William Mitchell Law Review

Volume 38 | Issue 1 Article 8

2011

Collaborating with a Digital Forensics Expert: Ultimate Tag-Team or Disastrous Duo?

Sean L. Harrington

COLLABORATING WITH A DIGITAL FORENSICS EXPERT: ULTIMATE TAG-TEAM OR DISASTROUS DUO?

Sean L. Harrington†

† J.D. Candidate, Taft Law School. The author is a digital forensics analyst, second Vice President of the Minnesota Chapter of the High Technology Crime Investigation Association (HTCIA), and certified as a Computer Hacking Forensic Investigator (CHFI), Certified Information Systems Security Professional (CISSP), Microsoft Certified Systems Engineer (MCSE), and Certified Sarbanes Oxley Professional (CSOXP). The author also serves on the council of the Minnesota State Bar Association Computer and Technology Law Section, and on the advisory boards for the Investigative Sciences for Law Enforcement Technologies (ISLET) and Computer Forensics programs of Century College, as part of the Minnesota State Colleges and Universities system. Special thanks to the following, who reviewed early drafts of this Comment and provided insightful guidance for the preparation of the same: Craig Ball, trial attorney, computer forensics examiner, and lecturer; Sharon D. Nelson, attorney, lecturer, and co-author of the Electronic Evidence & Discovery Handbook; John J. Carney, Minnesota attorney and mobile-device forensics examiner.

Put your message in a modem
And throw it in the Cyber Sea[1]

I. INTRODUCTION

At the risk of stating the obvious, electronic gadgets and digital media are ubiquitous in our modern world. Perhaps it seems that both the animate and inanimate objects around us have been reduced to digitized ones and zeros: from e-books to movies, spreadsheets to GPSs, music to family photos, dating to job-seeking, diaries to recipes, auctions to education, and stock-trading to holiday cards. People lumber around halls and sidewalks, staring at digital devices, texting, checking the weather, listening to music, seemingly oblivious to the physical world around them. In 2007, it was reported that the world created more electronic documents in the year prior than the documents in all the years combined since Gutenberg invented the printing press.[2] By then, at least ninety-three percent of all new information was created digitally,[3] and, of all electronically stored information ("ESI"), at least thirty percent would never be printed out.[4] In May 2011, the online merchant Amazon.com announced that its sales of electronic books overtook sales of printed books.[5] Meanwhile, the President has decreed the growing number of cyber security threats is "one of the most serious economic and national security challenges we face as a nation."[6] The volume of data breaches, mostly consisting of hacking and malware, is at the highest level ever, according to a

1. RUSH, *Virtuality, on* TEST FOR ECHO (Atlantic Records 1996).

2. William E. Mooz, Jr., *Technology Tips for Reducing EDD Review Costs*, 24 LEGAL TECH NEWSL., no.12, Mar. 2007, at 1, 1, *available at* http://www.catalystsecure.com/images/crs/articles/Technology_Tips_0307.pdf (noting the great increase in data as a result of new technologies and its effect on litigation).

3. James Larue et al., *Trails from the Aether: Cyber-Evidence*, *in* 54.1 STATE BAR OF TEXAS 33RD ANNUAL ADVANCED FAMILY LAW COURSE 1, 1 (2007), *available at* http://www.texasbarcle.com/Materials/Events/6367/110331_01.pdf.

4. *Id.*

5. Claire Cain Miller & Julie Bosman, *E-Books Outsell Print Books at Amazon*, N.Y. TIMES, May 19, 2011, http://www.nytimes.com/2011/05/20/technology/20amazon.html.

6. President Barack Obama, Remarks by the President on Securing Our Nation's Cyber Infrastructure (May 29, 2009), http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure/.

2011 joint report by Verizon and the U.S. Secret Service.[7] As one commentator wryly observed, "Hardly a month has gone by this year without a multinational company such as Google Inc. . . . , EMC Corp. or Sony Corp. . . . disclosing it's been hacked by cyber intruders who infiltrated networks or stole customer information."[8] Likewise, hardly a week goes by without a prominent figure becoming embroiled in a scandal because of a social media misstep.[9]

Societal trends, such as the foregoing, invariably manifest themselves in legal controversies,[10] and, as a consequence thereof, new fields of expertise such as "ethical hacking" and cloud forensics[11] are emerging. These trends have led to "a huge demand" for highly educated specialists in the discipline of digital forensics.[12] Consequently, lawyers have been—in both litigation support and law practice management—increasingly encountering or relying upon digital forensics experts.[13] And, although education in this emerging discipline has focused largely on its technical aspects,[14] there are significant legal and ethical challenges

7. Wade Baker et al., *2011 Data Breach Investigations Report*, VERIZON, 6 (2011), http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2011_en_xg.pdf.

8. Michael Riley et al., *Cyber Cops Stymied by Anonymity in Tracking Google, Sony Hacks*, BLOOMBERG (June 6, 2011, 11:01 PM), http://www.bloomberg.com/news/2011-06-07/google-sony-nintendo-hacker-anonymity-stymies-arrests-by-u-s-cyber-cops.html.

9. *See, e.g.*, Christian Boone, *Embarassing Online Exchanges Becoming Political Scandal Du Jour*, AJC, June 6, 2011, http://www.ajc.com/news/embarrassing-online-exchanges-becoming-969042.html.

10. *See generally* Lon L. Fuller, *Law as an Instrument of Social Control and Law as a Facilitation of Human Interaction*, 1975 BYU L. REV. 89 (1975) (positing that the law is simultaneously a means of social control, a means of facilitating human interaction, and the realization of reciprocal expectancies).

11. *See, e.g.*, OFFICE OF JUSTICE PROGRAMS, U.S. DEP'T OF JUSTICE, OMB NO. 1121-0329, SOLICITATION: ELECTRONIC CRIME AND DIGITAL EVIDENCE RECOVERY (Mar. 31, 2010), *available at* https://www.ncjrs.gov/pdffiles1/nij/sl000957.pdf ("NIJ seeks proposals for research and technology development leading to the introduction into practice of forensic tools that can overcome the challenges of the Cloud computing environment."); Joe McKendrick, *Cloud Forensics: New Practice Emerges Out of Necessity*, SMARTPLANET (Jan. 31., 2011, 9:39 AM), http://www.smartplanet.com/blog/business-brains/cloud-forensics-new-practice-emerges-out-of-necessity/13338.

12. BILL NELSON ET AL., GUIDE TO COMPUTER FORENSICS AND INVESTIGATIONS 508 (4th ed. 2010).

13. Jerry Wegman, *Computer Forensics: Admissibility of Evidence in Criminal Cases*, 8 J. LEGAL ETHICAL & REG. ISSUES 1, 2 (2005) (explaining the evolution of digital forensic experts and the legal challenges they face).

14. Gilbert Whittemore, *Report to the House of Delegates*, 2008 AM. BAR ASS'N

confronting investigators, for which they are ill prepared.[15]

This Comment is divided into four parts: the first section, following this introduction, is an overview of ethical rules and obligations governing attorneys and investigators in digital forensics investigations. This includes some possible ethical pitfalls in supervising investigators, and the investigator's obligations relating to the work product doctrine, attorney-client privilege, and information security. The second section urges that, notwithstanding the challenges and dangers discussed in the first section, the use of digital forensics examiners may be essential to prevailing in a case, or mitigating the harm incurred by the lawyer and client. Finally, the third section introduces and briefly analyzes special considerations in digital forensic investigations relating to cloud computing and social media.

The American Academy of Forensic Sciences classifies digital forensics as a forensic science. For the purposes of this Comment, digital forensics is defined as:

> The use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations.[16]

SEC. SCI. & TECH. L. 2, *available at* http://www.wired.com/images_blogs/threatlevel/files/aba_report_and_resolution.pdf ("Numerous professional certifications are available to computer forensic and network testing professionals that are based on rigorous curricula and competency examinations.").

15. Wegman, *supra* note 13, at 2.

16. Gary Palmer, *A Road Map for Digital Forensic Research*, DFRWS 16 (Nov. 6, 2001), http://www.dfrws.org/2001/dfrws-rm-final.pdf; s*ee also* THE SEDONA CONFERENCE GLOSSARY: E-DISCOVERY & DIGITAL INFORMATION MANAGEMENT (3d ed. 2010), *available at* http://www.thesedonaconference.org/content/miscFiles/glossary2010.pdf. For forensics:

> The scientific examination and analysis of data held on, or retrieved from, ESI in such a way that the information can be used as evidence in a court of law. It may include the secure collection of computer data; the examination of suspect data to determine details such as origin and content; the presentation of computer based information to courts of law; and the application of a country's laws to computer practice. Forensics may involve recreating "deleted" or missing files from hard drives, validating dates and logged in authors/editors of documents, and certifying key elements of documents and/or hardware for legal purposes.

Id. at 23.

The word "forensic" means "[u]sed in or suitable to courts of law."[17] So, it might seem natural that digital forensics practitioners and lawyers have occasion to work closely together. Yet, although digital forensics "is by no means a new field of endeavor,"[18] it is "a relatively new discipline to the courts and many of the existing laws used to prosecute computer-related crimes, legal precedents, and practices related to computer forensics are in a state of flux."[19]

To appreciate the benefits of pairing an astute lawyer with a digital forensics examiner who has a robust legal background, consider that benign ingredients exist within ordinary kitchen cupboards and pantries, which, when mixed together with care, create appetizing confections or healing concoctions. To appreciate the risks of an alternative arrangement, recall that baking soda mixed with vinegar results in a frothy mess. Accordingly, the prudent attorney must select a digital forensics expert carefully, and maintain strict adherence to both separation of duties and supervisory capacity.

II. ETHICS IN DIGITAL FORENSICS INVESTIGATIONS

A. Ethical Rules Governing Digital Forensics Investigations

In the United States, there are no digital forensics licensing bodies,[20] although a few states require digital forensics examiners to be licensed as private investigators.[21] The American Bar Association posits that "[i]nvestigation and expert testimony in computer forensics and network testing should be based upon the current state of science and technology, best practices in the industry, and knowledge, skills, and education of the expert."[22] And, although most private digital forensics organizations do impose a code of ethics as a condition of membership,[23] there is

17. BLACK'S LAW DICTIONARY 721 (9th ed. 2009).

18. NELSON ET AL., *supra* note 12, at 508.

19. *Computer Forensics*, U.S. COMPUTER EMERGENCY READINESS TEAM 3 (2008), http://www.us-cert.gov/reading_room/forensics.pdf.

20. NELSON ET AL., *supra* note 12, at 576.

21. *E.g.*, MICH. COMP. LAWS §§ 338.821–338.823 (2011); TEX. OCC. CODE §§ 1702.101, 1702.388, 1702.386 (2010); Stephen K. Lubega, *Is Your Computer Forensics Expert Required to Have a PI License?* MYRIAD LITIGATION SOLUTIONS (Apr. 2009), http://www.myriadlit.com/newsbyte_v3full.html; John Tredennick, *Collecting Computer Data in the U.S.: Pick the Wrong State and You Could Wind Up in Jail*, L. TECH. TODAY, July 2008, at 1–2.

22. Whittemore, *supra* note 14, at 2.

23. *See, e.g.*, *Code of Ethics*, EC-COUNCIL, https://www.eccouncil.org

little known about frequency of enforcement, efficacy of enforcement, or ethics awareness among the membership. As one court explained:

> One survey of civil trials estimated that experts appear in 86% of the cases with an average of 3.8 experts per trial. While expert witnesses are appearing in civil cases in increasing numbers, the topic of expert witness ethics and professionalism is largely undeveloped and there are few definitive statements about what exactly the expert witness's ethical obligations are and how they are to handle the subtle as well as the more blatant attempts to influence them. . . . Even where professional associations have established ethical guidelines for conducting investigations, forming opinions and writing reports, very few explain how the ethical boundaries imposed on judges and lawyers may bear on the performance of their role in the legal system regardless of whether they are employed as a retained forensic expert for one of the parties or as a court-appointed expert.[24]

In contrast, the legal profession is regulated by states' supreme courts, most of which have adopted the ABA model rules.[25] And, although there has long been criticism of the self-regulation model,[26] lawyers are generally cognizant of attorney regulation, are

/about_us/code_of_ethics.aspx (last visited Sept. 11, 2011); *Code of Ethics and Professional Responsibility,* INT'L SOC'Y OF FORENSIC COMPUTER EXAMINERS, http://www.isfce.com/ethics2.htm (last visited Sept. 11, 2011); *Code of Ethics and Conduct,* CYBERSECURITY INST., http://www.cybersecurityinstitute.biz/training /ethicsconduct.htm (last visited Sept. 11, 2011); Rob Lee, *Certification: Ethics,* SANS COMPUTER FORENSICS, http://computer-forensics11.sans.org /certification/ethics (last visited Sept. 11, 2011); *HTCIA Bylaws*, HIGH TECH. CRIME INVESTIGATION ASS'N (2010), http://www.htcia.org/bylaws.shtml; *(ICS)² Code of Ethics*, (ICS)², https://www.isc2.org/ethics/default.aspx (last visited Sept. 11, 2011); *New Membership: Code of Ethics*, INT'L ASS'N OF COMPUTER INVESTIGATIVE SPECIALISTS, http://www.iacis.com/new_membership/code_of_ethics (last visited Sept. 11, 2011).

24. Kenneth C. v. Delonda R., No. VXXXXXX/02, 2006 WL 47429, at *8 (N.Y. Fam. Ct. Jan. 4, 2006).

25. "The ABA Model Rules of Professional Conduct were adopted by the ABA House of Delegates in 1983. They serve as models for the ethics rules of most states." *ABA Model Rules of Prof'l Conduct: About the Model Rules,* AM. BAR ASS'N, http://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct.html (last visited Sept. 11, 2011).

26. *See, e.g.*, F. Raymond Marks & Darlene Cathcart, *Discipline Within the Legal Profession: Is it Self-Regulation?,* 1974 U. ILL. L.F. 193 (1974); AM. BAR ASS'N SPECIAL COMM. ON EVALUATION OF DISCIPLINARY ENFORCEMENT, PROBLEMS AND RECOMMENDATIONS 1, 3 (1970), *available at* http://www.americanbar.org/content

required to take ethics continuing education annually, and most were required to pass a course on professional responsibility in law school.[27]

B. The Lawyer's Ethical Obligations While Working with Digital Forensics Examiners

Whereas the digital forensics profession is not subject to formal ethics standards, the Rules of Professional Conduct may nonetheless be implicated by the use of a digital forensics examiner.[28] Practitioners should be especially mindful of Model Rule 5.3, which imposes ethical responsibilities upon lawyers who supervise nonlawyers:

> With respect to a nonlawyer employed or retained by or associated with a lawyer:
>
> . . . .
>
> (b) a lawyer having direct supervisory authority over the nonlawyer shall make reasonable efforts to ensure that the person's conduct is compatible with the professional obligations of the lawyer; and
>
> (c) a lawyer shall be responsible for conduct of such a person that would be a violation of the Rules of Professional Conduct if engaged in by a lawyer if:
>
> (1) the lawyer orders or, with the knowledge of the specific conduct, ratifies the conduct involved; or
>
> (2) the lawyer is a partner or has comparable

/dam/aba/migrated/cpr/reports/Clark_Report.authcheckdam.pdf; *2009 ABA Survey on Lawyer Discipline Systems*, AM. BAR ASS'N, http://www.americanbar.org/groups/professional_responsibility/resources/survey_lawyer_discipline_systems_2009.html (last visited Sept. 11, 2011); *How Accountable Is the Civil Justice System?*, HALT, http://www.halt.org/about_halt/press_room/pdf/Full_Media_Kit.pdf#Advocacy_by_the_Numbers (last visited Sept. 11, 2011).

27. *See* 2010–2011 ABA STANDARDS FOR APPROVAL OF LAW SCHOOLS, INTERPRETATION 302-2 (2010), *available at* http://www.americanbar.org/content/dam/aba/publications/misc/legal_education/Standards/2011_2012_aba_standards_chapter3.authcheckdam.pdf ("The substantial instruction in the history, structure, values, rules, and responsibilities of the legal profession and its members required by Standard 302(a)(5) includes instruction in matters such as the law of lawyering and the Model Rules of Professional Conduct of the American Bar Association."); *Multistate Professional Responsibility Examination*, NAT'L CONF. OF BAR EXAMINERS, http://www.ncbex.org/multistate-tests/mpre/ (last visited Sept. 11, 2011) ("The Multistate Professional Responsibility Examination (MPRE) . . . is required for admission to the bars of all but four U.S. jurisdictions.").

28. MODEL RULES OF PROF'L CONDUCT R. 5.1–.2 (2010) (governing the ethical responsibilities of both supervisory lawyers and subordinate lawyers).

> managerial authority in the law firm in which the person is employed, or has direct supervisory authority over the person, and knows of the conduct at a time when its consequences can be avoided or mitigated but fails to take reasonable remedial action.[29]

Although it is improbable that a court would construe Rule 5.3 to require attorneys to possess the same level of knowledge and skill as the digital forensics expert, the rule does impose a significant, perhaps underestimated, responsibility. One court recently ruled that lawyers have an affirmative duty to be actively engaged in the electronic discovery ("e-discovery") collection process such that the lawyer should meet with the client to physically review the client's data repositories wherever they may be located (including, if necessary, personal computers).[30] This is not a requirement that lawyers be digital forensics experts,[31] but rather that lawyers should "be active participants in setting [e-discovery] search criteria, screening for privileged information, and handling non-technical details."[32] If too much autonomy is reposed in experts (or technology), a lawyer can lose control of the case, leading to increased risk exposure and increased costs.[33]

The problem of costs is highlighted by a few recent cases concerning fee-related disputes of astonishing amounts that arose from seeming miscommunication between the law firm and the digital forensics firm.[34] Although such costs may be recoverable in

29. *Id.* R. 5.3.

30. Transcript of Telephone Conference on Discovery Dispute at 12, Roffe v. Eagle Rock Energy, L.P., No. 5258-VCL (Del. Ch. Apr. 8, 2010), *available at* http://www.iediscovery.com/files/Roffe_v_%20Eagle_Rock.pdf.

31. *See, e.g.*, SonoMedica, Inc. v. Mohler, 2009 U.S. Dist. LEXIS 65714, at *17–18 (E.D. Va. July 28, 2009) ("Forensic examinations are not a routine part of discovery.").

32. Larue, et al., *supra* note 3, at 13 (citing Jason Krause, *Discovery Channels*, A.B.A. J., July 2002, at 52); s*ee also* Rhoads Indus., Inc. v. Bldg Materials Corp. of Am., 254 F.R.D. 216, 220 (E.D. Pa. 2008) (noting that although an IT consultant and software programs are crucial to adhering to FED. R. EVID. 502, it is not enough to rely upon technology; it is the lawyer's responsibility to check for privileged documents).

33. Larue et al. *supra*, note 3, at 13.

34. United States v. Afremov, 611 F.3d 970, 973–74 (8th Cir. 2010) (involving a dispute over invoices of a Minnesota computer forensics firm in the amounts of $628,737 and $178,850); Henry v. Quicken Loans, Inc., No. 04-40346, 2008 WL 474127 (E.D. Mich. Feb. 15, 2008) (involving a disputed invoice of a Minnesota computer forensics firm in the amount of $94,903); Debra Cassens Weiss, *Computer Expert Sues Leonard Street Law Firm for $775K*, A.B.A. J. (May 21, 2009, 11:11 AM), http://www.abajournal.com/news/article/computer_expert_sues_leonard_street_

some cases against the non-prevailing party,[35] the proactive approach to cost containment is for the managing lawyer to define and limit the scope of the investigation. This is because digital forensics analysis "takes as much time as the analyst has to give it."[36] If the case is unusually important or the nature of the evidence sought is "not reasonably accessible,"[37] an examiner could spend several weeks or even months analyzing a single piece of media.[38] "If the case is less important or the nature of the case permits the [proponent] . . . to make its case more easily, the investigator may spend only a few hours."[39] This cost-benefit analysis has come to be known as the "proportionality" doctrine.[40]

Cost seems to be the anxiety most often cited concerning digital forensics examinations.[41] Indeed, "The use of experts is

law_firm_for_775k/ (involving an invoicing dispute of a Minnesota computer forensics firm in the approximate amount of $775,000).

35. *See, e.g.*, AssociationVoice, Inc. v. AtHomeNet, Inc., No. 10-cv-00109-CMA-MEH, 2011 U.S. Dist. LEXIS 1654, at *14 (D. Colo. Jan. 6, 2011) (stating that computer forensic investigation costs satisfy the "loss" requirement of the Computer Fraud and Abuse Act, 18 U.S.C. §§ 1030(g) and (c)(4)(A)(i)); Sonomedica, Inc. v. Mohler, No. 1:08-cv-230, 2009 U.S. Dist. LEXIS 65714, at *19 (E.D. Va. July 28, 2009) (assessing $108,212.15 of monetary sanctions, inclusive of digital forensics firm's fees against contemnors).

36. Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 544 (2005).

37. FED. R. CIV. P. 26(b)(2)(B) defines sources that are "reasonably accessible" as being so because of "undue burden or cost."

38. Kerr, *supra*, note 36, at 544.

39. *Id.* *But see* Craig Ball, *The End of Digital Forensics?*, FORENSIC FOCUS: ARTICLES/PAPERS (July 23, 2011) (alteration in original), http://articles .forensicfocus.com/2011/07/23/the-end-of-digital-forensics/ (discussing the size of modern hard-drives where the imaging alone of "multi-terabyte" media is "measured in days, not hours").

40. *See* ONT. E-DISCOVERY IMPLEMENTATION COMM., 10 GUIDING PRINCIPLES TO MINIMIZE E-DISCOVERY COSTS A.1 (2010), *available at* http://www.oba.org/En /publicaffairs_en/ediscovery_docs/10Guidingprinciplestominimizee-discoverycosts-v.2.1.DOC. The principles show that under the proportionality principle, determinant factors include relevance, the cost of production, importance of the records, importance of the case, and the amount in controversy. Thus, in a "case with a smaller dollar value, a party's e-discovery obligations should be less onerous than in a case with a larger dollar value, or in a case where the interests at stake are of greater importance." *Id.* See also FED. R. CIV. P. 26(b)(2)(C), which requires the court to limit "the frequency or extent of discovery" where "the burden or expense of the proposed discovery outweighs its likely benefit, considering the needs of the case, the amount in controversy, the parties' resources, the importance of the issues at stake in the action, and the importance of the discovery in resolving the issues." *Id.*

41. *See, e.g.*, Tyler Moore, *The Economics of Digital Forensics*, FIFTH WORKSHOP ON THE ECON. OF INFO. SEC., 1 (June 26–28, 2006), http://www.cl.cam.ac.uk

costly."[42] But another salient consideration is the possibility that the conduct of the digital forensics examiner could be imputed to the attorney in certain situations under Model Rule 5.3. Perhaps the most common of such conduct is negligence, but the list could also include deception because of its popularity and efficacy as an investigative technique.[43] Deceptive techniques are, however, proscribed in the practice of law by the Rules of Professional Conduct.[44] As an example, one state supreme court found that a prosecutor who impersonated a public defender in an attempt to induce the surrender of a murder suspect had committed an act of deception that violated the Rules of Professional Conduct.[45] And many states, including Minnesota, have held that "[t]here are circumstances where failure to make a disclosure is the equivalent of an affirmative misrepresentation."[46]

The question of whether deception, as used in Model Rule 8.4, exists in the context of a digital forensics, cloud forensics, or network forensics (intrusion detection) investigation is not well settled.[47] In one Minnesota attorney disciplinary proceeding, the

/users/twm29/weis06-moore.pdf ("It turns out that many of the important constraints on digital forensic practices are not technical, but economic.").

42. Paul Giannelli, Ake v. Oklahoma*: The Right to Expert Assistance in a Post-*Daubert*, Post-DNA World*, 89 CORNELL L. REV. 1305, 1307 (2004); *see also* Weiss, *supra* note 34.

43. *See, e.g.*, Allan Lengel, *Your New Facebook Friend May Be a Federal Agent*, AOLNEWS (Mar 26, 2010 11:44 AM), http://www.aolnews.com/2010/03/26/your-new-facebook-friend-may-be-a-federal-agent/; *see also* Craig Ball, *Cross-examination of the Computer Forensics Expert*, CRAIG D. BALL P.C. (2004), http://www.craigball.com/expertcross.pdf ("The world of computer forensics is heavily populated by former law enforcement officers from the Secret Service, FBI, Treasury, military investigative offices and local police forces."). The Supreme Court has tacitly approved deception as a valid law enforcement technique in investigations and interrogations. *See* Illinois v. Perkins, 496 U.S. 292, 297 (1990) ("*Miranda* forbids coercion, not mere strategic deception . . . ."); United States v. Russell, 411 U.S. 423, 434 (1973) ("Criminal activity is such that stealth and strategy are necessary weapons in the arsenal of the police officer.").

44. MODEL RULES OF PROF'L CONDUCT R. 8.4 (2009).

45. *In re* Paulter, 47 P.3d 1175, 1176 (Colo. 2002). *Paulter* quotes the Oath of Admission-Colorado State Bar (2002): "I will employ such means as are consistent with Truth and Honor; I will treat all persons whom I encounter through my practice of law with fairness, courtesy, respect, and honesty." *Id.*

46. *In re* Zotaley, 546 N.W.2d 16, 19 (Minn. 1996) (quoting MINN. RULES OF PROF'L CONDUCT R. 3.3 cmt. 3 (2009)).

47. *See* Sharon D. Nelson & John W. Simek, *Muddy Waters: Spyware's Legal and Ethical Implications*, GPSOLO MAG., Jan/Feb 2006, *available at* http://www.americanbar.org/newsletter/publications/gp_solo_magazine_home/gp_solo_magazine_index/spywarelegalethicalimplications.html ("The legality of spyware is murky, at best. The courts have spoken of it only infrequently, so there is precious

supreme court accepted an attorney's conditional admission of misconduct for violating Minnesota Rules of Professional Conduct Rule 8.4 after pleading guilty to misdemeanor unauthorized computer access by installing and using an e-mail spyware program.[48] Yet, even if a digital forensics investigator refrains from using technology that is unlawful or contains malicious executable code, he or she foreseeably could use technology that arguably constitutes "deception." For example, an investigator may employ a "Web bug," a surreptitious file object commonly used by spammers that is placed in an e-mail message or e-mail attachment (such as a PDF or Microsoft Word document) to monitor user behavior.[49] When the user opens the e-mail or attachment, and if the user did not preconfigure the e-mail client or program to refrain from retrieving images or HTML content from the Internet, the e-mail client or program will attempt to retrieve the file object from a Web server and, in the process, transmit an HTTP request that includes the user's IP address and other information.[50] This information becomes available to the sender either through an automated report service (e.g., ReadNotify.com) or simply by monitoring traffic to the Web server. In a recent project demonstrating a seemingly appropriate use, researchers employed such technology in decoy documents to track possible misuse of confidential documents.[51]

Adopting the view that the foregoing constitutes deception, one might also view as deceptive the creation of a decoy Web site for the purpose of attracting one or more visitors (perhaps as a URL-link contained in an invitation sent via e-mail) and reviewing Web traffic logs to collect identifying information and visitor browsing patterns and activity (such as in following certain decoy links or documents), assuming the visitors were unaware of the

little guidance.").

48. *In re* Trudeau, 705 N.W.2d 409, 409–10 (Minn. 2005).

49. Richard M. Smith, *Microsoft Word Documents That "Phone Home"* THE PRIVACY FOUNDATION (Aug. 30, 2000), *available at* http://web.archive.org/web/20001009091304/http://www.privacyfoundation.org/advisories/advWordBugs.html ("A 'Web bug' could allow an author to track where a document is being read and how often. In addition, the author can watch how a 'bugged' document is passed from one person to another or from one organization to another.").

50. *Id.*

51. Brian M. Bowen et al., *Baiting Inside Attackers Using Decoy Documents*, COLUM. UNIV. DEP'T OF COMPUTER SCI., 1 (Aug. 28, 2009), http://www.cs.columbia.edu/~angelos/Papers/2009/DecoyDocumentsSECCOM09.pdf.

site's true purpose.[52]

A few state bar associations have already begun to address these technology-related ethical pitfalls. The Philadelphia Bar Association Professional Guidance Committee advised in Opinion 2009-02 that an attorney who asks an agent (such as an investigator) to "friend" a party on Facebook in order to obtain access to that party's non-public information, would violate, among others, Rule 5.3 of the Pennsylvania Rules of Professional Conduct.[53] Likewise, the Association of the Bar of the City of New York Committee on Professional and Judicial Ethics issued Formal Opinion 2010-2, which provides that a lawyer violates, among others, New York Rules of Professional Conduct Rule 5.3, if an attorney employs an agent to engage in the deception of "friending" a party under false pretenses to obtain evidence from a social networking website.[54]

And, although Rule 5.3 appears to require scienter (viz. "knowledge of the specific conduct"),[55] an emerging body of ethics opinions concerning information technology appear to be at odds with such a requirement. California's proposed Formal Opinion 08-0002 requires a lawyer to evaluate information security and finds that "attorneys are faced with an ongoing responsibility of

52. Nelson & Simek, *supra* note 47. The authors characterize spyware as "deceptive, at best," and warn attorneys about running afoul of Rule 1.2 in that "a lawyer shall not counsel a client to engage, or assist a client, in conduct that the lawyer knows is criminal or fraudulent," and Rule 8.4 in that:

> [I]t is professional misconduct for a lawyer to: (a) violate or attempt to violate the Rules of Professional Conduct, knowingly assist or induce another to do so, or do so through the acts of another; (b) commit a criminal or deliberately wrongful act that reflects adversely on the lawyer's honesty, trustworthiness, or fitness to practice law; or (c) engage in conduct involving dishonesty, fraud, deceit, or misrepresentation that reflects adversely on the lawyer's fitness to practice law.

Id. (quoting MODEL RULES OF PROF'L CONDUCT R. 1.2, 8.4 (2009)).

53. Philadelphia Bar Ass'n Prof'l Guidance Comm., Op. 2009-2 (2009), *available at* http://www.philadelphiabar.org/WebObjects/PBAReadOnly.woa/Contents/WebServerResources/CMSResources/Opinion_2009-2.pdf.

54. Ass'n of the Bar of the City of New York Comm. on Prof'l & Judicial Ethics, Formal Op. 2010-2 (Sept. 2010), *available at* http://www2.nycbar.org/Publications/reports/show_html.php?rid=1134.

55. *See* MODEL RULES OF PROF'L CONDUCT R. 5.3(c)(1), (2) (2009) (explaining that a lawyer is responsible for conduct of a nonlawyer that would be a violation of the Rules of Professional Conduct if engaged in by a lawyer if the lawyer orders or, with the knowledge of the specific conduct, ratifies the conduct involved; or the if lawyer has direct supervisory authority over the person, and knows of the conduct at a time when its consequences can be avoided or mitigated but fails to take reasonable remedial action).

evaluating the level of security of technology that has increasingly become an indispensable tool in the practice of law."[56] Alabama's Ethics Committee Opinion 2010-02 requires attorneys to exercise reasonable care against unauthorized access, which includes becoming knowledgeable about a cloud provider's storage and security.[57] Arizona's Ethics Opinion 09-04 provides, in pertinent part, that

> [W]hether a particular system provides reasonable protective measures must be informed by the technology reasonably available at the time to secure data against unintentional disclosure. As technology advances occur, lawyers should periodically review security measures in place to ensure that they still reasonably protect the security and confidentiality of the clients' documents and information.[58]
>
> It is also important that lawyers recognize their own competence limitations regarding computer security measures and take the necessary time and energy to become competent or alternatively consult available experts in the field.[59]

Likewise, Opinion 842 of the New York State Bar Association requires lawyers to "stay abreast of technological advances,"[60] and Minnesota's Rule 1.6 requires that

> A lawyer must act competently to safeguard information relating to the representation of a client against inadvertent or unauthorized disclosure by the lawyer *or other persons* who are participating in the representation of the client or who are subject to the lawyer's supervision.[61]

56. State Bar of California Standing Comm. on Prof'l Responsibility & Conduct, Formal Op. Interim No. 08-0002 (2010), *available at* http://www.calbar.ca.gov/LinkClick.aspx?fileticket=odIjrEe0wjI%3d&tabid=2167.

57. Alabama State Bar, Ethics Op. 2010-02 (2010), *available at* http://www.alabar.org/ogc/fopDisplay.cfm?oneId=425.

58. State Bar of Ariz., Ethics Op. 09-04 (2009), *available at* http://www.myazbar.org/ethics/opinionview.cfm?id=704 (citations and quotations omitted).

59. *Id.*

60. New York State Bar, Ass'n Comm. on Prof'l Ethics, Op. 842 (2010), *available at* http://www.nysba.org/AM/Template.cfm?Section=Ethics_Opinions&CONTENTID=42697&TEMPLATE=/CM/ContentDisplay.cfm (quoting New York State Bar, Ass'n Comm. on Prof'l Ethics, Op. 782 (2004)).

61. MINN. RULES PROF'L. CONDUCT R. 1.6 cmt. 15 (2005) (emphasis added); *see also* Minnesota Lawyers Prof'l Responsibility Bd., Op. No. 22 (2010), *available at*

Another concern regarding lawyer supervision is whether lawful data-mining performed by investigators at the behest of attorneys outside of the formal discovery process could lead to invasion of privacy, intrusion upon seclusion, or other tort liability.[62] A few prominent cases suggest that individuals maintain a privacy right in data that can be reconstructed through aggregation and inference.[63] In *United States v. Maynard*,[64] the U.S. Court of Appeals for the D.C. Circuit, faced with the question of whether evidence obtained by police through the warrantless search of a GPS device was admissible, concluded that the defendant had a reasonable expectation of privacy in the sum of his movements, even though he had no expectation of privacy in his individual movements exposed to the public.[65]

Whereas the sum of one's movements being entitled to an expectation of privacy may seem novel, it is well settled as to the sanctity of the home.[66] And yet, new technologies will continue to test the limits of that expectation, such as a new geo-location technique announced by researchers from the University of Electronic Science and Technology in China and Northwestern University: they claim the ability to locate a target computer on the Internet to within 2,250 to 328 feet, a few blocks.[67]

http://lprb.mncourts.gov/rules/LPRBOpinions/Opinion%2022.pdf.

62. *See, e.g.*, Marshall Tanick, *The Privacy Paradox,* 65 BENCH & BAR MINN. 8 (Sept., 2008) (discussing privacy and investigative issues, and collecting cases).

63. *See, e.g.*, U.S. Dep't of Def. v. Fed. Labor Relations Auth., 510 U.S. 487, 500 (1994) ("An individual's interest in controlling the dissemination of information regarding personal matters does not dissolve simply because that information may be available to the public in some form."); United States v. Maynard, 615 F.3d 544, 558 (D.C. Cir. 2010).

64. 615 F.3d at 558 ("[The] whole reveals more—sometimes a great deal more—than does the sum of its parts.").

65. *Id.*

66. Griffin v. Wisconsin, 483 U.S. 868, 884 (1987) (noting that under the Fourth Amendment, it is axiomatic that people have a reasonable expectation of privacy in their own homes).

67. The researchers used Google Maps to physically locate over 76,000 known web servers, and measured the time it takes to send a data packet to a target. They then converted the time to a distance measurement. Where the target and any of the 76,000 web servers shared a common "hop" (a router connection) in the transmission, the researchers compared the time difference between the mapped Web servers and the common hop, and between the target and common hop. After performing multiple repetitive traces, the researchers claimed to locate the target computer to within 2,250 to 328 feet, thereby narrowing the location to within a few streets. Their findings were disclosed on April 1, 2011 at the 8th Usenix Symposium on Networked Systems Design and Implementation in Boston. Yong Wong et al., *Towards Street-Level Client-Independent IP Geolocation*, USENIX.ORG

In situations where technological tools or processes not readily available to the public are used to reveal the physical location of an internet user, it's not difficult to imagine that a court might look to *Kyllo v. United States* for the proposition that an individual's reasonable expectation of privacy has been violated.[68] But, if *Boring v. Google*[69] is any indication of a trend, tort plaintiffs must establish they've suffered some greater injury than having their approximate physical locations discovered through IP address routing. In *Boring*, plaintiff property owners filed suit against the internet search provider giant alleging, inter alia, invasion of privacy and trespass because Google publicly provided digital photographs of plaintiffs' home and property without their authorization. The court found that plaintiffs failed to allege facts showing the intrusion was substantial, highly offensive, or transgressed decency standards.[70]

C. The Digital Forensics Examiner's Obligations in a Litigation Support Role

As noted above, significant legal and ethical challenges confront digital forensics investigators, for which they are ill prepared. Accordingly, the focus of this Comment is not on the particular technical qualifications of the expert or methodologies necessary to establish admissibility under Rule 702 of the Federal Rules of Evidence, and *Daubert* and *Kumho Tire* (or state equivalents).[71] Indeed, digital forensics is a discipline that is inherently inhospitable to pretenders, because it is based upon the existence or non-existence of binary data, which ordinarily is discernable through proven, industry-standard, repeatable means. And: "Where a proffered expert knows himself or herself to be a

(Mar. 06, 2011), http://www.usenix.org/events/nsdi11/tech/full_papers/Wang_Yong.pdf.

68. 533 U.S. 27, 40 (2001) ("Where, as here, the Government uses a device that is not in general public use, to explore details of a private home that would previously have been unknowable without physical intrusion, the surveillance is a 'search' . . . .").

69. 598 F. Supp. 2d 695 (W.D. Pa. 2009), *aff'd in part, rev'd in part*, 362 F. App'x 273 (3d Cir. 2010).

70. *Id.* at 700.

71. FED. R. EVID. 702; Kumho Tire Co. Ltd. v. Carmichael, 526 U.S. 137, 141 (1999) (extending the *Daubert* standard to all expert testimony); Daubert v. Merrell Dow Pharm., Inc., 509 U.S. 579, 597 (1993) (holding that a trial judge is the "gatekeeper" of scientific testimony and may admit scientific testimony that is not generally accepted so long as the testimony is relevant and reliable).

quack or otherwise to be offering false testimony, the situation is like that of any other witness who is perpetrating a fraud on the court. Such acts are illegal as well as unethical."[72]

It is the legal and ethical issues that warrant further discussion. Just as a lawyer may be confounded by technology in dealing with digital forensics matters, many (perhaps most) digital forensics experts lack formal legal training, and are uninformed about their special obligations in the employ of a lawyer. These obligations include zealously guarding the attorney-client privilege, applying the work product doctrine, developing reports, exhibits, and testimony (that are both admissible and understandable to a lay jury or judge), and conducting their work in a way that does not compromise the integrity of the case or the rights, privileges, or immunities of the retaining party.

In certain situations, such as where digital forensics examiners serve as special masters[73] or third-party neutrals,[74] they are regarded as officers of the court, entitled to quasi-judicial immunity.[75] The use of a third-party neutral has significant advantages.[76] First, as an

72. Michael J. Saks, *Scientific Evidence and the Ethical Obligations of Attorneys*, 49 CLEV. ST. L. REV. 421, 425 (2001).

73. *See* FED. R. CIV. P. 53 (authorizing the court to appoint one who performs certain duties consented to by the parties, and hold trial proceedings and make or recommend findings of fact on issues to be decided without a jury, if the appointment is warranted by (1) some exceptional condition; (2) the need to perform accounting or resolve a difficult computation of damage; or (3) the need to address pre-trial and post-trial matters that cannot be effectively and timely addressed by an available Article III judge or magistrate judge).

74. MODEL RULES OF PROF'L CONDUCT R. 2.4 cmt. 1 (2009).

> A third-party neutral is a person, such as a mediator, arbitrator, conciliator or evaluator, who assists the parties, represented or unrepresented, in the resolution of a dispute or in the arrangement of a transaction. Whether a third-party neutral serves primarily as a facilitator, evaluator or decisionmaker depends on the particular process that is either selected by the parties or mandated by a court.

Id.

75. *See, e.g.*, Meyers v. Contra Costa Cnty. Dep't of Soc. Servs., 812 F.2d 1154, 1159 (9th Cir. 1987) ("[Investigators reporting to the court are] officers of the court [because they are] performing a judicial function at the direction of [the] court."); Ogden v. Ogden, 39 P.3d 513, 516 (Alaska 2001) ("[C]ourt-appointed custody investigators are officers of the court and perform quasi-judicial functions . . . ."); Davidson v. Sandstrom, 83 P.3d 648, 655 (Colo. 2004) (defining "investigators" as officers of the court); Kahre v. Kahre, 916 P.2d 1355, 1362 (Okla. 1995) (stating that investigators are officers of the court); s*ee also* Douglas R. Richmond, *The Emerging Theory of Expert Witness Malpractice*, 22 CAP. U. L. REV. 693, 706–09 (1993).

76. *See, e.g.*, Craig Ball, *Neutral Examiners*, FORENSIC FOCUS, http://www.forensicfocus.com/index.php?name=Content&pid=346 (last visited

officer of the court, the expert is subject to the court's inherent powers, thereby providing an extra measure of accountability for misconduct (e.g., confidentiality breaches).[77] Second, a third-party neutral is ostensibly impartial, and this impartiality presumptively aids in the fact-finding process and administration of justice. Third, the third-party neutral is aptly situated to resolve discovery disputes, including issues of confidentiality, relevance, and privilege, and, if necessary, obtain court intervention or in camera review to resolve such disputes.

If the examiner is not appointed by the court, but rather is retained by a party to an adversarial proceeding, he or she is nevertheless obliged to ferret out the truth.[78] Thus, in *Ferron v. Search Cactus, LLC*,[79] a U.S. district court deemed both the plaintiff's and the defendant's computer experts as officers of the court in order to protect the confidentiality of certain ESI found on the plaintiff's computer that was unrelated to the suit.

1. Work Product Doctrine

The work product doctrine enhances a lawyer's ability to render competent counsel, as the U.S. Supreme Court observed in

Sept. 11, 2011).

77. *See* Jones v. Lincoln Elec. Co., 188 F.3d 709, 738 (7th Cir. 1999) (holding that an expert witness is subject to court's remedial contempt authority); United States v. Paccione, 964 F.2d 1269, 1274–75 (2d Cir. 1992) ("A court may bind non-parties to the terms of an injunction or restraining order to preserve its ability to render a judgment in a case over which it has jurisdiction.").

78. NELSON ET AL., *supra* note 12, at 523 ("Your only agenda should be finding the truth, so don't think in terms of catching somebody or proving something. It's not your job to win the case. Don't become an advocate . . . ."); Sharon D. Nelson & John W. Simek, *Electronic Evidence: The Ten Commandments*, SENSEI ENTERPRISES, INC. (2003), http://www.senseient.com/articles/pdf/article18.pdf ("[G]ood experts are seekers of truth and will report their findings regardless of what those findings may be."). *Contra* Hutchinson v. People, 742 P.2d 875, 882 (Colo. 1987) ("As a practical matter, too, an expert hired by defense counsel is likely to feel a degree of loyalty to the defendant's cause. We need not ascribe this fact to base motives on the part of the experts; indeed, the nature of the adversary process, the confidentiality surrounding legal representation and professional norms and ethics of particular experts all may foster this attitude of loyalty to the defendant."); Christa L. Klopfenstein, *Discoverability of Opinion Work Product Materials Provided to Testifying Experts*, 32 IND. L. REV. 481, 503 (1999) ("Unlike other types of trial witnesses, experts are part of a party's litigation team who, like the attorney, are employed expressly for the purpose of analyzing the strengths and weaknesses of a party's case. . . . Experts are not impartial witnesses. Like attorneys, they are paid to advocate a point of view.").

79. No. 2:06-CV-327, 2008 WL 1902499, at *4 (S.D. Ohio Apr. 28, 2008).

Hickman v. Taylor:

> [I]t is essential that a lawyer work with a certain degree of privacy, free from unnecessary intrusion by opposing parties and their counsel. Proper preparation of a client's case demands that he assemble information, sift what he considers to be the relevant from the irrelevant facts, prepare his legal theories and plan his strategy without undue and needless interference.[80]

It is therefore imperative that both attorneys and examiners understand the doctrine and how it applies to digital forensics examinations. Enjoying the privilege of work product immunity is one of several reasons the expert should be directly retained by the attorney, rather than the attorney's client.[81]

Some practitioners conflate the work product doctrine with the attorney-client privilege (discussed below). Although the work product doctrine is broader than the attorney-client privilege, it is not a privilege, but rather a limited immunity from production, which can be overcome in certain situations.[82] The doctrine applies in both civil and criminal cases,[83] and protects not only documents and tangible things prepared by attorneys, but also those prepared by an attorney's "consultant, surety, indemnitor, insurer, or agent."[84] In the context of such examinations, the work product doctrine also covers the "mental impressions, conclusions, opinions, or legal theories of a party's attorney or other representative concerning the litigation."[85] A prudent expert

80. 329 U.S. 495, 510–11 (1947).

81. Other reasons the attorney should maintain the role of "quarterback," and that the expert should have very limited interaction with the client, include: preventing an attorney-client relationship from forming between the expert and client (if the expert also is an attorney, and the expert is likely to testify); avoiding fee disputes from arising between the client and expert; and maintaining the scope and strategy of the case. *See infra* note 111 and accompanying text; *supra* notes 33–34 and accompanying text.

82. *Hickman*, 329 U.S. 495 at 510–15 (holding that courts may order production of some materials protected by the work product doctrine under certain circumstances); *see also* FED. R. CIV. P. 26(b)(3)(A) ("[The] materials may be discovered if . . . they are otherwise discoverable under Rule 26(b)(1); and . . . the party shows that it has substantial need for the materials to prepare its case and cannot, without undue hardship, obtain their substantial equivalent by other means.").

83. United States v. Nobles, 42 U.S. 225, 236 (1975).

84. FED. R. CIV. P. 26(b)(3)(A).

85. FED. R. CIV. P. 26(b)(3)(B); *see also In re* San Juan Dupont Plaza Hotel Fire Litig., 859 F.2d 1007, 1014 (1st Cir. 1988) ("[The work product doctrine provides] a zone of privacy within which to prepare the client's case and plan strategy,

should, therefore, take affirmative steps to keep confidential the software and hardware used during the examination, as well as his or her theories, algorithms, cryptology, notes, tools, processes, methods, search queries, resource materials, mental impressions, and techniques. And, because the doctrine may be overcome in limited circumstances, attorneys should give careful consideration to whether they instruct their experts to memorialize preliminary findings in writing, or whether to destroy (or refrain from retaining) draft reports.[86]

In 2010, Federal Rule of Civil Procedure 26 was amended to give experts' draft reports the protection of the work product doctrine, exempting them from mandatory disclosure. The rule expressly provides that the doctrine applies to "protect drafts of any report or disclosure required under Rule 26(a)(2), regardless of the form in which the draft is recorded."[87] The amended rule also applies work product protection to communications between experts and the counsel who retain them,[88] with three exceptions: (1) communications pertaining to the expert's compensation; (2) facts or data that the attorney provided and the expert considered in forming opinions; and (3) assumptions that the attorney provided and that the expert relied on.[89] Critics contend the amendment affords attorneys too much latitude in drafting

without undue interference."); United States v. Horn, 811 F. Supp. 739 (D. N.H. 1992), *aff'd as to issue of work product doctrine*, *rev'd on other grounds*, 29 F.3d 754 (1st Cir. 1994); Stanley D. Davis & Thomas D. Beisecker, *Discovering Trial Consultant Work Product: A New Way to Borrow an Adversary's Wits?*, 17 AM. J. TRIAL ADVOC. 581, 619 (1994) ("[T]he attorney's discussions of case theory and the consultant's suggestions thereon should qualify for the higher protection accorded mental impressions.").

86. *See, e.g.*, NELSON ET AL., *supra* note 12, at 348–49 ("[The forensic tool] also produces a case log file, where you can maintain a detailed record of all activities during your examination, such as keyword searches and data extractions. . . . At times, however, you might not want the log feature turned on. If you're following a hunch, for example, but aren't sure the evidence you recover is applicable to the investigation, you might not want opposing counsel to see a record of this information because he or she could use it to question your methods and perhaps discredit your testimony. . . . Look through the evidence first before enabling the log feature to record searches. This approach isn't meant to conceal evidence; it's a precaution to ensure that your testimony can be used in court."). *But see* Univ. of Pittsburgh v. Townsend, No. 3:04-CV-291, 2007 U.S. Dist. LEXIS 24620 (E.D. Tenn. Mar. 30, 2007) (holding that it was improper for the counsel to have instructed or otherwise suggested to the experts that all e-mails be destroyed, as they became the subject of multiple discovery requests).

87. FED. R. CIV. P. 26(b)(4)(B).

88. FED. R. CIV. P. 26(b)(4)(C).

89. *Id.*

experts' reports or influencing their opinions.[90] The counter argument is that "[t]he risk of an attorney influencing an expert witness does not go unchecked in the adversarial system, for the reasonableness of an expert opinion can be judged against the knowledge of the expert's field and is always subject to the scrutiny of other experts."[91]

One area of particular concern relating to the work product doctrine and digital forensics investigations is the applicability of the Adam Walsh Act and similar state statutes. Under 18 U.S.C. § 3509(m), added by § 504 of Title V of the Adam Walsh Act, "any property or material that constitutes child pornography . . . shall remain in the care, custody, and control of either the Government or the court."[92] Title V of the Act contains congressional findings that: "[e]very instance of viewing images of child pornography represents a renewed violation of the privacy of the victims and a repetition of their abuse"; that "[c]hild pornography constitutes prima facie contraband, and as such should not be distributed to, or copied by, child pornography defendants or their attorneys"; and that "[i]t is imperative to prohibit the reproduction of child pornography in criminal cases so as to avoid repeated violation and abuse of victims, so long as the government makes reasonable accommodations for the inspection, viewing, and examination of such material for the purposes of mounting a criminal defense."[93]

"Ample opportunity" and "reasonable access" under the Act requires: (1) "the government [to] . . . supply reasonably up-to-date tools (hardware and software) and facilities [in order to] . . . construct a reasonable, available forensic defense," (2) "[the ability of] a defense expert to utilize his or her hardware or software," and (3) "that the analysis be performed in a situation where attorney-client privilege and work product will not be easily, accidentally exposed to the government, and in a facility which is open to the defense at its request during normal working hours, and to the extent feasible, during non-working hours."[94] In *State v. Boyd*,[95] the

90. Robert Ambrogi, *Changes to Rule 26 Bring Praise — Albeit Faint*, BULLSEYE LEGAL BLOG (June 1, 2011), http://www.ims-expertservices.com/blog/2011/changes-to-rule-26-brings-praise-albeit-faint.

91. Haworth, Inc. v. Herman Miller, Inc., 162 F.R.D. 289, 295–96 (W.D. Mich. 1995).

92. 18 U.S.C. § 3509(m)(1) (2006).

93. Adam Walsh Child Protection and Safety Act of 2006, Pub. L. No. 109-248, §§ 501(2)(D)–(F), 120 Stat. 587, 624 (2006).

94. United States v. Flinn, 521 F. Supp. 2d 1097, 1101 (E.D. Cal. 2007).

Supreme Court of Washington held that preparation for trial would "likely require revisiting the evidence many times before and during trial" and, therefore, where the evidence consists of a computer hard drive, "adequate representation requires providing a 'mirror image' of that hard drive; enabling the defense attorney to consult with computer experts who can tell how the evidence made its way onto the computer," and that anything less could place an undue burden on defense counsel or a defense expert, interfering with a defendant's constitutional rights.[96]

In this examiner's experience, most government agencies endeavor to provide reasonable access, but others, perhaps well-meaning, have sought to dictate what equipment the defense expert may use (including the number of computers, and a restriction of both optical read/write drives and solid state drives), or have proposed the examiner work in a small room alongside state staff,[97] or have required the examiner to use state equipment to conduct Internet research during the examination,[98] or have proposed limiting the examiner to a black-and-white printout of the forensic report or to an electronic copy on a read/write optical device supplied by the state, and have insisted that the work product be inspected by a state employee prior to removal from the facility.[99] The foregoing limitations not only violate the work product doctrine, but also implicate a defendant's right to effective

95. 158 P.3d 54, 57–62 (Wash. 2007).

96. *Id.* at 60–61.

97. *See* United States v. Winslow, No. 3:07-CR-00072-TMB-DMS, 2008 U.S. Dist. LEXIS 66855, at *6 (D. Alaska Jan. 28, 2008). The *Winslow* court examined the lack of privacy caused by placing a government agent inside the room with defense experts, such that the experts were not able to have the requisite confidentiality needed to talk about the results with other experts and to talk with defense counsel about their findings, and also because the agents inside the room may be distracting. "These restrictions impermissibly intrude upon both the defendant's Fifth and Sixth Amendment rights and are insufficient to 'assure the thorough preparation and presentation of each side of the case' allowing for a 'fair and accurate resolution of the question of guilt or innocence.'" *Id.* (quoting United States v. Nobles, 422 U.S. 225, 238–39 (1975)).

98. *See* State v. Johnson, No. 1 CA-CR 09-0300, 2010 WL 1424369, at *5 (Ariz. Ct. App. Apr. 8, 2010) ("[Defendant] argues that the expert could not access her reference materials if required to conduct the exam at the FBI office. . . . [The] argument is persuasive. The State did not proffer a remedy to the expert's inability to access her reference materials at the FBI facility.").

99. *See* United States v. Bortnick, No. 08-20151-CM, 2010 U.S. Dist. LEXIS 23407, at *9 (D. Kan. Mar. 11, 2010) (holding that electronic search imposes an unreasonable restriction on the defendant's ability to prepare a defense).

counsel and due process,[100] and are likely to result in relinquishment of the media containing the contraband to the defense expert under the Act's so-called "safety valve."[101]

2. Attorney-Client Privilege and Confidentiality

The attorney-client privilege is one of the most hallowed tenets of American common law.[102] The primary function of the privilege "is to encourage full and frank communication between attorneys and their clients and thereby promote broader public interests in the observance of law and administration of justice."[103] Without the privilege, which withholds otherwise relevant evidence, "the client would be reluctant to confide in his lawyer and it would be difficult to obtain fully informed legal advice."[104] In general, communications are protected under the attorney-client privilege if (1) a person is seeking legal advice from a lawyer acting in his legal capacity, (2) the communication is made for the purpose of obtaining legal advice, (3) the communication is made in confidence, and (4) the communication is made by the client.[105] So, how might this apply to digital forensics examinations?

> [A]s both a legal and practical matter, the defense expert's relationship with the defendant and counsel has been protected from intrusions by the state. The law has recognized several doctrines that afford a degree of confidentiality to the expert-defense relationship. Thus, statements made to the expert by the defendant and counsel may be protected by the attorney-client privilege.[106]

Compare the foregoing pronouncement from one state court with

100. Sharon Nelson et al., *In Defense of the Defense: The Use of Computer Forensics in Child Pornography Cases*, SENSEI ENTERPRISES, INC. (2009), http://www.senseient.com/articles/pdf/In_Defense_of_the_Defense.pdf.

101. 18 U.S.C. § 3509(m)(2)(B) (2006); *see, e.g.*, State v. Allen, No. E2007-01018-CCA-R3-CD, 2009 Tenn. Crim. App. LEXIS 114, at *17–19 (Tenn. Crim. App. Feb. 12, 2009) (applying 18 U.S.C. § 3509); United States v. Knellinger, 471 F. Supp. 2d 640, 650 (E.D. Va. 2007) (applying 18 U.S.C. § 3509 as well).

102. Upjohn Co. v. United States, 449 U.S. 383, 389 (1981) (citing 8 J. WIGMORE, EVIDENCE § 2290 (McNaughton rev. 1961)).

103. *Id.*

104. Fisher v. United States, 425 U.S. 391, 403 (1976).

105. United States v. El Paso Co., 682 F.2d 530, 538 n.9 (5th Cir. 1982) (quoting 8 J. WIGMORE, EVIDENCE § 2292 (McNaughton rev. 1961)); RESTATEMENT (THIRD) OF THE LAW GOVERNING LAWYERS § 68 (2000).

106. Hutchinson v. People, 742 P.2d 875, 881 (Colo. 1987).

that from another: "Attorney-client privilege is perhaps a misnomer, since only the client's statements enjoy a privilege. Communications of the attorney, on the other hand, are not privileged, except to the narrow extent to which they reveal communications made by the client."[107] Courts may, indeed, construe a client's direct communications to the digital forensics expert as privileged, if the expert is regarded an agent of the attorney.[108] And it is true that an expert is not considered a third-party whose presence destroys the privilege if the expert's presence is deemed necessary to secure and facilitate communication between the client and the attorney (not unlike an interpreter).[109] But it does not appear to this commentator that communications between an attorney and an expert should be afforded attorney-client privilege sui generis, because these are not communications made in confidence to an attorney while seeking legal advice.[110]

This view notwithstanding, both the expert and the attorney would owe a duty to the client—the holder of the privilege—to maintain confidentiality. The attorney's obligation is detailed in the Model Rules of Professional Conduct in Rules 1.6 (governing disclosure by a lawyer of information relating to the representation of a client during the lawyer's representation of the client),[111] 1.18

107. Kennedy v. Yamaha Motor Corp., 2010 Phila. Ct. Com. Pl. LEXIS 24, at *4 (Pa. C.P. Feb. 2, 2010).

108. Fin. Techs. Int'l, Inc. v. Smith, 49 Fed. R. Serv. 3d 961, 967 (S.D.N.Y. 2000).

109. *See* United States v. Kovel, 296 F.2d 918, 921–22 (2d Cir. 1961); *see also In re* Grand Jury Proceedings, 220 F.3d 568, 571 (7th Cir. 2000) ("However, material transmitted to accountants may fall under the attorney-client privilege if the accountant is acting as an agent of an attorney for the purpose of assisting with the provision of legal advice."); United States v. Cote, 456 F.2d 142, 143 (8th Cir. 1972) ("[The] test is whether the [expert's] services are a necessary aid to the rendering of effective legal services to the client."). *But see* United States v. Ackert, 169 F.3d 136, 139 (2d Cir. 1999) (holding the privilege is vitiated by the presence of third parties who do not translate information from the client to the attorney but rather provide information independently to the attorney).

110. *See* Matthew P. Matiasevich, *I (Might) Get By With a Little Help from my Expert: Expert Witnesses in Trust and Estate Litigation* (May 6–7, 2010), http://www.americanbar.org/content/dam/aba/events/real_property_trust_estate/symposia/2011/rpte_symposia_2011_m2903_te_expert_help_litigation.authcheckdam.pdf. Matiasevich presented at the 21st Annual Spring Symposia of the ABA Section of Real Property, Trust, and Estate Law. "The attorney-client privilege rarely applies to experts for the simple reason that the expert is almost never the client and hence communications are not confidential." *Id.*

111. MODEL RULES OF PROF'L CONDUCT R. 1.6 (1983). Other professionals, such as accountants, are governed by similar rules. *See* MINN. STAT. §§ 326A.12–A.13 (2010) (discussing confidential communications, working papers, and

(the lawyer's duties regarding information provided to the lawyer by a prospective client),[112] and 1.9 (the lawyer's duty not to reveal information relating to the lawyer's prior representation of a former client).[113] But the expert, who usually is not present at the time of the communication, is also obliged to zealously protect any information the expert discovers that implicates communications made by the client to his or her attorney.

Further, this expert obligation may be yet another compelling reason why an expert ideally should have legal acumen, because he or she needs to correctly recognize and, as necessary, segregate attorney-client privileged data. For example, if the expert encounters e-mails between a client and her attorney, which the client subsequently forwarded to a friend, will the expert recognize a privilege?[114] When in doubt, the expert should consider the communication privileged and consult with the attorney. Note this exhortation reveals that the integrity of the privilege itself could depend upon the integrity of the communication channel between the expert and the attorney.

Attorney-client privilege aside, a competent digital forensics expert should also have background and training in information security protocols and be able to observe strict confidentiality of all data entrusted to him or her:

> Not all cases are shrouded in secrecy, but a fair proportion of them are. There are well known figures getting divorced, major companies with proprietary information at issue, public figures in the headlines and people charged with felonies. . . . During the course of a major case where the expert has been identified, the press will undoubtedly come sniffing around the expert probing for information. A good expert knows the standard answer, 'I'm sorry, I have no comment' and is as immoveable as the Great Wall of China.[115]

clients' records).

112. MODEL RULES OF PROF'L CONDUCT R. 1.18 (1983).

113. *Id.* R. 1.9.

114. In this example, whether the e-mail is privileged depends on whether the jurisdiction recognizes the so-called selective-waiver doctrine. *See* Jonathan Feld & Blake Mills, *The Selective-Waiver Doctrine: Is It Still Alive?,* 16 BUSINESS CRIMES BULLETIN 4, 4 (Dec. 2008), http://www.kattenlaw.com/files/Publication/30990f16-1392-4523-928a-0ffd17e4c01a/Presentation/PublicationAttachment/2c7f533d-947f-427c-9773-179747282b76/Feld–Business_Crimes–Selective_Waiver.pdf (discussing the origins of the selective-waiver doctrine).

115. Sharon D. Nelson & John W. Simek, *Finding Wyatt Earp: Your Computer*

A recent Associated Press article, *Anthony Computer Expert Backs Off Reported Claims,* demonstrates the foregoing point well.[116] But, because the Rules of Professional Conduct do not apply to digital forensics examiners, the only enforcement mechanisms are contractual provisions (i.e., a confidentiality clause in the retainer agreement) and "loss of reputation and business."[117] The prudent attorney should, therefore, include a confidentiality provision in the engagement agreement, which may give rise to a breach of contract action if damages are sustained. Also, if the expert is retained while a case is active, either or both parties may move the court for a protective order regarding the expert's handling of confidential data, under which the expert would be subject to the court's inherent supervisory powers, including sanctions and contempt authority.[118]

Finally, cautious practitioners should also consider whether a compromise of the client's data by the expert could be imputed to the attorney. As discussed in an earlier section of this Comment, if the attorney knew or had reason to know that the expert would breach the attorney-client privilege (or otherwise compromise the client's confidential data), or if the attorney failed to obtain adequate assurances that the data would be secure while in the expert's custody, the attorney may be subject to discipline.[119]

3. The Expert's Report

Whether a digital forensics examiner will likely prepare a written report depends on the nature of the case, the examiner's initial impressions, the attorney's case strategy, and the jurisdiction. If the expert plans to testify in federal court and most state courts, a written report is mandatory unless otherwise stipulated or ordered by the court.[120] Although the expert's identity must be disclosed as

Forensics Expert, SENSEI ENTERPRISES, INC. (2005), http://www.senseient.com /articles/pdf/Finding_Wyatt_Earp.pdf.

116. Kyle Hightower, *Anthony Computer Expert Backs Off Reported Claims*, ABC NEWS (July 20, 2011), http://abcnews.go.com/US/wireStory?id=14115919.

117. Order Granting Motion to Compel Discovery at 10, State v. Blount, No. 81-CR-09-1180 (Minn. Dist. Ct. Apr. 7, 2010) ("The Court does not believe a violation of this protective order is likely, as any violation by defense counsel could adversely affect the attorney's license to practice and a violation by [the digital forensics expert] could result in loss of reputation and business.").

118. *See* MODEL RULES OF PROF'L CONDUCT R. 2.4 cmt. 1 (2009).

119. *See supra* text accompanying notes 54–58.

120. Fed. R. Civ. P. 26(2)(B).

part of the initial disclosures, "it is not uncommon for parties to agree to a different disclosure date as part of a pre-trial scheduling order.[121] Sometimes even the disclosure of the expert's identity is pushed off into the future per the scheduling order."[122]

As noted in a prior section of this Comment, Rule 26(a) of the Federal Rules of Civil Procedure was recently amended to protect draft reports from disclosure.[123] Prior to the rule amendment, and in states that have not adopted similar provisions, it is this examiner's experience that the standard practice has been to refrain from memorializing initial impressions in the form of notes or draft reports until the examiner and attorney have taken the opportunity to confer. If the examiner's preliminary findings and impressions appear to be unhelpful to the attorney's theory of the case, the attorney will usually halt further analysis and not call the expert to testify. Likewise, if the examiner is using a tool that includes case logging, such as earlier versions of AccessData FTK, enabled by default, the examiner should be instructed as to when and whether to disable it.[124]

And although it is beyond the scope of this Comment to discuss the structure of the expert's report and all that it should contain, a few words should be said about what the report should not contain. The report should not be tailored to support a particular outcome, as a material omission may constitute fraud.[125] Examiners must resist overtures by attorneys, however well-intended or abstract, to submit any testimony or work product that is disrespectful of the truth, including overstating, understating, or omitting findings. The findings, however, should be concise and carefully circumscribed. The report should not volunteer an overabundance of information, which may be vulnerable to scrutiny under cross-examination.[126] Further, all findings should be

121. Fed. R. Civ. P. 26(2)(A) (requiring that witnesses intended to be used at trial who will present evidence under Federal Rules of Evidence 702, 703, or 705 (the specific rules that apply to expert testimony) be disclosed in the initial witness disclosure required under Fed. R. Civ. P. 26(a)(1)).

122. Bruce A. Olson, *Preparing an Expert Report*, DIGITAL FORENSIC INVESTIGATOR NEWS, 1 (July 13, 2011), http://www.dfinews.com/article/preparing-expert-report.

123. Fed. R. Civ. P. 26(b)(4)(B)–(C).

124. *See supra* note 86 and accompanying text.

125. Fraud is defined as "[a] knowing misrepresentation of the truth or concealment of a material fact to induce another to act to his or her detriment." BLACK'S LAW DICTIONARY 731 (9th ed. 2009).

126. *See* Olson, *supra* note 122, at 3 ("Avoid volunteering information that is not specifically relevant. You are writing a report, not a thesis. If you volunteer

accurately qualified as to the limitations of the particular tool(s) used, the applicability of the current technology and industry standard best practices,[127] the methodology or techniques (such as search criteria or formulae), and the scope of the investigation. The scope of the investigation is not only limited by relevancy, but also by budget (i.e., time),[128] which almost always places legitimate and significant constraints on what data is found or not found, and the inferences to be drawn therefrom.

Data not found has an important, often overlooked, place in the report and may be as important (or more important) than what was found. When an examiner, through experience and information generally accepted in the profession, expects to find certain metadata (such as a browser internet history) or data to which extant metadata refers—but does not find this metadata or data—it should be so noted (also subject to the qualifications more fully discussed hereinabove). The absence of this metadata or data, whether in allocated (not deleted) or unallocated (deleted but recoverable) areas of the media, must be attributed to automated or manual processes, if possible. The examiner and attorney must then confer to determine whether the absence is the result of inadvertent spoliation, such as a defragmentation utility or metadata removal tool used for legitimate data privacy purposes, or intentional spoliation by the user.

D. Legality of Digital Forensics Investigation Techniques

Another important factor for consideration by both attorneys and examiners in digital forensics investigations is the legality of investigation techniques. Consider, for example, whether an attorney or the examiner may take possession of a computer

too much, all you are doing is providing the opposing attorney with ammunition to use in cross examination.").

127. For example, at the time of this writing, there is some debate between experts and vendors as to the methods for reliably recovering data from Microsoft Windows 7 "shadow volumes." The best practice, therefore, may evolve as the technology is better understood, if Microsoft alters the technology through patches, or if third-party products are able to alter or disable the feature.

128. *See* Kerr, *supra* note 36; *see also* NELSON ET AL., *supra* note 12, at 517 ("The . . . attorney . . . should define the investigation's goal or mission. All reports to the [attorney] should start by stating this mission or goal, which is usually to find information on a specific subject, recover certain important documents, or recover certain types of files or files with specific dates and times. Clearly defining the goals reduces the time and cost of the examination and is especially important with the increasing size of hard drives and networks.").

belonging to a husband but seized by a wife in preparation for marital dissolution proceedings. If a court finds that the wife did not have equal dominion over the computer (e.g., if the computer, or some portion thereof, was password-protected by the husband or belonged to the husband's employer), the taking of the computer for analysis might constitute a crime.[129] Likewise, evidence obtained from a keylogger or spyware deployed by the client or examiner may violate state or federal law (e.g., the Stored Communications Act).[130]

Also, certain types of "cyber sleuthing" or penetration testing may be unlawful under various state and federal statutes. For example, the Computer Fraud and Abuse Act, last amended in 2008, criminalizes anyone who commits, attempts to commit, or conspires to commit an offense under the Act.[131] Offenses include knowingly accessing without authorization a protected computer (for delineated purposes) or intentionally accessing a computer without authorization (for separately delineated purposes). Practitioners should be aware that various statutory phrases, such as "without authorization" and "access," have been the continuing subject of appellate review.[132]

Yet another area of legality concerns recently enacted laws in some states requiring digital forensics examiners to be licensed as private investigators. Texas passed such a law that provides for up to one year imprisonment and a $14,000 fine for persons

129. *See* Moore v. Moore, No. 350446/07, 2008 N.Y. Misc. LEXIS 5221, at *1 (N.Y. Sup. Ct. Aug. 4, 2008) (holding that a wife seeking a divorce could use evidence she found on a computer taken from husband's car just before she petitioned for marital dissolution because the computer was a family computer—not a work computer as alleged by husband—the taking occurred before the commencement of the dissolution case, and husband's car was considered the family car). *See generally* MINN. STAT. §§ 609.89, 609.891 (2010) (proscribing unauthorized computer access and theft).

130. Sean L. Harrington, *Why Divorce Lawyers Should Get Up to Speed on CyberCrime Law*, MSBA COMPUTER & TECH. L. SEC. (Mar. 24, 2010, 9:40 PM), http://mntech.typepad.com/msba/2010/03/why-divorce-lawyers-should-get-up-to-speed-on-cybercrime-law.html (collecting cases regarding unauthorized computer access).

131. 18 U.S.C. § 1030 (2006).

132. *See, e.g.*, State v. Allen, 917 P.2d 848 (Kan. 1996) (affirming the trial court's holding that the state did not prove the defendant committed a crime); *see also* Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. REV. 1596, 1624–42 (2003) (showing how and why courts have construed unauthorized access statutes in an overly broad manner that threatens to criminalize a surprising range of innocuous conduct involving computers).

conducting unlicensed computer investigations.[133] The attorney employing a non-licensed expert may also commit a criminal offense.[134] And Michigan's new law makes unlicensed digital forensics work a felony punishable by up to four years imprisonment, damages, and a $5,000 fine.[135] In 2008, North Carolina's Private Protective Services Board proposed to amend General Statute Section 74C-3 to include "Digital Forensic Examiner" among the roles that must be licensed by the state.[136] The measure was defeated.[137] Meanwhile, the American Bar Association has discouraged such legislation, observing, "[c]omputer forensic assignments often require handling data in multiple jurisdictions. For example, data may need to [be] imaged

133. TEX. OCC. CODE ANN. § 1702.104 (2011); *see also Private Security Bureau Opinion Summaries: Computer Forensics*, TEXAS DEP'T OF PUB. SAFETY, 4–5 (Aug. 21, 2007), http://www.txdps.state.tx.us/psb/docs/psb_opin_sum.pdf. The Opinion clarifies that the Act applies to computer forensics, defined as:

> [T]he *analysis* of computer-based data, particularly hidden, temporary, deleted, protected or encrypted files, for the purpose of discovering information related (generally) to the causes of events or the conduct of persons. We would distinguish such a content-based analysis from the mere scanning, retrieval and reproduction of data associated with electronic discovery or litigation support services.

Id. at 4.

134. TEX. OCC. CODE ANN. § 1702.386 (2011); *see also* Joseph L. Lanza, *Should Your Next Expert Witness Be a Licensed Private Investigator?*, 68 TEX. B.J. 118, 124 (2005) (discussing the Texas law, what it means to attorneys, who is exempt, and potential problems that may arise).

135. 2008 Mich. Pub. Acts 67.

136. Mack Sperling, *North Carolina May Require Licensing for Computer Forensic Consultants, but Do We Need It?*, NORTH CALOLINA BUS. LITIG. REP. (Sept. 24, 2008), http://www.ncbusinesslitigationreport.com/2008/09/articles/discovery-1/north-carolina-may-require-licensing-for-computer-forensic-consultants-but-do-we-need-it/ (reporting on proposed legislation and providing a draft at http://www.ncbusinesslitigationreport.com/uploads/file/Forensics%20Legislation.pdf).

137. S. 584, 2009 Gen. Assemb., Reg. Sess. (N.C. 2009), *available at* http://ncleg.net/Sessions/2009/FiscalNotes/Senate/PDF/SFN0584v3.pdf.

> [The Bill] [a]mends GS 74C-3(b) to exempt from the definition of *private protective services* a person engaged in (1) computer or digital forensic services or the acquisition, review, or analysis of digital or computer-based information, whether for the purposes of obtaining or furnishing information for evidentiary or other purposes, or for providing expert testimony before a court, or (2) network or system vulnerability testing, including network scans and risk assessment and analysis of computers connected to a network.

Id. at 1; *see also* North Carolina Statutes, LAWS.COM STATUTES, http://statutes.laws.com/north-carolina/Chapter_74C/GS_74C-3 (exempting digital forensic examiners) (last visited Sept. 9, 2011).

from hard drives in New York, Texas and Michigan. Does the person performing that work need to have licenses in all three states?"[138] The ABA Report concluded:

> The public and courts will be negatively impacted if e-discovery, forensic investigations, network testing, and other computer services can be performed only by licensed private investigators because not all licensed private investigators are qualified to perform computer forensic services and many qualified computer forensic professionals would be excluded because they are not licensed.[139]

Indeed, very few licensed private investigators are qualified to perform computer forensics services. At present, this commentator observes that the trend seems to be leading away from state licensing requirements and therefore is not likely to present a problem for most litigators seeking to retain digital forensic examiners.

Undoubtedly, one of the thorniest legal problems facing litigators and examiners is that of child pornography ("contraband") encountered in digital forensics investigations.[140] As discussed in a prior section of this Comment,[141] federal law prohibits the knowing production, receipt, shipment, distribution, reproduction, sale, or possession of any "visual depiction involv[ing] the use of a minor engaging in sexually explicit conduct," or of "any other material that contains an image of child pornography."[142] Violations are punishable by a mandatory minimum term of imprisonment for five years and up to twenty years,[143] except for mere possession, which is punishable for up to ten years.[144] Further, Congress, in enacting the Adam Walsh Act of 2006, reasoned that child pornography as prima facie contraband

138. Whittemore, *supra* note 14, at 14.

139. *Id.* at 2.

140. *See generally* BERYL HOWELL, DIGITAL CONTRABAND: FINDING CHILD PORN IN THE WORKPLACE, *reprinted in* WHITE COLLAR CRIMES 2008, ABA-CLE (2008), *available at* http://www.strozfriedberg.com/files/Publication/2ff70060-e3c5-43f8-bf98-024a2b4b3509/Presentation/PublicationAttachment/412a1aa4-562b-402d-800d-0097b96248b6/DigitalContrabandFindingChildPorntheWorkplaceWhiteCollarCrimeProgram.pdf.

141. *See supra* notes 92–96 and accompanying text; *see also* FED. R. CIV. P. 26(b)(4)(C); Ambrogi, *supra* note 90.

142. 18 U.S.C. §§ 2251(a), 2252(a), 2252A (a) (2006).

143. *Id.* §§ 1466A(a)(2)(B), 2252(b)(1), 2252A(b)(1).

144. *Id.* §§ 1466A(b)(2)(B), 2252(b)(2), 2252A(b)(2).

should not be distributed to or copied by defendants, their attorneys, or experts.[145] Therefore, an expert who encounters contraband during an investigation outside of a law enforcement facility must cease work and contact law enforcement to come to the place of the investigation to seize the contraband.[146] An expert or attorney who e-mails or delivers the contraband may be prosecuted for copying or distribution.[147]

It should be noted that § 3509(m) does not apply to state criminal proceedings; it expressly governs the Federal Rules of Criminal Procedure.[148] Although no Minnesota appellate court has yet ruled on the issue, a Minnesota district court, relying on the reasoning from appellate courts in Tennessee and Missouri, ruled that it does not apply to Minnesota state courts.[149] The court found that the State did provide reasonable access but, in light of the added costs of conducting the examination at law enforcement facilities ("approximately doubling the cost")[150] and severe funding cuts to the State Public Defender's Office, "[i]t would not be in the interests of the Public Defender's Office and the criminal justice system in general to have the Public Defender's Office unnecessarily expend additional funds to acquire the necessary forensic examination."[151] Accordingly, the court ordered a forensic copy be provided to the defense expert under a protective order,

145. Adam Walsh Child Protection and Safety Act, H.R. 4472, 109th Cong. § 501(2)(E) (2006).

146. NELSON ET AL., *supra* note 12, at 176 ("The evidence must be turned over to law enforcement. This material is contraband and must not be stored by any person or organization other than a law enforcement agency.").

147. United States v. Flynn, 709 F. Supp. 2d 737, 739 (D.S.D. 2010) (indicting an attorney—who claimed he was doing research for a potential client by investigating the existence of child pornography on a P2P network—for possession and distribution of child pornography); *see also* State v. Brady, No. 2005–A–0085, 2007 WL 1113969, at *2 (Ohio Ct. App. Apr. 13, 2007) (recounting that—notwithstanding a state court protective order—the Federal Bureau of Investigation executed a search warrant on court-appointed defense expert's residence, the Bureau seized his computer and media, and the Government threatened an indictment for violation of 18 U.S.C. § 2252A), *rev'd on other grounds*, 894 N.E.2d 671 (Ohio 2008).

148. Commonwealth v. Ruddock, No. 08–1439, 2009 WL 3400927, at *1 (Mass. Supp. Oct. 16, 2009); State *ex rel.* Tuller v. Crawford, 211 S.W.3d 676, 679 (Mo. Ct. App. 2007); Allen v. Tennessee, No. E2007-01018-CCA-R3-CD, 2009 WL 348555, at *6 (Tenn. Crim. App. Feb. 12, 2009).

149. *See* State v. Blount, No. 81-CR-09-1180, slip op. at 6 (Minn. Dist. Ct. Apr. 7, 2010).

150. *Id.* at 7 n.2.

151. *Id.* at 9.

which the court found would adequately serve the purpose of the Adam Walsh Act "to protect children from sexual exploitation and to prevent child abuse and child pornography."[152] Notwithstanding the inapplicability of the Act to state court criminal proceedings, and notwithstanding state court protective orders, the Government has nevertheless prosecuted defense attorneys and experts for contraband acquired in the performance of their official duties.[153] At least one federal district court has ruled that an attorney acting in accordance with the state's immunity statute may assert the operation of the statute as an affirmative defense.[154]

Arguably, there is merit to the argument that an expert should have access to the evidence in his or her own lab, because of the increased costs and inefficiencies of conducting the analysis at law enforcement facilities.[155] But, a useful analogy when considering whether a defense attorney should take possession of child pornography is that, in a drug possession case, the prosecutor does not keep samples of a controlled substance in the case files, and instead must inspect the evidence under controlled conditions where it is kept at the law enforcement facility.

E. Civil Liability Arising from Digital Forensics Investigation

Although it is beyond the scope of this Comment to discuss comprehensively the civil liabilities that could arise from digital forensics investigations, certain examples are more obvious than others. Under the Adam Walsh Act, any party that is "aggrieved" by the distribution of child pornography (an activity that could be undertaken by a careless, albeit well-intentioned, forensic

152. *Id.* at 10; *see also* Commonwealth v. Ruddock, No. 08–1439, 2009 WL 3400927, at *3 (Mass. Sup. Ct. Oct. 16, 2009) (issuing protective order to prevent "*unnecessary* disclosure").

153. United States v. Flynn, 709 F. Supp. 2d 737, 743 (D.S.D 2010); State v. Brady, 894 N.E.2d 671, 673 (Ohio 2008).

154. *Flynn*, 709 F. Supp. 2d at 743.

155. *See* Nelson et al., *supra* note 100 ("The beleaguered defense expert is forced, often by economics, to do whatever it is possible to do in one or two eight hour days. Frequently, the expert has to fight to use his/her own equipment and to work in privacy."); *see also* State v. Blount, No. 81-CR-09-1180, slip op. at 6 (Minn. Dist. Ct. Apr. 7, 2010) (crediting expert's testimony that conducting the examination at law enforcement facilities would approximately double the cost); United States v. Knellinger, 471 F. Supp. 2d 640, 647–48 (E.D. Va. 2007) (crediting testimony that conducting examination at law enforcement facilities would exacerbate costs).

investigator) may bring a civil action for damages.[156] Another example is invasion of privacy tort liability or civil liability under the Stored Communications Act resulting from accessing an e-mail account or computer without authorization.[157] And yet another example is the possibility that an attorney who retains a careless or incompetent expert could be liable for negligence.[158] In one recent case, the incompetence of one party's computer expert led the court to find the party's actions to be "grossly negligent, if not reckless," and issued an adverse jury instruction.[159] In another, when the court queried the expert whether a potential discovery problem could not be overcome by examining the "metadata," the expert made no response, prompting the court to observe that it created "the firm impression that he was not familiar with a term that we would expect a computer expert to know."[160]

F. Prosecutor's Interactions with Digital Forensics Examiners

Prosecutors have a few unique issues to contend with in digital forensics investigations. One is the perception or allegation of "shopping" for an expert, or reckless use of a tainted expert, which may constitute a violation of defendant's due process rights[161] and may also be a violation of Rule 3.8 of the Model Rules of Professional Conduct (special responsibilities of a prosecutor).[162] The following interview excerpt from *The Right to Expert Assistance in*

156. 18 U.S.C. § 2252A(f) (2006).

157. *See, e.g.*, Bailey v. Bailey, No. 07–11672, 2008 WL 324156, at *6–7 (E.D. Mich. Feb. 6, 2008).

158. RESTATEMENT (SECOND) OF TORTS §§ 411, 413 (1965).

159. Doe v. Norwalk Cmty. Coll., 248 F.R.D. 372, 379 (D. Conn. 2007).

160. *In re* Search of 3817 W. W. End, 321 F. Supp. 2d 953, 956 n.1 (N.D. Ill. 2004).

161. Imbler v. Craven, 298 F. Supp. 795, 807 (C.D. Cal. 1969), *aff'd per curiam,* 424 F.2d 631 (9th Cir. 1970) (holding that reckless use of highly suspicious false testimony violates due process); *see also* Paul C. Giannelli & Kevin C. McMunigal, *Prosecutors, Ethics, and Expert Witnesses*, 76 FORDHAM L. REV. 1493, 1506 (2007) ("Some of the most disturbing revelations that emerged from the DNA exonerations that occurred in the 1990s concern the misconduct of prosecutors. . . . [A] significant contributor to these miscarriages of justice was the misuse of expert testimony. . . . The reckless use of a tainted expert should be considered a due process violation.").

162. MODEL RULES OF PROF'L CONDUCT R. 3.8 (2010). *But cf.* Bennett L. Gershman, *Misuse of Scientific Evidence by Prosecutors*, 28 OKLA. CITY U.L. REV. 17, 39 (2003) ("Personal sanctions against a prosecutor for deliberate misconduct, such as civil liability and professional discipline, almost never happens.").

a Post-Daubert, Post-DNA World,[163] illustrates this problem:

> Because two police crime laboratories would not declare a positive bootprint match in the infamous Rolando Cruz prosecution, prosecutors sought out a third expert, Dr. Louise Robbins, who declared a match. A detective, who resigned because he believed the wrong people had been charged, later observed:
>
> "The first lab guy says it's not the boot. . . . We don't like that answer, so there's no paper [report]. We go to a second guy who used to do our lab. He says yes. So we write a report on Mr. Yes. Then Louise Robbins arrives. This is the boot, she says. That'll be $ 10,000. So now we have evidence."[164]

Another less frequent issue may arise when a digital forensics examiner encounters evidence during a non-criminal investigation and reports the findings to law enforcement. If law enforcement fails to obtain a warrant on probable cause to seize the media but instead gives directives to the examiner to search for additional corroborating evidence, the examiner may be regarded as "deputized." As an agent of the state, the examiner's search—absent a valid warrant exception—may be in violation of the suspect's Fourth Amendment rights from unreasonable searches, and any evidence procured therefrom may be inadmissible.[165]

III. DIGITAL FORENSICS MAY FACILITATE ZEALOUS ADVOCACY

Applying the so-called "Kovel Principle,"[166] where the court analogized an accountant to a translator whose presence would not destroy privilege as if the lawyer was meeting with a client who did not speak English, a digital forensic expert certainly facilitates a lawyer's ability to provide competent counsel. Just as technical accounting concepts important to a representation may be like a foreign language to the lawyer or the client, so too may the technical concepts in a digital forensics context important to a representation.

Indeed, preceding sections of this Comment have called attention to ethical traps for the unwary when attorneys retain digital forensics experts, but the decision not to retain a digital

163. 89 CORNELL L. REV. 1305.
164. *Id.* at 1308–09.
165. NELSON ET AL., *supra* note 12.
166. *See* United States v. Kovel, 296 F.2d 918 (2d Cir. 1961).

forensic expert at the appropriate time and for the appropriate reasons also implicates ethical considerations, including Model Rules of Professional Conduct 1.1 and 1.3.[167] Federal Magistrate Judge John Facciola, during his keynote speech at LegalTech New York in 2009, cited numerous examples of attorney incompetence regarding information technology and e-discovery, recalling one example from a child pornography case, where a defense attorney reasoned, "You know Judge, I just don't understand this computer stuff."[168] The magistrate concluded the defendant's Sixth Amendment rights had been compromised, and he said, "I can't think of a more obvious example of how ineffective the assistance of counsel [was]."[169] Another august commentator listed "lawyer incompetence," at the top of his recent article, *Ten Things that Trouble Judges about E-Discovery*.[170]

Yet, expert incompetence has the same effect as attorney incompetence on the outcome of cases and may compound the problems by creating malpractice liability for the well-intentioned attorney who retained the expert. Therefore, attorneys must strategically select experts who are able to assure authenticity, traceability, repeatability, data integrity, and confidentiality, all of which ultimately leads to admissibility.[171] Moreover, an expert, unburdened by the duty of advocacy, should be able to articulate under cross-examination the protocols and procedures that led to

167. MODEL RULES OF PROF'L CONDUCT (2009). Rule 1.1 requires lawyers to provide "competent representation," which is defined as "the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation." Likewise, Rule 1.3 requires that a lawyer "shall act with reasonable diligence and promptness in representing a client." *See also* Saks, *supra* note 72, at 431. "If there is scientific evidence that would help a party's claim or defense, counsel ought to find out about it and offer it. Failure to do so is a failure to provide competent representation." *Id.* (citing MODEL RULES OF PROF'L CONDUCT R. 1.1 cmt. 5 ("Thoroughness and Preparation . . . includes inquiry into and analysis of the factual . . . elements of the problem.")).

168. Interview by Karl Schieneman with Judge John Facciola, U.S. Magistrate Judge, U.S. Dist. Court for D.C., and Tom French, Solo Practitioner, (Mar. 2, 2009), *available at* http://www.esibytes.com/?p=371.

169. *Id.*

170. Craig Ball, *Ten Things that Trouble Judges About E-Discovery*, CRAIG D. BALL, P.C., 1 (2010), http://www.craigball.com/TenTroublesEDD.pdf.

171. *See, e.g.*, Lorraine v. Markel American Ins. Co., 241 F.R.D. 534, 538 (D. Md. 2007) ("[C]onsidering the significant costs associated with discovery of ESI, it makes little sense to go to all the bother and expense to get electronic information only to have it excluded from evidence or rejected from consideration during summary judgment because the proponent cannot lay a sufficient foundation to get it admitted.").

the findings in such a way that—in theory—can be repeated by another similarly situated expert under the substantially similar conditions, and lead to a substantially similar result.

The decision of when to retain such an expert is less difficult. The first steps in digital forensics work, according to the Palmer definition, are "preservation, collection, validation, [and] identification."[172] For the lawyer dealing with a potential client or evaluating an adversary's case, the first of these steps should instead be identification, then preservation and collection.[173] Identification is done preferably with the aid of an expert knowledgeable about probable sources of evidence,[174] but—depending on the fact scenario—is not always necessary. Preservation, depending on the circumstances and the attorney's knowledge of potential sources of data, may be initiated by little more than a litigation hold memorandum[175] or an instruction to a client to cease using a computer after the duty to preserve has attached.[176] In one case frequently cited at e-discovery seminars, the U.S. Court for the Southern District of New York ruled that the failure to issue a written litigation hold notice automatically constitutes gross negligence, "even if it results from a pure heart and an empty head."[177] In more complex scenarios, even where the potential sources of data are known, an expert is needed to

172. Palmer, *supra* note 16, at 16.

173. *EDRM Stages Explanation*, ELECTRONIC DISCOVERY REFERENCE MODEL, http://www.edrm.net/resources/edrm-stages-explanation (last visited Sept. 5, 2011).

174. Jason Krause, *Discovery Channels*, 88 A.B.A. J. 4, 51 (2002).

175. A "litigation hold," or "legal hold," is defined by *The Sedona Conference Glossary* as:

> [A] communication issued as a result of current or reasonably anticipated litigation, audit, government investigation or other such matter that suspends the normal disposition or processing of records. Legal holds may encompass procedures affecting data that is accessible as well as data that is not reasonably accessible. The specific communication to business or IT organizations may also be called a "hold," "preservation order," "suspension order," "freeze notice," "hold order," or "hold notice."

See THE SEDONA CONFERENCE GLOSSARY: E-DISCOVERY & DIGITAL INFORMATION MANAGEMENT, *supra* note 16, at 32.

176. The obligation to preserve evidence when a party "reasonably anticipates litigation" is "well established." Pension Comm. of Univ. of Montreal Pension Plan v. Banc of Am. Sec., LLC, 685 F. Supp. 2d 456, 466 (S.D.N.Y. 2010). "Once a party reasonably anticipates litigation, it must suspend its routine document retention/destruction policy and put in place a 'litigation hold' . . . ." Zubulake v. UBS Warburg, LLC, 220 F.R.D. 212, 218 (S.D.N.Y. 2003).

177. *Pension Comm.*, 685 F. Supp. 2d at 464.

establish how preservation should be accomplished (e.g., disabling automated defragmentation on workstations in an enterprise, disabling backup processes that overwrite older data, etc.), so that the later collection effort will be fruitful. Conversely, self-collection risks include under-collection, spoliation, changes to metadata, chain-of-custody challenges, and authentication.[178]

To avoid self-collection risks, many fact scenarios—even minor tasks, such as forensically capturing a web page[179]—warrant retaining a digital forensics expert, unless the costs clearly outweigh by the benefits. The decision to forgo an expert can lead to missing important evidence recoverable only by a forensics expert, alteration of the ESI or metadata, inability to establish a chain of custody,[180] or criminal prosecution.[181] This examiner participated in one case where the entirety of the inculpatory ESI, which led to a prompt settlement of the case, was located in "unallocated" areas of the hard drive (i.e., deleted files), and which was recoverable only with the use of specialized tools.

Finally, because lawyers must recognize their own competence limitations regarding information technology, and take the necessary time and energy to become competent or, alternatively,

178. Leonard Deutchman, *Steer Clear of the Perils of Self Collection*, LAW.COM (Apr. 16, 2008), http://www.law.com/jsp/article.jsp?id=900005508773&slreturn=1&hbxlogin=1 (discussing the various risks of self-collection and ways to avoid them).

179. Mark Kerzner, *Technology for Lawyers and Paralegals: Evidence Authentication—Web Site Content*, SHMSOFT BLOG (Sept. 1, 2008), http://shmsoft.blogspot.com/2008/09/technology-for-lawyers-and-paralegals.html ("If an item of evidence can be easily forged by a lay person, a developer, or a hacker, it is inherently inadmissible, because it may not be what it purports to be."); William R. Wohlsifer, *Internet Content Authentication*, 1 E-COM. 10 (2001), *available at* http://www.wohlsifer.com/publications.html ("Third-party authentication services help overcome multiple objections to admissibility and always increase the weight of the proffered evidence.").

180. *See, e.g.*, Green v. Blitz U.S.A., Inc., No. 2:07-CV-372, 2011 U.S. Dist. LEXIS 20353, at *19–20 (E.D. Tex. Mar. 1, 2011). Defendants were assessed substantial sanctions for "self-collection," where the defendant employee solely responsible for searching for and collecting relevant documents issued no litigation hold, conducted no keyword searches for e-mail, and made no effort to communicate with defendant's IT department about how to electronically search documents. *Id.* at *26–27.

181. United States v. Flynn, 709 F. Supp. 2d 737, 737 (D.S.D. 2010) (indicting defendant for possession of child pornography because defendant decided to undergo research in child pornography because one of his clients was accused of pedophilia); *see also* Michelle Lore, *Prosecution Serves as Warning*, WISC. L.J. (Feb. 1, 2011, 11:48 AM), http://wislawjournal.com/2011/02/01/prosecution-serves-as-warning/ ("[*Flynn* may] stifle the availability of representation for people confronting child pornography charges.").

consult experts in the field,[182] the failure to do so may result in a rule violation. Yet another risk of attorney self-collection is that of the attorney becoming a fact witness, in violation of Rule 3.7, where the attorney may be required to testify as to the collection, preservation, and authenticity of ESI. Moreover, to the extent that the attorney's testimony in authenticating evidence implicates communication with the client, it may endanger the attorney-client privilege.

IV. SPECIAL CONSIDERATIONS CONCERNING CLOUD COMPUTING AND SOCIAL MEDIA

Technologies affecting digital forensics investigations have come and gone over the years. These include varying operating systems, mobile devices, data storage size, data storage formats and architectures, peer-to-peer file-sharing, and Internet-based communications. Some of these changes have even given rise to predictions of "[t]he end of digital forensics."[183] Nevertheless, the core technological principles of observation, repeatability, traceability, and integrity have remained intact. Likewise, the legal, professional, and ethical obligations of confidentiality and fiduciary duties, as more fully discussed ante, have evolved relatively slowly. But two recent, exploding trends are pushing technological and ethical boundaries and necessitating novel approaches like never before.

The first of these is so-called "cloud computing." The National Institute of Standards and Technology ("NIST") defines cloud computing as a "model for enabling convenient, ondemand [sic] network access to a shared pool of configurable computing resources [(e.g., networks, servers, storage, applications, and services)] that can be rapidly provisioned and released with minimal management effort or service provider interaction."[184] The U.S. Government Accountability Office defines cloud computing as "an emerging form of computing where users have

182. *See* State Bar of Arizona, *supra* note 58.

183. *See, e.g.*, Ball, *supra* note 39; *see also* Graeme B. Bell & Richard Boddington, *Solid State Drives: The Beginning of the End for Current Practice in Digital Forensic Recovery?*, 5 J. DIGITAL FORENSICS, SEC., & L. 3 (Nov. 2010), *available at* http://www.jdfsl.org/subscriptions/JDFSL-V5N3-Bell.pdf (discussing that solid-state drives may destroy evidence without one telling them to do so).

184. *The NIST Cloud Computing Project*, NAT'L INST. OF STANDARDS AND TECH., http://csrc.nist.gov/nice/states/maryland/posters/cloud-computing.pdf (last visited Sept. 5, 2011).

access to scalable, on-demand capabilities that are provided through Internet-based technologies, . . . [with] the potential to provide information technology services more quickly and at a lower cost, but also to introduce information security risks."[185] Multiple cloud computing surveys reveal that, although some enterprises remain apprehensive about entrusting their data to the cloud, those that have already done so plan to increase their presence.[186]

Contrary to popular conception, cloud computing is not new. Anyone who has used Hotmail since the 1990s was using cloud computing. But it is novel as a widespread IT service delivery system for corporate enterprises:

> Cloud computing allows businesses and individuals to use the Internet to access software programs, applications, and data from computer data centers managed by [third-party] providers . . . . Cloud computing services are not a unitary product but rather a continuum of services which businesses are able to access on an as-needed basis. These services range from "public cloud" services—that is, pre-packaged standard services—to "private cloud" services—that is, highly individualized services designed specifically for a single client.[187]

185. U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-10-855T, INFORMATION SECURITY: GOVERNMENTWIDE GUIDANCE NEEDED TO ASSIST AGENCIES IN IMPLEMENTING CLOUD COMPUTING, 2 (2010), *available at* http://www.gao.gov/new.items/d10855t.pdf.

186. *2011 CIO Agenda Findings*, GARTNER, http://www.gartner.com/technology/cio/cioagenda_findings.jsp (last visited Sept. 5, 2011) (stating that although IT budget projects will remain flat in 2011, almost half of all CIOs expect to operate their applications and infrastructures via cloud technologies within the next five years); Dennis Drogseth, *The Road to the Responsible Cloud*, ENTERPRISE MGMT. ASSOCIATES (Feb. 2011), http://www.enterprisemanagement.com/web/ema_ac0211.php (discussing that companies can achieve the "Responsible Cloud" by using a step-by-step approach); s*ee also* Dennis Drogseth, *How to Make the Most of Cloud Computing without Sacrificing Control*, ENTERPRISE MGMT. ASSOCIATES, 3 (Sept. 27, 2010), http://www.businessandleadership.com/download/fs/doc/reports/howtom-1.PDF ("In general, the survey respondents were strongly positive about Cloud-computing related benefits, with 76% of those in deployment claiming real or measurable financial benefits from Cloud."); Press Release, Microsoft News Center, Digital Infrastructure, Cloud Computing Transforming Fragmented Manufacturing Industry Value Chain, According to Microsoft Study, (Apr. 4, 2011), http://www.microsoft.com/presspass/press/2011/apr11 /04-03mscloudfragmentspr.mspx ("'The survey shows . . . a growing number of forward-looking companies are exploring new and innovative business capabilities uniquely delivered through the cloud' . . . .").

187. IBM Corp. v. Visentin, No. 11 Civ. 399, 2011 U.S. Dist. LEXIS 15342, at

Not only is cloud computing novel as a corporate IT service delivery system, but the hardware used, which consists of virtualized data centers,[188] is also radically different today than even ten years ago. Consequently, traditional computer forensics approaches are likely to be stymied by both the data storage architecture and the data delivery infrastructure.[189]

> We no longer have the ability to physically acquire objects in these virtual environments where disks, memory, and networks are shared, and traditional ownership boundaries are blurred.
>
> To date, there has been very little research done on the current state of the tools, processes, and methodologies to obtain legally defensible digital evidence in the cloud.[190]

In addition, other constraints have been identified by commentators: the geographically disparate locations of the data (often implicating multiple jurisdictions, some outside of the United States),[191] and time.[192] These developments are troubling,

*15–16 (S.D.N.Y. Feb. 16, 2011) (citation omitted).

188. Aled Edwards et al., *Diverter: A New Approach to Networking Within Virtualized Infrastructures*, 109–10 (Aug. 21, 2009), *available at* http://conferences.sigcomm.org/sigcomm/2009/workshops/wren/papers/p103.pdf.

189. John J. Barbara, *Cloud Computing: Another Digital Forensic Challenge*, FORENSIC MAG. 2, http://www.forensicmag.com/article/cloud-computing-another-digital-forensic-challenge (last visited Sept. 8, 2011) ("Further forensic issues concern the potential effect the cloud services could have on the digital data itself and how the forensic examiner can explain, in a creditable manner, all these real and potential indiscretions to the court. Many forensic examiners recognize that 'there is no foolproof, universal method for extracting evidence in an admissible fashion from cloud-based applications, and in some cases, very little evidence is available to extract.'") (quoting Andrew D. Frowen, *Cloud Computing and Computer Forensics*, INTAFORENSICS (Jan. 15, 2010), http://www.intaforensics.com/Blog/Cloud-Computing-And-Computer-Forensics.aspx); Bernd Grobauer & Thomas Schreck, *Towards Incident Handling in the Cloud: Challenges and Approaches, in* PROCEEDINGS OF THE 2010 ACM CLOUD COMPUTING SEC. WORKSHOP (2010); Stephen D. Wolthusen, *Overcast: Forensic Discovery in Cloud Environments*, *in* FIFTH INT'L CONF, ON IT SECURITY INCIDENT MGMT. & IT FORENSICS, Sept. 15–17, 2009. *But see* Dan Morrill, *Cloud Computing Making Forensics Easier*, CLOUDAVE (Sept. 22, 2008), http://www.cloudave.com/2887/cloud-computing-making-forensics-easier/. Morrill contends that cloud computing makes forensics "easier" because, when a party is served with a preservation letter, he or she can "easily backup [the] environment and put it onto the cloud for the investigators to use, while the normal course of business happens." *Id.*

190. Scott Zimmerman & Dominick Glavach, *Cyber Forensics in the Cloud,* 14 IANEWSLETTER 4, 5 (2011), http://iac.dtic.mil/iatac/download/Vol14_No1.pdf.

191. *Id.* at 6; *see also Cloud Computing & National Security Law*, HARVARD NAT'L SEC. RES. GROUP, 8 (Aug. 27, 2010), http://www.law.harvard.edu/students

because, as one commentator observed, "The cloud is now used to store many of the same materials as a briefcase or backpack. Cloud computing has added an 'anywhere-access' function to Internet usage which provides a reasonable justification for storing private materials in the cloud."[193] In other words, data that has traditionally been subject to forensic investigation is now being rendered inaccessible in relative, practical terms.

At the time of this writing, this commentator believes data that is recoverable only through digital forensics tools and practices, but which may be in the custody of third-party cloud providers, is not "reasonably accessible" as that phrase is used in Federal Rule of Civil Procedure Rule 26(b)(2)(B).[194] First, third-party cloud providers would likely mount an obstreperous campaign against any intrusion by digital forensics examiners into their proprietary data warehousing. Second, the likelihood of retrieving residual data from voluminous, distributed, virtualized, and shared storage area networks seems remote at best,[195] and might be further frustrated by an inhospitable third-party content provider (even if the collection was authorized by court order). Third, the costs of attempting to forensically retrieve residual data from a cloud-

/orgs/nsrc/Cloud.pdf.

192. Zimmerman & Glavach, *supra* note 190, at 6 ("Once the information source is identified, do all involved entities have time synchronized via a consistent time source such as Network Timing Protocol (NTP)? If a forensic expert has a difficult time convincing your legal counsel that the time stamps from client-side log files match time stamps on provider-side log files, the forensics will be difficult to defend.").

193. David A. Couillard, *Defogging the Cloud: Applying Fourth Amendment Principles to Evolving Privacy Expectations in Cloud Computing*, 93 MINN. L. REV. 2205, 2223 (2009) (citing Benjamin J. Romano, *New Computing Strategy Sends Microsoft to Clouds,* SEATTLE TIMES, Oct. 28, 2008, at A10).

194. The rule states that "[a] party need not provide discovery of electronically stored information from sources that the party identifies as not reasonably accessible because of undue burden or cost." FED. R. CIV. P. 26(B)(2)(B); *see also* THE SEDONA CONFERENCE, THE SEDONA PRINCIPLES: BEST PRACTICES RECOMMENDATIONS & PRINCIPLES FOR ADDRESSING ELECTRONIC DOCUMENT PRODUCTION, at ii (Jonathan M. Redgrave et al. eds., 2d ed. 2007), *available at* http://www.thesedonaconference.org/content/miscFiles/TSC_PRINCP_2nd_ed_607.pdf ("Absent a showing of special need and relevance, a responding party should not be required to preserve, review, or produce deleted, shadowed, fragmented, or residual electronically stored information.").

195. Zimmerman & Glavach, *supra* note 190, at 6 ("There may only be traces of a virtual machine (VM) because the VM may reside on dispersed, internationally located physical drives; data may have been deleted from a striped multi-disk array unit; or forensics may reside within another cloud vendor storage system that involves court orders to retrieve.").

computing content provider's system (which costs are a matter of rank speculation at this time) would doubtless serve as a deterrent to most requesting parties or, alternatively, to a court applying the proportionality doctrine.[196] Consequently, data recovery concerning cloud computing content providers is likely to be limited to warrants and administrative subpoenas for the near future.

Just as some commentators urge, "Cloud computing is 'as important as the Web was 15 years ago,'"[197] others observe, "The world has embraced social networking with a fervor rarely seen."[198] And so, the second of new technologies requiring special consideration addressed by this Comment is social media. Social media is familiar to many readers: the American Bar Association reported in 2010 that fifty-six percent of lawyers surveyed maintained a presence in an online social network, such as LinkedIn, Facebook, or Legal OnRamp, compared with just fifteen percent in its 2008 survey.[199]

The methods of data recovery arising from social networking are widely varied. Discovery of social networking sites "requires the application of basic discovery principles in a novel context," because of the need to "define appropriately broad limits . . . on the discoverability of social communications."[200] Because much of the data is stored in the cloud, the same challenges discussed above apply to social media data collection. In addition, the Stored Communications Act ("SCA") may create another hurdle, requiring the user (often, the producing party), rather than the service provider, to consent.[201] With certain enumerated

196. *See* Kerr, *supra* note 36.

197. Grant Gross, *Cloud Computing May Draw Government Action*, INFOWORLD (Sept. 12, 2008), http://www.infoworld.com/d/security-central/cloud-computing-may-draw-government-action-825 (quoting Mike Nelson, visiting professor for the Center for Communication, Culture and Technology at Georgetown University and a former tech policy advisor for U.S. President Bill Clinton, speaking at a Google forum on the policy implications of hosted applications and services).

198. Sharon Nelson et al., *The Legal Implications of Social Networking*, 22 REGENT U.L. REV. 1, 1 (2010).

199. For a discussion of the American Bar Association's report, see Robert Ambrogi, *ABA Technology Survey on Social Networking* (Jul. 22, 2010), ROBERT AMBROGI'S LAWSITES, http://www.lawsitesblog.com/2010/07/aba-technology-survey-on-social-networking.html.

200. EEOC v. Simply Storage Mgmt., LLC, 270 F.R.D. 430, 434 (S.D. Ind. 2010).

201. 18 U.S.C. § 2701 (2006); *see also* Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965, 980 (C.D. Cal. 2010) (holding that Facebook, MySpace, and Media

exceptions, the SCA prohibits an electronic communications services ("ECS") provider from knowingly divulging to any person or entity the contents of a communication while in electronic storage by that service.[202] With regard to Webmail and private messaging, these forms of communications are protected by the SCA, but with regard to Facebook "wall postings" and MySpace comments, they may not be protected if the user's privacy settings allowed unrestricted access.[203]

Nevertheless, by the time digital forensics investigators get involved, it's usually because the producing party could not or would not produce data as obligated. And so, the good news for litigators is that recovery from the service provider (either through subpoena or forensic residual data recovery from the providers' servers) is usually not necessary, as the data is likely available from more accessible sources, especially mobile devices. Users of social media need to use computers or mobile devices to access these services and, therefore, the traces of that use are likely recoverable using traditional digital forensics techniques from these computers and mobile devices.

V. CONCLUSION

Expert witnesses have become an indispensible fixture to pre-trial practice and procedure, as well as to jury trials. The prevalence of ESI on personal computers, servers, mobile devices, and the cloud, has significantly increased the need for competent digital forensics experts in the roles of intrusion prevention, incident response, and the preservation, collection, analysis, and presentation of ESI in litigation. To make effective use of a digital forensic expert, and to manage the risks of ethical, civil, or criminal liability, attorneys must carefully supervise the expert without overstepping professional boundaries. Further, digital forensic experts benefit from having a robust legal background in order to be of greater efficacy in their service to the bench and bar, but should remain faithful to the vocation of neutral fact-finding. By adhering to an adaptive framework of both separation-of-duties and

Temple are ECS providers for the purposes of the SCA).

202. 18 U.S.C. § 2702(a)(1)–(b) (2006).

203. *Crispin*, 717 F. Supp. 2d at 991. *But see* Romano v. Steelcase, Inc., 907 N.Y.S.2d 650, 656–57 (N.Y. Sup. Ct. 2010). The court held that a user has no reasonable expectation of privacy "notwithstanding her privacy settings" because Facebook and MySpace did not guarantee "complete privacy." *Id.*

industry standard best practices, lawyers and digital forensics experts will be well-suited to work effectively together, and to meet the evidentiary challenges imposed by rapidly evolving technology.