DISCOVERY OF PORTABLE ELECTRONIC DEVICES

INTRODUCTION 193
I. THE TECHNOLOGY 194
A. *A Brief Overview of Data Storage Technology* 195
1. Volatile vs. Nonvolatile Data 196
2. Nonvolatile Data Storage 196
3. Volatile Data Storage 197
B. *The Old Paradigm: Static Data, Fixed Device* 198
C. *The Emerging Paradigm: Dynamic Data, Mobile Device* 199
II. THE FIRST CHALLENGE: PRESERVATION 200
A. *The Duty to Preserve* 201
1. Events that Trigger the Duty to Preserve 204
2. The Scope of the Duty to Preserve 205
3. The Duty to Preserve PED ESI 205
B. *The Hidden Danger of Sanctions* 207
1. Differing Standards for Electronic Discovery Sanctions 208
2. Applying the Rule 37 Good Faith Exception 211
C. *Special Problems with Preserving PED Data* 213
D. *Approaches to Preserving, or Not Preserving, PED Data* 214
1. Freeze the PED 214
2. Clone the PED 216
3. Forensic Acquisition and Preservation of PED Data 216
E. *Preservation Orders* 217
III. THE SECOND CHALLENGE: PRODUCTION 217
A. *Special Challenges with Producing and Presenting PED Data* 217
B. *Suggested Solutions to Producing PED Data* 218
1. Forensic PED Expert 218
2. Manual Acquisition 219
3. Direct Review 221
V. SUGGESTIONS FOR INNOVATION 222

INTRODUCTION

Portable electronic devices (PEDs) such as the Palm PDA, Blackberry, and Apple iPhone are rapidly becoming ubiquitous technology with a myriad of form factors, some reaching a level of sophistication and flex-

ibility rivaling the capabilities of the last decade's PCs.[1] As such devices continue to saturate our culture and become more important in our personal and professional lives, it is only natural that they should become an increasingly important repository of evidence in nearly all civil and criminal trials.[2] The Federal Rules of Civil Procedure have undergone a metamorphosis in recent years to address the problems presented by the rising tide of digital evidence,[3] yet most of these changes in the rules and the corresponding case law are a step behind the pace of developing technology. Courts, litigators, businesses, and individual parties will face fresh, unique, and especially difficult technological and legal challenges when attempting to fit the new and diverse data storage paradigms of PEDs into the "old" framework presented by traditional approaches to electronic discovery. Because discovery disputes rarely reach the appellate level, there has been little high-level judicial guidance on how to best handle discovery involving unconventional, but increasingly more common, portable electronic devices.[4] I intend in this Note to provide one of the first guideposts on the path toward a solution by presenting and explaining the technology, suggesting ways in which to best navigate the discovery process in which PEDs are involved, and proposing new directions for refining the existing model to best accommodate these emerging technologies.

I. THE TECHNOLOGY

The rapid pace of technological innovation leaves most lawyers understandably ignorant of the inner workings of computers. Simply learning the law and keeping abreast of emerging legal issues occupies more hours than most have in their day. However, in many courtrooms around the

1. Portable Electronic Devices are a loosely defined category of small consumer electronics designed to be carried by the user. These devices may or may not have networking capability, and they perform a wide array of functions. The category includes such devices as cellular phones, personal digital assistants (PDAs), smartphones, music players (such as the iPod), GPS navigation devices, and portable game systems (such as the Nintendo Gameboy). *See* National Center for Forensic Science, Digital Evidence (May 29, 2008), http://ncfs.ucf.edu/digital_evd.html. For a discussion of nomenclature and some of the nuances distinguishing different types of PEDs, see Vangie Beal, *The Difference Between a Cell Phone, Smartphone and PDA*, INTERNET.COM, May 2, 2008, http://www.webopedia.com/DidYouKnow/Har dware_Software/2008/smartphone_cellphone_pda.asp.

2. *See* SHARON D. NELSON, BRUCE A. OLSON & JOHN W. SIMEK, THE ELECTRONIC EVIDENCE AND DISCOVERY HANDBOOK xiv–xv (2006). A BlackBerry PED has even managed to create a small bit of controversy for President Obama due to legal and security issues. *See* Jeff Zeleny, *Obama Digs In for His BlackBerry*, N.Y. TIMES, Jan. 8, 2009, at A22.

3. *See generally* Adam I. Cohen, *The Revised Federal Rules of Civil Procedure: Where We Are One Year Later*, CORP. COUNS., Feb. 2008, at 1, *available at* http://legalholds.typepad.com/files/defensible-legal-hold-process-beyond-notifications-2.pdf.

4. *See* RICHARD VAN DUIZEND, CONFERENCE OF CHIEF JUSTICES: GUIDELINES FOR STATE TRIAL COURTS REGARDING DISCOVERY OF ELECTRONICALLY-STORED INFORMATION ix (2006), *available at* http://www.ncsconline.org/images/EDiscCCJGuidelinesFinal.pdf.

nation, technological ignorance is no longer a valid excuse when electronic discovery blunders lead to embarrassing or crippling mistakes.[5] All lawyers involved in the modern discovery process must understand at least two things: the basic ways that computers store discoverable information and the technical terms necessary to competently communicate with others about electronic discovery.[6] In order to lay a foundation for a more detailed discussion of PED discovery, I aim in this Part to provide a simplified overview of electronic discovery, data storage technology, and the technical jargon commonly associated with both.

A. A Brief Overview of Data Storage Technology

Electronic discovery involves using existing discovery rules to gather "electronically stored information," or ESI.[7] The process of electronic discovery parallels traditional "paper discovery" except that instead of seeking the production of physical documents or things, electronic discovery seeks the production of data stored on a computer.[8] Reduced to the most basic level, the data comprising ESI consists of sequences of zeros and ones, also known as "binary."[9] These sequences of zeros and ones encode a pattern that stands for meaningful information, much in the same way a Morse code message encodes English words. A computer or other electronic device can decode the sequence and display something meaningful to a human user.

There are as many ways to store and decode these sequences of zeros and ones as human ingenuity will permit. Methods for data storage continue to advance, and many are quite technically complex, but they all retain

5. *See, e.g.*, Ernest Svenson, *E-discovery—does anybody really know what it is?*, http://www.ernietheattorney.net/ernie_the_attorney/2005/06/ediscovery_does.html (June 30, 2005, 06:14 CST) (citing sanctions levied against Morgan Stanley attorneys likely resulting from a lack of understanding of their client's e-mail systems). For the Morgan Stanley case, see *Coleman (Parent) Holdings, Inc. v. Morgan Stanley & Co.*, No. CA 03-5045 AI, 2005 WL 674885 (Fla. Cir. Ct. Mar. 23, 2005).

6. *See* Svenson, *supra* note 5 (explaining that nearly all modern discovery involves electronic information, and lawyers who wish to perform competently must understand at least the basics of the involved technology).

7. *See* FED. R. CIV. P. 26 advisory committee's notes, 2006 amends., subdiv. (a) ("The term 'electronically stored information' has the same broad meaning in Rule 26(a)(1) as in Rule 34(a). This amendment is consistent with the 1993 addition of Rule 26(a)(1)(B). The term 'data compilations' is deleted as unnecessary because it is a subset of both documents and electronically stored information.").

8. *See id.* Despite the advisory committee's comment deprecating the use of the term "data," since this Note is concerned only with data in the electronic sense, I will use the terms ESI and data interchangeably.

9. *See* SCOTT MUELLER, UPGRADING AND REPAIRING PCS 584 (2003) ("The data a PC stores on it, however, is digital information—that is, 1s and 0s."). *See also The Sedona Conference Glossary: E-Discovery & Digital Information Management*, The Sedona Conference Working Group Series, at 6 (Conor R. Crowley et al. eds., 2d ed. 2007), *available at* http://www.thesedonaconference.org/dltForm?did=TSCGlossary_12_07.pdf (defining "binary").

one basic characteristic: they all encode zeros and ones in some format readable by a machine.[10] Many of the technologies discussed below are used currently or are usable in PEDs.[11] Even if not, any type of data, including PED data, could still be found on any medium discussed.[12] It does not matter how exotic the device or the storage medium is; the data being stored is ultimately in binary code form. This means that data can be moved freely from one storage medium to another or from one device to another without altering the data.

1. Volatile vs. Nonvolatile Data

Data comprising ESI can be classified into two major types: relatively stable, nonvolatile data, used for permanent storage, and volatile data, which is usually used by a running computer system to temporarily store data that needs to be accessed quickly.[13] Nonvolatile storage is akin to a book: relatively permanent, fixed, and difficult to delete. Volatile storage is more akin to the writing on a lecturer's whiteboard: intended to be temporary, quickly and easily viewed, and easy to erase and overwrite. The most important practical implication for electronic discovery is that volatile data is evanescent, constantly changing, and extremely difficult to preserve and produce.[14] Many PEDs use volatile data in unusual ways or even as the primary mode of data storage, giving rise to some unique discovery challenges discussed later.[15]

2. Nonvolatile Data Storage

In early days, e-discovery, like ordinary discovery, might have involved the production of paper because punch cards were the prevalent

10. The bleeding edge of data storage appears to be in nanotechnology currently under development that aims to put one terabyte of data storage on a single square inch of physical material, sufficient to allow the entire Library of Congress to be stored on a Palm Pilot. *See* Eric Berger, *Library of Congress in Your Palm*, HOUS. CHRON., Jan. 25, 2005, at B2. This same research team estimates the upper limit of data storage per square inch using their approach to be 20–40 terabits per square inch. *See* Lisa Zyga, *New Data Storage Design Likely to Increase Data Capacity*, PHYSORG.COM, Apr. 7, 2006, http://www.physorg.com/news63627394.html.

11. *See generally* Thomas M. Coughlin, *Data Storage for Mobile Devices*, MOBILE IMPERATIVE, May 23, 2003, at 41.

12. For that matter, any type of data might be found on a PED as well. It is not inconceivable that backups of PC files or other more exotic types of data might be found on a PED.

13. ALBERT J. MARCELLA, JR. & DOUG MENENDEZ, CYBER FORENSICS 145, 147–48 (2d ed. 2008).

14. *See* Kenneth J. Withers, *"Ephemeral Data" and the Duty to Preserve Discoverable Electronically Stored Information*, 37 U. BALT. L. REV. 349, 376 (2008).

15. For example, some PEDs use volatile data as "permanent" data storage in the same way that a standard desktop computer uses its hard disk drive. MICHAEL G. SOLOMON, DIANE BARRETT & NEIL BROOM, COMPUTER FORENSICS JUMPSTART 108 (2005). To further complicate matters, there is no easy way to tell which PEDs use volatile data to store critical ESI and which PEDs do not! *See* GREGORY KIPPER, WIRELESS CRIME AND FORENSIC INVESTIGATION 64 (2007).

form of nonvolatile data storage.[16] The data was literally punched into a paper card with a hole representing a one, and a nonpunched space representing a zero, or vice-versa.[17] When magnetic tapes came into vogue, instead of being encoded as a pattern of punched holes, data was then stored in the form of magnetic fluxes: for example, a positive magnetic "charge" representing a one, and a negative charge representing a zero.[18] Hard disk drives, floppy disks, and other types of data disks—zip and jaz—use a similar magnetic system for encoding data, but instead of arranging the data in a straight line as it appears on a tape, the data is laid out in circular "tracks" around a platter.[19] Optical media, most commonly seen today in the form of CDs and DVDs, store data in the form of microscopic pits or "dark spots" on a highly reflective surface.[20] Though optical discs look very modern, the pits in a CD or DVD are not so dissimilar in concept from the punched holes in an archaic punch card—they are microscopic and read by a laser, but they are still physical markings on a physical medium.

More recently, "flash" devices have become popular for storing data.[21] These technologies come with a fixed set of electronic "switches" inside that can be flipped on, for one, or off, for zero, by applying an electrical charge.[22] The switches stay on or off in the pattern they are set, storing the encoded data.[23]

3. Volatile Data Storage

Volatile data is usually stored in random-access memory (RAM) and is intended for quick, temporary use while the computer is running.[24] As a

16. *See, e.g.*, Nat'l Union Elec. Corp. v. Matsushita Elec. Indus. Co., 494 F. Supp. 1257, 1262 (E.D. Pa. 1980) ("In the computer context, the basic types of machine records commonly utilized include: (1) punched cards; (2) paper and magnetic tapes; and (3) a variety of other machine oriented components which record and store data.") (quoting MANUAL FOR COMPLEX LITIGATION § 2.715 (4th ed. 1977)). For a fascinating history of punch card computing, see Douglas W. Jones, *Punched Cards: A Brief Illustrated Technical History*, http://www.cs.uiowa.edu/~jones/cards/history.html (last visited Oct. 7, 2009).

17. This is, of course, a simplification of how actual punch card computers worked. Many had much more complex and efficient data encoding schemes, but the principle of punching the data into a card in sequence was the same. *See* Jones, *supra* note 16.

18. Again, this is a simplification of the actual physics involved, but sufficiently correct in principle for the scope of this Note. For a deeper explanation, see MUELLER, *supra* note 9, at 575–93.

19. *Id.* at 597–604.

20. *Id.* at 719–27.

21. Flash memory devices include such technologies as Compact Flash, Memory Stick, Secure Digital (SD), and an array of USB "thumb drives." *See* MIKE MEYERS, COMPTIA A+ GUIDE TO MANAGING AND TROUBLESHOOTING PCS 380–82 (2007).

22. *See* VOJIN G. OKLOBDZIJA, DIGITAL DESIGN AND FABRICATION 6-4 to 6-5 (2008).

23. *See id.*

24. *See* BRUCE MIDDLETON, CYBER CRIME INVESTIGATOR'S FIELD GUIDE 99 (2d ed. 2005); *The Sedona Conference Glossary: E-Discovery & Digital Information Management*, *supra* note 9, at 43. *See also* Columbia Pictures, Inc. v. Bunnell, 245 F.R.D. 443, 446–47 (C.D. Cal. 2007) (discussing

result, volatile data storage has the advantage of being quickly accessible by a computer system, but it is unstable and prone to being overwritten, deleted, or orphaned.[25] Cryptic, but important, ESI such as network settings, recently used files, and password information often manifest as volatile data stored in RAM.[26] Unlike nonvolatile data, which is typically stored on a distinctly packaged and removable storage medium, volatile data is typically stored on integrated electronic circuitry hidden entirely within the guts of the device. Also, unlike nonvolatile data storage media, volatile data storage media require a constant or near-constant flow of electricity to remain accessible.[27] Just like a picture on a TV screen or the words on a JumboTron, cut the power and the data disappears.[28]

B. The Old Paradigm: Static Data, Fixed Device

The field of electronic discovery developed primarily around ESI stored on servers, PCs, and nonvolatile storage media such as tapes, CDs, and floppy disks.[29] In the more traditional model of electronic discovery, ESI is usually created or received by employees or individuals in the form of memos, database entries, spreadsheets, reports, or e-mails.[30] Upon creation or receipt, ESI would then be stored in semi-permanent fashion on a PC hard drive, a company document or e-mail server, or on other nonvolatile data storage media.[31] In business environments, frequently the business's servers, and possibly other important PCs, will also be backed up to tape or some other form of stable, long-term storage.[32] Businesses also usually have a document retention policy in place that covers what ESI

RAM in the context of a company server and holding that such RAM is subject to the obligation of preservation under Rule 34).

25. *See* Kevin Mandia & Kris Harms, *Don't Forget Your Memory*, FORENSIC MAG., Dec. 2007/Jan. 2008, *available at* http://www.forensicmag.com/articles.asp?pid=179.

26. *See id.*; *see also* MARCELLA & MENENDEZ, *supra* note 13, at 147–50. Some forms of volatile data can also be found written on nonvolatile storage media. Examples of volatile data that can be stored on nonvolatile media (usually the system hard disk) include the operating system swap file or page file, file slack, and free space. *Id.* at 147.

27. *See, e.g.*, HARLAN CARVEY, WINDOWS FORENSIC ANALYSIS 3 (2007); KIPPER, *supra* note 15, at 63–64.

28. *See* KIPPER, *supra* note 15, at 64. *See also* Coughlin, *supra* note 11, at 41.

29. *See generally* AMY JANE LONGO, ALLEN W. BURTON & ALLAN D. JOHNSON, ELECTRONIC DISCOVERY PRACTICE UNDER THE FEDERAL RULES (2007); *The Sedona Principles: Best Practices, Recommendations & Principles for Addressing Electronic Document Production*, The Sedona Conference Working Group Series (Jonathan M. Redgrave et al. eds., 2005), *available at* http://www.thesedonaconference.org/content/miscFiles/7_05TSP.pdf.

30. *See* DUIZEND, *supra* note 4, at v.

31. Nonvolatile data storage and backup systems in business range from the prosaic—ordinary hard drives and floppy disks—to the highly exotic: RAID arrays, Network Attached Storage (NAS), Storage Area Networks (SANs), and nearline Virtual Tape Storage systems. *See generally* R. J. T. Morris & B. J. Truskowski, *The Evolution of Storage Systems*, 42 IBM SYSTEMS J. 205 (2003), *available at* http://www.ssrc.ucsc.edu/PaperArchive/morris-ibmsj03.pdf.

32. *See* 7 JOHN K. RABIEJ, MOORE'S FEDERAL PRACTICE § 37A.05 (3d ed. 2009); MANUAL FOR COMPLEX LITIGATION (FOURTH) § 11.446 (2004).

needs to be stored, where it needs to be stored, and when it may or must be destroyed.[33] Discovery of ESI stored on established computer platforms continues to present challenges, but a great deal of documentation and guidance exists for attorneys and litigants on this front. I reference the traditional model of electronic discovery to provide a contrast for the novel challenge presented by PED discovery. The traditional framework also provides the foundation upon which a model for PED discovery must be built.

C. The Emerging Paradigm: Dynamic Data, Mobile Device

Where once computers were relegated to business environments, or stuck under a desk in the family den or home office, the computers of today are ubiquitous, portable, and even wearable.[34] As our society continues to integrate technology into the daily lives of ordinary people, devices inevitably become smaller, faster, and more mobile in response to consumer demand.[35] The impact of this technological sea change is that not only large businesses, but individual litigants now stand to fear (or benefit from) electronic discovery.[36]

Discovery of ESI stored on PEDs is in some ways similar to discovery of ESI stored on non-PED computers, and in some ways it is very different. The differences arise from technical dissimilarities between the data storage paradigms of PEDs and conventional computers. For example, many of the technical challenges of traditional e-discovery tend to stem from the sheer volume of ESI found on traditional computers and media.[37]

---

33. Good faith destruction of ESI in the normal course of business and in adherence to a document retention policy is one of the safe harbors provided by Rule 37. *See* FED. R. CIV. P. 37(e). This safe harbor has been held to be relatively narrow, however, and should not be relied on when litigation is anticipated. FED. R. CIV. P. 37 advisory committee's notes, 2006 amends., subdiv. (f). *See also* Doe v. Norwalk Cmty. Coll., 248 F.R.D. 372, 373–81 (D. Conn. 2007) (holding that sanctions were proper for spoliation of electronic evidence where university adhered to policy of wiping hard drive of ex-employee and university had notice that hard drive may contain data important to future litigation).

34. *See* Coughlin, *supra* note 11, at 44 ("Within a few years we may see data-storage devices so small that they can be incorporated as part of a personal electronic network built into the fabric of a person's clothing and perhaps powered by the heat generated by their host. This would be nearly the ultimate in portable electronics.").

35. *See id.* at 41.

36. *See* Richard L. Marcus, *E-discovery Beyond the Federal Rules*, 37 U. BALT. L. REV. 321, 344 (2008) ("Computer use is no longer the preserve of the big corporation, and computer capabilities mean that large numbers of Americans have accumulated large amounts of electronically stored information. So preservation and access may begin to be headaches for parties on both sides of the 'v.'"). *See also* Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 569 (D. Md. 2007) ("The prevalence of electronic communication devices, and the fact that many are portable and small, means that people always seem to have their laptops, PDA's, and cell phones with them, and available for use to send e-mails or text messages describing events as they are happening."); BARBARA J. ROTHSTEIN, RONALD J. HEDGES & ELIZABETH C. WIGGINS, MANAGING DISCOVERY OF ELECTRONIC INFORMATION: A POCKET GUIDE FOR JUDGES 1 (2007), *available at* http://www.fjc.gov/public/pdf.nsf/lookup/eldscpkt.pdf/$file/eldscpkt.pdf.

37. Technical issues usually drive up costs by increasing the amount of time or expertise required to

The amount of data on a large corporation's document and e-mail servers can weigh in at several terabytes.[38] Additionally, the backup copies of critical system data, usually stored on tape, potentially create many more, less-accessible terabytes to be searched.[39] Notwithstanding the continuing advances in PED data storage technologies, the relatively small size of PEDs will always mean that they store significantly less data than their larger, less-portable cousins.[40] As a result, some of the perennial issues arising from virtual tidal waves of data are attenuated or simply absent when dealing with PEDs.

As for similarities, traditional electronic discovery has confronted issues surrounding both the preservation of ESI and satisfactory forms of production.[41] Preservation and production problems posed by PED ESI are analogous to those presented by ESI stored on conventional computers and media, but amplified. However, preservation and production of PED ESI can be considerably more challenging due to the unique and highly variable characteristics of PED data storage technology. Not only is PED data storage more volatile, the pace of progress in the PED realm is faster and the technologies more divergent. This exacerbates the "technological ignorance" problem, placing a heavier burden on lawyers to stay informed.[42] The remainder of this Note will focus on framing these challenges and proposing practical solutions for them.

II. THE FIRST CHALLENGE: PRESERVATION

Compared to physical documents and tangible things, ESI is both easier and more difficult to preserve.[43] ESI may prove easier to preserve because no large warehouse must be secured to store it: 100,000 documents can be easily stored on a single DVD locked in a file cabinet.[44] Additional-

fulfill discovery obligations. *See* Wiginton v. CB Richard Ellis, Inc., 229 F.R.D. 568, 572 (N.D. Ill. 2004) ("As contrasted with traditional paper discovery, e-discovery has the potential to be vastly more expensive due to the sheer volume of electronic information that can be easily and inexpensively stored on backup media.") (citing Zubulake v. UBS Warburg LLC, 217 F.R.D. 309, 316 (S.D.N.Y. 2003) (*Zubulake I*) and Byers v. Ill. State Police, No. 99 C 8105, 2002 WL 1264004, at *10 (N.D. Ill. June 3, 2002)).

38. *See* MANUAL FOR COMPLEX LITIGATION, *supra* note 32.

39. *See generally* Zubulake v. UBS Warburg LLC, 220 F.R.D. 212 (S.D.N.Y. 2003) (*Zubulake IV*).

40. The traditional e-discovery concerns created by overwhelming amounts of data (overwhelming cost, review time, filtering for privilege, inadvertent disclosure of privileged or work product ESI) are less pressing when discussing PEDs, and I will not address these concerns in this Note. For an overview, see generally *The Sedona Conference Best Practices Commentary on the Use of Search and Information Retrieval Methods in E-Discovery*, 8 SEDONA CONF. J. 189 (2007).

41. *See generally Zubulake IV*, 220 F.R.D. 212 (S.D.N.Y. 2003); RABIEJ, *supra* note 32, at § 37A.41.

42. *See supra* notes 5–6 and accompanying text.

43. *See* FED. R. CIV. P. 26 advisory committee's notes, 2006 amends., subdiv. (b)(2) ("Electronic storage systems often make it easier to locate and retrieve information. . . . But some sources of electronically stored information can be accessed only with substantial burden and cost.").

44. *See* MANUAL FOR COMPLEX LITIGATION, *supra* note 32.

ly, once stored, software may be used to search and filter data files much more quickly than a physical review of the same information printed on paper could be accomplished.[45] Alternatively, ESI can be more difficult to preserve because it is easily destroyed and often hard to identify for storage. Compared to more conventional ESI stored on a hard drive, tape, or disk, the nature of PED data storage amplifies ESI preservation difficulties while diminishing the advantages. PED ESI is not generally voluminous, so the benefits of easy searching and storage are minimal. PED data also tends to be much more vulnerable to damage or destruction than conventional data, and until PED discovery becomes streamlined and commonplace, PED data is also easily overlooked. PED data must nonetheless be preserved in the same way as all other ESI.

A. The Duty to Preserve

A duty to preserve evidence may be judicially imposed pursuant to a preservation order, or it may simply arise from a set of circumstances under which litigation should be expected.[46] In either case, the duty to preserve evidence arises not out of any particular rule of civil procedure, but rather out of the common law duty to avoid spoliation.[47] Depending on the jurisdiction and subject matter of a case, preservation duties may also be defined by statutes or regulations.[48]

---

45. *See* FED. R. CIV. P. 26 advisory committee's notes; 2006 amends., subdiv. (b)(2).

46. The exact source of power underlying a court's ability to issue preservation orders or impose a duty of preservation is debatable, though no authority calls into question the court's power to issue preservation orders. *See* Disability Rights Council v. Wash. Metro. Transit Auth., 242 F.R.D. 139, 146 (D.D.C. 2007) ("A preservation obligation may arise from many sources, including common law, statutes, regulations, or a court order in the case."); Capricorn Power Co. v. Siemens Westinghouse Power Corp., 220 F.R.D. 429, 431–34 (W.D. Pa. 2004) (citing as possible sources of authority Federal Rules 16, 26, 34, and 37, as well as inherent authority of courts to issue injunctions and regulate discovery conduct).

47. *See supra* note 46. *See also* Silvestri v. Gen. Motors Corp., 271 F.3d 583, 590 (4th Cir. 2001) (discussing the obligation of preservation as an extension of the federal common law duty to avoid spoliation of evidence potentially relevant to pending litigation).

48. *See* Sarbanes-Oxley Act, 18 U.S.C. § 1519 (2002) ("Whoever knowingly alters, destroys, mutilates, conceals, covers up, falsifies, or makes a false entry in any record, document, or tangible object with the intent to impede, obstruct, or influence the investigation or proper administration of any matter within the jurisdiction of any department or agency of the United States or any case filed under title 11, or in relation to or contemplation of any such matter or case, shall be fined under this title, imprisoned not more than 20 years, or both."); 29 C.F.R. § 1602.14 (2008) ("Preservation of records made or kept"); 18 C.F.R. § 125.2(l) (2008) ("[I]f a public utility or licensee is involved in pending litigation, complaint procedures, proceedings remanded by the court, or governmental proceedings, it must retain all relevant records."); FED. R. CIV. P. 37 advisory committee notes, 2006 amends., subdiv. (f) ("A preservation obligation may arise from many sources, including common law, statutes, regulations, or a court order in the case."); *The Sedona Conference® Commentary on Legal Holds: The Trigger & the Process*, The Sedona Conference Working Group Series, at 1 (Conor R. Crowley et al. eds., Public Comment Version, Aug. 2007), *available at* http://www.thesedonaconference.org/dltForm?did=Legal_holds.pdf.

Under the federal common law duty to preserve, parties have a duty to safeguard any evidence that they believe might be relevant to expected litigation.[49] This duty extends somewhat beyond the affirmative misconduct traditionally sanctioned by courts under the "power to control the judicial process and litigation."[50] The duty to preserve resembles a negligence standard in that it attaches not only when a party has actual notice that evidence is relevant to current or future litigation, but also "when a party should have known that the evidence may be relevant to future litigation."[51] It is very important to note that the preservation duty is ongoing and ever-present. Parties must be ever vigilant to possible lawsuits because the duty to preserve may arise even where no lawsuit has yet been filed.[52] Though often discussed as a burden borne by defendants, preservation duties apply equally to plaintiffs as well as defendants, and they may even extend to third parties.[53]

Though it appears very broad at first glance, there are significant limitations on the duty to preserve that allow potential evidence to be neglected or destroyed pursuant to normal practices. First, a party need not preserve *every* document—only those documents or evidence the party reasonably believes might be subject to discovery.[54] Second, the party must have sufficient notice that a certain document or piece of evidence is relevant.[55] Until such notice is given or imputed to the preserving party, there is no duty to preserve that particular evidence.[56]

The duty to preserve ESI was elaborated upon in the oft-cited case of *Zubulake v. UBS Warburg LLC* (*Zubulake V*).[57] Though *Zubulake V* did not involve discovery of PED data specifically, its holding is broadly worded such that it extends to all ESI, including ESI stored on PEDs.[58] The technical responsibility placed on attorneys by *Zubulake V* is sweeping

49. *See* Turner v. Hudson Transit Lines, Inc., 142 F.R.D. 68, 72 (S.D.N.Y. 1991).

50. *Silvestri*, 271 F.3d at 590.

51. Fujitsu Ltd. v. Fed. Express Corp., 247 F.3d 423, 436 (2d Cir. 2001).

52. *See Turner*, 142 F.R.D. at 73 ("[T]he obligation to preserve evidence even arises prior to the filing of a complaint where a party is on notice that litigation is likely to be commenced.").

53. *See, e.g.*, Smith v. Café Asia, 246 F.R.D. 19, 22 (D.D.C. 2007) (plaintiff's duty of preservation was raised); *The Sedona Conference® Commentary on Legal Holds: The Trigger & the Process*, *supra* note 48, at 5.

54. *See Turner*, 142 F.R.D. at 72 ("While a litigant is under no duty to keep or retain every document in its possession once a complaint is filed, it is under a duty to preserve what it knows, or reasonably should know, is relevant in the action, is reasonably calculated to lead to the discovery of admissible evidence, is reasonably likely to be requested during discovery and/or is the subject of a pending discovery request.") (quoting William T. Thompson Co. v. Gen. Nutrition Corp., 593 F. Supp. 1443, 1455 (C.D. Cal. 1984)).

55. *See id.* at 72–73.

56. *See id.*

57. 229 F.R.D. 422 (S.D.N.Y. 2004) (*Zubulake V*).

58. *Id.* at 432. The preservation duty applies to "all sources of potentially relevant information," which in *Zubulake V* included ESI stored on computer hard drives and backup tapes and printed out on paper. *Id.*

indeed. One major responsibility imposed by *Zubulake V* is to know the client's data storage paradigm.[59] This includes finding out what sorts of devices are commonly used, how (or if) the data on these devices propagates through other computing infrastructures, and, most importantly, the procedures by which data is retained or purged from those devices.[60] An attorney cannot effectively gather this information without speaking with information technology (IT) personnel as well as the users of the devices.[61] *Zubulake V* clearly states that an attorney must be thorough in interviewing all relevant users and IT personnel or else risk missing a potential source of ESI.[62] Attorneys' failure to familiarize themselves with clients' IT infrastructures may lead to sanctions or even ethical violations depending on the jurisdiction and the egregiousness of the circumstances.[63]

Another major directive of *Zubulake V* is to use the information gathered under the first directive to implement an effective litigation hold that lets no pertinent ESI slip through the net.[64] The analysis was first propounded in a predecessor case to *Zubulake V*, *Zubulake IV*,[65] which breaks the duty to preserve into two steps: the "trigger," which causes the preservation duty to arise, and the "scope," which determines what documents or evidence are subject to preservation.[66] In order to allow practitioners to more easily understand their preservation obligations, *The Sedona Conference Commentary on Legal Holds* provides specific examples and guidelines.[67]

---

59. *Id.* ("[C]ounsel must become fully familiar with her client's document retention policies, as well as the client's data retention architecture.").

60. *Id.*

61. *Id. See also* RALPH C. LOSEY, E-DISCOVERY 55 (2008) (the "*Zubulake* duty" is "to supervise e-discovery by speaking directly with your client's IT personnel and understand what they say").

62. *Zubulake V*, 229 F.R.D. at 432.

63. *See, e.g.*, Pastorello v. City of New York, No. 95 Civ. 470 (CSH), 2003 U.S. Dist. LEXIS 5231, at *29–42 (S.D.N.Y. Mar. 31, 2003) (finding gross negligence to support sanctions for spoliation where destruction of relevant evidence occurred because of unfamiliarity with record-keeping policy by employee responsible for preserving and producing documents); Ophir D. Finkelthal, *Scope of Electronic Discovery and Methods of Production*, 38 LOY. L.A. L. REV. 1591, 1602 n.58 (2005) ("See Danis v. USN Communications, Inc., 53 Fed. R. Serv. 3d (West) 828 (N.D. Ill. 2000) (granting the part of the plaintiff's motions for sanctions that requested a jury instruction indicating that gaps in production of documents are attributable to the defendant telecommunications company, and fining the company's CEO where the defendants did not adequately discharge the duty that arose on the date litigation commenced to preserve discoverable, primarily electronic, documents due to a lack of decisive steps to adequately implement the defendant company's internal document retention policy and the defendants' lack of understanding of the uses, significance or method of generation of its own documents, but denying the sanction of default judgment)"). *See also* LOSEY, *supra* note 61, at 55 ("Lawyers today must rise to the occasion and learn enough about IT to carry this load [of competently supervising e-discovery] . . . . Failure to do so may constitute a breach of their professional and ethical duty of competent representation and may also lead to sanctions by the court.").

64. *See Zubulake V*, 229 F.R.D. 422, 432 (S.D.N.Y. 2004) ("Once a 'litigation hold' is in place, a party and her counsel must make certain that all sources of potentially relevant information are identified and placed 'on hold,' to the extent required in *Zubulake IV*.").

65. Zubulake v. UBS Warburg LLC, 220 F.R.D. 212 (S.D.N.Y. 2003) (*Zubulake IV*).

66. *Id.* at 216–17.

67. *The Sedona Conference® Commentary on Legal Holds: The Trigger & the Process*, *supra* note 48,

1. Events that Trigger the Duty to Preserve

Trigger events include anything that causes parties to reasonably anticipate litigation in which evidence in their control may be relevant.[68] Some events are obvious triggers: a letter from counsel, a subpoena, service of process, or the filing of a lawsuit.[69] Other triggers, especially for defendants and third parties, may be more subtle. *The Sedona Conference Commentary on Legal Holds* describes these triggers as follows:

> On the defendant's side, credible information that [the defendant] is the target of legal action may be sufficient to trigger the duty to preserve. The duty to preserve may arise as to a third party when credible information is received that they possess relevant information that may be sought by one of the parties.[70]

To be credible, however, the threat of litigation must be more than a mere possibility.[71] In order for a potentially expensive and burdensome duty of preservation to attach, the party must conclude, based on the facts and circumstances, that some legal action is likely.[72] Because the presence or absence of a triggering event turns on notice, good faith, due diligence, and agency obligations of the parties, these are important elements courts look at to determine whether a triggering event has occurred.[73] If a court finds that a party should have known that litigation was likely to occur, and that a party ignored its preservation obligations due to lack of actual notice, the court may impose sanctions for a breach of the duty of preservation.[74]

---

at 5.

68. *See id.*

69. *See id.*

70. *Id.*

71. *See id.*

72. *See id.*

73. *See id.* at 5–6, 9–10.

74. *See, e.g.*, KCH Services, Inc. v. Vanaire, Inc., No. 05-777-C, 2009 U.S. Dist. LEXIS 62993, at *3–7 (W.D. Ky. July 21, 2009) (finding duty to preserve triggered where plaintiff software company president called defendant regarding unauthorized use of plaintiff's software; sanctions imposed after defendant deleted software prior to any other communications or litigation filings); Doe v. Norwalk Comm. Coll., 248 F.R.D. 372, 377 (D. Conn. 2007) (holding that duty to preserve a sexual harassment suspect's computer and e-mail arose at the time the defendant college, the suspect's employer, became "aware of . . . allegations of sexual assault" after a meeting between the dean and the suspect before the filing of any complaint); *Zubulake IV*, 220 F.R.D. 212, 216–17 (S.D.N.Y. 2003) (finding that defendant's duty to preserve certain e-mails was triggered five months prior to the filing of plaintiff's EEOC complaint because "almost everyone associated with [the plaintiff within the defendant company] recognized the possibility that she might sue").

2. The Scope of the Duty to Preserve

Though the standard for what constitutes a trigger event is relatively liberal, the *Zubulake IV* court provided balance by restricting the scope of the duty to preserve to only ESI likely to be relevant to the anticipated litigation.[75] Therefore, a party need not "preserve every shred" of ESI out of fear that it may possibly be relevant.[76] Blanket preservation orders are both terribly expensive and potentially crippling to a party's affairs or business.[77] To narrow the scope of the duty of preservation, *Zubulake IV* requires attorneys to ask "Whose Documents Must Be Retained?" and "What Must Be Retained?"[78] The respective answers to each of these questions is that at least the ESI from "key players" in the litigation must be preserved,[79] and for these individuals, all potential sources of relevant ESI must be identified and preserved.[80] Once the scope of preservation is set, the duty to preserve is both retroactive and proactive. All potentially relevant ESI from the past must be identified and preserved.[81] All potentially relevant ESI created in the future must also be identified and preserved.[82]

3. The Duty to Preserve PED ESI

There is little doubt that data stored on PEDs is subject to a duty of preservation equivalent to other ESI.[83] In *Smith v. Café Asia*,[84] the only reported decision to date to have discussed the preservation of PED ESI that this author could find, the U.S. District Court for the District of Columbia placed a burden of preservation on the plaintiff by ordering that

75. *Zubulake IV*, 220 F.R.D at 217 ("[A litigant] is under a duty to preserve what it knows, or reasonably should know, is relevant in the action, is reasonably calculated to lead to the discovery of admissible evidence, is reasonably likely to be requested during discovery and/or is the subject of a pending discovery request.").

76. *Id.*

77. *See id.* ("Such a rule would cripple large corporations, like UBS, that are almost always involved in litigation.").

78. *Id.* at 217–18.

79. Key players are "those employees likely to have relevant information." *Id.* at 218. In *Zubulake IV*, these were the individuals with whom the plaintiff had had e-mail contact regarding the events being litigated. *Id.*

80. *Id.* at 218. Duplicative ESI need not be preserved, however. If many different copies of the same data file are stored in different locations, only one copy need be preserved. *See id.*

81. *See Zubulake IV*, 220 F.R.D. 212, 218 (S.D.N.Y. 2003). A "mirror-image" of all of a key player's present data plus a compilation of all of that individual's available and identifiable backup data would suffice. *Id.*

82. *Id.*

83. *See* FED. R. CIV. P. 26 advisory committee's notes, 2006 amends., subdiv. (b)(2). *See also* DUIZEND, *supra* note 4, at v, 1 (listing PEDs such as pagers, web-enabled portable devices, cellular phones, personal digital assistants, handheld wireless devices, and "other portable devices" alongside other computer technologies as repositories for discoverable electronic information).

84. 246 F.R.D. 19 (D.D.C. 2007).

digital photographs stored on the phone be preserved pending review by the trial court for relevancy.[85] While the *Café Asia* court's analysis primarily focused on the relevancy and privacy concerns surrounding the production of the images—and therefore did not directly address the issue of preservation of digital images on a cellular phone—the effect of the court's order to preserve the images was to at least bring digital photographs on a cellular phone under the purview of Rule 26 of the Federal Rules of Civil Procedure.[86]

Because PEDs are essentially small computers, the analysis of the duty to preserve PED ESI parallels the duty to preserve other ESI already outlined.[87] The first thing an attorney must do is become educated about a client's use of PEDs—who has them; how they are used; what types of ESI might be stored on them; whether ESI is backed up to other locations; and, if it is, where and how the ESI is backed up to other locations.[88] Without this foundational knowledge, it is impossible to ascertain the scope of the preservation obligation and implement an effective litigation hold.[89]

Given the modern trend toward constant communication and connectivity through PEDs, it is increasingly likely that data stored on PEDs will be subject to an early preservation obligation in nearly all litigation involving communication between individuals. This is so because PEDs are becoming a much more important primary mode of communication and can no longer be casually overlooked as a source of relevant ESI. Certainly, if an individual is identified as a key player, relevant ESI from that person's PEDs, as well as computers and e-mail accounts, must be preserved in order to satisfy *Zubulake IV*'s obligations.[90] PEDs from other individuals

85. *Id.* at 22 (sexual harassment plaintiff ordered to preserve allegedly sexually explicit photographs stored on his personal cellular phone pending trial court's determination of the relevance of the images).

86. Unfortunately, *Café Asia* gives little further guidance on what the plaintiff was to do next and what would have been considered adequate to preserve the data. *See* 2 ANDREW B. SERWIN, Information Security and Privacy: A Practical Guide to Federal, State and International Law § 26:20 (2008) ("Outside of the rather unique factual scenario of [*Café Asia*], generally cell phone camera images would be generally discoverable.").

87. *See* discussion of duty to preserve *supra* Part III.A.

88. *See, e.g.*, Hopson v. Mayor of Baltimore, 232 F.R.D. 228, 245 (D. Md. 2005) ("[C]ounsel have a duty to take the initiative in meeting and conferring to plan for appropriate discovery of electronically stored information at the commencement of any case in which electronic records will be sought. . . . At a minimum, they should discuss: the type of information technology systems in use and the persons most knowledgeable in their operation; preservation of electronically stored information that may be relevant to the litigation; the scope of the electronic records sought (i.e. e-mail, voice mail, archived data, back-up or disaster recovery data, laptops, personal computers, PDA's, deleted data) . . . .").

89. Under *Phoenix Four*, discussed *infra* Part III.B, a failure to investigate and inform opposing counsel of relevant ESI contained on PEDs would constitute sanctionable gross negligence. Phoenix Four, Inc. v. Strategic Res. Corp., No. 05-CIV-4837, 2006 U.S. Dist. LEXIS 32211 (S.D.N.Y. May 22, 2006).

90. *See* Zubulake v. UBS Warburg LLC (*Zubulake IV*), 220 F.R.D. 212, 217–18 (S.D.N.Y. 2003).

may also come within the scope of preservation, perhaps more easily than other types of more stationary computers.[91]

B. The Hidden Danger of Sanctions

Due to the various, and potentially volatile, PED data storage formats discussed above, PED data is inherently more unstable, and its continued existence less certain than data from more conventional computer sources.[92] Many PEDs and the communication systems behind them destroy data during the regular course of use. Also, because they are relatively novel, PEDs are easily overlooked in the discovery process.[93] No doubt a number of cases have gone by in which ESI contained on PEDs has been either negligently or deliberately undisclosed or destroyed. In the future, however, it is likely that an increasing awareness of PED ESI will lead to waves of sanctions for which ignorance will be no excuse.[94]

A federal court's power to sanction for breach of the duty to preserve arises out of two potential sources: Rule 37 of the Federal Rules of Civil Procedure[95] and the inherent power of courts to regulate parties' conduct during litigation.[96] State courts have similar sources of sanctioning authority in common law and, to the extent that they exist, in state rules of civil procedure.[97] The rapid development of technology, coupled with recent changes in federal and state laws, has made electronic discovery sanctions something of a sword of Damocles hanging over unsuspecting litigants and their counsel.[98] Courts and legislatures have yet to iron out exactly what

91. The ubiquity of these devices, and the frequency with which they are used makes them more like personal video or audio recording devices than personal computers in the sense that, without the user's conscious intent, they capture many details of the user's life, location, thoughts, and interactions with others. Indeed, most modern PEDs have the ability to capture photos, audio, and video recordings. Many also store data related to GPS navigation. *See* Personal Electronic Device Notification System, U.S. Patent No. 6,650,231 (filed June 14, 2002) (issued Nov. 18, 2003), *available at* http://www.patentstorm.us/patents/6650231/description.html.

92. *See* KIPPER, *supra* note 15, at 64 (discussing the volatility and ever-changing nature of PDA data).

93. To many attorneys, electronic discovery is synonymous with e-mail discovery, while many other sources of ESI are ignored. *See, e.g.*, Svenson, *supra* note 5.

94. As has been the case with conventional electronic discovery, an attorney's "computer illiteracy" may be seen by some judges as tantamount to an admission of malpractice. *See, e.g.*, Martin v. N.W. Mut. Life Ins. Co., No. 8:04-CV-2328-T-23MAP, 2006 U.S. Dist. LEXIS 2866, at *6 (M.D. Fla. Jan. 19, 2006) ("Plaintiff's [attorney's] reasons for non-production are unsatisfactory and warrant sanctions. . . . His claim that he is so computer illiterate that he could not comply with production is frankly ludicrous.").

95. Turner v. Hudson Transit Lines, Inc., 142 F.R.D. 68, 72 (S.D.N.Y. 1991).

96. *Id.*

97. More than half of states have amended their civil discovery rules specifically to address electronic discovery. For a listing of these states and corresponding statutory amendments, see Electronic Discovery Law, *Current Listing of States that Have Enacted E-Discovery Rules*, http://www.ediscoverylaw.com/2008/10/articles/resources/current-listing-of-states-that-have-enacted-ediscovery-rules (Oct. 10, 2008).

98. *See, e.g.*, Svenson, *supra* note 5. *See also* Thomas J. Smith & Michael J. Crossey, Jr., *E-Discovery Alert: E-Discovery Sanctions: A Continuing Trend*, K&L GATES, Apr. 2007, at 1, *available*

level of negligence or malfeasance is required to impose e-discovery sanctions. [99] No case yet has addressed sanctions for PED e-discovery specifically,[100] but the cases cited below give a sense of the law as it is currently unfolding and as it will probably apply to PED e-discovery.

1. Differing Standards for Electronic Discovery Sanctions

Doe v. Norwalk Community College, a non-PED federal district court case out of Connecticut, suggests that e-discovery sanctions can be imposed for mere negligence in failing to preserve ESI relevant to likely future litigation.[101] In *Norwalk Community College*, a sexual harassment plaintiff moved for an adverse inference sanction after her expert found that the defendant college had wiped all data from the hard drive of a former faculty member, the alleged harasser.[102] The college wiped at least some of the data pursuant to its internal policy of no data retention,[103] and

at http://www.klgates.com/files/upload/eDAT_2007_04_E_Discovery_Alert.pdf ("[C]ourts have broad discretion regarding the type and degree of sanctions they can impose. Depending on the egregiousness of the e-discovery missteps, companies that have engaged in intentional, negligent, or even *innocent*, spoliation of electronic evidence have been assessed monetary sanctions (including both civil penalties and costs and attorneys' fees associated with discovery), preclusion sanctions (*i.e.*, precluding the offer or other use of certain evidence), adverse inferences (*i.e.*, directing a jury to assume missing ESI is adverse to the spoliator), so-called 'rummaging' (*i.e.*, giving the discovering party hands-on access to an adversary's computer system), revocation of *pro hac vice* admission of counsel, and even default judgments.").

99. *Compare* Fed. R. Civ. P. 37(f) *and The Sedona Principles: Best Practices Recommendations & Principles for Addressing Electronic Document Production*, The Sedona Conference Working Group Series, at i, ¶ 14 (Jonathan M. Redgrave et al. eds., 2004), *available at* http://www.thesedonaconference.org/dltForm?did=SedonaPrinciples200401.pdf ("a clear duty to preserve," "intentional or reckless failure to preserve and produce," and "a reasonable probability" of material prejudice) *with* DUIZEND, *supra* note 4, at 10 ("Absent exceptional circumstances, a judge should impose sanctions because of the destruction of electronically-stored information only if: A. There was a legal obligation to preserve the information at the time it was destroyed; B. The destruction of the material was not the result of the routine, good faith operation of an electronic information system; and C. The destroyed information was subject to production under the applicable state standard for discovery.").

100. The *Café Asia* opinion alludes to the possibility of sanctions for the spoliation of the digital photographs contained on the plaintiff's cellular phone in the case that the plaintiff fails to preserve data that he actually knows to be potentially relevant to reasonably anticipated litigation. Smith v. Café Asia, 246 F.R.D. 19, 21 n.1 (D.D.C. 2007).

101. Doe v. Norwalk Cmty. Coll., 248 F.R.D. 372, 379 (D. Conn. 2007). *See also* Reilly v. Natwest Mkts. Group Inc., 181 F.3d 253, 268 (2d Cir. 1999) ("[A] finding of bad faith or intentional misconduct is not a *sine qua non* to sanctioning a spoliator with an adverse inference instruction."); Glover v. BIC Corp., 6 F.3d 1318, 1329 (9th Cir. 1993) ("Surely a finding of bad faith will suffice [to support an adverse inference], but so will simple notice of 'potential relevance to the litigation.'") (citation and internal quotation marks omitted); Stender v. Vincent, 992 P.2d 50, 59 (Haw. 2000) ("This court has never regarded bad faith or intentionality as a talisman in the imposition of discovery sanctions . . . ."); Hamann v. Ridge Tool Co., 539 N.W.2d 753, 756–57 (Mich. Ct. App. 1995) (exclusion of expert testimony justified even where evidence was unintentionally lost); DeLaughter v. Lawrence County Hosp., 601 So. 2d 818, 822 (Miss. 1992) (jury may draw adverse inference based on deliberate or negligent loss of evidence).

102. *Norwalk Cmty. Coll.*, 248 F.R.D. at 375–76.

103. *Id.* at 377 ("[T]he defendants admit that they 'scrubbed' Masi's hard drive 'pursuant to normal

because of this, the college attempted to invoke the good faith exception provision of Rule 37(f).[104] The court rejected the defendant's invocation of the exception and granted the adverse inference motion.[105]

Norwalk Community College also effectively limits the good faith exception of Rule 37 by allowing the exception to apply only if a party has complied with their *Zubulake IV* preservation obligations.[106] The data destroyed was that of a "key player," and under the two-step analysis of *Zubulake IV*, once the individual had been identified, all of his reasonably accessible data should have been preserved.[107] The court explained that "in order to take advantage of the good faith exception, a party needs to act affirmatively to prevent the system from destroying or altering information, even if such destruction would occur in the regular course of business."[108] Under the *Zubulake IV* framework, the college should have reasonably anticipated litigation at the time they became aware of a police report naming the faculty member as a sexual assault suspect.[109] At that time, they should have taken action to preserve the harasser's computer and not allowed it to be wiped pursuant to normal procedures.[110]

Other jurisdictions are more forgiving and require a showing of bad faith before imposing harsh sanctions for spoliation.[111] In these jurisdic-

---

NCC practice.'").

104. *Id.* at 378 ("Absent exceptional circumstances, a court may not impose sanctions under these rules on a party for failing to provide electronically stored information lost as a result of the routine, good-faith operation of an electronic information system.") (quoting FED. R. CIV. P. 37(f)).

105. *Id.* at 378, 382–83.

106. *See* discussion *infra* Part III.D.1.

107. *See* Zubulake v. UBS Warburg LLC (*Zubulake IV*), 220 F.R.D. 212, 217–18 (S.D.N.Y. 2003).

108. Doe v. Norwalk Cmty. Coll., 248 F.R.D. 372, 378 (D. Conn. 2007).

109. Several "trigger" events occurred prior to the college permitting the harasser's hard drive to be wiped including a meeting regarding the sexual assault incident held between the harasser and the college dean, a demand letter sent by the plaintiff's lawyer, the harasser's resignation under suspicious circumstances, and the fact that there was an ongoing police investigation into the incident. *Id.* at 377–78.

110. *Id.* It should be noted that the *Norwalk Community College* court also failed to find that a policy of wiping the drives of past employees fit into the scope of the Rule 37 good faith exception.

> [A]s the Commentary to Rule 37(f) indicates, the Rule only applies to information lost "due to the 'routine operation of an electronic information system'—the ways in which such systems are generally designed, programmed, and implemented to meet the party's technical and business needs". . . . This Rule therefore appears to require a routine *system* in order to take advantage of the good faith exception, and the court cannot find that the defendants had such a system in place.

Id. at 378 (internal citations and emphasis omitted).

111. *See* Aramburu v. Boeing Co., 112 F.3d 1398, 1407 (10th Cir. 1997) ("The adverse inference must be predicated on the bad faith of the party destroying the records. Mere negligence in losing or destroying records is not enough because it does not support an inference of consciousness of a weak case.") (internal citations omitted); Bashir v. Amtrak, 119 F.3d 929, 931 (11th Cir. 1997) ("'Mere negligence' in losing or destroying the records is not enough for an adverse inference, as 'it does not sustain an inference of consciousness of a weak case.'") (internal quotations omitted); Vodusek v. Bayliner Marine Corp., 71 F.3d 148, 156 (4th Cir. 1995); Spesco, Inc. v. Gen. Elec. Co., 719 F.2d 233, 239 (7th Cir. 1983); Gumbs v. Int'l Harvester, Inc., 718 F.2d 88, 96 (3d Cir. 1983); Inventory Locator Serv., LLC v. PartsBase, Inc., No. 02-2695-MaV, 2005 U.S. Dist. LEXIS 46252, at *40 (W.D. Tenn. Oct. 19, 2005); Hamilton v. Signature Flight Support Corp., No. C 05-0490 CW (MEJ),

tions, mere negligence in failing to preserve ESI is either not sanctionable, or the sanctions imposed are relatively light and remedial in nature. One such recent decision is the *Phoenix Four* case, another non-PED case from the Southern District of New York.[112] The *Phoenix Four* case involved a corporate defendant that failed to inform the plaintiff of ESI contained on hidden partitions of two servers. One year later, and six weeks after the close of discovery, an independent IT consultant hired by the defendant discovered the hidden data and notified defense counsel.[113] The court found that defendants had breached their *Zubulake IV* duty, noting that "[d]efendants abandoned at least ten computer workstations without bothering to make any search whatsoever in order to discover whether they contained [relevant] information. Their indifference constituted an act of gross negligence that is not excused by the disarray of their business affairs."[114] Finding no bad faith, the court declined to grant plaintiff's motion for an adverse inference and instead imposed relatively light remedial sanctions in the form of plaintiff's costs involved in bringing the motion and for costs associated with redeposing witnesses in light of the newly disclosed evidence.[115]

Sanctions may not be the only adverse effect of failing to preserve ESI. *Lee v. U.S. Secretary Associates, Inc.*, a recent opinion from the Western District of Texas, mentions that an allegation that the defendant destroyed cellular phone records cut against the defendant on a motion for summary judgment even where the court declined to consider the issue of spoliation.[116] Though the *Lee* case did not specify whether it involved destruction of ESI stored on the phone itself or whether the destroyed records were stored elsewhere, had the records been contained on the phone itself, it is likely that the analysis would have proceeded in the same fashion. Data, after all, is the same no matter where it is stored.[117]

2005 U.S. Dist. LEXIS 40088, at *21 (N.D. Cal. Dec. 20, 2005) ("[B]ecause the Court cannot find that Signature consciously disregarded its obligation to preserve the surveillance recording, this factor weighs in favor of denying Plaintiffs motion for sanctions."); State v. Langlet, 283 N.W.2d 330, 333 (Iowa 1979); Brown v. Hamid, 856 S.W.2d 51, 56–57 (Mo. 1993).

112. Phoenix Four, Inc. v. Strategic Res. Corp., No. 05-CIV-4837, 2006 U.S. Dist. LEXIS 32211 (S.D.N.Y. May 22, 2006). *See also* LOSEY, *supra* note 61, at 58–60 (discussing the *Phoenix Four* decision and its impact on electronic discovery).

113. *Phoenix Four*, 2006 U.S. Dist. LEXIS 32211 at *7.

114. *Id.* at *14–15.

115. *Id.* at *23–26, *28–29.

116. Lee v. U.S. Sec. Assoc., No. A-07-CA-395-AWA, 2008 WL 958219, at *7 n.5 (W.D. Tex. Apr. 8, 2008) ("Plaintiff notes that he will be seeking a spoilation instruction at trial as Defendant destroyed the cell phone records which would have indicated the number and duration of calls. The Court will not address the spoliation issue at this time, but the lack of these records as a result of the Defendant's destruction of them is another factor the Court has considered in denying the motion for summary judgment on this issue.").

117. *See* discussion of data storage *supra* Part II.A.

2. Applying the Rule 37 Good Faith Exception

Rule 37(e) provides a limited safe harbor for "good faith" spoliation of electronic evidence where ESI was lost or destroyed through the "routine, good-faith operation of an electronic information system."[118] Though this safe harbor does not negate the duty to preserve ESI, it prevents a court from imposing sanctions under the rules of civil procedure that might otherwise be appropriate.[119] The good faith exception of Rule 37(e)[120] may apply where PED data is inadvertently lost, but this provision should not be relied on as a panacea for the loss of volatile data. Even where the destruction of data is automatic, the Rule 37(e) exception applies only if a party takes reasonable steps to stop any automatic destruction after the duty to preserve is triggered.[121] This means that where computer systems automatically purge data as part of their normal operation, a party with a duty to preserve must actively intervene to prevent that destruction in order for Rule 37(e) to apply.[122] This limitation significantly restricts the protection promised by Rule 37, which seems to have little application left except to cases where data was lost due to a genuine mistake.[123]

Arguments can be made both for and against the applicability of Rule 37(e) to volatile PED ESI lost for reasons associated with its volatility.[124] Data stored in volatile memory is likely ESI subject to the same duty of preservation as data stored in nonvolatile memory.[125] If a party knows that relevant ESI on a PED is liable to be destroyed by either being erased or overwritten, then that party has an affirmative duty to prevent this from happening.[126] Even if the party does not know whether ESI on their PED is at risk, they (or their attorney) may have a duty to find out whether this

118. FED. R. CIV. P. 37(e). *See also* discussion *infra* Part III.B.

119. *See* FED. R. CIV. P. 37(e).

120. The restyled Federal Rules of Civil Procedure went into effect in December of 2007. What was Rule 37(f) prior to the restyling is now Rule 37(e). The text of the rule remains unchanged.

121. *See* FED. R. CIV. P. 37 advisory committee's notes, 2006 amends., subdiv. (f); Peskoff v. Faber, 244 F.R.D. 54, 60 (D.D.C. 2007) ("The Advisory Committee comments to amended Rule 37(f) make it clear that any automatic deletion feature should be turned off and a litigation hold imposed once litigation can be reasonably anticipated.").

122. *See Peskoff*, 244 F.R.D. at 60. *See also* Disability Rights Council v. Wash. Metro. Transit Auth., 242 F.R.D. 139, 146 (D.D.C. 2007).

123. Forgivable mistakes are the "Oops, I hope that wasn't important!" variety. These are actions taken without bad intent that result in an inadvertent and unexpected deletion of relevant data. A failure to investigate the data retention policies of an organization or to determine the schedule by which a computer system purges old data are breaches of the *Zubulake IV* duty to be reasonably informed and are not excused under Rule 37(e).

124. *See* discussion of characteristics of volatile data *supra* Part II.A.3.

125. *See, e.g.*, Columbia Pictures, Inc. v. Bunnell, 245 F.R.D. 443, 446 (C.D. Cal. 2007) (holding that information stored in a server's volatile RAM memory was discoverable ESI despite the fact that it was never intended to be permanently stored).

126. *See id.* at 448.

is the case. Therefore, if ESI is lost due to being overwritten, automatically deleted, or because of a dead battery, the safe harbor of Rule 37(e) may not apply.

On the other hand, if PED ESI is lost by a good-faith mistake while using the device, (for example, an accidental deletion by a slip of the hand or other user error), then Rule 37(e) probably does apply. Similarly, loss of the PED or accidental damage to the PED causing certain ESI to be irretrievable may be excusable so long as the party using the PED had good reason for not backing the data up to a more stable medium.[127] Normal good faith operation of a PED entails carrying the device around, meaning that it will necessarily be exposed to a number of risks. If data on a PED is vital to a case, however, one should not rely on Rule 37(e) as a shield against sanctions where common sense would require the user to stop using the device in order to preserve the data. In addition to being tenuous protection conditioned on faithful discharge of *Zubulake IV* duties, Rule 37(e) only guards against sanctions levied under the rules of civil procedure.[128] It provides no shield against other types of court-imposed penalties or costs. The cost of attempting recovery of PED data, in the event that it is carelessly lost, or the cost of damages could be steep.[129]

The safest way to avoid sanctions when dealing with PEDs is to follow the directives of *Zubulake V* as carefully as possible.[130] Aggressive and informed information gathering coupled with early consultation with a PED expert to impose an effective litigation hold is probably sufficient to ward off any danger of sanctions. For those who seek to wield the sword, the cases cited above and their progeny provide quite a few avenues of attack against an opponent who has been less than diligent or is unfamiliar

---

127. Undue burden or expense are very good reasons not to back up ESI from some PEDs, but not for others. Blackberry and Palm devices, for example, provide backup software that is easy for a nontechnical user to use. Many other PEDs come with backup software with varying degrees of functionality.

128. *See* FED. R. CIV. P. 37, advisory committee's notes, 2006 amends., subdiv. (f):

> The protection provided by Rule 37(f) applies only to sanctions "under these rules." It does not affect other sources of authority to impose sanctions or rules of professional responsibility.
>
> This rule restricts the imposition of "sanctions." It does not prevent a court from making the kinds of adjustments frequently used in managing discovery if a party is unable to provide relevant responsive information. For example, a court could order the responding party to produce an additional witness for deposition, respond to additional interrogatories, or make similar attempts to provide substitutes or alternatives for some or all of the lost information.

Id.

129. *See id.*

130. *See* Zubulake v. UBS Warburg LLC, 229 F.R.D. 422 (S.D.N.Y. 2004) (*Zubulake V*):

> Once a "litigation hold" is in place, a party and her counsel must make certain that all sources of potentially relevant information are identified and placed "on hold" . . . . [C]ounsel must become fully familiar with her client's document retention policies, as well as the client's data retention architecture.

Id. at 432.

with his or her client's use of PEDs. Such an attack should be well informed and precise; however, the party moving for sanctions may be required to demonstrate not just that it was possible for data to have been destroyed or undisclosed, but that certain relevant data was *in fact* destroyed or undisclosed.[131]

C. Special Problems with Preserving PED Data

Anyone who has ever upgraded to a new cellular phone knows that PED data is difficult to physically access and preserve. By way of example, suppose a client has a photo on a cellular phone, as was the case in *Café Asia*, and there is a duty to preserve that photo because it is important to pending litigation. Suppose that in addition to the photo, there are also several phone calls and text messages stored on the phone that are also potentially important to the pending litigation. Clearly, this ESI cannot be deliberately deleted without risking sanctions (and probably worse), but how can counsel be sure that critical ESI is not inadvertently deleted?[132] Many PEDs store ESI in volatile memory, and unless you or your client is an expert on the PED in question, you and your client may always be a dead battery away from potentially sanctionable negligence.[133]

Consider also that PEDs store their data in a number of different places. A combination device may include data storage on internal memory, in a SIM card, on removable media such as Secure Digital (SD) or memory sticks, and on a company or service provider's servers. Before one can implement an effective litigation hold, one must know where relevant data may be stored. In order to save time and money, it is just as important to know what data storage locations are irrelevant and duplicative.[134]

PEDs have relatively limited data storage space internally, and, as a result, many PEDs store only a certain fixed amount of the most recent

131. *See* Treppel v. Biovail, Corp., 233 F.R.D. 363, 371–72 (S.D.N.Y. 2006) (non-PED e-discovery case wherein plaintiff's motion for sanctions was denied, even though defendants appeared to be negligent in fulfilling their preservation duties under the *Zubulake* cases).

132. *See generally* Lockheed Martin Corp. v. L-3 Commc'ns Corp., 2007 U.S. Dist. LEXIS 54606 (M.D. Fla. July 29, 2007) (trade secret case in which all data from a PDA belonging to a key player was lost due to the battery discharging while in storage).

133. No case has yet ruled on this issue as it has yet to come up. Rule 37(e) safe harbor provisions may protect a party if the dead battery was a good faith mistake. *See* FED. R. CIV. P. 37(e). *But see supra* note 49. At the very least, such a situation would be costly and embarrassing, especially if it makes new law. The community of PED experts has long been aware of data loss due to dead batteries or use of the device on a network. *See, e.g.*, WAYNE JANSEN & RICK AYERS, GUIDELINES ON CELL PHONE FORENSICS: RECOMMENDATIONS OF THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY 34–35 (2007), *available at* http://csrc.nist.gov/publications/nistpubs/800-101/SP800-101.pdf.

134. *Zubulake V* specifically excludes duplicative data from the duty of preservation. 229 F.R.D. at 495 n.88 (citing Zubulake v. UBS Warburg LLC, 220 F.R.D. 212, 218–19 (S.D.N.Y. 2003) (*Zubulake IV*), for the proposition that it was sufficient to preserve one copy of all relevant electronic files).

data before systematically overwriting older data.[135] This means that as a client or a third party continues to use a PED, critical ESI may be inadvertently destroyed merely by innocent, normal use of the device.[136] In fact, in the case of wireless devices connected to any sort of communications network, the device need not even be used to change or delete ESI stored on the device.[137] A cellular phone or PDA sitting on a shelf will still receive incoming calls, text messages, or e-mail, and may overwrite old data as it receives new data from the network.[138]

Finally, consider that PEDs are fragile and portable, prone to being broken, stolen, lost, or water-damaged, and likely to suffer any number of horrible fates in the hands of dogs, children, or angry (or deliberately malicious) parties.[139] With all of their inherent vulnerabilities, PEDs are a decidedly poor choice for long-term storage of critical ESI.

D. Approaches to Preserving, or Not Preserving, PED Data

Preservation of PED data in most cases is a highly technical task that requires proper expertise. There are essentially three options for preserving PED data that may be elected, depending on the circumstances. These options are to preserve the PED by "freezing" the device itself; to "clone" the PED and freeze either the original or the clone (allowing the user to continue to use the device); or to copy the ESI stored on the PED to a secure medium using a forensic expert.[140] Because the duty of preservation is ongoing and applies to ESI generated in the present and future as well as in the past, a combination of these methods might be needed to implement an effective litigation hold.

1. Freeze the PED

The first option is to simply keep the data on the PED in its existing form by either storing the PED, or allowing the user to continue using the device with instructions not to delete or alter relevant data. This option has the advantage of being simple and cheap in terms of initial e-discovery costs, but it has two major disadvantages. As discussed above, PEDs are not the best choice for long-term data storage, and there is some risk of

135. *See* JANSEN & AYERS, *supra* note 133, at 31. Cellular phones in particular usually have limited call registers and limited storage of text messages. *See* Don Kohtz & Matt Churchill, *Cell Phone Forensics: The New "Evidentiary" Gold Mine*, NEB. LAW. 11, 12 (Oct. 2008), *available at* http://www.continuumww.com/images/stories/cww/docs/cell_phone_forensics_the_new_evidentiary_gold_mine.pdf.

136. *See* JANSEN & AYERS, *supra* note 133, at 29–37.

137. *See id.*

138. *See id.*

139. *See id.*

140. *See infra* Part II.D.1–3.

relevant data being inadvertently lost or corrupted.[141] The second disadvantage is that the client is placed in a no-win situation regarding the choice of whether to remove and store the PED or whether to allow the user to continue using the device with appropriate caution. The choice is a painful one between continuing to use a PED that may contain discoverable data (risking data loss and sanctions) and losing productivity by permanently or temporarily taking PEDs out of the hands of employees simply to preserve the data contained on them.

If the decision is made to allow the user to continue using the device, this approach may not be a great risk for certain types of data,[142] though for other types, continued use may guarantee that relevant data is lost.[143] Some users may also be more or less trustworthy than others. This option is best used in low-value cases where the ESI on the PED is either available from other sources, likely to be tangential to the issues raised by litigation, or stored in a relatively stable storage medium such as a removable memory card or other known nonvolatile storage.

If the device is to be stored, most clients are likely to balk at the prospect of losing the use of their PED for the amount of time required for litigation to pan out, and some businesses would suffer substantial productivity losses. Modern PED users typically rely on their devices for business and personal matters on a daily, if not hourly, basis. This option is best used in situations where the PED can be safely stored, where there is little risk of data being lost or corrupted, and where the user can easily do without the device. It may be particularly appropriate where the user is a previous employee who no longer has the need or right to continue using a company PED.

Additionally, what constitutes adequately "safe" storage can vary greatly. A case-by-case determination must be made by evaluating the sensitivity and importance of the ESI on the PED and the delicacy of the device. In all cases, a stored PED must be physically secured from loss, theft, damage, and unauthorized use. A PED's stored data must also be secured from accidental loss from discharge of batteries and from change through connection to a wireless network. For an average employment or sexual harassment case, it may be sufficient to keep the device on a charger in a locked office or cabinet, either in a powered-off state or with wire-

141. A PED sitting on a shelf may need to be kept on a charger in order to avoid data loss from a dead battery. A PED connected to a network may also continue to communicate with the network, downloading e-mail, receiving calls or text messages, or installing automatic software updates. In some cases, a devious user may even be able to access the PED remotely, corrupting or destroying stored data.

142. *E.g.*, stored photos, video and audio recordings, or other files intended to be more or less permanent.

143. *E.g.*, call registers, text messages, or instant messages for some PEDs.

less capabilities disabled.[144] For cases involving more sensitive data, such as trade secrets or information with national security concerns, correspondingly greater (and more expensive) security measures may be necessary.[145]

2. Clone the PED

A second and slightly better option is to have an expert back up the client's data to a new and similar device and equip the client with the new device. They get an upgrade, and the old device can be either directly preserved or taken for further processing by experts. Generally, the process of upgrading a user to a new device can be accomplished relatively quickly, minimizing the productivity costs while hedging against the possibility of data being lost or corrupted. Of course, if the original device is simply shelved for preservation, an expert should be consulted to determine if volatile memory or network connectivity are potential issues that could result in data being lost or corrupted while the data is in storage.[146] The discovery costs for using this intermediate approach are greater than in the first option, but less than a full-scale forensic preservation of all potentially relevant PEDs.

3. Forensic Acquisition and Preservation of PED Data

The third option involves an all-out expert acquisition and preservation of ESI from potentially relevant devices, including PEDs and conventional computers. Such an approach is commonly used in the context of government searches and seizures of data, but in the private sector it is usually too disruptive and expensive to be practical.[147] The advantage to this approach is that there should be absolutely no doubt regarding spoliation or admissibility of ESI. Aside from expense, the other major downside of this method is that there are, at the time of this article, very few qualified PED discovery experts. Because of the infancy of the field of PED forensics, and the highly fluid state of the art of PED technologies, some "experts"

144. To ensure that devices are not accessed over the network and do not continue to receive data, it is usually wise to turn the device off or enable "airplane mode."

145. Physical security measures can be quite stringent and include access control lists, chain of custody tracking, and locked storage. Data security measures may include device handling protocols, certification requirements for examiners, and storage of wireless devices in shielded enclosures or rooms that block all wireless signals from being transmitted or received.

146. *See* discussion of appropriate storage of PEDs *supra* Part III.D.

147. In the criminal context, evidentiary concerns as well as crime lab accreditation standards require forensically sound data acquisition and preservation, usually an expensive, intrusive, and counterproductive process for the owner of the data being preserved. *See generally* MIDDLETON, *supra* note 24; Regional Computer Forensics Lab National Program Office, *Best Practices for a Quality Digital Forensics Examination*, http://www.rcfl.gov/downloads/documents/ExaminationBestPractices.doc (last visited Oct. 8, 2009).

may have less than satisfactory training, experience, and tools to handle a client's particular PED.[148] An expert, if one can be found, should be chosen and interviewed carefully to make sure he or she is able to complete the job required.[149]

E. Preservation Orders

PEDS are ideal candidates for a preservation order.[150] Of course, relevance challenges to PED data may help some litigants avoid burdensome preservation or production obligations, but only if the preservation order sought is overly broad and poorly researched.[151] It may be that the data sought on PEDs is unrelated to the case, tangential to the issues in the case, or merely cumulative with other evidence.[152] If this is the case, there is obviously no duty to preserve irrelevant data, though this fact should be documented to avoid future complications. It is difficult to prove that data, long ago lost or destroyed, was irrelevant at the time the decision was made not to preserve it, and a decision not to preserve could in hindsight be misinterpreted as negligence or affirmative misconduct (especially if the lost data later turns out to be relevant due to an unforeseen twist in the case).

III. THE SECOND CHALLENGE: PRODUCTION

A. Special Challenges with Producing and Presenting PED Data

It is now well settled that a request for "documents" under Rule 34 of the Federal Rules of Civil Procedure includes ESI as well as paper documents. [153] Consequently, most attorneys are used to producing server,

148. *See generally* Matthew I. Cohen et al., *Best Practices for the Selection of Electronic Discovery Vendors: Navigating the Vendor Proposal Process*, The Sedona Conference Working Group Series, at 3–4 (2007), *available at* http://www.thesedonaconference.org/dltForm?did=RFP_Paper.pdf.

149. *See, e.g.*, *id.* at 8–10.

150. *See* Capricorn Power Co. v. Siemens Westinghouse Power Corp., 220 F.R.D. 429 (W.D. Pa. 2004); DUIZEND, *supra* note 4, at 9–10.

151. *See, e.g.*, Treppel v. Biovail, 233 F.R.D. 363, 372 (S.D.N.Y. 2006) (plaintiff's motion for a blanket preservation order covering "electronic data, including email data, whether on back-up tapes, computer hard drives, servers, PDA's, Blackberries, or other physical media" denied as premature on grounds that it would be "prohibitively expensive and unduly burdensome for parties dependent on computer systems in their day-to-day operations.") (quoting MANUAL FOR COMPLEX LITIGATION (FOURTH) §11.442 (2004)). The court went on to comment, "a preservation order will likely be ineffective if it is formulated without reliable information from the responding party regarding what data-management systems are already in place, the volume of data affected, and the costs and technical feasibility of implementation." *Id.*

152. *See, e.g.*, Anderson v. Mergenhagen, 642 S.E.2d 105, 110–11 (Ga. App. 2007) (district court denial of subpoena of defendant's cellular phone records upheld where such records were not directly relevant to the issue of the intrusiveness of defendant's behavior in a physical stalking case).

153. *See* RABIEJ, *supra* note 32, at § 37A.11[2] ("Although the distinction between 'documents' and 'electronically stored information' is very real, it is generally assumed that a request for documents

desktop, and laptop data in response to requests for production.[154] However, because PED e-discovery is relatively unknown, most of these same attorneys may not think to look to their clients' PEDs, even if this is their obligation under Rule 34.[155] To avoid difficulties, and to provide a foundation for future motions to compel or for sanctions, it is a good idea to specifically include a request for PED data even if it is not known whether or what kinds of PEDs are being used by the target of the request.[156]

Rule 34 mandates that ESI be produced either in a "medium from which information can be obtained . . . directly" or "after translation by the responding party into a reasonably usable form."[157] Some PED ESI can be relatively easily viewed after being copied from the device, and this information presents no production challenge whatsoever.[158] Other types of PEDs, most notably those with a cellular phone component, require special expertise to access their stored data.

B. Suggested Solutions to Producing PED Data

In order for e-discovery to go smoothly, especially when PED data is at issue, it is imperative that parties specify the form of production that will be satisfactory during the Rule 26(f) parties planning conference and that agreements reached during this conference be documented in the Rule 16 case-management order.[159] In this Part, I have outlined some forms of production that can be requested or proposed.

1. Forensic PED Expert

The best, but most expensive, method is to engage a forensic expert or firm specializing in PEDs to extract and produce requested data in a cus-

---

includes a request for electronically stored information. In recognition of this reality, a request for documents must be considered to include a request for electronically stored information, unless the discovery request clearly distinguishes between the two.") (citing FED. R. CIV. P. 34(b)).

154. *See id. See also The Rules of Digital Evidence and AccessData Technology*, ACCESSDATA, http://www.accessdata.com/downloads/media/Rules_of_Digital_Evidence_and_AccessData_Technology.pdf (last visited Oct. 8, 2009).

155. *See* RABIEJ, *supra* note 32, at § 37A.11[2] ("[T]he responding party must produce electronically stored information, if otherwise discoverable, even though the discovery request asks only for 'documents.'") (citing FED. R. CIV. P. 34 advisory committee's note, 2006 amends., subdiv. (b)).

156. *See, e.g.,* NELSON, OLSON & SIMEK, *supra* note 2, at 78–79; *Sample Preservation Letter to Client*, in E-DISCOVERY SAMPLE FORMS AND PLEADINGS, KROLL ONTRACK, http://www.abanet.org/la bor/annualconference/2007/materials/data/papers/v2/046.pdf (last visited Oct. 8, 2009).

157. FED. R. CIV. P. 34(a)(1)(A).

158. This includes cases where the ESI to be produced is stored on the PED as a standard file type such as MP3 music files, JPG images, or text documents. Such standard file types are relatively easy to produce and review because they are readable by all modern computers.

159. *See* RABIEJ, *supra* note 32, at § 37A.40 (citing FED. R. CIV. P. 16(b)(3)(B)(iii) and FED. R. CIV. P. 26(f)(3)).

tomary form. The advantage of retaining such an expert is that production should be relatively worry-free. Usually the data can be produced in a number of different forms, and the data can be reviewed by the attorney or the expert for privileged information prior to being produced. The disadvantages are the same as noted above under the discussion of forensic preservation of PED data, namely: high cost, scarcity of qualified experts, and uncertainty regarding the quality of results.[160]

2. Manual Acquisition

If the scope of the requested information is sufficiently narrow, or if the number of relevant PEDs and the amount of data on each PED is relatively small, the simplest, most economical solution may be systematic photography of each screen of displayed data.[161] A lawyer or a designee may simply take the device, display relevant data on the device's screen as it would normally be seen by a user, and photograph the device. This method is analogous to photocopying paper documents and has several advantages. For one, no special technical expertise is required, resulting in substantial savings in time and money. Another advantage is that such a production method necessarily incorporates a review of the ESI being disclosed. The form of the production in the form of photographs is also guaranteed to be readable by the opposition, unlike production of some PED data in its native format.

There are also several disadvantages to this method. The landmark case of *National Union Electric Corp. v. Matsushita Electric Indus. Co.*[162] sets a standard that ESI should be produced in electronic form (and not printed form) unless the amount of data to be produced is very small and presents minimal challenges to a reviewer seeing it in paper form.[163] Of course, such a slow and ham-fisted e-discovery technique would not be feasible unless the amount of data to be produced was manageably small.[164] There is also the possibility that photographed data could be con-

160. *See supra* Part III.D. for a discussion of forensic preservation of PED ESI.

161. *See, e.g.*, Rothstein, Hedges & Wiggins, *supra* note 36, at 13 ("ESI may be produced as a TIFF or PDF file, which is essentially a photograph of an electronic document.").

162. 494 F. Supp. 1257 (E.D. Pa. 1980).

163. *Id.* at 1262 (holding that a hard copy printout of approximately 1,000 pages of computer data would only be in "reasonably usable form" as required by Rule 34(a)(1)(A) if it was produced in electronic form so that it could be searched for pertinent information).

164. Some courts engage in a balancing test in which the need of the requestor to have ESI in electronic form is balanced with the expense and inconvenience to the producing party. *See* RABIEJ, *supra* note 32, at § 37A.41[2]:

> The decisions turned on a wide range of factors, including, for example, the burden in maintaining confidentiality of documents, the relative resources of the parties, and the importance of the requested information. However, the primary factors continue to be the requesting party's need for the information and the burden imposed on the responding party

verted to text using optical character recognition (OCR) software, and the resulting text could then be indexed for searching in order to overcome any *Matsushita* issues.[165]

Another disadvantage of using the device's interface to display data is that this process necessarily alters the device's memory somewhat and puts stored data in some jeopardy of alteration or deletion. Consequently, this method is rather marginal in terms of its forensic soundness, especially if undertaken by a non-expert. If it seems likely that the opposition will want to challenge the source, completeness, or validity of data produced in the form of display-screen photographs, this method should not be used. Ideally, parties should only use this method after agreeing during the planning conference that its relative ease and low cost, when compared to more rigorous forensic procedures, outweigh potential evidentiary drawbacks.

Another disadvantage is that this method only captures the portion of data viewable from the display of the device. This method does not capture metadata unless the interface of the device allows metadata to be displayed and photographed. The producing party must consider carefully whether producing metadata is required or beneficial, since the extra photography and organization involved in documenting the metadata associated with PED files can substantially increase the amount of time involved in documenting this additional information.[166] The requesting party should be certain to specify that metadata is to be photographed if it can be displayed. If metadata cannot be displayed and photographed, but a requesting party believes it will be necessary, another form of production should be requested that includes the necessary metadata.

Closely connected with the metadata issue is the issue of "hidden" system data normally inaccessible to the device's user. If there is a way to acquire this system data, and it is necessary or requested by the other side, another method may be needed to acquire this data since photographing it from the device's user interface will not be possible.[167] Using the device

---

> to produce electronic information, including the difficulties in protecting privileged material.

Id.

165. *See* OCR and Indexing, http://www.ediscoveryevangelist.com/2009/03/ocr-and-indexing.html (Mar. 4, 2009, 09:23 EST). A number of software packages exist that provide OCR (optical character recognition) scans of photographs. *See, e.g.*, *ImageMaker Discovery Assistant Project Specification*, ImageMAKER Discovery Assistant, http://www.discoveryassistant.com/Nav_Top/TechNotes.asp ("[A] software product designed to process email, electronic documents and image files to produce TIFF/PDF, metadata, and extracted text.") (last visited Oct. 8, 2009).

166. *See* ROTHSTEIN, HEDGES & WIGGINS, *supra* note 36, at 13. *See also* Williams v. Sprint/United Mgmt. Co., 230 F.R.D. 640, 657 (D. Kan. 2005) (holding that defendant was obligated to produce spreadsheets with metadata intact).

167. Forensic data acquisition is always best unless there is no doubt it is not necessary. *See, e.g.*, Gates Rubber Co. v. Bando Chem. Indus., 167 F.R.D. 90 (D. Colo. 1996):

> Wedig pointed out that Voorhees should have done an "image backup" of the hard drive, which would have collected every piece of information on the hard drive, whether the information was allocated as a file or not. Instead, Voorhees did a "file by file" backup,

interface also changes the data stored on the device in subtle ways.[168] This may or may not be a concern, depending on the nature of the case and the ESI requested, but this method should not be used if a strict forensically acquired copy of all device data is necessary. If metadata or hidden system data is a concern, or if there is any doubt as to whether digital photographs would be an acceptable method of production for PED data, these issues should be met head-on in the parties planning conference in order to avoid future discovery disputes and possible sanctions.[169]

Due to these numerous drawbacks, the manual acquisition method should only be used in low-value cases where the PED ESI is not expected to be of central importance to the case.

3. Direct Review

Another easy, though perhaps less desirable, option is to have the opposing counsel or their expert review a client's PED directly. The glaring disadvantage of this method is that the other side has full, unfiltered access to all of the client's data, including privileged and sensitive information.[170] Fortunately, or unfortunately, depending on which side you are on, this is probably the default position of Rule 34. Rule 34 mandates the responding party to produce ESI "stored in any medium from which information can be obtained either directly or, if necessary, after translation by the responding party into a reasonably usable form . . . ."[171] A "medium from which information can be obtained . . . directly" would be the PED itself, and the plain language of the rule seems to suggest that there must be underlying necessity before the respondent could produce the data in an alternative "reasonably usable form."[172]

> which copies only existing, nondeleted files on the hard drive. The technology for an image backup was available at the time of these events, though rarely used by anyone. Wedig testified that Gates was collecting evidence for judicial purposes; therefore, Gates had a duty to utilize the method which would yield the most complete and accurate results. I agree with Wedig. In these circumstances, Gates failed to preserve evidence in the most appropriate manner. Gates' failure to obtain an image backup of the computer is a factor which I have weighed against Gates as I considered a number of the claims which Gates has asserted.

Id. at 112.

168. *See generally* BEST PRACTICES FOR SEIZING ELECTRONIC EVIDENCE: A POCKET GUIDE FOR FIRST RESPONDERS, U.S. DEPARTMENT OF HOMELAND SECURITY; UNITED STATES SECRET SERVICE (3d ed. 2007) *available at* http://www.forwardedge2.com/pdf/bestpractices.pdf.

169. *See* ROTHSTEIN, HEDGES & WIGGINS, *supra* note 36, at 13. *See also Williams*, 230 F.R.D. at 657 (holding that defendant was obligated to produce spreadsheets with metadata intact).

170. *See, e.g.*, Smith v. Café Asia, 246 F.R.D. 19, 22 (D.D.C. 2007) (defendant moved to compel production of images on the plaintiff's cellular phone that the plaintiff insisted were private and irrelevant).

171. FED. R. CIV. P. 34(a)(1)(A).

172. *Id.*

This reading of Rule 34 puts two substantial burdens on the responding party wishing to avoid direct review of their client's PED. First, there is a legal burden to justify that an alternative form of production is necessary. Second, there is the technical burden of actually producing all responsive ESI in a "reasonably usable form." Usually, these issues can be negotiated around by agreement between the parties.[173] If the litigation is particularly contentious, however, or if the device contains extremely sensitive information, a neutral third party (special master or taint reviewer) should be requested to perform at least the initial examination of the device.[174]

V. SUGGESTIONS FOR INNOVATION

Manufacturers, developers, and industry leaders must embrace standardization. Without an appropriate set of standards, any technological landscape becomes a patchwork of non-interchangeable parts. While this gives rise to numerous and lucrative niche specialties for those with appropriate knowledge, divergent technologies create chaos and confusion in the marketplace until standardization eventually takes root by consensus or by popular demand.[175] Already, a number of PEDs are taking advantage of standardized data storage. Most modern PEDs on the market today have SD, miniSD, or microSD slots from which data can easily be preserved and produced.[176] Most current PEDs also have standardized interconnectivity using a USB cable or Bluetooth.[177] Finally, the way in which devices communicate with the larger telecom infrastructure has always been limited to a few basic technologies, and this fact is unlikely to change for the simple reason that building out infrastructure according to a different standard is extremely expensive.[178] Global System for Mobile communications (GSM) devices, for example, use standardized SIM cards to store data needed to connect to the network.[179]

173. One such way around these issues is by negotiating a "claw-back" agreement. *See* Zubulake v. UBS Warburg LLC, 216 F.R.D. 280, 290 (S.D.N.Y. 2003) (*Zubulake III*).

174. *See generally* New Niche for e-Discovery: Special Masters, http://estrinlegaled.typepad.com/my_weblog/2008/02/new-niche-for-e.html (Feb. 11, 2008, 17:10 EST). See MIDDLETON, *supra* note 24, at 198, for a discussion of use of special master or taint team in criminal cases.

175. Rest In Peace (or geeky obscurity) Betamax, HD-DVD, and the myriad non-TCP/IP networking standards.

176. JANSEN & AYERS, *supra* note 133, at 8–9.

177. *Id.* at 15.

178. The predominant PED network types in the United States are CDMA, used primarily by Verizon and Sprint, and GSM, used by AT&T, T-Mobile, and others. *Id.* at 6–7.

179. Two e-discovery benefits arise from this standardization. First, when dealing with a GSM phone, one always knows to expect to request or produce SIM card data. Second, a long period of standardization has allowed experts and forensic software developers to create methods for preserving and producing SIM card data. *Id.* at 17–18.

The trend toward standardization will likely continue with regard to hardware and connectivity in order to allow PEDs to more easily connect with other technologies. However, there is no guarantee that the internal software of PEDs will converge toward any set of standards without significant industry cooperation or consumer compulsion. The traditional computing world saw a dizzying array of different computer architectures and operating systems in the late 1970s and early 1980s before the industry finally pared itself down to a few basic hardware and software paradigms.[180] When the dust cleared, there was the Mac paradigm and the PC paradigm, with various UNIX flavors filling the niches left over, though this process took nearly three decades to play out.[181] A similar turn of events would probably greatly benefit the PED market with the side effect of simplifying e-discovery involving these devices.

Cellular phone platforms, in particular, desperately need standardization. The current state of the art has every manufacturer making its own proprietary set of hardware as well as software to run on that hardware.[182] Furthermore, the pace of developing technology is relatively rapid, meaning that forensic experts and developers of forensic software are constantly challenged to keep up to date.[183] The standardization must percolate from the basic hardware and chipsets used by the phones up through the operating system software that runs on the phone. Only when hardware and software platforms are relatively standardized can programmers and forensic experts create reliable tools and methods for preserving data, and only then will the costs for e-discovery services come down to a reasonable level.[184]

Erik Harris

180. *See generally* Ayman Moumina, History of Operating Systems (May 3, 2001) (unpublished graduate student research paper, Computing History Museum), *available at* http://www.computinghistory museum.org/teaching/papers/research/history_of_operating_system_Moumina.pdf.

181. While some may object to standardization as anticompetitive, witness the relative commercial stagnation of the industry before and the flourishing of the computer industry after some standardization began to emerge. When minor players do not need to re-invent or re-define the standard, they are free to focus on the innovation that gives them a real competitive edge.

182. *See* JANSEN & AYERS, *supra* note 133, at 13.

183. *Id.* at 22.

184. *Id.* at 13 ("Short product release cycles are the norm for cellular phones, requiring tool manufacturers to update their tools continually to keep coverage current. The task is formidable and tool manufacturers' support for newer models often lags significantly. Some have argued that the current state is likely to continue, keeping the cost of examination significantly higher than if a few standard operating systems prevailed . . . .").