

# Northwestern Journal of Technology and Intellectual Property

---

Volume 9

Issue 1 *October*

Article 1

---

Fall 2010

## Legally Correct But Technologically Off the Mark

Daniel B. Garrie

Bill Spernow

---

### Recommended Citation

Daniel B. Garrie and Bill Spernow, *Legally Correct But Technologically Off the Mark*, 9 Nw. J. TECH. & INTELL. PROP. 1 (2010).  
<https://scholarlycommons.law.northwestern.edu/njtip/vol9/iss1/1>

This Perspective is brought to you for free and open access by Northwestern Pritzker School of Law Scholarly Commons. It has been accepted for inclusion in Northwestern Journal of Technology and Intellectual Property by an authorized editor of Northwestern Pritzker School of Law Scholarly Commons.

N O R T H W E S T E R N  
JOURNAL OF TECHNOLOGY  
AND  
INTELLECTUAL PROPERTY

**Legally Correct But  
Technologically Off the Mark**

*Daniel B. Garrie & Bill Spernow*



# Legally Correct But Technologically Off the Mark

By Daniel B. Garrie\* & Bill Spernow\*\*

## I. INTRODUCTION

¶1 Today's judges face numerous challenges in determining the truth of the matter at hand, but none is more challenging than ruling on issues that pivot on digital evidence.<sup>1</sup> Gone are the days when the most technically challenging decision was determining if evidence on a floppy disk<sup>2</sup> had been destroyed because a litigant exposed it to a strong magnetic field.<sup>3</sup> Today's legal challenges are extremely technical when it comes to determining the integrity of digital evidence and assigning responsibility for direct or indirect acts of spoliation.<sup>4</sup> While judges are entirely capable of arriving at the correct decision when it comes to ruling on the value of digital evidence,<sup>5</sup> they are at the mercy of the "experts" involved when it comes to issues of spoliation.<sup>6</sup>

---

\* Mr. Daniel Garrie, Esq., B.A. & M.A. Computer Science is a lawyer and technologist, and is recognized as one of the eminent thought leaders specializing in electronic discovery. Mr. Garrie is a managing partner at Focused Solution Recourse Delivery Group LLC (FSRDG), a national legal risk management consulting firm, and serves as an e-Discovery arbitrator and special master all over the United States. He has also held technology positions in both the private and public sector. He can be reached at dgarrie@fsrdg.com.

\*\* Mr. Bill Spernow, MBA, CISSP, CEH, PMP, Net+, Sec+, CHS III, GAPPI/GCP combined a career as a computer engineer and California Police Officer and quickly obtained a national reputation as one of the first Cyber Cops. He has held IT Security positions in both the public and private sectors and currently provides litigation and forensic support services in the Atlanta area.

Special thank you to Mr. Elan Raffel. Mr. Raffel is entering his second year at Cardozo Law School of Yeshiva University in New York and is interested in practicing corporate law when he graduates.

<sup>1</sup> Eckhardt v. Bank of Am. Corp., No. 3:06CV512-H, 2008 WL 1995310, at \*6 (W.D.N.C. May 6, 2008) (finding that the defendant did not act in bad faith but commenting on the challenges raised by "the changing face of discovery in an electronic world").

<sup>2</sup> A floppy disk is a "[s]mall removable disk[], also known as [a] diskette[], that come[s] in two sizes, 3.5" and 5.25". The amount of data that can be stored on a diskette depends on the size, and can be 360 kilobytes to 1.4 megabytes." TOM O'CONNOR, LEGAL ELECTRONIC DOCUMENT INSTITUTE, BASIC PRINCIPLES OF AUTOMATED LITIGATION SUPPORT 51 (2005), available at <http://www.legal-edocs.org/Basic%20Principles%20of%20Automated%20LitigationSupport%20Primer.pdf>.

<sup>3</sup> Nathan Wiebe, *Regarding Digital Images: Determining Courtroom Admissibility Standards*, 28 MAN. L.J. 61, 63 (2002).

<sup>4</sup> Spoliation can be defined as "the destruction or alteration of evidence during on-going litigation or during an investigation or when either might occur sometime in the future. Failure to preserve data that may become evidence is also spoliation." *Spoliation—Working EDRM*, EDRM: ELECTRONIC DISCOVERY REFERENCE MODEL, [http://edrm.net/wiki2/index.php/Spoliation#ref\\_fenwickglossary](http://edrm.net/wiki2/index.php/Spoliation#ref_fenwickglossary) (last visited Sept. 6, 2010).

<sup>5</sup> "According to Black's law dictionary, evidence is 'any species of proof, or probative matter, legally presented at the trial of an issue, by the act of the parties and through the medium of witnesses, records, documents, exhibits, concrete objects, etc. for the purpose of inducing belief in the minds of the court or jury as to their contention.' Electronic information (like paper) generally is admissible into evidence in a legal proceeding." *eDiscovery Glossary*, RENEWDATA, <http://www.renewdata.com/ediscovery-glossary.php#e> (last visited Sept. 6, 2010) (defining electronic evidence). Digital evidence can be defined

¶2 In an expanding trend, judges are basing important decisions on inaccurate or incomplete technical details concerning digital evidence.<sup>7</sup> As a result, for cases where digital evidence plays a pivotal role, either dangerously erroneous precedent will be established based upon legally sound but technically flawed logic, or successful appeals will increase dramatically as the technical weaknesses of the decision are subsequently exposed. This thesis—that technological ignorance leads to legal error—is the primary focus behind this article.

¶3 We have identified a group of recent cases where digital evidence played a significant role in the judicial decisions. From this group a single case was selected to serve as a “test case” for our thesis. The remainder of this article will discuss the decisions reached in this “test case,” and demonstrate how a limited understanding of low-level computer functions,<sup>8</sup> especially at the level where files are created and deleted, contributed to legal decisions by the court that were fundamentally incorrect.

¶4 At this point a disclaimer is in order. To present our argument, we need to discuss technical issues related to computer storage techniques<sup>9</sup> and file structures.<sup>10</sup> Clearly the restricted length of this article prevents a detailed discussion. Where possible, analogies will be used to compensate. In other cases we ask that you to take our word that the opinions presented are expert ones formed after decades of experience with cases involving digital evidence. Our goal is not to overwhelm you with technical-level geek talk, rather to help you to come away from the article with a deeper, but common sense appreciation for the impact a limited understanding of computer technology can have on even the most basic of judicial decisions.

¶5 The case we selected to highlight is *TR Investors, LLC v. Genger*.<sup>11</sup> In *Genger* a determination of spoliation was made by the Delaware Court of Chancery, and Vice Chancellor Strine sanctioned defendant Arie Genger for his actions.<sup>12</sup> The sanctions were issued due to the defendant’s involvement in overwriting the content of deleted files in the “unallocated space” of computers under his control.<sup>13</sup> The first part of the article will

---

as “[a]ny computer-generated data that is relevant to a case. Included are email, text documents, spreadsheets, images, database files, deleted email and files and back-ups. The data may be on desktops, laptops, servers, hard drive, backup tape, CD or DVD.” *TransPerfect Legal FAQs*, TRANSPERFECT LEGAL SOLUTIONS, [http://www.transperfect.com/TLS/resources/resources\\_faq.html](http://www.transperfect.com/TLS/resources/resources_faq.html) (last visited Sept. 6, 2010) (defining Electronic Stored Information (ESI)).

<sup>6</sup> Mark D. Robins, *Computers And The Discovery of Evidence—A New Dimension To Civil Procedure*. 174 J. MARSHALL J. COMPUTER & INFO. L. 411, 509–10 (1999).

<sup>7</sup> Eric Van Buskirk, *Digital Evidence: Challenging the Presumption of Reliability*. J. DIGITAL FORENSIC PRAC., 19, 22–23 (2006).

<sup>8</sup> In programming, a computer function can be defined as a self-contained software routine that performs a task. Functions can do large amounts of processing as well as small tasks.

<sup>9</sup> Computer storage refers to the act of placing information on a disk where it available for later use. O’CONNOR, *supra* note 2.

<sup>10</sup> “The file structure of a program refers to the way information on a disk or tape is organized. Programs often need to read data from files and write information to files in order to keep permanent records. How these files are organized and used is an important part of the design of a program.” Randall Davis, *The Nature Of Software And Its Consequences For Establishing And Evaluating*, 5 SOFTWARE L.J. 299, 320 (1992).

<sup>11</sup> *TR Investors, LLC v. Genger*, No. 3994-VCS, 2009 WL 4696062 (Del. Ch. Dec. 9, 2009).

<sup>12</sup> *Id.* at \*17–19.

<sup>13</sup> *Id.* at \*7 n.21 (citing *Ohana Aff.* at ¶ 13, *Genger*, 2009 WL 4696062; *Genger Aff.* at ¶¶ 12–14, *Genger*, 2009 WL 4696062; *Tr.* at 257:4–258:2, *Genger*, 2009 WL 4696062).

focus on the decision itself. We will then discuss why, in our considered opinion, the court's decision was incorrect.

## II. *TR INVESTORS, LLC v. GENGER*

¶6 The storage systems of most computers have two primary areas where files<sup>14</sup> reside. Those two areas are “existing file space” where valid files can be found, and deleted-free space,<sup>15</sup> or more globally “unallocated space,”<sup>16</sup> which for purposes of analogy can be considered as a garbage dump where unwanted and discarded information goes to await recycling. This “garbage dump” space exists on every hard drive<sup>17</sup> and server,<sup>18</sup> and is what forensic experts typically examine when recovering deleted files that have been emptied from the recycle bin.<sup>19</sup>

¶7 In the *Genger* case, the court determined that a consultant employed by the defendant had used a wiping utility<sup>20</sup> to overwrite the unallocated space of a desktop computer with the intention of preventing the plaintiff from recovering deleted files relevant to the case. The court reached this conclusion after it was informed by the plaintiff's computer experts that electronic versions of documents known to be in the defendant's possession could not be located as either valid<sup>21</sup> or deleted files on the

---

<sup>14</sup> A “file” can be defined as “[a] collection of data or information that has a name, called the filename. Almost all information stored in a computer must be in a file. There are many different types of files: data files, text files, program files, directory files, and so on.” *E-Discovery Knowledge Center: Search the Glossary*, FIOS, INC., <http://www.fiosinc.com/e-discovery-knowledge-center/electronic-discovery-glossary.aspx?cid=DG> (last visited Sept. 15, 2010).

<sup>15</sup> “Deleted Data” is “[d]ata that once existed on a computer and has subsequently been deleted by the user. Deleted data actually remains on the computer until it is overwritten by new data or ‘wiped’ with a specific software program.” LEGAL ELECTRONIC DOCUMENT INSTITUTE, BASIC PRINCIPLES OF AUTOMATED LITIGATION SUPPORT 74 (2005) available at <http://www.legal-edocs.org/Basic%20Principles%20of%20Automated%20LitigationSupport%20Primer.pdf>.

<sup>16</sup> “Unallocated space” is “space on a hard drive that potentially contains intact files, remnants of files, subdirectories, or temporary files which were created and then deleted by either a computer application, the operating system or the operator.” *eDiscovery Glossary*, RENEWDATA, <http://www.renewdata.com/ediscovery-glossary.php#e> (last visited Sept. 8, 2010).

<sup>17</sup> The “hard drive” is “the primary computer storage medium in desktop and laptop computers.” *Hard Drive—EDRM*, EDRM: ELECTRONIC DISCOVERY REFERENCE MODEL, [http://www.edrm.net/wiki/index.php/Hard\\_drive](http://www.edrm.net/wiki/index.php/Hard_drive) (last visited Sept. 8, 2010).

<sup>18</sup> A “server” is “[a]ny computer on a network that contains data or applications shared by users of the network on their client PCs.” *Glossary of Terms*, KROLL ONTRACK 9 (Oct. 1, 2008), [http://www.krollontrack.com/library/glossary\\_krollontrack2008.pdf](http://www.krollontrack.com/library/glossary_krollontrack2008.pdf) (last visited Sept. 24, 2010).

<sup>19</sup> The “recycle bin” on a computer is the location on the hard drive where deleted folders or files are temporarily stored. The recycle bin keeps the files intact in case the user wants to restore them, but can be completely erased from the computer by the user.

<sup>20</sup> Wipe is the “term for deliberately overwriting a piece of media and removing any tract of files or file fragments.” *Wipe—EDRM*, EDRM: ELECTRONIC DISCOVERY REFERENCE MODEL, <http://www.edrm.net/wiki/index.php/Wipe> (last visited Sept. 8, 2010).

<sup>21</sup> “Active data is information residing on the direct access storage media of computer systems, which is readily visible to the operating system and/or application software with which it was created and immediately accessible to users without undeletion, modification or reconstruction (i.e., word processing and spreadsheet files, programs and files used by the computer's operating system).” *Glossary of Terms*, KROLL ONTRACK 1 (Oct. 1, 2008), [http://www.krollontrack.com/library/glossary\\_krollontrack2008.pdf](http://www.krollontrack.com/library/glossary_krollontrack2008.pdf) (last visited Sept. 24, 2010).

defendant's computer systems.<sup>22</sup> The inability to forensically locate these documents in digital form resulted in sanctions against the defendant Genger.<sup>23</sup>

¶8 Our review of the actions taken by all involved, per the court record, establishes that the court, through no fault of its own, reached the wrong conclusions on several levels. Had the court been properly informed of the following technical facts, it is highly likely that it would have reached a more informed decision in favor of the defendant. *Genger* involved the battle for control of an investment company known as TRI.<sup>24</sup> The dispute was between the Trump Group, the new owners, and Arie Genger, the original owner.<sup>25</sup> As is standard in such cases, the court entered a "status quo order," enjoining both parties from "tampering with, destroying, or in any way disposing of any [c]ompany-related documents, books, or records."<sup>26</sup>

¶9 The problem was that the court acknowledged Mr. Genger as an "international man of mystery,"<sup>27</sup> who had used TRI's computer system not just to conduct TRI business,<sup>28</sup> but to create and receive documents implicating Israel's national security and as a storage device for his own personal financial and legal documents.<sup>29</sup> To protect the sensitive documents, TRI retained a law firm that in turn engaged a forensic consulting firm to untangle this Gordian knot.<sup>30</sup>

¶10 Over the course of a weekend, the court permitted the defendant's attorneys and consultants to open documents and e-mails on the TRI computers and encrypt those files containing personal and Israeli government information.<sup>31</sup> The consulting firm created file level snapshots of the "existing files" on the potentially responsive hard drives.<sup>32</sup> However, as is common in e-discovery cases, the consultants never created a forensic image<sup>33</sup> of the entire hard drive, which would have included all of the unallocated space allowing it to be preserved for additional forensic analysis. After the consultants took a "snapshot" of the existing valid files, the computers and hard drives were reviewed by the law firm in accordance to the process agreed to by the parties.<sup>34</sup> Where Genger's personal items were discovered on these systems, the court permitted these items to be individually encrypted.<sup>35</sup> Once an encrypted version of the file was created the original was deleted using the standard delete function of the Windows operating system. The court acknowledged that during this encryption process, non-encrypted, temporary copies

---

<sup>22</sup> TR Investors, LLC v. Genger, No. 3994-VCS, 2009 WL 4696062, at \*6-7 (Del. Ch. Dec. 9, 2009).

<sup>23</sup> *Id.* at \*15-20.

<sup>24</sup> *Id.* at \*1-15.

<sup>25</sup> *Id.* at \*1.

<sup>26</sup> *Id.* at \*1 n.1 (citing Status Quo Order, *Genger*, 2009 WL 4696062).

<sup>27</sup> *Id.* at \*5.

<sup>28</sup> *Id.* at \*15-20.

<sup>29</sup> *Id.*

<sup>30</sup> *Id.* at \*11.

<sup>31</sup> *Id.*

<sup>32</sup> *Id.* at \*12.

<sup>33</sup> A Forensic Image or Copy is a "precise bit-by-bit copy of a computer system's hard drive, including slack and unallocated space." O'CONNOR, *supra* note 2.

<sup>34</sup> *Genger*, 2009 WL 4696062, at \*5-6.

<sup>35</sup> Encryption can be defined as the "[a] procedure that renders the contents of a message or file scrambled or unintelligible to anyone not authorized to read it." *Glossary of Terms*, AMERICAN DOCUMENT MANAGEMENT, <http://www.amdoc.com/section/Glossary/18/interior.php#E> (last visited Sept. 8, 2010).

of Genger’s documents were created in the unallocated space of the hard drive.<sup>36</sup> Those temporary copies, if recovered later from the unallocated space, would have defeated the point of the encryption process.

¶11 Apparently motivated by this concern, Genger and his technical advisor later ran a wiping software program on the unallocated space after the file level review had been completed, destroying (by overwriting) all previous data contained in the unallocated space, before turning over the computers and hard drives to the Trump Group.<sup>37</sup>

¶12 Although Genger did create a file level copy of the computer systems in order to have a snapshot of every valid file on the system, the court found Genger’s actions of wiping the unallocated space to be a deliberate attempt at spoliation.<sup>38</sup> As a result, the court imposed a series of heavy sanctions upon Genger, fining him and shifting the burden of proof to him.<sup>39</sup> The court’s logic in imposing sanctions was based on a fundamental misunderstanding of the nature of unallocated computer space and the data that resides within that space. Moreover, in imposing sanctions upon Genger, Vice Chancellor Strine has expanded preservation orders in the Delaware courts to include unallocated space in all computers and servers involved in litigation—an unintended result that is unworkable, unreasonable, and prohibitively expensive.<sup>40</sup>

### III. WHY THE COURT’S DECISION TO IMPOSE SANCTIONS WAS WRONG

¶13 The court’s logic in imposing sanctions was faulty on a number of technical levels. While the defendant wiped the unallocated space of these hard drives, it was only after first taking and saving externally a file-level snapshot of the “existing files” on the hard drives in question.<sup>41</sup> After any sensitive documents that contained national security or personal information were encrypted the protocol required that the original hard drives be turned over to the plaintiff. It was this “turn-over” protocol requirement that triggered the wiping of unallocated space. The wiping was necessary to delete unencrypted copies of the sensitive documents automatically generated as part of the encryption process.<sup>42</sup> It should be noted that after the encryption process was completed, thousands of sensitive files (that were not encrypted) which had been deleted now resided in the unallocated space. The later use of forensic analysis tools by the plaintiff would have allowed for the recovery of a significant percentage of these sensitive files in their original state. The court was wrong to find spoliation and impose sanctions for a number of reasons. Our first example is significant: the court did not properly determine if the wiping software had destroyed relevant documents.<sup>43</sup> In its opinion, the court references a memorandum,

---

<sup>36</sup> *Genger*, 2009 WL 4696062, at \*5 n.13 (citing *Leicht Aff.* at ¶¶ 1–4, *Genger*, 2009 WL 4696062; Tr. at 251:6–252:11, *Genger*, 2009 WL 4696062).

<sup>37</sup> *Id.* at \*7.

<sup>38</sup> *Id.* at \*17.

<sup>39</sup> *Id.* at \*19.

<sup>40</sup> Thomas Y. Allman, *Managing Preservation Obligations After the 2006 Federal E-Discovery Amendments*, 13 RICH. J.L. & TECH. 9 (2007), available at <http://jolt.richmond.edu/v13i3/article9.pdf>.

<sup>41</sup> *Genger*, 2009 WL 4696062, at \*6.

<sup>42</sup> See *John B. v. Goetz*, 531 F.3d 448, 460–61 (6th Cir. 2008) (holding that district court orders calling for forensic imaging of media primarily for the purpose of preservation was an abuse of discretion, citing the fact that the record lacked any evidence that defendants have intentionally destroyed relevant ESI and noting the significant privacy and confidentiality concerns raised by the order).

<sup>43</sup> *Phillips v. Potter*, No. 7-815, 2009 WL 1362049, at \*6 (W.D. Pa. May 14, 2009) (finding there was no

the “Lentz Memo,” as one of the missing documents that could have been recovered from unallocated space as a deleted file—assuming the unallocated space had not been wiped by the defendant.<sup>44</sup> The court’s determination, however, was based solely on cause and effect (it should be here, it’s not, hence it must have been wiped), not independently verifiable forensic evidence.<sup>45</sup> In addition, other technological reasons related to the normal day-to-day operation of any Windows-based computer system would also explain why the missing files could not be found in the unallocated space.

¶14

What the court perhaps did not fully understand is that every action, including just turning on the computer in the morning, creates, deletes, and modifies hundreds of files and overwrites data in the unallocated space.<sup>46</sup> Given the nature of the encryption process expressly permitted by the court, it is more than likely that all, or almost all, of the data assumed to be available for recovery by the court in the unallocated space had already been overwritten.<sup>47</sup> This is because, as the court recognized, the encryption process creates at least one or more temporary files, a final “encrypted” file, and the need to delete the original file. All of this activity consumes resources in the unallocated space area of the hard drive.<sup>48</sup> Given the large number of documents reviewed over the course

---

evidence of destruction of relevant documents and refusing to order sanctions based upon “mere speculation” that relevant documents were destroyed, also noting that there was no indication of any bad intent on the part of the defendant); *Wong v. Thomas*, No. 05-2588 (AET), 2008 WL 4224923, at \*4 (D.N.J. Sept. 10, 2008) (denying motion for sanctions due to inability to establish relevance); *Pandora Jewelry, LLC v. Chamilia, LLC*, No. CCB-06-3041, 2008 WL 4533902, at \*9–10 (D. Md. Sept. 30, 2008) (refusing to impose sanctions based on lack of evidence of data’s relevancy); *School-Link Techs., Inc. v. Applied Res., Inc.*, No. 05-2088-JWL, 2007 WL 677647, at \*3–4 (D. Kan. Feb. 28, 2007) (refusing to order sanctions despite finding that the defendant breached its duty to preserve evidence as there was no showing that the breach caused relevant documents and information to be destroyed); *Lexis-Nexis v. Beer*, 41 F. Supp. 2d 950, 955 (D. Minn. 1999) (The court was not convinced that defendant could show that evidence pertinent to the litigation was actually destroyed. Additionally, even if information had been deleted—for example, when Defendant’s counsel overwrote inactive data while attempting to make a copy of the laptop hard drive—the court found that Lexis-Nexis had failed to demonstrate that the loss of this evidence would prejudice its case.); *Hildreth Mfg., LLC v. Semco, Inc.*, 785 N.E.2d 774, 780–81 (Ohio Ct. App. 2003) (holding that sanctions for deleting e-data were unwarranted when there was no reasonable possibility that data was relevant).

<sup>44</sup> *Genger*, 2009 WL 4696062, at \*11 n.34 (citing Mem. from David Lentz to Arie Genger, William Dowd, and Christopher Gengaro, *Genger*, 2009 WL 4696062 [hereinafter *Lentz Memo*]).

<sup>45</sup> See *Technical Sales Assocs., Inc. v. Ohio Star Forge Co.*, Nos. 07-11745, 08-13365, 2009 WL 728520, at \*2–3 (E.D. Mich. Mar. 19, 2009) (denying the defendant’s motion for contempt since the stipulated order protected the “discovery of *actual data*, not the absence of data”); see also *Se. Mech. Servs., Inc., v. Brody*, No. 8:08-CV-1151-T-30EAJ, 2009 WL 2242395, at \*3–4 (M.D. Fla. July 24, 2009) (denying the defendants’ motion to impose sanctions against the plaintiff despite finding of spoliation because plaintiff did not act in bad faith and the defendants failed to show that any “crucial evidence” existed on the destroyed backup tapes).

<sup>46</sup> *Mintel Int’l Group, Ltd. v. Neergheen*, No. 08-cv-3939, 2010 WL 145786, at \*8 (N.D. Ill. Jan. 12, 2010) (The court found that any programs on the laptop that would have destroyed metadata, such as antivirus software, were not user initiated. The court held that the defendant’s destruction of any evidence was unintentional, resulting from typical computer use—rather than a *pattern* that is easily recognized by forensic experts as spoliation. (Emphasis in original.)); see Christopher D. Wall & Michelle S. Lange, *Electronic Discovery: Recent Developments*, WASH. LAWYER (Mar. 2003), available at [http://www.dbar.org/for\\_lawyers/resources/publications/washington\\_lawyer/march\\_2003/electronic.cfm](http://www.dbar.org/for_lawyers/resources/publications/washington_lawyer/march_2003/electronic.cfm), (noting that “[s]imply booting a computer can possibly destroy valuable metadata (data about the data, such as *to*, *from*, *bcc*, and *date* fields in e-mail and the ‘last accessed’ or ‘last modified’ date in a document) that could be relevant in a lawsuit”) (citing *Antioch Co. v. Scrapbook Borders, Inc.*, 210 F.R.D. 645, 652–54 (D. Minn. 2002)).

<sup>47</sup> *Mintel*, 2010 WL 145786, at \*8; Wall & Lange, *supra* note 46.

<sup>48</sup> See Allman, *supra* note 40.



of days by a team of attorneys, any data in the unallocated space could have easily been overwritten by the encryption process itself, or the normal day-to-day operation of the computer.<sup>49</sup> Thus, the Vice Chancellor's order, by permitting the encryption of files stored on the systems in question, most likely resulted in overwriting substantial blocks of data that previously had existed in the unallocated space. If, as the court found, there was a smaller dedicated unallocated space for electronic mail and email attachments, then all email derived data in this smaller, segregated segment was almost certainly overwritten before the wiping software was utilized.<sup>50</sup> If the Lentz Memo, as an example, had been deleted from the unallocated space, it could have been innocently overwritten by the thousands of files created during the encryption process specifically allowed by the court.<sup>51</sup> So even if the defendant did not run the wiping software, the Lentz Memo may well have never been found due to the impact the normal day-to-day operations of the computer has on the unallocated space. Its absence does not demonstrate that the defendant intentionally wiped it.<sup>52</sup>

¶15 It is also unclear if the file-level copying process created a copy of the \$MFT file for each computer backed up. This is important because the \$MFT file, a Windows system file that is really a small database, contains technical details about all valid files and most deleted files.<sup>53</sup> Think of the \$MFT file as the table of contents for a hard drive that points you to the page of interest.<sup>54</sup> That this file was not examined to determine what details existed about previously deleted files was a significant technical oversight that ignored valuable potential evidence. This is critical because a review of the \$MFT could have likely resolved the courts concern regarding intentional spoliation by specifically identifying the names and sizes of the files that had been recently deleted.<sup>55</sup>

¶16 The court also did not appear to understand that a vast majority of data in unallocated space are random fragments.<sup>56</sup> The analogy here is expecting entire pristine documents in an area that consists mostly of confetti. This is probably why TRI's computer consultants never preserved the unallocated space before the encryption process was initiated. The initial judicial preservation order issued by the court prohibited the

---

<sup>49</sup> *Genger*, 2009 WL 4696062, at \*5 n.13 (citing *Leicht Aff.* at ¶¶ 1–4, *Genger*, 2009 WL 4696062; Tr. At 251:6–252:11, *Genger*, 2009 WL 4696062).

<sup>50</sup> *Maxpower Corp. v. Abraham*, 557 F. Supp. 2d 955, 962 (W.D. Wis. 2008) (denying plaintiff's motion for sanctions due to insufficient evidence showing that wiping of hard drive was deliberate spoliation even though the plaintiffs, computer forensics expert examined the defendants, laptops, finding evidence of hard drive wiping software and of text strings referring to information about outdated products).

<sup>51</sup> *Wall & Lange*, *supra* note 46.

<sup>52</sup> *United States v. Kimoto*, 588 F.3d 464, 489–90, 497 (7th Cir. 2009) (Defendant appealed his conviction, arguing that the government had destroyed or withheld exculpatory evidence and failed to provide forensic copies of hard drives, which resulted in a Brady violation. In affirming the conviction, the court determined there was no Brady violation. To support its ruling, the court noted that no destruction or spoliation on behalf of the government existed, there was a material lack of proof that certain alleged evidence was missing.); *Floeter v. City of Orlando*, No. 6:05-cv-400-Orl-22KRS, 2007 WL 486633, at \*7 (M.D. Fla. Feb. 9, 2007) (denying sanctions for lost hard drives and destroyed backup tapes); *MGE UPS Sys., Inc. v. Fakouri Elec. Eng., Inc.*, 422 F. Supp. 2d 724, 741–42 (N.D. Tex. Mar. 17, 2006).

<sup>53</sup> Orin S. Kerr, *Searches and Seizures in a Digital World*. 119 HARV. L. REV. 531, 539–40 (2005).

<sup>54</sup> *Id.*

<sup>55</sup> *Id.*

<sup>56</sup> See Robert Douglas Brownstone, *Collaborative Navigation of the Stormy e-Discovery Seas*, 10 RICH. J.L. & TECH. 53, ¶ 8 n.22 (2004), available at <http://law.richmond.edu/jolt/v10i5/article53.pdf>.

destruction of any company related documents, books, or records.<sup>57</sup> It is not clear how Vice Chancellor Strine bridged the technology world from that routine mandate to the finding that deleted files, that per normal descriptive terms are already destroyed and are *unrecoverable within the Windows Operating System*, fall within those parameters. A routine e-Discovery process paying no attention to deleted files was transformed, to the defendant's disadvantage, into an e-Forensic investigation about deleted files.

¶17 It is unreasonable for courts to expect litigants to preserve the unallocated space of their computers, or understand they are required to preserve unallocated space, as the result of a routine preservation order.<sup>58</sup> To expand preservation orders to include unallocated space in computers and servers on pain of sanction, as Vice Chancellor Strine now has done in the Delaware courts, is unworkable and unreasonable.<sup>59</sup> To preserve this storage space, a company would effectively have to shut down all their computers and servers prior to imaging—grinding the business to a halt.<sup>60</sup> Even then, it is not always possible to recover deleted files from unallocated space, as opposed to random bits and pieces of the whole.

¶18 Moreover, because of the random nature of the unallocated space, it is impossible to know with certainty where the previously deleted information sought is located.<sup>61</sup> It is a simple matter to segregate active files by custodian. If employee John Smith has information regarding the litigation, you segregate his active files and search them for useful information. With fragments of files, as typically found in unallocated space, no such segregation is possible. The analogy here is searching for a needle in a field of haystacks. The cost will always outweigh the benefits, if any, of such a search.<sup>62</sup> For a company that has a number of servers, even the cost of imaging and maintaining the unallocated space, as will be required if unallocated space is now part of every “status quo” preservation order and litigation hold, may be prohibitively expensive.<sup>63</sup>

¶19 Finally, the court was correct to note that the timing of the wiping activity by TRI's consultant, at night after everyone was done for the day, might provide reason for suspicion. However, undertaking such a lengthy process at night is a common practice that minimizes the impact of the e-Discovery process on the business.<sup>64</sup> Accordingly, such actions on their own should not have led the court to conclude a nefarious intent.<sup>65</sup>

---

<sup>57</sup> Status Quo Order, *supra* note 26.

<sup>58</sup> Corinne L. Giacobbe, Note, *Allocating Discovery Costs in the Computer Age: Deciding Who Should Bear the Costs of Discovery of Electronically Stored Data*, 57 WASH. & LEE L. REV. 257, 262 (2000).

<sup>59</sup> Allman, *supra* note 40.

<sup>60</sup> See Brownstone, *supra* note 57 (discussing the complexities of e-Discovery and the high costs associated with preserving data, the different methods of production and review, and the difficulties posed by judicial sanctions).

<sup>61</sup> Allman, *supra* note 40.

<sup>62</sup> Citizens for Responsibility & Ethics in Wash. v. Exec. Office of the President, Nos. 07–1707, 07–1577 (HHK/JMF), 2008 WL 2932173, at \*3 (D.D.C. July 29, 2008) (declining to order imaging of hard drives due to cost-benefit analysis); Giacobbe, *supra* note 59 at 262.

<sup>63</sup> Giacobbe, *supra* note 58 at 262.

<sup>64</sup> *Id.*

<sup>65</sup> United States v. Bunty, 617 F. Supp. 2d 359, 369–71 (E.D. Pa. 2008) (dismissing a spoliation claim finding lack of bad faith); Ed Schmidt Pontiac-GMC Truck, Inc. v. Chrysler Motors Co., LLC, 575 F. Supp. 2d 837, 841–42 (N.D. Ohio 2008) (requiring evidence of intent to deprive opposing party of useful information for spoliation claim); New York State Nat'l Org. for Women v. Cuomo, No. 93 CV 7146(RLC) JCF, 1998 WL 395320, at \*3 (S.D.N.Y. July 14, 1998) (declining to award spoliation sanctions where no showing of intentional failure to preserve electronically stored information).

Indeed, if the defendant's consultant was really trying to hide his actions from discovery, he could easily have removed all forensic trace evidence of his wiping activities.<sup>66</sup> The failure to do so supports the innocent explanation for the wipe offered by the defendant.<sup>67</sup>

#### IV. CONCLUSION

¶20 Armed with partial or incomplete information regarding digital matters as noted above, courts unfortunately can reach the wrong conclusion. As illustrated in *TR Investors, LLC v. Genger*, where the plaintiff successfully, but mistakenly, asserted the defendant committed spoliation of evidence and unwittingly led Vice Chancellor Strine to impose an unreasonable and expensive burden upon this defendant and all future litigants and companies in the State of Delaware—the burden of preserving unallocated space on pain of spoliation sanctions.<sup>68</sup>

---

<sup>66</sup> *Scalera v. Electrograph Sys. Inc.*, 262 F.R.D. 162, 179 (E.D.N.Y. 2009) (declining to issue sanctions despite party's negligent failure to preserve ESI).

<sup>67</sup> *Port Auth. Police Asian Jade Soc'y of N.Y. and N.J. Inc. v. Port Auth. of N.Y. and N.J.*, 601 F. Supp. 2d 566, 570–71 (S.D.N.Y. 2009) (denying sanctions despite document destruction and finding other available evidentiary sources available); *Bunty*, 617 F. Supp. 2d 359, 369–71 (Defendant argued the government destroyed important and potentially exculpatory evidence. Despite determining data was altered after the government opened a floppy disk, the court found the defendant failed to demonstrate the government acted in bad faith or that the alteration prejudiced his case, and denied the motion to dismiss based on spoliation.); *Gippetti v. UPS, Inc.*, No. C07-00812 RMW(HRL), 2008 WL 3264483, at \*3 (N.D. Cal. Aug. 6, 2008) (denying spoliation claim finding destruction in accordance with retention policy); *Anadarko Petroleum Corp. v. Davis*, No. H-06-2849, 2006 WL 3837518, at \*27–28 (S.D. Tex. Dec. 28, 2006) (The plaintiff asked the court for sanctions based on spoliation of evidence. It argued the defendant deliberately destroyed evidence when he was under a preservation obligation. The court ruled there was not enough evidence in the record at that time to demonstrate the defendant destroyed records in bad faith.); *Williams v. Saint-Gobain Corp.*, No. 00-CV-0502E(SC) 2002 WL 1477618, at \*3 (W.D.N.Y. June 28, 2002) (refusing to award sanctions for withholding or destroying emails where no evidence of bad faith).

<sup>68</sup> *Benton v. Dlorah, Inc.*, No. 06-CV-2488-KEV-GLR, 2007 WL 2225946, at \*3 (D. Kan. Aug. 1, 2007) (refusing to compel production of personal hard drive); *Convolve, Inc. v. Compaq Computer Corp.*, 223 F.R.D. 162 (S.D.N.Y. 2004) (refusing to issue sanctions for spoliation of electronic evidence).