Baggili, *supra* note 85, at 1-2 (testing has not occurred on cell phone forensic tools in order to establish error rates for the determination of the validity of such practices); NIST GUIDELINES, *supra* note 82 (providing guidance on how to use the software without the establishment of national standards).

228. *See Young*, 391 N.W.2d. at 283 (disapproving of scientists verifying their own work); Baggili, *supra* note 85, at 3 (noting lack of testing on mobile forensics tools leaves technicians unable to explain why processes occur).

Handwriting analysis is similar to ballistic evidence because it uses objective measurements but the final conclusion rests on the subjective determination of the expert.[229] The method has no conclusive testing, standards, calculated error rates, or truly peer-reviewed publication.[230] Under the *Daubert* factors, the two fields are almost identical, and yet recently many courts have held handwriting analysis inadmissible.[231]

An example of this lies in *United States v. Saelee*, 162 F. Supp. 2d 1097 (D. Alaska 2001), where a man stood trial for importing opium into the United States by mailing it concealed in Butterfinger candy bars.[232] The government's expert testified that the handwriting on the package matched the defendant's.[233] Under the *Daubert* factors, the court excluded the entire testimony.[234] It cited that "there has never been any empirical research done on the theory of probability on which handwriting

229. *See* Giannelli, *supra* note 191 (summarizing the principle behind ballistic evidence). *See also* United States v. Saelee, 162 F. Supp. 2d 1097, 1101 (D. Alaska 2001) (outlining *Daubert* factors for handwriting analysis).

230. *See Saelee*, at 1101-02 (detailing faults in the expert's testimony); United States v. Starzecpyzel, 880 F. Supp. 1027, 1038 (S.D.N.Y. 1995) (noting experts do not conduct a "critical self-examination").

231. *See* Robert Epstein, *Fingerprints Meet* Daubert*: The Myth of Fingerprint "Science" is Revealed*, 75 S. CAL. L. REV. 605, 620 n.81 (2002) (analyzing the ways in which fingerprint evidence has been assessed in the wake of *Daubert*). *See also Saelee*, 162 F. Supp. 2d at 1106 (excluding handwriting comparison evidence testimony); United States v. Fujii, 152 F. Supp. 2d 939, 942 (N.D. Ill. 2000) (holding handwriting expert's testimony not sufficiently reliable); United States v. Rutherford, 104 F. Supp. 2d 1190, 1194 (D. Neb. 2000) (precluding expert from offering his conclusion or degree of certainty as to his opinions); United States v. Santillan, No. CR-96-40169 DLJ, 1999 WL 1201765, at *5 (N.D. Cal. Dec. 3, 1999) (limiting expert's testimony to comparing similarities in handwritten evidence); United States v. Hines, 55 F. Supp. 2d 62, 73 (D. Mass. 1999) (restricting experts testimony to identifying similarities and dissimilarities of the written evidence); Pre-Trial Transcript at *35, United States v. McVeigh, 958 F. Supp. 512 (D. Colo. 1997) (No. 96-CR-68), 1997 WL 47724 at *1 (requiring hearing about validity of "the science of handwriting comparison" to indentify the writer).

232. *See Saelee*, 162 F. Supp. 2d at 1098 (outlining factual background of the case).

233. *See id.* (providing government expert testimony by a forensic document analyst).

234. *See id.* at 1105 (rejecting expert's testimony under *Daubert* as misleading).

analysis is based," and the "lack of controlling standards."[235] Furthermore, while there is general acceptance, it is only within the "closed universe of forensic document examiners."[236]

The court in *United States v. Starzecpyzel*, 880 F. Supp. 1027 (S.D.N.Y. 1995) further criticized the field of handwriting analysis, noting that the publications in the field lacked the critical, unbiased nature of true peer-reviewed works.[237] It also addressed the method's unknown error rate, stating: "Certainly an unknown error rate does not necessarily imply a large error rate. However if testing is possible, it must be conducted if forensic document examination is to carry the imprimatur of 'science.'"[238]

The same reasoning that renders handwriting analysis inadmissible, also applies to cell phone forensic technology. No empirical research has been conducted to determine error rates, despite the fact that their calculation is possible.[239] The field has no standards regarding data acquisition or national certification.[240] There is general acceptance, but only within the closed community of mobile forensic experts, and its publications are not critically peer-reviewed.[241] Cell phone forensic evidence fails is all the same categories as handwriting analysis, and thus, courts should rule it as inadmissible.

C. Cell Site Analysis

235. *Id.* at 1102, 1104.
236. *See id.* at 1104 (discounting interested scientists under the general acceptance prong).
237. *See Starzecpyzel*, 880 F. Supp. at 1038 (noting that the publications "technically satisfy" the *Daubert* requirements, but are not enough for "valid science").
238. *Id*. at 1037 (analyzing handwriting analysis under the error rate prong of *Daubert*).
239. *See* Baggili, *supra* note 85, at 1-2 (indicating that the cell phone forensic process has remained untested for validity).
240. *See* NIST GUIDELINES, *supra* note 82, at 24, 45 (offering guidance on the roles and procedures of acquisition without setting firm requirements for the process).
241. *See* NIST TESTING, *supra* note 128, at 1 (showing that cell phone forensics toolkits are geared strictly toward assisting forensic examiners).

One type of evidence that directly involves cell phones that has been reviewed under *Daubert* is cell site analysis.[242] On the surface, it seems to be very similar because it is dealing with the same device, it is a new technology, and has not been fully tested.[243] There are also no known error rates or peer reviewed literature.[244] This would make it tempting for a mobile forensic proponent to assert that the analysis for the admissibility of one would extend to the other.

Cell site analysis is the technique of determining the location of a cell phone at a given time.[245] An expert takes measurements of signal strength at various locations, then calculates where the cell phone was when it switched towers.[246] This will give an approximate position of where the device was located when a call was placed.[247]

In *United States v. Allums*, No. 2:08-CR-30 TS, 2009 WL 806748 (D. Utah 2009), a man was charged with three counts of robbery.[248] The government obtained the defendant's mobile phone records, which contained phone calls he placed the day of the crimes.[249] These records indicated which cell phone towers he connected to when placing the calls.[250] The expert for the government drove around the area where these towers were

242. *See* United States v. Allums, No. 2:08-CR-30 TS, 2009 WL 806748, at *1-2 (D. Utah Mar. 24, 2009) (reviewing use of cell phone calls to determine location of defendant at time of crime).
243. *See id.* (holding methodology reliable despite failing some *Daubert* prongs).
244. *See id.* (dismissing issues with cell cite analysis).
245. *See id.* at *1 (introducing cell site analysis technology); United States v. Mendoza-Morales, 2007 WL 4388100, at *1 (D. Or. Dec. 12, 2007) (defining cell site analysis).
246. *See Allums*, 2009 WL 806748, at *1 (demonstrating how to use cell site technology).
247. *See id.* (recalling expert's testimony regarding how to pinpoint the location of where a cell phone call was placed).
248. *See id.* (laying out facts of the case).
249. *See id.* (explaining how police came into possession of defendant's cell phone).
250. *See id.* (describing process of investigating placement of cell phone call).

located, and measured their signal strength at various points.[251] Using this data, he then determined the geographic location where a phone would switch towers, pinpointing the defendant's position.[252]

The defense challenged the reliability of this method under the *Daubert* test.[253] They pointed out that between the time the calls were made and when the expert made his measurements, one of the towers the defendant's cell phone used had been demolished.[254] The government's expert had previously testified that he needed to visually inspect every tower to ensure accuracy.[255] In addition, they argued that signal strength can vary greatly due to weather conditions, high call volume, or numerous other plausible circumstances.[256]

Despite these seemingly glaring deficiencies, the court found the evidence admissible.[257] The method had been used hundreds of times previously to track down fugitives.[258] The court considered this sufficient testing.[259] It further concluded, without much discussion, that this meant it also enjoyed general acceptance in the area of law enforcement.[260] The court admitted that it could find no error rates or peer review for the method, but held that the other two factors were enough.[261] The court in *United States v. Mendoza-Morales*, 2007 WL 4388100 (D. Or. Dec.

251. *See id.* (listing steps investigator took in using signal strength to measure exactly where cell phone call was placed).
252. *See Allums*, 2009 WL 806748, at *1 (explaining basis for expert's conclusion).
253. *See id.* (outlining the procedural history).
254. *See id.* at *2 (listing the defense's contentions that the cell site analysis was demonstrably inconclusive).
255. *See id.* (illustrating inconsistencies in expert's testimony).
256. *See id.* (expressing defense's concerns with expert's methodology).
257. *See id.* at *2-*3 (stating the reasons behind the soundness of the expert's methodology).
258. *See Allums*, 2009 WL 806748, at *2 (concluding that the success rates of earlier cell site investigation bolstered the veracity of the expert's conclusions).
259. *See id.* (noting that the method had undergone sufficient testing).
260. *See id.* (basing conclusion on the FBI's utilization of the technology in "hundreds of prior investigations . . . .").
261. *See id.* (concluding that the success of the technique outweighed other factors).

12, 2007) reached the same result, finding cell site analysis reliable.[262] It held that the technique "more than met any *Daubert* concerns," but does not elaborate further.[263] It gave no indication of considering peer-review or error rates.[264]

Proponents of cell phone forensics could cite these two cases as indicating the admissibility of cell phone forensic evidence.[265] The courts either ignored or disregarded two of the *Daubert* factors (error rates and peer review).[266] Instead, the focus lay on testing and general acceptance.[267] The testing that the *Alums* court considers is the fact that it has been used successfully in hundreds of previous investigations.[268] Likewise, cell phone forensics has been utilized in the past, but it does not share the same clear success rate.[269] In *Allums*, the FBI used the technology to capture fugitives.[270] There is no doubt when it succeeds because the suspect is physically captured.[271] For cell phone forensics, an expert can tell whether something has been obtained, but not if it is accurate or complete.[272] Therefore, the testing prong of the *Daubert* test met by cell site analysis is distinct from testing for cell phone forensics because it obtains clear and indisputable results.[273] This leaves only the general

262. *See id.* at *3 (deeming expert's testimony admissible).
263. *See id.* (concluding that the expert clearly established his knowledge of cell site analysis).
264. *See Allums*, 2009 WL 806748, at *1 (making no reference to peer-review or error rates).
265. *See id.* at *3 (holding that cell site evidence is admissible); *Mendoza-Morales*, 2007 WL 4388100, at *3 (admitting cell site evidence).
266. *See Allums*, 2009 WL 806748, at *2 (holding other factors outweighed lack of error rates or peer-reviewed publications); *Mendoza-Morales,* 2007 WL 4388100, at *3 (finding admissibility without reference to peer-review or error rates).
267. *See Allums*, 2009 WL 806748, at *2 (holding these two factors were sufficient to meet *Daubert* requirements).
268. *See id.* (relying on past investigations to demonstrate accuracy of cell site analysis).
269. *See id.* at *2 (touting success of cell site analysis).
270. *See id.* (summarizing the use of the expert's methodology).
271. *See id.* (using the FBI's success rates to demonstrate the reliability of the methodology).
272. *See* McCarthy, *supra* note 7, at 57 (describing how an expert can view the result, but does not have access to the commands that produce such results).
273. *See Allums*, 2009 WL 806748, at *2 (relying on the past success of cell

acceptance test, but *Daubert* makes clear that this is no longer the only test.[274]

These cases show that courts have been accepting of new technology even without peer-review or error rates, but admitting this type of evidence has little bearing on the admissibility of cell forensic evidence.[275] The technologies are very different, despite involving the same device.[276] In cell site analysis, the data comes from the service provider and involves signal strength calculations.[277] Cell phone forensics extracts the data from the phone, with varying degrees of success.[278] The two are tested differently, and have different types of errors.[279] Therefore, despite the two disciplines dealing with the same device, the analysis of the admissibility of one should not extend to the other.

VII. Methods for Improvement

Traditionally, scientific fields develop out of the desire to discover the unknown. Cell phone forensics, on the other hand, was created to serve a need created by the justice system.[280] The entire field developed to produce evidence that is admissible in court, making the research and development entirely market-driven.[281] This means that until the courts require more from the

site analysis technology to infer reliability).

274. *See Daubert*, 509 U.S. at 593-94 (expanding the test for admissibility of scientific evidence to include evidence other than that which is "generally accepted").

275. *See Allums*, 2009 WL 806748 (allowing expert testimony of cell site analysis); *Mendoza-Morales*, 2007 WL 4388100, at *3 (admitting cell site analysis evidence).

276. *Compare* MOORE, *supra* note 74, at 3 (describing cell phone forensics), *with Allums*, 2009 WL 806748, at *1 (detailing cell site analysis methodology).

277. *See Allums*, 2009 WL 806748, at *1 (explaining the technology used to determine the location at which a cell phone call was made).

278. *See* McCarthy, *supra* note 7, at 53 (acknowledging four major limitations and problems with current extraction methods).

279. *See, e.g.*, *Daubert*, 509 U.S. at 590-594 (enumerating the four part test).

280. *See* Baggili, *supra* note 85, at 2 (explaining that scientific data offered by an expert witness that assists the trier of fact in understanding the evidence may be admissible in court).

281. *See* Baggili, *supra* note 85, at 3 (noting the "market driven nature" of digital forensics limits forensic tool testing).

mobile forensic industry, the same lax testing and authentication procedures will continue.[282]

The problems with reliability in this field stem from the proprietary phone systems.[283] Because cell phone experts do not know how each new phone works, they must spend most of their time "cracking" the operating system.[284] With new phones being released every three-to-six months, there is little time left over for extensive testing.[285] A lack of testing means no error rates are determined.[286] Furthermore, the tools are also proprietary, so their function is never published, thus they cannot be peer reviewed.[287] Because of all these deficiencies, a scientific community comprised of more than just cell phone technicians has no scientific basis to accept the technology as reliable.

The clear solution to this problem would be for cell phone manufacturers to release the code that runs their phones so mobile forensic experts could verify that the commands they send do not alter data.[288] In fact, the trend recently has been for phone companies to release the source code for their operating systems.[289] Without this impediment, cell phone forensics

282. *See Green*, 405 F. Supp. 2d at 109 (concluding that "sloppy practices" will continue as long as courts fail to hold researchers to a higher standard).
283. *See* Baggili, *supra* note 85, at 4-5 (summarizing difficulties in testing new phones due to their proprietary nature and rapid release); McCarthy, *supra* note 7, at 59 (enumerating specific limitations with cell phone forensic methods).
284. *See* Hylton, *supra* note 93 (explaining the catch-up process required to keep up with the latest cell phone technology).
285. *See* Hylton, *supra* note 93 (emphasizing the disadvantage cell phone forensics investigators have in keeping up with the fast-moving cell phone industry).
286. *See* Baggili, *supra* note 85, at 1-2 (criticizing the lack of published error rates in order to establish sound forensic testing).
287. *See* Baggili, *supra* note 85, at 2-3 (analyzing technology under peer review prong of *Daubert*).
288. *See* McCarthy, *supra* note 7, at 33 (highlighting problems with proprietary codes on cell phones).
289. *See* Priya Granapati, *Symbian Operating System, Now Open Source and Free*, WIRED, Feb. 3, 2010, *archived at* http://www.webcitation.org/5x0jiz2cz (announcing free release of Symbian source code). In February 2010, the most popular operating system, Symbian, had its source code released to the public. *See id. See also* Dave Bort, *Android is Now Available as Open Source*, ANDROID OPEN SOURCE PROJECT, Oct. 21, 2008, *archived at*

experts should now be able to test tools much faster, since they will know what changes from phone to phone.[290]

The open-source trend has not extended to forensic tools and most remain proprietary.[291] The development of these tools is market driven, and since their market is derived from producing evidence, the only way to force change is for courts to require more for admissibility.[292] This does not necessarily mean that they should be forced to share their source code with the public.[293] Several compromises are possible. First, tool developers could allow a testifying expert to privately review their source code before testifying to its reliability.[294] Alternatively, the code that performs data extraction could be made public, but the code for the presentation and aesthetics of the program would remain secret.[295] This allows the developer to have their method validated, but still maintain what makes their product marketable.[296]

If these solutions are not possible, then mobile forensics could instead implement comprehensive, scientific testing. Experts have introduced several proposals regarding how to accomplish this goal.[297] One such idea is to create a centralized

http://www.webcitation.org/5x0jqwPUK (announcing the release of the Android Open Source Project).

290. *See* Baggili, *supra* note 85, at 4-5 (noting the difficulties of testing proprietary phone systems).

291. *See* Baggili, *supra* note 85, at 4-5 (explaining the proprietary nature of cell phones).

292. *See* Baggili, *supra* note 85, at 3 (observing that while cell phone forensics fail *Daubert* testing standards, the results are none-the-less often found admissible).

293. *See* Brian Carrier, *Open Source Digital Forensics Tools: The Legal Argument*, DIGITAL-EVIDENCE.ORG 1, 7 (2003), *archived at* http://www.webcitation.org/5wUnYMj6P (explaining possible alternatives to public source code sharing).

294. *See* Carrier, *supra* note 293 (advocating for open source tools to enhance reliability).

295. *See* Carrier, *supra* note 293, at 8 (presenting case for more open forensic tools).

296. *See* Carrier, *supra* note 293, at 8 (stressing that "many new features in file system digital forensic analysis tools are based on presentation").

297. *See* Baggili, *supra* note 85, at 5 (outlining possible solution to proprietary information problem).

database where forensic scientists from across the country input data from cell phone data acquisition.[298] By combining the work of a vast array of experts, the database could keep up with the speed with which phones are churned out.[299] The data collected could also serve as a basis for calculating error rates for various tools on a wide range of phones.[300]

VIII. Conclusion

In *Daubert*, the Supreme Court rejected the decades old practice of deferring to experts in matters of scientific evidence.[301] Before the decision, an expert would simply have to testify that a given scientific technique was accepted, and it would be admitted.[302] The frequent admission of dubious, unreliable science troubled the Court and they clearly established that judges must act as "gate-keepers."[303] They now have a duty to protect the jury from an expert's conclusions drawn from pseudo-science.[304]

Performing this duty has produced mixed results. Courts reexamined ballistic evidence, but held it admissible, despite a lack of standards, testing, or error rates, because of its long-standing admissibility.[305] Handwriting analysis received similar treatment, but in the end, many courts found it inadmissible. Cell

298. *See* Baggili, *supra* note 85, at 5-6 (proposing a database-driven approach to aggregate testing data).
299. *See* Baggili, *supra* note 85, at 9 (creating a database solution that could be used by various technicians, which would make their past and present results available to all, keeping pace with ever-changing technology).
300. *See* Baggili, *supra* note 85, at 7-8 (using error rates in order to establish the validity of testing methods).
301. *See Daubert*, 509 U.S. at 597 (increasing judge's role in determining admissibility of scientific evidence).
302. *See* RICE, *supra* note 12, at 465-68 (explaining the elements of the *Frye* general acceptance test).
303. *See Daubert*, 509 U.S. at 589 n.7 (requiring judges to be more active in determining scientific reliability of evidence).
304. *See Daubert*, 509 U.S. at 595 (stressing the potential harm that unreliable evidence can have on a jury).
305. *See Green*, 405 F. Supp. 2d at 108 (stipulating that every post-*Daubert* court admitted similar evidence despite scientific deficiencies).

site analysis provides an example of how the courts are receptive to more recent scientific discoveries under *Daubert.*

Given the disparate treatment of scientific evidence, one cannot be sure how the courts will view cell phone evidence despite the fact that it fails all the *Daubert* factors. The tools are untested, no standards for data extraction exist and error rates are unknown. Their source code is proprietary, shielding it from peer-review. Without any of this information, it could not reach general acceptance with any true scientific community.

A jury presented with this type of evidence will only see the conclusions reached. The entire process to produce the data lies hidden. This is not unique to a juror. With proprietary tools and phone software, most of the process is hidden from the expert as well. Judges need to accept the duty laid upon them in *Daubert* and keep this unsubstantiated evidence out of the courtroom.