Strafford

Presenting a live 90-minute webinar with interactive Q&A

Mobile Device Privacy and Security Compliance for Corporations

Designing and Implementing Policies for Accessing, Monitoring and Protecting Business Data on Portable Devices

TUESDAY, MAY 13, 2014

1pm Eastern | 12pm Central | 11am Mountain | 10am Pacific

Today's faculty features:

Chuck Cosson, Senior Corporate Counsel, Privacy, **T-Mobile**, Bellevue, Wash.

Daniel B. Garrie, Executive Managing Partner, **Law & Forensics**, Seattle and Special Counsel to **Zeichner, Ellman and Krause,** New York

Darren Kress, Director, Enterprise Security Operations, **T-Mobile**, Bellevue, Wash.

Elizabeth Rogers, Chief Privacy Officer, **Texas Comptroller of Public Accounts**, Austin, Tex.

Aaron K. Tantleff, Partner, **Foley & Lardner**, Chicago

The audio portion of the conference may be accessed via the telephone or by using your computer's speakers. Please refer to the instructions emailed to registrants for additional information. If you have any questions, please contact **Customer Service at 1-800-926-7926 ext. 10**.

HUFF POST TECH

Daniel Garrıe
Managing Partner and General Counsel,
Law & Forensics LLC

Posted: 02/06/2014 3:51 pm EST

Email Follies Plague Corporate America
By Daniel B. Garrie, Esq

Email Follies Plague Corporate America

The modern world of Corporate America runs on email and web-based applications; consequently, employees of Corporate America are continuously sending emails, at all hours of the day and night, using their corporate email accounts. These emails, which must be automatically archived by the corporation in order to remain in compliance with data management regulations, frequently end up creating costly problems. Corporations must avail themselves of behavioral modification tools to break the expensive habits that employees armed with smartphones and mobile work email accounts have formed. Email communications can and have captured dishonest and illegal activities on the part of employees, but that is a larger issue than I can address here today. In this article, I will discuss only the relatively simple case of email "foot-in-mouth" -- offhand comments made in the course of a conversation that later could be misinterpreted in a negative way.

One major problem is an information gap between top executives and mid- or lower-level employees. While IT security personnel may have educated the execs on proper "email hygiene" and the permanence of email, other employees may be quite unaware of that aspect of their communications. The assumption that emails can be deleted by simply moving them to the trash folder is inaccurate and can lead to serious trouble for an organization.

Take, for example, a case that emerged in the recent banking crisis: mid-level Goldman Sachs trader Fabrice Tourre, known jokingly to his co-workers as "Fabulous Fab," sent several emails touting the role of the products he was selling in the looming banking catastrophe. "The whole building is about to collapse," he wrote, "anytime now ... Only potential survivor, the fabulous Fab ... standing in the middle of all these complex, highly leveraged, exotic trades he created without necessarily understanding all of the implications of those monstruosities [sic]!!!" This email, among others, implicated Goldman Sachs with knowingly misleading investors. While the suit eventually resolved in Fabrice Tourre being found liable for fraud , Goldman Sachs suffered from a major loss of reputation and endured a great deal of media outrage. Ethics and business practices aside, Fabrice Tourre clearly did not understand that anything written via a company email client, to paraphrase the Miranda warning, can and will be used against its author and indeed its host company as well.

Another example involved the London Interbank Offered Rate, or "Libor," which is a key interest rate estimated by major London banks in order to determine the rate that a bank would pay if it borrowed money from other banks. This rate is then used throughout all lending that those banks conduct, thereby affecting borrowers throughout the world. In December of 2012, amidst the infamous Libor-rigging scandal, the UK's Financial Services Authority's report quoted UBS employee-emails blatantly manipulating and attempting bribes to control the Libor: "If you keep 6s unchanged today ... I will f---- do one humongous deal with you ... Like a 50,000 buck deal, whatever ... I need you to keep it as low as possible ... if you do that ... I'll pay you, you know, 50,000 dollars, 100,000 dollars... whatever you want ... I'm a man of my word." The email from which that desperate and unethical request was cited, along with a host of others in a similar vein, are both incriminating and highly embarrassing for UBS.

Despite the many high-profile cases involving email evidence, employees in corporate America still send these foolish emails. Employees and employers alike must remember that whether or not an employee email actively implicates the employee (and therefore the company, by association) in a very public criminal investigation with hundreds of millions of dollars on the line, such emails can still severely damage a company's business and reputation. In some cases, the loss of reputation can in itself be a killing blow. When it comes to modern court cases, email evidence often comprises the difference between a winning and losing lawsuit.

It is beyond refute that for every email sent, there's an excellent chance that someone, or many persons, may have kept a copy: the individual (both the sender and any receivers), the company mail server, the backup provider for either the sender or receiver, or the smart phone from which the email was sent. Regulations require that companies archive emails to some extent, and major companies who are under major scrutiny must store all their data to the furthest possible extent of technology. There are very few cases in which it is impossible for data to be retrieved or restored. How, operating in a world where any unthinking (or unethical) email sent by an employee could mean their employer's downfall, are companies to protect themselves?

I will leave the ethics education for companies to handle on their own. As for protecting against email folly, the solution is simple: use a tried and tested behavioral modification approach. Put a program in place that clearly outlines your company email policy (I recommend teaming this with a BYOD policy for the greatest effect), and includes examples of email communications that are prohibited during working hours, from company email clients and via company machines. Let employees know that if they send an email violating any one of those policies, the company will take immediate action against that person. This means that the next time an employee sends out, for benign example, a personal email about an eBay transaction while at work or via a work email account, the company will notify the user that such email communication is prohibited and notate the infraction on their employee file. While this change in policy may be draconian, employees will adapt much faster than one might think, and it will alleviate the worries of countless legal counsels, IT security professionals, and indeed the employees themselves -- this policy protects them as well, removing the risk of having their personal communications examined in a court of law.

Daniel B. Garrie is the executive managing partner at www.lawandforensics.com. For more information, or with questions and comments, please email at Daniel@lawandforensics.com. Daniel would like to thank Kelsey Fredston-Hermann for her editorial assistance on this article.

http://www.huffingtonpost.com/daniel-garrie/email-follies-plague-corp_b_4725856.html?view=print&comm_ref=false

HUFF POST TECH

Daniel Garrie
Managing Partner and General Counsel,
Law & Forensics LLC

Attacking the Weakest Link: BYOD in the Law Firm Culture

Posted: 09/10/2013 5:40 pm

Attacking the Weakest Link: BYOD in the Law Firm Culture
By Daniel B. Garrie, Esq., co-authored by Valerie Strumwasser, Esq., Associate General Counsel at Law & Forensics

Law firm culture has long focused on the ability of its attorneys to bring a high level of thought and analysis to every legal case on its roster. However, similar care has not been spent by firms when it comes to data security. For many firms, hiring world class security engineers to work full time is seen as impractical. And, acquiring the right hardware and software solutions is too costly. What firms do not realize is that data security is essential to good client service. Without it, client's files may inadvertently end up on a file server somewhere like China, Brazil, or Russian.

Consider the following hypothetical:

A 500-attorney global law firm had a policy allowing employees to use their personal devices, including cell phones, tablets, and laptops, for work purposes. One senior partner used his smartphone for work email, viewing files, and remotely connecting to the law firm network to access client materials and to get documents stored in the Cloud. This senior cost-conscious partner chose to use his smartphone for both work and personal use, as no one brought to his attention the need to segregate data and users. One day, while driving his son to school, the senior partner lets his son use the smartphone to surf the Internet and download a new game. But, this game came with malware code attached to it, which accessed the smartphone data. More importantly, when the senior partner logged onto the firm's intranet, the malware program infiltrated the firm's servers. This silent intrusion allowed the malware to transmit back to the developer data, which includes bank account information, credit card information, and confidential information for high-profile clients, all available to the highest bidder.

Within days of the breach, the law firm was floundering to determine how their networks were hacked, how to stop the leak, how to manage their client relationships, and how to remedy the reputation fall out.

While the above hypothetical may seem like a doomsday scenario, a simplified copycat version of Stuxnet could easily do just that.

Most recently, two security researchers at the Georgia Institute of Technology unveiled a modified USB charger for the iPhone that cost approximately $45 to build. Quite an expensive cord (even by Apple standards!), but the real purpose of this charger is to hack into the iPhone without the user knowing. Not only does it hack the iPhone, it does it in under a minute.

So let's modify our hypothetical above. Our same partner goes on a business trip to Shanghai to meet with a new client. He stays in a fancy new boutique hotel that comes with USB ports built right into the wall. How handy! Except that on the other side of the wall was placed this same $45 device waiting to push malware onto any iPhone, allowing outside access to data on the phone. Now, the hacker on the other end has access to the attorney's linked email and cloud drive, where he keeps his clients' pending patent applications.

Like most enterprises, hacking is generally about making money. Whether you are a criminal stealing credit card information, or a sovereign nation stealing intellectual property or trade secrets, with the right amount of planning you can easily target business travelers who will inevitably hold a certain amount of unprotected valuable information at any given time.

Even without a direct link to the attorney's confidential client information, any other data on the phone can easily be bought and sold on the underground market. Take, for example, a personal email account. Within this account, our attorney friend has emailed his bank account information in 2007 to his brother so a transfer could be made (and never deleted the email from his Sent folder). Between 2005 and 2010, before his law firm bought laptops for attorneys, our attorney would often send himself client documents to work on from home; those files still sit in a Work Documents folder in his Yahoo! account. As a highly organized attorney, our friend keeps all copies of receipts from Internet transactions in a folder in his Gmail account. His photos are tagged with the latest geo-positioning information and a subject-line reading "Our new beach house! Too bad we only get to visit on the weekends." He is wise not to save his username on his mobile-banking and credit-card-payment app, but he does maintain an email in his Drafts folder with a list of all passwords for those less important sites like his mobile phone account, his iTunes account, and his Netflix account. Even a marginally savvy criminal with access to this information can withdraw funds from the attorney's bank account, impersonate the attorney in a number of situations, and gather enough information and access to use the email accounts to send spam. If the attorney is unlucky enough to lose his phone and the criminal is local, there is also an exact geo-position of his vacation home and a quick search in Gmail reveals an email to the attorney's sister telling her the key to the back door is under the jar of sea shells.

These examples are not meant as scare tactics, but merely an explanation of a few possible ramifications of a data breach. We all take calculated risks in our everyday lives, and now those risks must include how we handle our personal and business-related information online.
Our experience advising law firms and in-house legal departments on these issues has shown that there are cost-efficient methods that can dramatically improve a firm's data security both on local hardware and mobile devices.

While investing millions is not practical, if the law firm has a security-aware culture and has purchased and implemented one of the current solutions available in the marketplace, it can provide a secure and easy-to-use file transfer solution, a highly advanced email encryption service, an integrated malicious-code-detector for both the Internet connection and physical devices, a solution that manages and protects data in transit between mission critical system and security platforms, and technology that provides network protection from all outside threats.

The list of software discussed above seems long and complex, but these services can be found in a single solution and managed by in-house or third-party vendors. One such single-solution product is Safe-T, which offers manageable and easy-to-implement solutions for the entire scope of data security. There will always be criminals who find your cell phone and the data on it to be profitable. However, our entire hypothetical can be averted by some thoughtful pre-planning and a little amped up security (unless you're trying to keep out the NSA, of course).

Law firms have long been the vault for personal and corporate confidences. But the increasing number of hacks should leave clients questioning the strength and security with which their law firm protects their data. The simple principle of attacking the weakest link often may lead back to law firms' devices, as they often do not invest in the technology, people, and cultural awareness necessary to provide strong security.

A recent Wall Street Journal article lauded law firms as the first stop in cyber security response, praising the benefits of attorney-client privilege and knowledge of corporate disclosure laws. But simply knowing the law is half the battle - the physical hardware and software piece is equally critical. For a more tangible public example, one can turn to the article published by Bloomberg on January 31, 2012. This article details how Chinese hackers zeroed in on the Canadian law firms handling a $40 billion dollar acquisition. The article further details how the hack breached seven different law firms as well as Canada's Finance Ministry and the Treasury Board. While the acquisition fell apart for unrelated reasons, the incident illustrates the vulnerability of law firms. According to Mandiant, and in-line with our experience, an estimated 80 major U.S. law firms were hacked last year.

Unfortunately, neither individual nor state-sponsored hackers are deterred by the tenets of attorney-client privilege. Just as you would not put your money in a bank without a vault, you should not trust critical, sensitive, or material corporate data to a law firm with a weak "data protection vault."

Unlike the physical structure of a bank, the level of information security readiness and effectiveness is not readily apparent to law firm clients, especially to those that are not technically skilled. Thus, any company should require counsel to demonstrate that the law firm knows how to securely hold and manage an organization's data. This is particularly true in cases involving technology, trade secrets, or sensitive corporate data. In turn, law firms who know how to manage and secure technological assets should use that competitive advantage in marketing themselves to existing and potential clients.

Law firm's apparent lack of response to data threats prompted Jeff Brandt to create an essentially-viral campaign to promote internal discussion of law firm security measures. He

created a fake email and internal memo that detailed circumstances surrounding a supposed breach due to lax security standards and a bring-your-own-device policy. It created quite the stir in certain circles before Brandt outed himself as a provocateur of digital security policy.

There are a few critical steps that law firms can take to simultaneously enter this new area of practice and ensure that their clients' data remains safe. The firm should create network data maps, monitor digital access logs, hire in-house and outside experts, acquire appropriate computer hardware and software, and create a culture that is security-centric. Often the weakest link is not the technology, but the people, so it is essential firms make sure ingrained in every employee's mind is the need to be security aware. These are a few of the preventive and prophylactic measures that are at the disposal of law firms. There is not a single solution befitting all firms, and the right solution will vary based on the size, geography, people, and systems a firm has deployed. That said, every firm should seek and employ the right solution for it and their clients.

http://www.huffingtonpost.com/daniel-garrie/attacking-the-weakest-lin_b_3862354.html

Northwestern Journal of Technology and Intellectual Property

Volume 9
Issue 1 October

Article 1

Fall 2010

Legally Correct But Technologically O the Mark

Daniel B. Garrie

Bill Spernow

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

October 2010 VOL. 9, NO. 1

Northwestern Journal of Technology and Intellectual Property
Volume 9, Number 1 (October 2010)

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.[1] Gone are the days when the most technically challenging decision was determining if evidence on a floppy disk[2] had been destroyed because a litigant exposed it to a strong magnetic field.[3] 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.[4] While judges are entirely capable of arriving at the correct decision when it comes to ruling on the value of digital evidence,[5] they are at the mercy of the "experts" involved when it comes to issues of spoliation.[6]

---

[*] 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.

[1] 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").

[2] 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.

[3] Nathan Wiebe, *Regarding Digital Images: Determining Courtroom Admissibility Standards*, 28 MAN. L.J. 61, 63 (2002).

[4] 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 (last visited Sept. 6, 2010).

[5] "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.[7] 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,[8] 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[9] and file structures.[10] 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*.[11] 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.[12] 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.[13] 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 (last visited Sept. 6, 2010) (defining Electronic Stored Information (ESI)).

[6] 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).

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

[8] 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.

[9] Computer storage refers to the act of placing information on a disk where it available for later use. O'CONNOR, *supra* note 2.

[10] "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).

[11] TR Investors, LLC v. Genger, No. 3994-VCS, 2009 WL 4696062 (Del. Ch. Dec. 9, 2009).

[12] *Id.* at *17–19.

[13] *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[14] reside. Those two areas are "existing file space" where valid files can be found, and deleted-free space,[15] or more globally "unallocated space,"[16] 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[17] and server,[18] and is what forensic experts typically examine when recovering deleted files that have been emptied from the recycle bin.[19]

¶7 In the *Genger* case, the court determined that a consultant employed by the defendant had used a wiping utility[20] 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[21] or deleted files on the

---

[14] 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).

[15] "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.

[16] "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).

[17] 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 (last visited Sept. 8, 2010).

[18] 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 (last visited Sept. 24, 2010).

[19] 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.

[20] 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).

[21] "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 (last visited Sept. 24, 2010).

defendant's computer systems.[22] The inability to forensically locate these documents in digital form resulted in sanctions against the defendant Genger.[23]

¶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.[24] The dispute was between the Trump Group, the new owners, and Arie Genger, the original owner.[25] 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."[26]

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

¶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.[31] The consulting firm created file level snapshots of the "existing files" on the potentially responsive hard drives.[32] However, as is common in e-discovery cases, the consultants never created a forensic image[33] 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.[34] Where Genger's personal items were discovered on these systems, the court permitted these items to be individually encrypted.[35] 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

---

[22] TR Investors, LLC v. Genger, No. 3994-VCS, 2009 WL 4696062, at *6–7 (Del. Ch. Dec. 9, 2009).
[23] *Id.* at *15–20.
[24] *Id.* at *1–15.
[25] *Id.* at *1.
[26] *Id.* at *1 n.1 (citing Status Quo Order, *Genger*, 2009 WL 4696062).
[27] *Id.* at *5.
[28] *Id.* at *15–20.
[29] *Id.*
[30] *Id.* at *11.
[31] *Id.*
[32] *Id.* at *12.
[33] 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.
[34] *Genger*, 2009 WL 4696062, at *5–6.
[35] 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.[36] 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.[37]

¶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.[38] As a result, the court imposed a series of heavy sanctions upon Genger, fining him and shifting the burden of proof to him.[39] 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.[40]

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.[41] 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.[42] 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.[43] In its opinion, the court references a memorandum,

---

[36] *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).

[37] *Id.* at *7.

[38] *Id.* at *17

[39] *Id.* at *19.

[40] 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.

[41] *Genger*, 2009 WL 4696062, at *6.

[42] *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).

[43] 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.[44] 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.[45] 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.[46] 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.[47] 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.[48] 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).

[44] *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]).

[45] *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).

[46] 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.dcbar.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)).

[47] *Mintel*, 2010 WL 145786, at *8; Wall & Lange, *supra* note 46.

[48] *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.[49] 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.[50] 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.[51] 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.[52]

¶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.[53] Think of the $MFT file as the table of contents for a hard drive that points you to the page of interest.[54] 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.[55]

¶16 The court also did not appear to understand that a vast majority of data in unallocated space are random fragments.[56] 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

---

[49] *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).

[50] 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).

[51] Wall & Lange, *supra* note 46.

[52] 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).

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

[54] *Id.*

[55] *Id.*

[56] *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.[57] 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.[58] 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.[59] 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.[60] 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.[61] 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.[62] 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.[63]

¶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.[64] Accordingly, such actions on their own should not have led the court to conclude a nefarious intent.[65]

---

[57] Status Quo Order, *supra* note 26.

[58] 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).

[59] Allman, *supra* note 40.

[60] *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).

[61] Allman, *supra* note 40.

[62] 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.

[63] Giacobbe, *supra* note 58 at 262.

[64] *Id.*

[65] 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.[66] The failure to do so supports the innocent explanation for the wipe offered by the defendant.[67]

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.[68]

[66] 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).

[67] 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).

[68] 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).