

January 2013

Burn after Reading: Preservation and Spoliation of Evidence in the Age of Facebook

John G. Browning

Recommended Citation

John G. Browning, *Burn after Reading: Preservation and Spoliation of Evidence in the Age of Facebook*, 16 SMU Sci. & Tech. L. Rev. 273 (2013)

This Article is brought to you for free and open access by the Law Journals at SMU Scholar. It has been accepted for inclusion in SMU Science and Technology Law Review by an authorized administrator of SMU Scholar. For more information, please visit <http://digitalrepository.smu.edu>.

Burn after Reading: Preservation and Spoliation of Evidence in the Age of Facebook

John G. Browning*

I. INTRODUCTION

It is a scenario that now occurs with increasing frequency in the offices of lawyers and their clients everywhere: In responding to discovery requests and assessing the universe of what might be considered relevant, files are searched and hard drives are scoured, and then someone pipes up “What about the Facebook posts?” In the Digital Age, evidence gleaned from online sources—particularly content from social networking sites like Facebook, Twitter, YouTube, LinkedIn, and others—has assumed a front and center role in all types of litigation. Social media content can be game-changing evidence, whether one seeks something to contradict personal injury claims of physical limitations, evidence to undermine a company’s defenses in a complex commercial dispute, or proof of consumer confusion in a trademark infringement suit. This is due, in part, to the pervasiveness of social media and the sheer volume of content that social media users generate. Facebook, founded in 2004, now boasts over 1.12 billion users worldwide. In the United States, Facebook users generate over 30 billion pieces of content in a given month, and Twitter processes approximately 400 million tweets in a given day. According to the latest Pew Research Center survey, 72% of American adults use social networks.¹ Corporate America has fervently embraced social networking as well. According to a 2013 survey by Modern Survey and DHR International, roughly 9 out of 10 (88%) of business executives use LinkedIn “often” or “very often.”² The majority of the executives surveyed reported using social media on a daily basis.³ In 2013, a survey by BRANDfog asked employees about CEOs’ social media use, and 81% of the respondents said they considered executives who engaged in social media to be better equipped than their peers to lead companies in the contemporary

* Administrative partner of the Dallas office of Lewis Brisbois Bisgaard & Smith LLP, where he handles a wide variety of civil litigation, including cyberliability and technology-related legal issues. He received his B.A. with general and departmental honors from Rutgers University in 1986 and his J.D. from the University of Texas School of Law in 1989. He is the author of *The Lawyer’s Guide to Social Networking: Understanding Social Media’s Impact on the Law* (West 2010), and two other forthcoming books on social media and the law.

1. Joanna Brenner & Aaron Smith, *72% of Online Adults are Social Networking Site Users*, PEW RESEARCH CENTER, <http://www.pewinternet.org/Reports/2013/social-networking-sites.aspxd> (last visited Oct. 25, 2013).
2. T.J. McCue, *LinkedIn is Preferred by Executives*, DHR INTERNATIONAL, <http://www.forbes.com/sites/tjmccue/2013/04/09/linkedin-is-preferred-by-executives> (last visited Oct. 15, 2013).
3. *Id.*

business environment.⁴ The respondents regarded executives who used social media as more likely to improve engagement with stockholders, communicate better with customers and employees alike, and improve the business' brand image.⁵

In addition, in-house counsel have witnessed firsthand social networking's importance, not only as a tool, but as a source of critical evidence. According to a study by Greentarget, Zeughauser Group, and *Inside Counsel*, more than 67% of in-house attorneys report having used sites like LinkedIn within the past day or week.⁶ Moreover, the 2013 Annual Survey by In-House Counsel by Norton Rose Fulbright LLP revealed that 20% of corporate counsel have had to collect social media content from their employees, whether in the course of production in formal discovery during litigation or in the course of internal investigations.⁷

When the Federal Rules of Civil Procedure were amended, effective December 1, 2006, to address issues related to preserving, disclosing, or seeking electronically-stored information (ESI), social networking was in its infancy and its paradigm-shifting impact on how people communicate and share information was yet to be felt. With the inexorable spread of social media, and as these sites have become fertile ground for both formal and informal discovery, it is more vital than ever for attorneys, on both sides of the docket and every practice area, to be aware of their clients'—and their own—obligations regarding the preservation of such evidence and the consequences of spoliating this evidence. While the concept of preserving or destroying paper documents or tangible physical evidence is easy to grasp, ESI in general and social networking content in particular pose unique challenges. After all, the mere act of opening a document in Microsoft Word, or copying it to a mobile storage device, results in changes to that document system's metadata.⁸ In addition, to be used, data must first be interpreted through the use of a particular application (or a particular version of that application). The preservation of data also entails the preservation of the applications needed to correctly interpret the data. Furthermore, a hard drive

4. *2013 CEO, Social Media & Leadership Survey*, BRANDfOG, http://www.brandfog.com/CEOSocialMediaSurvey/BRANDfog_2013_CEO_Survey.pdf (last visited Oct. 15, 2103).

5. *Id.*

6. *The 2012 In-House New Media Engagement Survey*, GREENTARGET, <http://www.greentarget.com/wp-content/uploads/2012/01/2012GTZGICSurveyReportFinal-WebsiteVersion.pdf> (last visited Oct. 15, 2013).

7. *Fulbright's 9th Annual Litigation Trends Survey: Litigation Bounces Back; Regulation Hits High—U.S. Release*, NORTON ROSE FULBRIGHT, <http://www.nortonrosefulbright.com/us/news/93066/fulbrights-9th-annual-litigation-trends-survey-litigation-bounces-back-regulation-hits-high-us-release> (last visited Oct. 15, 2013).

8. Metadata is, in fact, data about data.

constantly changes and recycles its contents, which creates a document that may overwrite an earlier version. In terms of social media in particular, the dynamic nature of a social networking profile can further complicate things as profile pictures, newsfeeds, lists of friends, etc., often change rapidly.

The changes to the Federal Rules in 2006, the increasing significance of electronic discovery (e-discovery), and milestone rulings in cases like the *Zubulake* series of decisions⁹ have all combined to make preservation and spoliation of electronic evidence in general a popular topic for discussion among practitioners and legal academics alike. However, to date, there has been no analysis of evidence preservation and spoliation in the social media context. This article aims to fill that void. What constitutes spoliation in the age of Facebook and Twitter, and how are courts around the country dealing with the failure to preserve evidence from such sites? Even more intriguing, what are the implications for spoliation of evidence in an era in which “delete” is no longer tantamount to obliteration from the information landscape, and in which enterprising technology companies offer applications like Snapchat, in which the communication purportedly self-destructs and is not preserved? Because the August 2012 Amendments to the Model Rules of Professional Conduct include a change in what is considered competent representation (lawyers must now keep abreast not only of changes in the law and its practice, but also of “the benefits and risks associated with relevant technology”) attorneys must be sufficiently conversant in social media to ethically and competently advise their clients.¹⁰ The unwary attorney, in attempting to navigate the often murky waters of social media use, must be aware of ethical restrictions, particularly when it comes to preserving and not spoliating social media content.¹¹ May a lawyer direct his client to delete or take down potentially damaging or incriminating tweets or Facebook posts? Is it okay for a lawyer to advise a client to place once publicly-viewable content behind a privacy setting or screen? In answering these questions and others, the discussion of pertinent case authority (and at least one ethics opinion to date), in this article underscores the truism that the law can never truly hope to catch up with the leaps and bounds of technology.

This article aims to provide a better understanding of evidence preservation and spoliation in the age of social networking by examining the sources of the duty to preserve evidence; by looking at how the courts’ treatment of

9. *Zubulake v. U.B.S. Warburg*, 217 F.R.D. 309 (S.D.N.Y. 2003).

10. ABA COMM. ON ETHICS 20/20, REPORT TO THE HOUSE OF DELEGATES RESOLUTION 105A (Aug. 2012), available at http://www.americanbar.org/content/dam/aba/administrative/ethics_2020/20120808_revised_resolution_105a_as_amended.authcheckdam.pdf (specifically, changes to Rule 1.1, cmt. 6).

11. For a lengthier discussion of the potential ethical pitfalls posed by attorneys’ use and misuse of social media, see generally John G. Browning, *Keep Your “Friends” Close and Your Enemies Closer: Walking the Ethical Tightrope in the Use of Social Media*, 3 ST. MARY’S J. LEGAL MALPRACTICE & ETHICS 204 (2013).

spoliation of ESI generally informs the discussion of social media evidence in particular; by analyzing those cases involving spoliation of social media content; and by discussing the potential impact of new technology and applications on existing duties of evidence preservation. For attorneys, the litigants they represent, and the judges charged with applying and interpreting the law, the popularity and metrics of social media, combined with a seemingly never-ending parade of technological innovations, can be daunting, to say the least. This article hopes to demystify these concepts and provide helpful guidance.

II. THE DUTY TO PRESERVE EVIDENCE

A. Ethical Obligations

At the most fundamental level, lawyers have an ethical obligation, independent of the duties imposed on their clients, to preserve evidence. Most state ethical rules governing evidence preservation and addressing spoliation are derived from Rule 3.4 of the ABA Model Rules of Professional Conduct. This Rule prohibits a lawyer from unlawfully altering or destroying evidence and from assisting others in doing so.¹² Specifically, under the heading of “Fairness to Opposing Party and to Counsel,” it states that a lawyer shall not “unlawfully obstruct another party’s access to evidence or unlawfully alter, destroy, or conceal a document or other material having potential evidentiary value . . . or counsel or assist another person to do any such act.”¹³ The Texas analogue to this is found in Rule 3.04 of the Texas Disciplinary Rules of Professional Conduct. Under the heading of “Fairness in Adjudicatory Proceedings,” it states that lawyers shall not “(a) unlawfully obstruct another party’s access to evidence; in anticipation of a dispute unlawfully alter, destroy, or conceal a document or other material that a competent lawyer would believe has potential or actual evidentiary value; or counsel or assist another person to do any such act.”¹⁴ California, the only state that has not adopted the ABA Model Rules, sets forth its ethical prohibition against spoliating evidence in California Rule of Professional Conduct 5-220, Suppression of Evidence.¹⁵ This rule provides that “A member shall not suppress any evidence that the member or the member’s client has a legal obligation to reveal or to produce.”¹⁶

To date, only one ethics opinion has addressed an attorney’s ethical obligations regarding the preservation or spoliation of a client’s social media

12. MODEL RULES OF PROF’L CONDUCT R. 3.4 (2012).

13. *Id.*

14. TEX. DISCIPLINARY RULES PROF’L CONDUCT R. 3.04 (West 2005).

15. CAL. RULES OF PROF’L CONDUCT R. 5-220, Suppression of Evidence (West 2012).

16. *Id.*

content.¹⁷ While this recent ethics opinion from the New York County Lawyers Association (NYCLA) is discussed in greater detail later on in this article, it bears noting here that although the opinion controversially states that an attorney may direct a client to remove or “take down” certain materials from an existing social media site, a more mainstream approach appears elsewhere in the opinion.¹⁸ The NYCLA opinion notes that as part of an attorney’s duty to competently represent clients, he or she may advise the client about the implications of the client’s social media activities.¹⁹ However, the opinion went on to observe that, following New York Rules of Professional Conduct, a lawyer shall not “(a)(1) suppress any evidence that the lawyer or the client has a legal obligation to reveal or produce . . . [nor] (3) conceal or knowingly fail to disclose that which the lawyer is required by law to reveal.”²⁰

NYCLA Ethics Opinion 745 does note that while “[a]ttorneys’ duties not to suppress or conceal evidence involve questions of substantive law and are therefore outside the purview of an ethics opinion,”²¹ it does take the time to reference this substantive law. For example, the opinion states that, following certain New York state precedent, there may be a duty to preserve “potential evidence” in advance of any actual discovery request.²²

B. Other Sources of the Duty to Preserve Evidence

Besides the ethical obligations incumbent upon the attorney and which govern the attorney’s relationship with his or her client, the duty imposed on a party to preserve evidence may be rooted in common law, statutory, regulatory, or court-ordered obligations. The common law of many states imposes a duty on a party to preserve evidence when the party knows or reasonably should know that (1) there is a substantial likelihood that a claim or litigation will be filed; and (2) evidence in the party’s possession or control will be material and relevant to such a claim.²³ Statutory and regulatory duties to preserve evidence are inherent in those laws and regulations that mandate that certain types of records shall be preserved for specific periods of time. These include, for example, 29 C.F.R. § 1602.40 (requiring a two-year retention of school personnel or employment records), 17 C.F.R. § 240.17a-4

17. N.Y. CNTY. LAWYERS ASS’N, ETHICS OP. 745: ADVISING A CLIENT REGARDING POSTS ON SOCIAL MEDIA SITES (2013) *available at* http://www.nycla.org/site/Files/Publications/Publications1630_0.pdf [hereinafter “NYCLA Opinion”].

18. *Id.*

19. *Id.*

20. *Id.* (quoting N.Y. RULES OF PROF’L CONDUCT R. 3.4).

21. *Id.*

22. *Id.* (citing *VOOM HD Holdings L.L.C. v. EchoStar Satellite L.L.C.*, 93 A.D.3d 33 (N.Y. App. Div. 2012)).

23. *See, e.g., Wal-Mart Stores, Inc. v. Johnson*, 106 S.W.3d 718, 722 (Tex. 2003).

(specifying a six-year retention of certain brokerage firm records), or, on a state level, Texas Business and Commerce Code Section 72.002 (stipulating a three-year retention of business records that are required to be kept by the state, unless another law specifically provides otherwise).²⁴

In addition, a court order may impose a duty to preserve evidence. This is particularly true in the social media context, where parties frequently seek judicial intervention when concerned about potential alteration or deletion of profile content. One such example arose during a class action suit that pitted (parents of) girls who suffered from eating disorders against the health insurance carrier who declined them coverage.²⁵ During the course of litigation, defendant requested e-mails, journals, diaries, and online writings from social networking sites wherein which plaintiffs' beneficiaries' discussed eating disorders and related health conditions.²⁶ A lengthy and contentious dispute arose over discoverability of this social media content.²⁷ Ultimately, U.S. Magistrate Judge Patty Schwartz ordered preservation of the social networking evidence at issue, including all communications shared via social media.²⁸

Parties increasingly address preservation of social media content during discovery prior to a judge's order. This can include sending preservation letters prior to or in conjunction with formal discovery requests. Additionally, parties may request opposition preserve and store social networking content by use of readily available technology. For example, Facebook offers a "Download My Information" "Expanded Archive" mechanism. Essentially, this mechanism is a data export tool that permits the user to store her entire profile—from the first profile picture to the last wall post—to a zip file for easy retrieval. Use of this data export feature has become ubiquitous enough that parties faced with discovery requests (sometimes for their entire Facebook profile) are now making use of it as a way of preserving their Facebook data in electronic format.²⁹

24. 29 C.F.R. § 1602.40 (2013); 17 C.F.R. § 240.17a-4 (2013); TEX. BUS. & COM. CODE ANN. § 72.002 (West 2009).

25. *See generally* Beye v. Horizon Blue Cross Blue Shield, 568 F. Supp. 2d 556 (D.N.J. 2008); Beye v. Horizon Blue Cross Blue Shield, 2007 U.S. Dist. LEXIS 100915, at *3 (D.N.J. Dec. 12, 2007) (denying plaintiff's order to reconsider previous order to turn over documents and ordering documents be turned over to defendant).

26. Beye, 2007 U.S. Dist. LEXIS 100915, at *3.

27. *See generally id.*

28. *Id.* at *13.

29. *Id.* *See also, e.g.,* Higgins v. Koch Dev. Corp., 2013 U.S. Dist. LEXIS 94139 (S.D. Ind. July 5, 2013). Plaintiffs who claimed to have sustained personal injuries while at the defendant's theme park received request to use Facebook's "Download My Information" feature as a way of maintaining their entire Facebook profile pending resolution of any discovery disputes. *Id.*

Applicable rules of civil procedure also address the preservation of electronic evidence, albeit often more by implication. For example, Federal Rule of Civil Procedure 26(a)(1)(A)(ii) mandates that parties, in their initial disclosures, provide either copies or a description of ESI (by category and location) that supports a party's claims or defenses.³⁰ Under Rule 26(f), preservation of ESI must be discussed when parties are required to "meet and confer".³¹ In Texas, which promulgated its rule regarding ESI in 1999 (seven years before the federal rules were changed) Texas Rule of Civil Procedure 196.4 provides that parties seeking ESI must request the production of electronic data and specify the form of production requested.³² Producing parties, on the other hand, must provide ESI that is "responsive" and "reasonably available to the responding party in its ordinary course of business."³³

III. JUDICIAL TREATMENT OF SPOILIATION OF ELECTRONIC EVIDENCE GENERALLY

Concerns over spoliation of evidence were around long before the existence of electronic evidence; in fact, spoliation concerns have probably persisted for as long as evidence itself. For example, in the 18th century English case of a jeweler who had wrongfully kept the stone from a ring brought to him for appraisal, the court instructed the jury to "presume the strongest case against the jeweler and make the value of the best jewels the measure of damages" (since the stone was no longer available for valuing).³⁴ But with the more ephemeral world of digital evidence, concerns over spoliation are enhanced. Not surprisingly, courts in recent years have developed a body of jurisprudence centered on preservation and spoliation of ESI. For example, in one of the seminal *Zubulake* opinions, Judge Shira Scheindlin of the U.S. District Court for the Southern District of New York delineated the responsibility for attorneys dealing with clients in possession of relevant electronic information.³⁵ According to Judge Scheindlin, attorneys have a duty to (1) be familiar with the client's computer system and document retention policies; (2) issue a litigation hold; (3) speak directly with the client's "key players" about preservation duties; (4) tell all employees to produce electronic copies of relevant electronic files; and (5) identify all backup media and make sure it is preserved.³⁶

Over the years, the cases that discuss preservation have refined and honed key concepts. Since the duty to preserve evidence "does not exceed

30. FED. R. CIV. P. 26(a)(1)(A)(ii).

31. FED. R. CIV. P. 26(f)(3)(C).

32. TEX. R. CIV. P. 196.4.

33. *Id.*

34. *Armory v. Delamirie*, 92 Eng. Rep. 664 (K.B. 1722).

35. *Zubulake v. U.B.S. Warburg*, 229 F.R.D. 422, 432 (S.D.N.Y. 2004).

36. *Id.*

beyond evidence that is relevant and material to the claims at issue in the litigation,” a number of cases have focused on precisely what constitutes “relevant evidence.”³⁷ For example, in a recent consumer fraud case, the judge declined to impose spoliation sanctions on the defendant cable company for its failure to preserve phone recordings.³⁸ There was no evidence to suggest that the deleted call recordings were relevant and supported the plaintiff’s claim.³⁹ While the court agreed that two of the three requirements under California’s three-prong test were met—the party with control over the evidence had an obligation to preserve it, and the records were destroyed negligently—the critical third requirement that the destroyed evidence be relevant was simply not met.⁴⁰

This article will later explore how evidence from social networking sites poses even greater spoliation concerns than other forms of ESI. Such additional concerns are due to a variety of factors. For one, volume of communications (the number of Facebook posts, tweets, etc.) for an individual can easily run into the thousands. Moreover, use of social networking is casual yet pervasive. Additionally, users frequently update their profiles with new profile pictures or other changes. Finally, a variety of data can be resident on a single social networking profile (from photos and video to audio recordings, text, etc.).

One problem that arises as a result of multiple courts having addressed spoliation issues (at least in the federal context) is the degree of inconsistency, in terms of both results and sanctions imposed. For precisely this reason (and the resulting concerns over uncertainty and unpredictable sanctions), the United States Courts’ Advisory Committee on Civil Rules has included a proposed amendment to Rule 37(e) of the Federal Rules of Civil Procedure.⁴¹ This amendment “is intended to create a uniform national standard regarding the level of culpability required to justify severe sanctions for spoliation.”⁴² In essence, it would create two categories of measures a court may impose when it finds that a party failed to preserve information needed for litigation purposes. The first category includes “remedies” and other “cur-

37. See generally *Hynix Semiconductor, Inc. v. Rambus, Inc.*, 2006 WL 565893 (N.D. Cal. Jan. 5, 2006).

38. *Cottle-Banks v. Cox Commc’ns, Inc.*, 2013 U.S. Dist. LEXIS 72070, at *44 (S.D. Cal. 2013).

39. *Id.*

40. *Id.*

41. ADVISORY COMM. ON CIVIL RULES, REVISION OF RULE 37(E) AS APPROVED FOR PUBLICATION 35 (2013), available at <http://www.uscourts.gov/uscourts/RulesAndPolicies/rules/Agenda%20Books/Civil/CV2013-04.pdf>.

42. Henry Kelston, *Are We on the Cusp of Major Changes to E-Discovery Rules?*, LAW TECH. NEWS (Apr. 17, 2013), <http://www.law.com/jsp/lawtechnologynews/PubArticleLTN.jsp?id=1202596362366&slreturn=20131004174837>.

ative” steps short of being considered “sanctions.”⁴³ For instance, a court may require a party “recreate or obtain” lost information, conduct additional discovery to compensate for the missing data, or pay “reasonable expenses resulting from the loss of the information” at issue.⁴⁴ The second category of measures to be included in the proposed rule is already listed in Rule 37(b)(2)(A) as appropriate for use when a party violates a court order to comply with discovery. Accordingly, a court may strike a party’s pleadings, dismiss the action in whole or in part, preclude certain evidence from being introduced or issues from being raised, or give the jury an instruction that it may draw an adverse inference from the absence of such evidence.⁴⁵

Arguably the most debated section of the proposed amendment provides the court may impose sanctions or order an adverse jury instruction only if it finds either the failure to preserve caused “substantial prejudice” and was “willful or in bad faith;” or “irreparably deprived a party of any meaningful opportunity” to litigate the claims in the case.⁴⁶ The court may determine the “willful or in bad faith” factor (meriting more extreme sanctions) by examining the extent to which a party was on notice of probable litigation, and/or the reasonableness of a party’s efforts to preserve information that was ultimately lost.⁴⁷

Those critical of the proposed amendment to Rule 37(e) apparently include Judge Shira Scheindlin, a towering figure in the world of electronic discovery. Judge Scheindlin is renowned for her highly influential decisions in *Zubulake* as well as *Pension Committee of the University of Montreal Pension Plan v. Banc of America Securities, LLC*.⁴⁸ In a recent breach of contract case, Judge Scheindlin sanctioned plaintiffs Sekisui America Corp. and Sekisui Medical Co. for deleting emails and failing to institute a litigation hold for fifteen months; a failure she termed “inexcusable given that Sekisui is the plaintiff in this case and, as such, had full knowledge of the possibility of future litigation.”⁴⁹ Noting that “prejudice is presumed precisely because relevant evidence—i.e., evidence presumed to be unfavorable to the spoliating party—has been intentionally destroyed and is no longer available to the innocent party,” Judge Scheindlin left no doubt as to her position on the proposed amendment to Rule 37(e). The judge wrote, “I do not agree that the burden to prove prejudice from missing evidence lost as a result of willful or

43. *Id.*

44. *Id.*

45. *Id.*

46. *Id.*

47. *Id.*

48. See generally *Zubulake v. U.B.S. Warburg*, 229 F.R.D. 422 (S.D.N.Y. 2004); 2010 WL 184312 (S.D.N.Y. Jan. 15, 2010).

49. *Sekisui Am. Corp. v. Hart*, Case No. 1:12-cv-03479 SAS FM, 2013 U.S. Dist. LEXIS 115533, at *32 (S.D.N.Y. Aug. 15, 2013).

intentional misconduct should fall on the innocent party. Furthermore, imposing sanctions only where evidence is destroyed willfully or in bad faith creates perverse incentives and encourages sloppy behavior.”⁵⁰ The court hit Sekisui with an adverse jury instruction as well as costs and fees to be determined at a later date.⁵¹

Courts previously dealt with spoliation issues in other manners of ESI, including text messages,⁵² digital photos from a cellphone camera,⁵³ and e-mail.⁵⁴ As noted earlier, all of these forms of ESI (amongst other forms) are often found on a typical social networking profile. Under both the Federal Rules of Civil Procedure and many state counterparts, spoliation sanctions may not be imposed when ESI is lost as a result of “routine, good faith operation of an electronic information system,” absent exceptional circumstances.⁵⁵ Consequently, routine deletion of Facebook wall posts or altering profile pictures will not rise to the level of spoliation unless a party has notice that this content is relevant to pending or “reasonably foreseeable” litigation. Pre-suit demand letters and even an oral threat of litigation have been held to trigger the duty to preserve evidence.⁵⁶ In one instance, a court held that a community college’s duty to preserve ESI arose once it merely became aware of sexual assault allegations against a professor (long before suit was ever filed or even threatened).⁵⁷

In the social media context, it is important to keep in mind that spoliation encompasses not just the destruction of evidence, but its alteration, as well, or where a party fails “to preserve property for another’s use as evidence in pending or reasonably foreseeable litigation.”⁵⁸ For example, in a sexual harassment claim, it should come as no surprise that the plaintiff who alters her Facebook profile to replace risqué or suggestive photos with more demure ones casts doubt on her claims, and has engaged in a form of spolia-

50. *Id.*

51. *Id.* The timing of this ruling could prove meaningful, given that it was handed down shortly after the proposed amendment was released for comments.

52. *Christou v. Beatport, LLC*, 2013 U.S. Dist. LEXIS 9034, at *39 (D. Col. Jan. 20, 2013).

53. *Evans v. N.Y. City Transit Auth.*, No. 102654/09, at *3 (Sup. Ct. N.Y. Co. Jan. 9, 2013).

54. *VOOM HD Holdings L.L.C. v. EchoStar Satellite L.L.C.*, 93 A.D.3d 33, 43 (N.Y. App. Div. 2012).

55. *FED. R. CIV. P.* 37(e).

56. *See, e.g., UMG Recordings, Inc. v. Hummer Winblad Venture Partners (In re Napster, Inc. Copyright Litigation)*, 462 F. Supp. 2d 1060, 1069 (N.D. Cal. 2006).

57. *Doe v. Norwalk Cmty. Coll.*, 248 F.R.D. 372, 377 (D. Conn. 2007).

58. *Mosaid Tech. Inc. v. Samsung Elec. Co.*, 348 F. Supp. 2d 332, 335 (D.N.J. 2004) (citation omitted).

tion. An example “ripped from the headlines” of social media spoliation is seen in the criminal prosecution of former Rutgers student Dharun Ravi for the cyber-harassment of his roommate, Tyler Clementi, which occurred prior to Clementi’s suicide.⁵⁹ Ravi not only attempted to electronically broadcast Clementi in an intimate episode with another man via webcam, but he also sent various tweets about his activities.⁶⁰ After Clementi’s suicide, Ravi went back and attempted to delete and alter his tweets to make them seem more benign; the result was a charge of obstruction of evidence.⁶¹

As the discussion later on in this article of specific cases of social media spoliation will reveal, the recent development of social media as a societal phenomenon has proven one of the biggest challenges for attorneys, litigants, and courts alike grappling with the evidence preservation and spoliation issues cropping up in litigation. Well before the advent of social media, courts had already begun grappling with the ins and outs of other forms of ESI, such as email.⁶² Consequently, attorneys have had a long time to caution their clients about how what is expressed in email may later become fair game for discovery, but it is only relatively recently that courts have begun exploring the parameters of discoverability of social media content. Clients accustomed to carefree tweeting and posting on Facebook are still, more often than not, surprised to see their own social media activities used against them in litigation.⁶³ So, too, are employers belatedly realizing some of the harsh realities that can accompany a Bring Your Own Device workplace, where employees may transact company business on the same smartphone on which they update their Facebook status or tweet to friends.⁶⁴ Thanks to the realities of the Digital Age, evidence preservation and spoliation concerns must necessarily include social media. Attorneys must update their litigation hold letters to admonish clients about preserving social media content. Although more and more attorneys are realizing the importance of seeking social media evidence

59. See *Tyler Clementi*, N.Y. TIMES (Mar. 16, 2012), http://topics.nytimes.com/top/reference/timestopics/people/c/tyler_clementi/index.html.

60. See *id.*; ‘I Apologize,’ Ex-Rutgers Student Says Before Going to Jail, N.Y. TIMES (May 29, 2012), <http://www.nytimes.com/2012/05/30/nyregion/dharun-ravi-convicted-in-webcam-spying-apologizes-before-going-to-jail.html>.

61. Megan DeMarco, *Rutgers Webcam Trial: Ravi Deleted Dozens of Text Messages from Cell Phone, Expert Says*, THE STAR-LEDGER (Mar. 7, 2012), http://www.nj.com/news/index.ssf/2012/03/rutgers_webcam_trial_ravi_delete.html.

62. See Kristen L. Mix, *Discovery of Social Media*, 40 COLO. LAW. 27, 32 (2011).

63. See generally Henry Z. Horbaczewski & Ronald I. Raether, *BYOD: Bring Your Own Device Know the Privacy and Security Issues Before Inviting Employee-Owned Devices to the Party*, 30.3 ACC DOCKET 70, 76 (2012).

64. See generally *id.* at 72.

in discovery, they also would be well-advised to specifically reference it in preservation letters to adverse parties or opposing counsel.⁶⁵

Due to the potential for a spoliation finding to dramatically alter the posture of a case, maintaining control over the universe of electronically stored formation—including social media content—is more important than ever for attorneys. As U.S. Magistrate Judge Craig Shaffer recently observed (as part of a broader analysis of the proposed Federal Rules of Civil Procedure amendments):

In the past, particularly in an asymmetrical case (such as a simple employee discrimination action brought under Title VII), plaintiff's counsel might have paid only fleeting attention to his or her client's preservation obligation since it was presumed that the defendant employer had possession, custody, or control of all the relevant ESI. That confidence may be misplaced, however, with the advent of social media. As one court recently observed, there is "no principal reason to articulate different standards for the discoverability of communications through email, text message, or social media platforms." A party is presumed to have control over their social networking accounts and relevant information on those sites is discoverable. . . . Since the plaintiff controls when litigation commences, as well as the nature and scope of any claims asserted, a plaintiff's attorney who does not take early and affirmative steps to preserve social media content risks spoliation sanctions.⁶⁶

In short, while many of the same questions and concerns over preservation and spoliation of ESI apply equally to social media evidence, there are aspects unique to the social networking realm.⁶⁷ At first blush, one might think that in a world where everything lives forever on the Internet and "delete" no longer means "gone forever" thanks to digital forensic tools, concerns about spoliation would be few and far between. However, as the rapidly developing body of case law on spoliation and social media demonstrates, the opposite is true.⁶⁸ As a result, complying with the duty to preserve evidence in the Digital Age demands that lawyers and their clients address

65. See, e.g., *Carr v. Bovis Lend Lease*, No. 107413/10, 2012 N.Y. Misc. LEXIS 6095, at *3 (N.Y. Sup. Ct. Sept. 5, 2012) (discussing a New York personal injury case where the defendants served the plaintiff not only with discovery requests for posts on Facebook, Myspace, Twitter, and YouTube, but also with a Demand for the Preservation of Electronically Stored Information that specifically referenced Facebook and other social media sites).

66. Craig B. Shaffer & Ryan T. Schaffer, *Looking Past the Debate: Proposed Revisions to the Federal Rules of Civil Procedure*, 7 FED. COURTS L. REV. 180 (2013).

67. See generally Mix, *supra* note 62, at 29.

68. See generally *id.*

social media not only in gathering evidence, but in implementing effective protocols and procedures for preserving it as well.⁶⁹

IV. CASES INVOLVING SPOILIATION OF SOCIAL MEDIA

With preservation and spoliation issues prominently featured in the jurisprudence of electronic evidence generally, what kind of guidance can they lend to the discussion of spoliation of social media content? As it turns out, questions regarding spoliation in the social networking context have been circulating just about as long as the actual use of social media evidence. However, the unique qualities of social networking communications raise interesting questions that courts have not always addressed with other forms of electronically stored information.⁷⁰

For example, can a lawyer counsel a client to refrain from social media activities, like posting on his Facebook wall or those of others? Certainly—a party is under no obligation to *create* evidence for the other side, and it is simply good lawyering to direct a client to avoid such conduct, just as one would counsel a client to avoid any behavior that could later be used against her.⁷¹ What about counseling a client not to delete evidence, but to take affirmative steps to keep such information from being readily available, such as using the privacy settings on a Facebook profile to restrict it to “private?”⁷² Initially, this would seem to be fairly logical, innocuous advice: i.e., do not destroy any evidence, but do not leave it out in the open for the public to see, either. A proper discovery request will likely render any relevant content behind the privacy “screen” discoverable anyway, so what is the harm?⁷³ As one court has suggested, however, under the right circumstances the mere act of taking one’s Facebook profile from publicly viewable to private can give rise to an adverse inference.⁷⁴

A. *In re Platt*

In re Platt was an adversary proceeding stemming from a state court personal injury suit.⁷⁵ Plaintiff Will Rhodes and Defendant Justin Platt had gotten into a physical altercation at an Austin nightclub and bar, in which a

69. See NYCLA Opinion, *supra* note 17, at 4 (discussing the advice an attorney may give a client regarding posts on social media sites).

70. See Mix, *supra* note 62, at 29 (discussing the dynamic distinction on the applicability of federal rules for traditional ESI and social networking).

71. See generally NYCLA Opinion, *supra* note 17, at 1.

72. See generally *id.* at 2.

73. See generally *id.*

74. See *In re Platt*, No. 11-12367-CAG, 2012 WL 5337197, at *3 (Bankr. W.D. Tex. Oct. 29, 2012).

75. *Id.* at *1.

beer glass was allegedly thrown at Rhodes' face, injuring him.⁷⁶ Platt denied that he had intended to injure Rhodes, claiming instead that he had planned in good fun to pour the beer over Rhodes' head, only to be startled and toss the glass in Rhodes' direction.⁷⁷

Early on in the state court civil suit that Rhodes filed, Platt filed a Chapter 7 bankruptcy case.⁷⁸ Rhodes filed an adversary proceeding in bankruptcy court, asserting that any debt arising from his injury would be nondischargeable under Section 523(a)(6) of the Bankruptcy Code since Platt's conduct was "willful and malicious."⁷⁹ To determine if the conduct was indeed "willful and malicious," the court had to examine Platt's behavior and credibility, including his conduct after the incident, to see if Platt had the intent to injure Rhodes.⁸⁰ The court pointed, in particular, to Platt's activity regarding his Facebook account:

Defendant fled the bar immediately after the incident, breaking part of the club's front door as he left. Although the bar staff were initially able to identify Defendant by finding his Facebook account, Defendant made his Facebook account private soon after the incident occurred. During the same time period, [he] removed the last names—including his own—from a webpage promoting his band.⁸¹

The court noted that this act in which "Defendant's account was 'made private' such that an unknown third party searching for Defendant would no longer be able to find him on Facebook," supported an adverse inference that the Defendant acted with the specific intent to injure the Plaintiff, and therefore the debt was *not* dischargeable.⁸²

B. New York County Lawyers Association Ethics Opinion 745

The *Platt* case raises issues that resonate with many lawyers wondering just how far to go in counseling their clients. NYCLA Ethics Opinion 745 poses several questions about just what sort of advice is appropriate to give a client regarding existing or proposed postings on social media sites, including the following:

May attorneys advise clients about what should or should not be posted on social media sites?

76. *Id.*

77. *Id.* at *2.

78. *Id.* at *1.

79. *Id.*

80. *Platt*, 2012 WL 5337197, at *3.

81. *Id.*

82. *Id.* at *3.

May lawyers direct their clients to remove certain materials from existing social media profiles?

May lawyers counsel clients about the legal ramifications of their activities on social media?⁸³

The NYCLA opinion begins by describing that the modern practice environment in the Digital Age (not to mention society) is a very different atmosphere from the one many attorneys experienced early in their careers.

It is commonplace to post travel logs, photographs, streams of consciousness, rants, and all manner of things on websites so that family, friends, or even the public-at-large can peer into one's life For example, teenagers and college students commonly post photographs of themselves partying, binge drinking, indulging in illegal drugs or sexual poses, and the like. The posters may not be aware, or may not care, that these posts may find their way into the hands of family, potential employers, school admission offices, romantic contacts, and others. The content of a removed social media posting may continue to exist, on the poster's computer, or in cyberspace It is now common for attorneys and their investigators to seek to scour litigant's social media pages for information and photographs. Demands for authorizations for access to passwords, protected portions of an opposing litigant's social media site are becoming routine.⁸⁴

The opinion then turns to cite previous ethics opinions that make it clear that, ethically speaking, there is no restriction on attorneys accessing someone's publicly-viewable social media profile, although attorneys must still avoid engaging in misrepresentation in order to gain information.⁸⁵ Set against this backdrop, the opinion then turns to the issue of privacy, noting that all major social networking sites feature varying privacy settings and that they exist for a reason.⁸⁶ Because of this, the opinion states, "[t]here is no ethical restraint in advising a client to use the highest level of privacy/security settings that is available. Such settings will prevent adverse counsel from having direct access to the contents of the client's social media pages, requiring adverse counsel to request access through formal discovery channels."⁸⁷

While the result in the *Platt* case might indicate that such advice runs the risk of costing the client an adverse inference, it is important to remember that the court's ruling in *Platt* hinged on the totality of the circumstances and the timing of Platt's sudden decision to make his profile private.⁸⁸ Simply directing a client to avail him or herself of the privacy settings available is no different from counseling the client to pull the shade down at his house or to

83. See NYCLA Opinion, *supra* note 17, at 1.

84. *Id.* at 1–2.

85. *Id.* at 2 (citations omitted).

86. See *id.*

87. *Id.*

88. See *Platt*, 2012 WL 5337197, at *2.

avoid discussing the facts of the case with outsiders. The act of shielding potentially discoverable information from prying eyes and ears is common-sense, and it is hardly the equivalent of counseling a client to spoliage evidence.

The opinion next asks whether an attorney may prescreen “what a client posts on a social media site.”⁸⁹ It observes that part of providing competent representation is the obligation to advise clients regarding what steps they may take (within the bounds of the law and ethics) to mitigate any adverse effects on the clients’ position that might arise out of their use of social media.⁹⁰ The opinion concludes that because of this, “an attorney may properly review a client’s social media pages, and advise the client that certain materials posted on a social media page may be used against the client for impeachment or similar purposes.”⁹¹ The reasoning here is sound: just as a client should not volunteer information beyond the bounds of answering a question in a deposition, she should not engage in the digital equivalent by baring her soul for all to see on her social networking profile, and it is simply good lawyering to counsel a client about how information in a publicly-accessible forum can come back to haunt her.

NYCLA Opinion 745 even goes on to remind attorneys that yet another ethical obligation can come into play here: the ethical responsibility not to “bring or defend a proceeding, or assert or controvert an issue therein, unless there is a basis in law and fact for doing so that is not frivolous.”⁹² Frivolous conduct, the opinion reminds us, “includes the knowing assertion of ‘material factual statements that are false.’”⁹³ Accordingly, it is important for lawyers to be aware of what their clients are posting on social media sites so that the lawyers can avoid giving their implicit approval to conduct that reveals the baselessness for a case. As the opinion details, “if a client’s social media posting reveals to an attorney that the client’s lawsuit involves the assertion of material false factual statements, and if proper inquiry of the client does not negate that conclusion, the attorney is ethically prohibited from proffering, supporting or using those false statements.”⁹⁴ For similar reasons, the opinion warns, lawyers must remain vigilant with regard to clients’ altering of their social media profiles.⁹⁵ Because clients are required to testify truthfully at a deposition, trial, or other proceedings, and because lawyers may not offer or use evidence the lawyer knows to be false (and may not fail to correct a false statement of material fact), lawyers have a duty to take “prompt

89. NYCLA Opinion, *supra* note 17, at 3.

90. *Id.*

91. *Id.*

92. *Id.*

93. *Id.* at 4 (citation omitted).

94. *Id.*

95. See NYCLA Opinion, *supra* note 17, at 4.

remedial action” if a client does not answer truthfully when asked “whether changes were ever made” to his social media site.⁹⁶

Following the reasoning of this opinion, a lawyer should communicate regularly with his client and be aware of his client’s social media postings—all sensible advice. Summarizing what a lawyer can do in terms of advising the client of the realities of litigating in the age of Facebook and Twitter, the opinion even provides a kind of checklist of tasks that a lawyer can do for his client. The tasks include reviewing “what a client plans to publish on a social media page in advance of publication, to guide the client appropriately, including formulating a corporate policy on social media usage” and counseling the client/witness to publish truthful information favorable to the lawyer’s client; discuss the significance and implications of social media posts (including their content and advisability); advise the client how social media posts may be received and/or presented by the client’s legal adversaries and advise the client to consider the posts in that light; discuss the possibility that the legal adversary may obtain access to ‘private’ social media pages through court orders or compulsory process; review how the factual context of the posts may affect their perception; review the posts that may be published and those that have already been published; and discuss possible lines of cross-examination.⁹⁷

Again, all of this is sensible advice in any legal scenario that might be impacted by social media posts. Attorneys can avoid the problem of contending with ongoing social media posting by insisting that, during the pendency of the litigation or throughout the attorney-client relationship, the client refrain from engaging in any social media.⁹⁸ However, the portion of NYCLA Opinion 745 that has attracted the most attention (while receiving scant discussion in the opinion itself) is its answer to the second questions addressed—any lawyers instruct clients to “take down” certain materials from existing social media sites?⁹⁹ The opinion’s answer is a qualified “yes,” a controversial position that would seem to sanction (in a positive way) the act of spoliation of evidence. Although the opinion makes fleeting reference to the fact that a duty to preserve evidence may arise under substantive law, it concludes that:

provided that such removal does not violate the substantive law regarding destruction or spoliation of evidence, there is no ethical

96. *Id.* (citation omitted).

97. *Id.*

98. *See id.* at 3. While not palatable to many clients, this approach may relieve a lawyer of the pressure of playing “social media cop” to his client. In the course of the author’s own research, he has encountered a number of attorneys who incorporate “social media bans” into their engagement agreement or initial correspondence with clients setting forth the respective responsibilities of lawyers and client.

99. *See id.* at 4.

bar to “taking down” such material from social media publications, or prohibiting a client’s attorney from advising the client to do so, particularly in as much as the substance of the posting is generally preserved in cyberspace or on the user’s computer.¹⁰⁰

The opinion drops this bombshell and then moves on to an unrelated point, offering no further explanation or rationale and providing no examples or hypothetical scenarios by way of illustration. In fact, it drops the topic entirely, only returning to offer a brief summary in the opinion’s last line, which states, “provided that there is no violation of the rules or substantive law pertaining to the preservation and/or spoliation of evidence, an attorney may offer advice as to what may be kept on ‘private’ social media pages, and what may be ‘taken down’ or removed.”¹⁰¹

In analyzing this apparent license to spoliage, one must examine both the caveat and the justification provided. Cautioning attorneys that taking down social media content damaging to the client’s case is acceptable, as long as it does not violate the ethical rules or substantive law is not quite the *carte blanche* that some observers might think. It is somewhat akin to handing the car keys to someone and saying, “You may drive as fast as you want, as long as you obey the posted speed limits.” Essentially, the only “limit” amidst the rules and substantive law prohibiting spoliation that provides any sort of wiggle room that might permit deletion or destruction of evidence is the requirement of relevance. Cases have consistently pronounced that there can be no sanction-worthy spoliation if the evidence is not relevant: i.e., the destroyed or unavailable evidence would have been helpful to the movant.¹⁰² If the social networking content taken down was not relevant, then, technically it is not spoliation.

For example, a client who is the plaintiff in a personal injury case plans to update her social media profile. She is an avid marathon runner, and frequently posts pictures from her races along with her times on her Facebook page. She is also a “foodie” who posts photos of meals on her Instagram account. Taking down the Instagram photos would not equate to spoliation, unless her eating habits somehow became relevant to her personal injury claims. However, taking down the Facebook posts, either pre-accident or post-accident, could constitute spoliation. Photos depicting her physical capabilities before the accident could certainly be relevant to the plaintiff’s own claims, while depictions of her successfully competing since could be relevant to a defendant’s position that she has fully recovered.

100. *Id.* at 3.

101. NYCLA Opinion, *supra* note 17, at 4.

102. See, e.g., *Residential Funding Corp. v. DeGeorge Fin. Corp.*, 306 F.3d 99, 108–09 (2d Cir. 2002); *MRT, Inc. v. Vounckx*, 299 S.W.3d 500, 510 (Tex. App.—Dallas 2009, no pet.) (articulating the standard that under Texas law, a duty to preserve evidence only arises when the evidence in the party’s possession or control “will be material and relevant” to the claim).

However, while relevance is a prerequisite for a spoliation finding, who decides what is relevant? In the social media context, the question of what content is truly relevant and, therefore, discoverable continues to be the subject of discovery disputes. At the heart of this problem is the subjectivity that often accompanies the analysis: what one party deems relevant may be considered irrelevant by another. At least one court confronted with a social media discovery battle (in which the plaintiff's Facebook profile was about 750 pages long, and the plaintiff produced only 100 of those pages to the defense) has recognized this "relevance is in the eye of the beholder" dilemma:

Facebook usage depicts a snapshot of the user's relationships and state of mind at the time of the content's posting. Therefore, relevance of the content of the plaintiff's Facebook usage as to both liability and damages in this case is more in the eye of the beholder than subject to strict demarcations, and production should not be limited to Plaintiff's own determination of what may be 'reasonably calculated to lead to the discovery of admissible evidence.'¹⁰³

Another problem with the NYCLA Opinion's apparent blessing of taking down damaging content is its casual attempt at justification. It notes in passing that "the substance of the posting is generally preserved in cyberspace or on the user's computer." If this were a valid reason to intentionally delete evidence—in today's world of digital forensics and hard drive mirror-imaging, "delete" no longer means "delete"—it would undermine the core principles behind punishing those who engage in spoliation. While the ability to recover content is certainly a factor to be considered in assessing the degree of punishment and the fact that the content can be recreated or electronically retrieved (albeit at some cost) militates in favor of a lesser measure, it does not excuse the intent behind the original act itself of spoliation. NYCLA Opinion 745 is deeply flawed in this respect, and it would be surprising to see it form the basis of advice to clients to "go forth and spoliate."

C. *Torres v. Lexington Insurance Co.*

The earliest known social networking spoliation case not only illustrates the fact that courts will regard spoliation of social media content by applying concepts that apply to any other kind of evidence destruction, but it also showed the value of preserving or capturing the opposition's incriminating postings early on—just in case an attempt at spoliation is made. In *Torres v. Lexington Insurance Co.*, the plaintiff claimed to have been the victim of a sexual assault while receiving a massage at a hotel spa in Puerto Rico.¹⁰⁴ Following the incident, the plaintiff claimed she had developed "intense

103. *Bass ex rel. Bass v. Miss Porter's Sch.*, No. 3:08cv1807 (JBA), 2009 WL 3724968 (D. Conn. Oct. 27, 2009).

104. *Torres v. Lexington Ins. Co.*, 237 F.R.D. 533, 533 (D.P.R. 2006).

mental anguish, feelings of shame, humiliation, depression, unworthiness, weeping, and has been forced to undergo psychological treatment and therapy.”¹⁰⁵ She further maintained that the assault had damaged her marriage, hurt her job prospects, and left her a recluse with little, if any, social interaction.¹⁰⁶

However, as the district court would later point out, “[a]t some point during the case, defendants learned outside of discovery that [plaintiff] possessed several web pages depicting an active social life, and an aspiring singing and modeling career.”¹⁰⁷ These web pages were in direct contradiction to [plaintiff’s] assertions of continued and ongoing mental anguish.”¹⁰⁸ The court went on to note that, at the time the web pages were discovered, neither plaintiffs nor plaintiffs’ counsel had knowledge that defense counsel had made this discovery.¹⁰⁹ Because of this, the defense was able to download and print out much of the content of the web pages.¹¹⁰ Defense counsel subsequently sent a preservation letter, informing plaintiff’s counsel that “eliminating or altering the sites could be considered spoliation or evidence tampering.”¹¹¹ Alas, as the court pointed out, “[t]wo days after plaintiffs were alerted about defendants’ knowledge of the websites, the same were deleted in their entirety. No plausible explanation has been offered for this.”¹¹²

Not surprisingly, the defense moved for sanctions, asking that plaintiffs’ case be dismissed in its entirety or, alternatively, that her damages claims be eliminated or reduced.¹¹³ The court was not amused. The court described Torres’ deletion of the social networking profile as an “unconscionable scheme calculated to interfere with the judicial system’s ability to impartially adjudicate the matter or unfairly hamper the prosecution of the opposing party’s claims or defenses.”¹¹⁴ The court went on to observe that, far from coming clean about her acting and modeling aspirations, the plaintiff:

attempted to depict the life of a recluse with no or little social interaction. Instead, [plaintiff] led an active social life and announced this information to the world by posting it on very public [I]nternet sites. Then, immediately upon defendant’s discovery of evidence, which could be used to contradict or impeach her alle-

105. *Id.*

106. *Id.* at 533–34.

107. *Id.*

108. *Id.* at 534.

109. *Id.*

110. *Torres*, 237 F.3d at 534.

111. *Id.*

112. *Id.*

113. *Id.*

114. *Id.*

gations, [plaintiff] removed the information from the [I]nternet. This is the type of unconscionable conduct the court seeks to deter.¹¹⁵

While the court did not dismiss the plaintiffs' claims in their entirety, it did sanction her by "eliminat[ing] all possibility of introducing evidence of continuous or ongoing mental anguish on her part."¹¹⁶ In a case where the biggest component of damage is likely to be mental anguish, that is indeed a harsh sanction.

Therefore, the *Torres* case illustrates two key points. First, practitioners need to take measures to preserve any impeaching social media content as soon as they encounter it. While this is an extreme case in which the actual pages were taken down, less nefarious actions—such as changing a Facebook profile picture—may occur in a far more routine fashion. When information helpful to one's case is spotted online, it is critical that immediate steps be taken to preserve it, even with a screenshot. Second, this case illustrates the importance of sending an early preservation letter. The *Torres* letter from the defense was well-timed—right after the defense had discovered and printed out the impeaching social media content. Pointing out that the other side was warned, in the form of a preservation letter, not to engage in spoliation and of the potential consequences of doing so can only reinforce a moving party's later efforts to sanction the party who is accused of spoliation.

D. *Katiroll Co. v. Kati Roll & Platters, Inc.*

As mentioned earlier, not all purported spoliation is as blatant as the *Torres* plaintiff's complete takedown of her profile. It is a common feature of social networking users to update their profiles, change profile pictures, etc. How should courts regard these less egregious actions? The 2011 case of *Katiroll Co. v. Kati Roll & Platters, Inc.* is a useful illustration.¹¹⁷ This trademark and trade dress infringement case involved two competing restaurants selling similar types of food.¹¹⁸ The court granted the plaintiff's request for an injunction based on infringement of the restaurant's distinctive trade dress and gave the defendant twenty days to change its infringing trade dress to another color.¹¹⁹ The plaintiff also sought PDF copies of the defendant's Facebook pages displaying the infringing trade dress.¹²⁰ However, by the time it attempted to create PDFs of the Facebook page in question, the defen-

115. *Id.*

116. *Torres*, 237 F.3d at 534.

117. *Katiroll Co. v. Kati Roll & Platters, Inc.*, No. 10-3620 GEB, 2011 WL 3583408 (D.N.J. Aug. 3, 2011).

118. *Id.* at *1.

119. *Id.* at *2.

120. *Id.* at *3.

dant had already changed its profile picture (the new image did not contain the infringing trade dress) in an effort to comply with the court's order.¹²¹ The plaintiff moved for sanctions, seeking a spoliation inference due to the changed profile picture.¹²²

The court methodically went over the four-part test for a spoliation inference, examining such factors as whether 1) the evidence was in the party's control; 2) the evidence was actually suppressed or withheld; 3) the destroyed evidence was relevant to the claims or defenses at issue; and 4) it was reasonably foreseeable that the evidence in question would subsequently be discoverable.¹²³ The court had little difficulty concluding that the first and third factors were met, but it struggled with the second and fourth requirements.¹²⁴ While ultimately determining that the loss of information was "somewhat prejudicial," the court found that, despite the fact that the defendant owner knew that he had to preserve evidence, it would not have been immediately clear that changing his profile picture "would undermine discoverable evidence."¹²⁵ The court came to this ruling even though changing the profile picture admittedly "changes the picture associated with each and every post that user has made in the past."¹²⁶

In this case, the court also considered the unique features of social networking sites. Chief Judge Brown found it "hardly surprising" the defendant changed the profile picture, noting that "the change of a profile picture on Facebook is a common occurrence," and "[a]ctive users often change their pictures weekly."¹²⁷ Finding that the spoliation was not intentional and imposing a lesser negligence standard for the spoliation conduct, the court declined plaintiff's request for an adverse inference instruction.¹²⁸ Instead, the court crafted its own solution and directed the defendant to post the image of the allegedly infringing photo for a designated period of time so that the plaintiff could then print relevant posts as evidence for the trial in the case.¹²⁹ Thereafter, the defendant would be permitted to re-post its non-infringing profile picture.¹³⁰ Chief Judge Brown stated that concluding otherwise would be "unjust."¹³¹

121. *Id.* at *3.

122. *Id.*

123. *Katiroll*, 2011 WL 3583408, at *1.

124. *Id.* at *4.

125. *Id.*

126. *Id.* at *3.

127. *Id.* at *4.

128. *Id.*

129. *Katiroll*, 2011 WL 3583408, at *4.

130. *Id.*

131. *Id.* at *3.

The *Katiroll* case is a useful demonstration of how courts should consider the actual prejudice or harm to the moving party in a spoliation claim before determining what level of sanction would be appropriate: an adverse inference instruction for the jury, dismissal of certain claims, or a lesser penalty.¹³² Yet at the same time, this case shows that an understanding of the very nature and features of social networking sites can be critical when fashioning novel solutions when spoliation occurs in the social media context.¹³³

E. *Patel v. Havana Bar, Restaurant & Catering*

Another 2011 federal court case also provides a useful illustration of the varying ways in which spoliation can occur in the world of social media, as well as the appropriateness of lesser sanctions when warranted by the facts.¹³⁴ *Patel v. Havana Bar, Restaurant & Catering* appears at first glance to be a garden-variety premises liability case.¹³⁵ On September 8, 2007, plaintiff Yogesh Patel was at the Havana Bar & Restaurant to attend an engagement party when he allegedly fell from a balcony and sustained personal injuries.¹³⁶ His federal court complaint alleged multiple claims, including dangerous conditions at the restaurant as well as purportedly being overserved alcohol while already intoxicated, but the tale devolved into one of spoliation on both sides.¹³⁷ Havana Bar owner Mark Stevens allegedly viewed surveillance footage from the time of the incident, but was unable to preserve it, and contacted his system's provider.¹³⁸ However, he apparently failed to follow up with the provider, and the footage was lost.¹³⁹

On the plaintiff's side, a game of social networking "hide and seek" was taking place and as the plaintiff seemed to shift the emphasis in the case from one theory of liability to another, so too did Facebook messages change.¹⁴⁰ In 2008, Sruti Patel (the plaintiff's sister-in-law) sent out a Facebook message to those who attended the party, soliciting favorable witness statements of what happened that night, stating,

We're just asking that everyone give accurate accounts of the night because we all know [Yogesh] did not drink enough to be wasted by that point and we all know that the kid is always acting

132. *See id.*

133. *See id.*

134. *See Patel v. Havana Bar, Rest. & Catering*, No. 10-1383, 2011 WL 6029983 (E.D. Pa. Dec. 5, 2011).

135. *See id.*

136. *Id.* at *1.

137. *Id.*

138. *Id.* at *2.

139. *Id.*

140. *Patel*, 2011 WL 6029983, at *2-3.

crazy even when he's sober because he just loves being the life of the party.¹⁴¹

But by 2010, Sruti was changing course due to plaintiff's counsel's change in focus and sent out a Facebook message seeking witness statements averring that Yogesh did not jump, but rather "fell over the railing."¹⁴²

As troubling as the two Facebook solicitations seeking inconsistent statements were, to compound the situation, the plaintiff failed to produce any of the witness statements he received in response to the 2008 Facebook message.¹⁴³ In fact, the 2010 Facebook message had gone so far as to request that previous witness statements be revised to reflect the "new version" of events, and that statements that were not favorable would not be "included" in what Sruti Patel was gathering to provide to plaintiff's counsel.¹⁴⁴ Only after a witness, during her deposition, acknowledged that he had given a statement did plaintiff's counsel produce any witness statements.¹⁴⁵ Even at that point, only statements responsive to the 2010 Facebook solicitation were turned over; none of the 2008 witness statements were produced.¹⁴⁶ When Sruti Patel was deposed, she testified that the Facebook messages had been pasted into a Microsoft Word document that was printed before all digital copies of it were deleted.¹⁴⁷

The defense sought the ultimate sanction for the spoliation—outright dismissal of the plaintiff's claims.¹⁴⁸ Applying the traditional four-factor test, the court agreed that sanctions were warranted:

First, the 2008 witness statements were in Plaintiff of Plaintiff's family's possession prior to their disappearance. In addition, the statements have never been produced, and the Plaintiff's conduct with respect to the statements, as well as the conduct of his wife and sister-in-law, is very suspect. Furthermore, the statements are relevant as they are witness accounts of the night in question. Lastly, it was reasonably foreseeable that the statements would later be sought in discovery given that witness testimony as to Plaintiff's appearance is crucial to his claim.¹⁴⁹

141. *Id.* at *3.

142. *Id.*

143. *Id.* at *4.

144. *Id.* at *3.

145. *Id.* at *4.

146. *Patel*, 2011 WL 6029983, at *4.

147. *Id.*

148. *Id.* at *10.

149. *Id.*

But the court stopped short of the ultimate sanction of dismissal by holding that such a remedy should only be granted in the most serious of circumstances.¹⁵⁰ Any such decision would depend on the consideration of six factors: 1) the extent of the party's personal responsibility; 2) the prejudice caused to the adversary; 3) any history of dilatoriness; 4) whether the conduct was willful or in bad faith; 5) the extent to which sanctions short of dismissal would be effective; and 6) how meritorious the claim or defense is.¹⁵¹ Based on all of these considerations (and likely the defendant's own spoliation with the video footage), the court granted an adverse inference instruction request, thus allowing the jury to draw its own conclusion about what the evidence would have revealed had the plaintiff been forthcoming.¹⁵² The court also ordered that the defendant be allowed to re-depose several of the plaintiff's witnesses (since their statements had not been furnished prior to their earlier depositions), and awarded defense counsel \$20,000 for attorney's fees and costs associated with trying to obtain the 2008 and 2010 witness statements.¹⁵³

The *Patel* case illustrates not only the importance for attorneys of being aware of what their clients (and, as it turns out, their clients' families) may be up to on Facebook during the pendency of a lawsuit, but also the fact that courts will carefully scrutinize all relevant factors in an effort at crafting a remedy that addresses spoliation and wrongful conduct while stopping short of the "death penalty" sanction of dismissal.¹⁵⁴

F. *Cajamarca v. Regal Entertainment Group*

In this fairly entertaining sexual harassment case, a box office cashier in one of the defendant Regal's theaters complained that a coworker had exposed himself and masturbated in front of her in the break room, a claim vehemently denied by the defense.¹⁵⁵ The court granted summary judgment for the defendants, in part due to electronic evidence that—once recovered after the plaintiff had deleted data from her laptop—seriously undermined the plaintiff's assertions as well as her credibility. As the court observed, there was "little doubt" that the spoliated data "contained pornography and communications that would have undermined her claim regarding the extent of the trauma she suffered as a result of the break room incident, especially since she had prior convictions for prostitution, had worked as a call girl, and

150. *Id.*

151. *Id.* at *11 n.5.

152. *Patel*, 2011 WL 6029983, at *10.

153. *Id.* at *11.

154. *See id.*

155. *Cajamarca v. Regal Entm't Grp.*, 2012 WL 3782437 (E.D.N.Y. Aug. 31, 2012).

had a rather fulsome sexual history, including an interest in sado-masochism.”¹⁵⁶ The court went on to note:

Plaintiff lied at her deposition, and to her own expert psychiatrist, in describing the emotional effects of the break room incident and omitting her own sexual history. In fact, she enjoyed an extraordinarily active travel and social life during the time she described herself as being “bedridden” and in a “vegetative state” as a result of the incident, including enjoying in sexual banter with friends on Facebook.¹⁵⁷

In entertaining a subsequent motion for sanctions against plaintiff’s counsel, the court concluded that it was undisputed that the lawyer “never advised her to preserve the data on the hard drive on her laptop,” and that plaintiff had “deleted information that would be relevant to her claim of PTSD, including social media communications.” Finding that the defendants had been prejudiced by the obstruction of discovery by both the plaintiff and her attorney, the court awarded \$3,000 in sanctions against the plaintiff’s counsel, along with court costs.¹⁵⁸

The *Cajamarca* case underscores the need for attorneys to counsel their clients appropriately to preserve social media content, but also undertake their own due diligence in reviewing the clients’ online selves. As this case illustrates, most reputable lawyers would have thought long and hard before bringing a sexual harassment case on behalf of someone with a history of prostitution and many other skeletons in her digital closet.

G. *Gatto v. United Air Lines, Inc.*

Making a Facebook profile private, changing Facebook profile pictures, and failing to turn over witness statements solicited via Facebook may get a party into trouble, but what about deactivating one’s Facebook account during the middle of discovery? That was the situation confronted by the New Jersey federal court in *Gatto v. United Air Lines, Inc.*¹⁵⁹ Frank Gatto, a baggage handler at JFK Airport, brought a personal injury suit after being struck by a set of stairs used for aircraft refueling on January 21, 2008.¹⁶⁰ Gatto sued Allied Aviation Services (which owned the stairs) and United Airlines (which owned the plane), claiming to be permanently disabled, unable to work, and limited in his physical activities and social life.¹⁶¹

156. *Id.*

157. *Id.*

158. *Id.*

159. See *Gatto v. United Air Lines, Inc.*, No. 10-CV-1090-ES-SCM, 2013 WL 1285285 (D.N.J. Mar. 25, 2013).

160. *Id.* at *1.

161. *Id.*

In July 2011, the defendants sought discovery pertaining to Gatto's social media activities, asking for Facebook "posts, comments, status updates, and other information posted [by the defendant before the accident.]"¹⁶² United Airlines also sent Gatto authorization forms for him to sign that would permit social media and sites such as eBay and PayPal to release his information.¹⁶³ Other discovery requests inquired more specifically into Gatto's mentions of the accident on social media and, also, any eBay business operated by Gatto.¹⁶⁴ Gatto signed the authorization forms for all sites except for Facebook, but ultimately, following a December 1, 2011 conference before U.S. Magistrate Judge Cathy Waldor, the plaintiff was ordered to execute this authorization as well.¹⁶⁵ Gatto agreed to change his Facebook password to "alliedunited" for the purpose of defense counsel accessing documents and information from his Facebook account.¹⁶⁶

From this point, the case sharply diverges. Gatto claimed that he thought there would not be "unauthorized access to the Facebook account online," and his attorney claimed he understood that defense counsel would use the changed password to obtain information from Facebook's corporate offices rather than through online access.¹⁶⁷ In any event, as of December 5, 2011, Gatto had not yet changed the password, prompting United's attorney to contact plaintiff's counsel and request that it be done that day.¹⁶⁸ It was, and defense counsel was able to access Gatto's Facebook account and print off certain materials that day.¹⁶⁹

On December 6, Gatto was notified by Facebook that his account had been accessed by an unknown IP address in New Jersey. Gatto, claiming that he had been through contentious divorce proceedings and was worried about his account being "hacked into," deactivated his Facebook account on December 16, 2011, because "unknown people were apparently accessing my account without my permission."¹⁷⁰ Facebook automatically deleted the data on December 30, 2011.¹⁷¹ Gatto maintained that he was unaware that United's counsel was the one accessing his account until later.¹⁷²

162. *Id.* at *3.

163. *Id.* at *1.

164. *Id.*

165. *Gatto*, 2013 WL 1285285, at *1.

166. *Id.*

167. *Id.*

168. *Id.* at *2.

169. *Id.*

170. *Id.*

171. *Gatto*, 2013 WL 1285285, at *1.

172. *Id.* at *2.

Meanwhile, the attorneys were oblivious to these developments. Facebook advised United's counsel that it would not disclose Gatto's data, but Gatto himself could download the account contents through a "download my profile" button. It was agreed during a January 6, 2012 conference with Judge Waldor that Gatto would download the contents of his Facebook profile, and then provide a copy to the defense along with a certification that he had not made any changes to it since the December 1 conference.¹⁷³ Two weeks later, Plaintiff's counsel had to inform the defense of Gatto's account deactivation and the sad fact that once an account is deleted or deactivated, it cannot be reactivated.¹⁷⁴

As one would expect, the defendants moved for sanctions based on spoliation, claiming not only that the deactivation was intentional, but also that, had all the lost postings been recovered, they would have refuted Gatto's damages claims.¹⁷⁵ Gatto maintained that there was no intentional destruction or suppression of evidence.¹⁷⁶

The court disagreed with Gatto, pointing out that:

Even if plaintiff did not intend to permanently deprive the defendants of the information associated with his Facebook account, there is no dispute that Plaintiff intentionally deactivated the account. In doing so, and then failing to reactivate the account within the necessary time period, plaintiff effectively caused the account to be permanently deleted. Neither defense counsel's allegedly inappropriate access of the Facebook account, nor Plaintiff's belated efforts to reactivate the account, negate the fact that plaintiff failed to preserve the relevant evidence.¹⁷⁷

Applying the familiar four-factor test for spoliation, the court easily concluded that the evidence was 1) within a party's control; 2) relevant; and 3) reasonably foreseeable that it would be discoverable.¹⁷⁸ With the fourth factor—whether or not there was "an actual suppression or withholding" of evidence—the court struggled a bit before finding that this prong, too, had been satisfied.¹⁷⁹ In weighing the appropriate sanction, U.S. District Judge Mannion ultimately declined to assess monetary sanctions since Gatto's "destruction of evidence does not appear to be motivated by fraudulent purposes

173. *Id.*

174. *Id.*

175. *Id.* at *4. The limited materials printed out by defense counsel purportedly showed Gatto taking vacations, participating in social activities, and running an eBay business.

176. *Id.*

177. *Gatto*, 2013 WL 1285285, at *24.

178. *Id.* at *3.

179. *Id.* at *4.

or diversionary tactics, and the loss of evidence will not cause unnecessary delay.”¹⁸⁰ However, the court did grant the defense’s request that an instruction be given at trial to the jury that it may draw an adverse inference against Gatto for failing to preserve his Facebook account and for intentional destruction of evidence.¹⁸¹

As this recent case shows, with social media evidence playing an increasingly pivotal role in litigation courts have embraced its importance, are very willing to consider deleting such data as spoliation, and assess punishment accordingly. Yet *Gatto* should also serve as a cautionary tale, not only for litigants, but also for their attorneys. Allowing any kind of unfettered access to a client’s social networking account is never a good idea, and as the *Gatto* case illustrates, a number of misunderstandings can ensue.¹⁸² Narrowly-tailored discovery requests are always preferable to the broad, global “give us your entire Facebook profile” type of request.

Additionally, client communication and careful drafting of discovery rulings and agreements are key, and could very well have avoided the *Gatto* scenario in which the attorneys on each side have different concepts of how the access will take place (i.e., via Facebook’s corporate offices or by directly accessing the account itself with the changed password). Plaintiff’s counsel was unaware of his client’s actions before making representations on his behalf in a conference with the court. Finally, the attorneys on both sides would have benefited from being more familiar with social networking sites and their functionality, as well as with the severe limitations of seeking information directly from a site like Facebook.

H. *Allied Concrete Co. v. Lester*

Allied Concrete v. Lester is arguably the most talked-about case of social networking spoliation, where the issue of attorney involvement in and direction of a party’s obstructionist efforts regarding social media evidence comes to fruition.¹⁸³ *Lester* looked like a slam-dunk wrongful death case for the plaintiff’s attorney: on June 21, 2007, a speeding Allied Concrete cement truck crossed the center line, tipped over, and crushed the vehicle containing Jessica Lester.¹⁸⁴ Jessica, a young wife, later died from her injuries.¹⁸⁵ Liability was not an issue—the cement truck driver pleaded guilty to manslaughter—

180. *Id.* at *5.

181. *Id.*

182. See, e.g., John G. Browning, *With “Friends” Like This, Who Needs Enemies? Passwords, Privacy, and the Discovery of Social Media Content*, 36 AM. J. TRIAL ADVOC. 505 (Spring 2013) (discussing the recent trend in favor of rejecting parties’ demands for an opponent’s Facebook passwords).

183. See *Allied Concrete Co. v. Lester*, 736 S.E.2d 699 (Va. 2013).

184. *Id.* at 701.

185. *Id.*

ter.¹⁸⁶ The surviving husband, Isaiah Lester, filed a wrongful death lawsuit in May 2008.¹⁸⁷ He had capable counsel—Matthew B. Murray, a partner in the largest plaintiffs personal injury firm in the state and a past president of the Virginia Trial Lawyers Association. In December 2010, a Charlottesville, Virginia jury awarded Mr. Lester \$8.58 million in damages (Jessica Lester's surviving parents each received \$1 million).¹⁸⁸

Interestingly, a curious thing happened on the way to the courthouse. On January 9, 2009—while the lawsuit was pending—Isaiah Lester sent a message on Facebook to one of the defense attorneys at Patton Boggs, David Tafuri.¹⁸⁹ No court order or pleading has ever explained this bizarre turn of events, but in an interview with the author, Mr. Tafuri shed some light:

Mr. Lester sent me a message on Facebook, saying something along the lines of “see you in March,” referring to an upcoming trial setting. It was meant as kind of a taunt—that’s the kind of plaintiff Lester was. On Facebook at that time, that message opened up his profile for viewing. I did not respond to his message, since it would be unethical to communicate with him directly and not go through his attorney.¹⁹⁰

The defense printed off a number of photos from Lester's Facebook page thanks to his inadvertent invitation, and on March 25, 2009, the defense counsel issued a discovery request to the plaintiff, seeking “screen print copies on the day this request is signed of all pages from Isaiah Lester's Facebook page including, but not limited to, all pictures, his profile, his message board, status updates, and all messages sent or received.”¹⁹¹ Attached to the discovery request was a copy of one of the photographs Mr. Tafuri had downloaded off of Lester's Facebook page.¹⁹² It depicted Lester surrounded by women, holding a beer can, and wearing a T-shirt that reads “I [heart] hot moms”—not quite the portrait of a grieving widower!¹⁹³ That evening, Mr. Murray sent an email to his client about the discovery request and the attached photo.¹⁹⁴ The following day, Murray instructed his paralegal to have Lester “clean up” his Facebook page because “[w]e do not want any blow-

186. *Id.*

187. *Id.*

188. *Id.*

189. *Lester*, 736 S.E.2d at 701

190. Interview with David Tafuri, Partner, Patton Boggs (July 15, 2013).

191. *Lester*, 736 S.E.2d at 702.

192. *Id.*

193. *Id.*

194. *Id.*

ups of this stuff at trial.”¹⁹⁵ The paralegal emailed Lester (as part of a thread that would later be referred to as “the stink bomb email”) directing him to “clean up” his Facebook page because “[w]e do NOT want blow ups of other pics at trial so please, please clean up your [F]acebook and [M]yspace!”¹⁹⁶

On April 14, 2009, Lester informed the paralegal that he had deleted his Facebook page.¹⁹⁷ The next day, plaintiff’s counsel served an answer to the discovery request, with Lester’s statement that “I do not have a Facebook page on the date this is signed, April 15, 2009.”¹⁹⁸ Allied Concrete’s lawyers filed a motion to compel, and plaintiff’s counsel contacted Lester.¹⁹⁹ He reactivated his Facebook page, and his lawyers were able to print off copies of what was then on the profile; however, consistent with the advice to “clean up” his Facebook page, Lester had already deleted at least sixteen photos from his profile.²⁰⁰ However, according to Mr. Tafuri, there was evidence to suggest that considerably more than sixteen photos had been deleted, but the defense forensics expert was only able to definitively show spoliation of sixteen photos.²⁰¹

In May and October 2009, plaintiff’s counsel provided additional, “updated” copies of Lester’s Facebook page.²⁰² At a December 2009 deposition, Lester denied deactivating his Facebook page, but Allied Concrete would later subpoena Facebook and obtain testimony that contradicted Lester.²⁰³

As a sanction for the spoliation, the trial court gave two adverse inference instructions to the jury (one while Lester was testifying, the other before closing arguments), instructing them to presume “that the photograph or photographs [Lester] deleted from his Facebook account were harmful to his case.”²⁰⁴ The court also sanctioned Lester and his attorney \$722,000 for their misconduct (\$542,000 against Murray and \$180,000 against Lester) and to cover Allied Concrete’s attorney’s fees and costs in addressing the Facebook spoliation.²⁰⁵ The court, in response to a motion for new trial, also sharply

195. *Id.*

196. *Id.*

197. *Lester*, 736 S.E.2d at 702.

198. *Id.*

199. *Id.*

200. *Id.*

201. *Id.* at 702–703.

202. Interview with David Tafuri, *supra* note 190.

203. *Lester*, 736 S.E.2d at 703. The Virginia Supreme Court would later note that Lester made a number of false statements during discovery, including lying about supposed volunteer work, his use of antidepressants, and his history of depression.

204. *Id.*

205. *Id.*

reduced the plaintiff's verdict by \$4.127 million, but ostensibly for reasons unrelated to the spoliation.²⁰⁶ In his order sanctioning the Plaintiff and plaintiff's counsel, Charlottesville Circuit Judge Edward Hogshire was appalled at the spoliation and misconduct on the plaintiff's side, referring to "the extensive pattern of deceptive and obstructionist conduct of Murray and Lester."²⁰⁷ However, he denied the defense's request for a new trial.²⁰⁸

In January 2013, the Virginia Supreme Court vacated the remittitur and reinstated the original verdict, but the sanctions levied against Murray and Lester remained in place.²⁰⁹ It upheld Judge Hogshire's denial of the defendant's motion for new trial, holding that "Allied Concrete was fully aware of the misconduct of Murray and Lester prior to trial and the trial court took significant steps to mitigate the effect of the misconduct."²¹⁰

Was this the correct result? Probably so; after all, the trial court levied whopping sanctions in response to the spoliation and related misconduct, and gave an adverse inference instruction to the jury. When applying one factor in any instance of spoliation to the *Lester* case—the prejudice or harm to the moving party—Allied Concrete suffered relatively little prejudice in the sense it had the relevant evidence available at trial, although it was initially unavailable due to plaintiff's deletion.

More importantly, *Lester* leaves an important legacy for lawyers and litigants alike. First of all, lawyers should know what their clients are doing. Allied Concrete stumbled across Lester's digital treasure trove only because he chose to tauntingly communicate with a defense attorney on Facebook—not the smartest move. Second, *Lester* underscores the importance of lawyers' duty of competent representation encompassing familiarity with the risks and benefits of technology. Murray should have known enough about Facebook, or retained someone with enough knowledge, to not attempt the misconduct and misrepresentations that were made. When an attorney sends opposing counsel discovery requests with the opposing party's Facebook pictures, he clearly already has most, if not all, of what he is seeking. Murray even went so far as to accuse the defense of hacking into his client's Facebook account in a motion for sanctions, which was denied, and for which Murray himself was sanctioned.

As a postscript, Murray later resigned from his firm. That, however, did not shield him from Virginia State Bar disciplinary charges. After a Bar in-

206. *Id.* at 704.

207. *Lester v. Allied Concrete Co.*, 2011 WL 9688369, ¶ 4 (Va. Cir. Ct. Oct. 21, 2011).

208. *Id.*

209. *Lester*, 736 S.E.2d at 709.

210. *Id.*

vestigation found misconduct, Murray faced a disciplinary hearing.²¹¹ Prior to that taking place, he and the Virginia State Bar entered into an agreed disposition of the charges, which were based on violations of candor, fairness to opposing parties and counsel, and engaging in “dishonesty, fraud, deceit, or misrepresentation.”²¹² On July 17, 2013, Murray’s law license was suspended for five years.²¹³

V. WHAT DOES THE FUTURE HOLD?

At least one commentator has made a Swiftian “modest proposal” for dealing with the information overload that comes with the ever-expanding world of electronic communications subject to discovery.²¹⁴ “Without a showing of extraordinary circumstances by the requesting party,” says Douglas J. Good, “treat electronic communications like conversation and eliminate production of electronic communications in either electronic or hard copy format.”²¹⁵ Such an approach is unlikely at best in an increasingly complex world of discovery in the Digital Age, as people share more than ever using a bewildering array of digital platforms that almost render Facebook quaint by comparison. Lawyers will continue to push the envelope of electronic discovery as long as individuals increasingly share more of themselves online, hoping for the ever-elusive smoking gun piece of evidence.

In today’s world, a spoliation claim may never even get out of the gate, thanks to the self-editing applications that currently populate the Internet. Want to delete your web history to thwart Google’s combining of your online browsing history with data from YouTube and Google Plus? The Electronic Frontier Foundation will give you step-by-step directions. Want to “moderate” (i.e., delete) the comments on your own Facebook posts? As of May 2013, there is an Android app for that.²¹⁶ Want to go in the opposite direc-

211. *Lawyer in Wrongful-Death Suit Murray Faces Disciplinary Hearing*, DAILY PROGRESS (July 9, 2013), http://www.dailyprogress.com/news/local/lawyer-in-wrongful-death-suit-murray-faces-disciplinary-hearing/article_2ecd1c58-e8f9-11e2-aa10-001a4bcf6878.html.

212. Bryan McKenzie, *Charlottesville Attorney’s Law License Suspended*, DAILY PROGRESS (July 30, 2013), http://www.dailyprogress.com/news/charlottesville-attorney-s-law-license-suspended/article_8c84b89a-f990-11e2-91d5-0019bb30f31a.html.

213. *Disciplinary System Actions*, VIRGINIA STATE BAR, <http://www.vsb.org/disciplinary.html> (last visited Nov. 4, 2013).

214. See Douglas J. Good, *A Modest Proposal to Resolve the E-Discovery Crisis*, N.Y. L.J., May 16, 2011, available at http://rmfpc.com/wp-content/uploads/2012/10/Good_ModestProposal.pdf.

215. *Id.* at 4.

216. Jason Cipriani, *How to Delete Facebook Activity Using iPhone, Android App*, CNET (Aug. 1, 2013), http://howto.cnet.com/8301-11310_39-57477912-285/how-to-delete-facebook-activity-using-iphone-android-app.

tion, and locate those deleted tweets that some elected official or celebrity probably never should have tweeted in the first place? If you did not feel like researching the 73 billion or so tweets archived by the Library of Congress, you could have had an easier time by consulting the site Undetweetable—at least until it shut down at Twitter’s request.²¹⁷

Tinkering with existing platforms, however, is not the only factor that may impact considerations of spoliation. New technology is making it easier for a person’s bad decisions to vanish into thin air. Consider Snapchat, a photo-messaging application developed by four Stanford students in September 2011. Snapchat purportedly allows users to take photos or record videos, add text, and send them to a controlled list of recipients; the user sets a time limit (up to 10 seconds) for how long recipients can view the photo—after which it will be deleted from the recipient’s device and Snapchat’s servers. The app has been very successful, particularly in the 13–25 year-old demographic. As of May 2013, users were uploading over 150 million photos using Snapchat.²¹⁸ But Snapchat has not existed without controversy. Critics say it has encouraged teens to “sext” inappropriate photos to each other. In May 2013, the Electronic Privacy Information Center filed a complaint against Snapchat with the Federal Trade Commission (FTC), claiming the company’s representations that pictures self-destruct within seconds of viewing was deceptive, since a number of experts report that photos can be retrieved well after the expiration of their time limits.²¹⁹

Wickr is a security-focused app that uses military-grade encryption to send text, video, voice, and document files that can self-destruct after a designated period of time.²²⁰ Similarly, the Android app Gryphn serves as an encryption tool for text messages, videos, and images; such encryption makes it difficult for recipients to “capture” the information sent through a screen grab or other methods.²²¹ Ansa, an app that promises its users that “you can communicate off the record, so no trace of your conversation is left behind,” deletes messages and media seconds after being read—from the

217. Sarah Anne Hughes, *Undetweetable Archives Deleted Tweets, Gets Warning from Twitter*, WASH. POST (Aug. 4, 2011), http://www.washingtonpost.com/blogs/blogpost/post/undetweetable-archives-deleted-tweets-gets-warning-from-twitter/2011/08/04/gIQAqlBuI_blog.html.

218. Maude Standish, *New Tech Makes Our Bad Decisions Disappear*, HUFFINGTON POST (May 21, 2013), http://www.huffingtonpost.com/maude-standish/new-tech-makes-our-bad-de_b_3307697.html.

219. Lorenzo Franceschi-Bicchierai, *Forensic Experts Poke Holes in Snapchat and Facebook*, MASHABLE (Aug. 7, 2013), <http://mashable.com/2013/08/07/forensic-snapchat-facebook-poke>.

220. *About*, WICKR, <https://www.mywickr.com/en/about.php>.

221. Jeffrey Taylor, *Android App Review: Gryphn Secure Mobile Messaging*, THE DROID LAWYER (Jan. 30, 2013), <http://thedroidlawyer.com/2013/01/android-app-review-gryphn-secure-mobile-messaging>.

sender's mobile device, the recipient's mobile device, and Ansa's servers. This "self-destruct option," for those prone to drunk texting or other exercises in poor judgment, is free and available for iOS as well as Android devices.²²²

However, few tools have attracted the attention that Vaporstream has when it comes to keeping electronic communications confidential by adding a "vanishing act" component.²²³ When Vaporstream software is installed on a computer or smartphone, messages disappear from the sender's device as soon as they are sent, and vanish from the recipient's device as soon as they are read or replied.²²⁴ The software itself is peer-to-peer, so unlike email, the messages are never stored on an intermediate server.²²⁵ Vaporstream's limitations are straightforward but daunting: you can use it only to communicate with other subscribers, like top executives at a given company, and it comes with a hefty price tag costing as much as \$25,000 per month for as many as fifty employees.²²⁶

According to Vaporstream's website, Vaporstream does not create ESI and "[m]essages cannot be intercepted, copied, forwarded, printed, stored or even traced."²²⁷ Moreover, Vaporstream's developers seem to have anticipated the typical lawyer questions. Preservation obligations and litigation holds would not apply, according to the Vaporstream website, since "[u]sing Vaporstream would be no different than talking face-to-face over lunch or at the water cooler."²²⁸ Elsewhere, the site says reassuringly that "[j]ust because Vaporstream does not create a record in the first place, does not make one guilty of spoliation."²²⁹ Vaporstream boasts that it protects the private information "of over 150 corporate customers," ranging from the military and government entities, to banking and financial institutions, healthcare companies, and even law firms.²³⁰

222. Tim Baran, *Ansa—App of the Week: Make Sent Texts, Videos and Photos Disappear*, LEGAL PRODUCTIVITY (Nov. 1, 2013), <http://www.legalproductivity.com/apps/mobile-apps-ansa-disappearing-messages/>.

223. *FAQ*, VAPORSTREAM, available at <https://www.vaporstream.com/faq> (last visited Aug. 23, 2013).

224. *Id.*

225. *Id.*

226. David Hechler, *Electronic Messages that Vanish Without a Trace*, CORPORATE COUNSEL (Apr. 22, 2013), http://www.law.com/corporatecounsel/PubArticleCC.jsp?id=1366357473618&Electronic_Messages_That_Vanish_Without_a_Trace&goback=%2Egde_3746417_member_235301621#%21.

227. VAPORSTREAM, *supra* note 223, at 2.

228. *Id.* at 3.

229. *Id.* at 4.

230. *Id.*

What are the legal implications of technology seemingly engineered to frustrate the efforts of a legal system that has carefully cultivated a body of jurisprudence to protect against those who would thwart discovery? Could white-collar criminals use a product like Vaporstream for insider trading tips? Vaporstream CEO Jim Howe says he is aware of at least 31 cases in which lawyers tried to introduce evidence of a company's use of Vaporstream—none of which succeeded, according to Howe.²³¹ There are those who welcome advances in technology that would allow electronic communications, like the *Mission: Impossible* tapes of the 1960s television show, to “self-destruct in five seconds.” Tarun Wadhwa observes that “[t]he same generation being blamed for the supposed ‘death of privacy’ has become wiser than those who are criticizing them.”²³²

Thanks to technology, concerns over spoliation of evidence have moved past more mundane worries about shredding documents to confronting a world of seemingly endless data and metadata being shared (some might say overshared) with the frightening speed of a search engine on social networking platforms like Facebook, YouTube, and Twitter. The permanence of the Internet has ensured that even the most questionable digital legacies on some individual's social media profiles will live on in cyber-infamy—what Jimmy Buffett might describe as a “permanent reminder of a temporary feeling.”²³³

As the cases analyzing spoliation in the social media context illustrate, the law continues to struggle with the application of 20th century (and earlier) concepts to 21st century technology. Sadly, the most consistent theme throughout the social media spoliation cases discussed in this article is that of casual disregard for, or even discomfort with, the social networking platforms that now permeate our lives. Litigants freely and casually post the most intimate details of their lives online—digital intimacy having become the new norm—only to be outraged over the violation of “privacy” as they are hoisted on their own digital petard during discovery. Meanwhile, lawyers and judges continue to wrestle with the challenges that social media content presents to the traditional litigation framework of discovery and evidentiary issues. As technology continues to advance toward more quicksilver modes of communication, lawyers and judges have no choice but to acknowledge the new reality: being competent means knowing the benefits and risks that technology poses to one's practice and consciously choosing to leave dinosaurs behind in favor of avatars.

231. Hechler, *supra* note 226.

232. Tarun Wadhwa, *Beyond Sexting: We Should Celebrate Snapchat and Encourage Ephemeral Communication*, HUFFINGTON POST (May 22, 2013), http://www.huffingtonpost.com/tarun-wadhwa/ephemeral-texting_b_3316942.html.

233. JIMMY BUFFET, *Permanent Reminder of a Temporary Feeling*, on BEACH HOUSE ON THE MOON (Island Records 1999).