Arkansas Association of Defense Counsel

March 7, 2016

PRACTICE POINTERS FOR NON-TECHIES

By: Edie Ervin, Jamie Huffman Jones, and Kathy McCarroll

Friday, Eldredge & Clark, LLP

Practice Point No. 1: competent representation requires knowledge of Tweets, Tumblr, and almost everything in between.

Model Rule of Professional Conduct 1.1 governs the attorney's duty of competent representation.[1] In 2012, the American Bar Association revised the Rule to clarify that competent representation includes keeping current with "the benefits and risks associated with relevant technology."[2] Although the Arkansas Rules have not been amended to encompass this change, it is clear that the sheer pervasiveness of social media now requires practitioners to familiarize themselves with the various platforms, stay abreast of technological changes, and inform their clients accordingly. Indeed, when it comes to social media, "[t]he proverbial train has left the station, and those lawyers who remain behind are likely to find themselves not only behind the learning curve and subject to humiliation, but also with heightened exposure to court sanctions, disciplinary action, and malpractice claims."[3]

---

[1] ABA, Model Rules of Professional Conduct, R. 1.1, available, http://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/model_rules_of_professional_conduct_table_of_contents.html (last visited January 13, 2016).

[2] *See id.* at cmt. 8. Note that the ABA Commission on Ethics 20/20 stated that it intended the amendment to remind lawyers that to remain competent, they should stay up to date on technology. The amendment was not intended to create an additional obligation. ABA Commission on Ethics 20/20, Resolution & Report to the House of Delegates on Technology & Confidentiality, http://www.americanbar.org/content/dam/aba/administrative/ethics_2020/2012_hod_annual_meeting_105a_filed_may_2012.authcheckdam.pdf.

[3] Jan L. Jacobowitz & Danielle Singer, *The Social Media Frontier: Exploring a New Mandate for Competence in the Practice of Law*, 68 U. Miami L. Rev. 445, 460 (2014).

Thus, in today's world, competent representation includes "advis[ing] clients . . . concerning what steps to take to mitigate any adverse effects on the clients' position emanating from the clients' use of social media."[4] Failure to so advise may have significant consequences for the client. For example, consider the case of Patrick Snay, the former head of Gulliver Preparatory School in Miami.[5] He sued his employer for age discrimination and obtained an $80,000 settlement, plus $10,000 in back pay and $60,000 in attorney's fees. Shortly after the deal, Snay's daughter took to Facebook and posted the following message to her 1,200 friends:

> Mama and Papa Snay won the case against Gulliver. Gulliver is now officially paying for my vacation to Europe this summer. SUCK IT.

As the message went viral, school officials learned about it and refused to honor the settlement. Specifically, they contended that the Facebook message violated a confidentiality agreement included in the deal. An appellate court agreed and voided the settlement—meaning no more European vacation for the Snays.

Your client's social media use may also land him or her in jail. That's what happened to Thomas Gagnon, a Massachusetts man who had recently given his girlfriend a $4,000 diamond engagement ring.[6] Not only did Gagnon's girlfriend reject his offer, she then got a restraining order prohibiting him from contacting her. Soon thereafter, the girlfriend received an invitation to join Gagnon's Google+ circle. She promptly printed the invitation and delivered it to the local authorities, which then arrested Gagnon for violating the restraining order. Gagnon's attorney claimed that his client did not send the Google+ invitation and suggested "it might have been sent by a robot." The judge set Gagnon's bail at $500, ordered him to stay away from his girlfriend's home, and mandated he obey the restraining order going forward.

In addition to advising clients about the ramifications of social media use, the lawyer's duty of competence may require use of the Internet and social media in certain situations.[7] This is because social media can be a treasure trove of information, especially for personal injury, employment, and family lawyers, who can find "evidence of

---

[4] NY Cnty. Lawyers' Ass'n, Formal Op. 745 (2013), https://www.nycla.org/siteFiles/Publications/Publications1630_0.pdf ("Thus, 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.").

[5] Matthew Stucker, *Girl Costs Father $80,000 with 'SUCK IT' Facebook Post*, CNN, http://www.cnn.com/2014/03/02/us/facebook-post-costs-father/index.html (Mar. 4, 2014).

[6] Julie Manganis, *Unwanted Invitation Lands Beverly Man in Trouble*, The Salem News, http://www.salemnews.com/local/x1221263334/Unwanted-invitation-lands-Beverly-man-in-trouble (Dec. 21, 2013).

[7] Jacobowitz & Singer, *supra* note 2, at 466.

infidelity, bad tempers, bad behavior, and exaggeration or lying about injuries sustained."[8] A failure to adequately investigate social media may also give rise to a malpractice claim.[9]

Generally, electronically stored information, including social media content, is discoverable.[10] Competent (and successful) lawyers now use social media content to open the doors to much more than publicly available content. For example, in the principal case of *Romano v. Steelcase, Inc.* the plaintiff claimed permanent injuries requiring her to give up many of her life activities and essentially rendering her bed ridden.[11] Yet, the defendants presented evidence from the public portions of the plaintiff's Facebook and MySpace pages showing that subsequent to the incident, the plaintiff enjoyed an active lifestyle and had even traveled out of state to Florida and Pennsylvania.[12] Indeed, photographs on Facebook showed her outside her home "smiling happily."[13] As a result, the court ordered the plaintiff to provide access to the private portions of her social media sites, as there was a "reasonable likelihood" of finding further evidence material and necessary to the defense.[14]

Note that social media usage has also become a tool for law enforcement and prosecutors in the criminal arena. For example, in *United States v. Meregildo*, the government obtained access to a suspects Facebook profile through one of his "friends" that agreed to cooperate as a witness.[15] The government then relied on the Facebook content as the probable cause for a search warrant.[16] In a motion to suppress evidence obtained from the warrant, the court held that there is no expectation of privacy when Facebook messages are published to "friends," and as a result, the government does not violate the Fourth Amendment by accessing the content through a cooperating witness who is a "friend."[17]

As the case law in this arena is growing, one thing seems to be clear: competent lawyers must familiarize themselves with social media. While one need not have 1,000 followers on Twitter or maintain a microblog, lawyers at a minimum must know these platforms exist. And more importantly, lawyers must be cognizant of the fact that their clients, as well as adverse parties, are likely using them. As such, competent representation requires two things:

---

[8] E. Lackey Jr., *Lawyers and Social Media: The Legal Ethics of Tweeting, Facebooking and Blogging*, 28 Touro L. Rev. 149, 173–74 (2012).

[9] Jacobowitz & Singer, *supra* note 2, at 483.

[10] *See* Fed. R. Civ. P. 26(b)(2)(B); Ark. R. Civ. P. 26.1.

[11] 907 N.Y.S.2d 650, 653–54 (N.Y. Sup. Ct. 2010).

[12] *Id.* at 653.

[13] *Id.* at 654.

[14] *Id.*

[15] 883 F. Supp. 2d 523, 525–26 (S.D.N.Y. 2012).

[16] *Id.* at 526.

[17] *Id.*

advising clients about the consequences of social media activities and investigating social media networks for potential evidence.

Practice Point No. 2: The ethical duty to preserve information extends to the Facebook photo of your client holding a beer and sporting an "I ♥ hot moms" t-shirt.

Because social media and other electronic content is often relevant evidence, lawyers have a duty to preserve it.[18] A failure to do so may result in a variety of sanctions for spoliation of evidence.[19] Spoliation is defined as "the intentional destruction of evidence and when it is established, the factfinder may draw an inference that the evidence destroyed was unfavorable to the party responsible for its spoliation."[20] This is exactly what occurred in the recent case of *Gatto v. United Airlines, Inc.*[21] In *Gatto*, the plaintiff allegedly sustained permanent and debilitating injuries when he was hit by a United baggage aircraft, operated by Allied Aviation Services, while working as a grounds operations supervisor for JetBlue at JFK Airport.[22] The defendants, United and Allied, requested information related to the plaintiff's social media accounts, including Facebook.[23] Before a magistrate, both parties agreed that the plaintiff would change his password and provide the defendant with it to access his Facebook account.[24] Shortly, thereafter counsel for United logged into the account although Allied did not.[25] Plaintiff then claimed to have received a notification from Facebook that his account had been accessed by an unknown IP address.[26]

Meanwhile, Facebook was served with a subpoena to provide information about the plaintiff's account.[27] Facebook objected and suggested that plaintiff download the content and provide it to the defendants.[28] The parties agreed to this proposal; however, a month later counsel for the plaintiff advised that the account had been deactivated and all data was lost.[29] Plaintiff asserted that he deactivated the account in response to Facebook's

---

[18] *See Zubulake v. UBS Warburg, LLC*, 220 F.R.D. 212, 217 (S.D.N.Y. 2003); *see also* Paul G. Lannon, Jr., *The Duty to Preserve Electronic Evidence: When It Is Triggered and How to Satisfy It*, Boston B.J., March/April 2007.

[19] *See* Fed. R. Civ. P. 37(e).

[20] *Rodgers v. CWR Constr. Inc.*, 343 Ark. 126, 33 S.W.3d 506, 510 (2000) (quoting *Goff v. Harold Ives Trucking, Co.,* 342 Ark. 143, 27 S.W.3d 387, 388 (2000)).

[21] No. 10–cv–1090–ES–SCM, 2013 WL 1285285 (D. N.J. Mar. 25, 2013).

[22] *Id.* at *1.

[23] *Id.*

[24] *Id.*

[25] *Id.* at *2.

[26] *Id.*

[27] *Gatto*, 2013 WL 1285285 at *2.

[28] *Id.*

[29] *Id.*

notification that an unknown IP address had accessed it, even though counsel for United had admitted to using the password provided to view the Facebook page.[30] As a result, the court ordered that a jury instruction be given at trial that it may draw an adverse inference against the plaintiff for failing to preserve his Facebook account and intentionally destroying evidence.

Spoliation can also result in heavy monetary sanctions for both the offending attorney and his or her client. Take the case of *Allied Concrete Co. v. Lester*,[31] which involved a wrongful death action against Allied concrete stemming from a car's collision with a concrete-laden truck.[32] During the course of the litigation, the plaintiff sent a Facebook message to an attorney for Allied Concrete, which gave him access to the plaintiff's profile.[33] Counsel for Allied then downloaded a picture of the plaintiff holding a can of beer and sporting an "I ♥ hot moms" t-shirt.[34] Counsel attached the image to a discovery request propounded to plaintiff's counsel.[35] Plaintiff's counsel then instructed a paralegal to tell the client to clean up his Facebook page. [36]Accordingly, the paralegal emailed the plaintiff about the photo and told him that there were "some other pics that should be deleted" from his Facebook page.[37] In a follow-up email, the paralegal reiterated to the client that "[w]e do NOT want blow ups of other pics at trial so please, please clean up your facebook and myspace!"[38]

Thereafter, plaintiff deleted his Facebook page, and his counsel replied to the defendant's discovery request by stating, "I do not have a Facebook page on the date this is signed."[39] Defendants then brought a motion to compel.[40] Although the plaintiff later reactivated his account, he had deleted sixteen photos.[41] After compelling production of the emails between the plaintiff, paralegal, and plaintiff's attorney, and hiring an expert, all of the photos were later produced to defendants.[42] Nonetheless, the court sanctioned the plaintiff's attorney to the tune of

---

[30] *Id.*

[31] 736 S.E.2d 699 (Va. 2013).

[32] *Id.* at 701.

[33] *Id.* at 702.

[34] *Id.*

[35] *Id.*

[36] *Lester*, 736 S.E.2d at 702.

[37] *Id.*

[38] *Id.*

[39] *Id.*

[40] *Id.*

[41] *Id.*

[42] *Lester*, 736 S.E.2d at 703.

$542,000.[43] It also sanctioned the client in the amount of $180,000 to cover Allied's attorney's fees and costs incurred by the misconduct.[44] In addition, the trial court gave the jury an instruction about the misconduct twice, once during the plaintiff's testimony and once before the case went to the jury for deliberations.[45]

The aforementioned cases are just the most recent examples of courts' disciplining attorneys, and their clients, for the spoliation of social media evidence. Deleting emails and text messages can result in similar penalties.[46] To avoid sanctions, attorneys should be aware of relevant electronic evidence, including in the social media sphere, and preserve it accordingly when litigation is anticipated.

Practice Point No. 3: HIPAA violations lurking online, in your iPhone, and on your social networks.

Attorneys who handle medical data or who represent healthcare clients should be aware of the perils of social media, as well as texting and email, with respect to the Health Insurance Portability and Accountability Act of 1996 (HIPAA). HIPAA's primary mandates—the Privacy Rule and the Security Rule—apply only to "covered entities" and "business associates."[47] Covered entities generally include: (1) health care providers, such as doctors, nurses, pharmacies, and nursing homes; (2) health plans, such as HMO's, employer health plans, and health insurance companies; and (3) healthcare clearinghouses, which are entities that take nonstandard health information and process it into a standard.[48] "Business associates" are generally those entities or persons that are engaged by a covered entity, such as a hospital, to carry out some of its functions, like payment processing.[49] In performing that function, the business associate receives and uses protected health information (PHI).[50] Attorneys who provide legal services to a covered entity are by definition "business associates."[51] In January 2013, the U.S. Department of

---

[43] *Id.*

[44] *Id.*

[45] *Id.* at 705.

[46] *See Se. Mech. Servs., Inc. v. Brody*, 657 F. Supp. 2d 1293, 1302 (M.D. Fla. 2009) (imposing adverse instruction for wiping Blackberries of emails, text messages, and other information).

[47] *Health Information Privacy: For Covered Entities and Business Associates*, U.S. Dep't of Health & Human Servs., http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/index.html (last visited April 10, 2014)

[48] *Id.*

[49] *Id.*

[50] 45 C.F.R. § 160.103; *see also* 45 C.F.R. §§ 160.103 and 164.501 (definition of PHI).

[51] *Id.* § 160.103 (1)(ii).

Health issued its Final Rule implementing several changes to HIPAA, including making business associates directly liable for violating the HIPAA Privacy and Security Rules.[52]

Under the Privacy Rule, generally, a covered entity or business associate may not use or disclose PHI except for an authorized purpose.[53] Emails, Facebook posts, Tweets, and other social media discussion about a patient to an unauthorized individual are electronic forms of PHI if the patient is identifiable and the post discloses something about the patient's condition or status.[54] Thus, disclosure in this context by an attorney or a client who is a covered entity may result in criminal penalties and significant fines, including up to $1.5 million for repeated violations of an identical HIPAA provision within the same calendar year.[55] Similarly, texting or emailing about PHI in an insecure environment can result in violations of HIPAA's Security Rule.[56]

Recent examples of HIPAA violations stemming from social media and online activities include:

- Lawsuit following doctor's discharge for violating HIPAA by commenting on a Facebook picture of an ER patient's backside, identifying the patient by her initials;[57]
- $500 fine, discharge, and reprimand by state medical board given to doctor who talked about a patient on a Facebook page;[58]
- Investigation into potentially the largest HIPPA violation in history involving medical personnel who maintained a group on Facebook about a patient, called "Did you know this alcoholic Indian?"[59]
- Medical center employee discharged and investigated for posting a picture of a patient's x-rays on his Facebook page, despite employee's defended his actions by saying, "People, it's just Facebook...Not

---

[52] Lisa J. Acevedo et. al., *New HIPAA Liability for Lawyers*, GPSOLO July/August 2013: Retirement Planning and Elder Law, http://www.americanbar.org/publications/gp_solo/2013/july_august/new_hipaa_liability_lawyers.html (last visited April 10, 2014).

[53] *See* 45 C.F.R. § 164.506.

[54] *See* D'Arcy Guerin Gue and Steven J. Fox, *Guide to Medical Privacy and HIPAA*, ¶840 Legal Concerns, 2005 WL 4172329 (2013).

[55] Office of the Federal Register, *Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules*, Section 160.404—Amount of a Civil Monetary Penalty, https://www.federalregister.gov/articles/2013/01/25/2013-01073/modifications-to-the-hipaa-privacy-security-enforcement-and-breach-notification-rules-under-the#h-75 (Jan. 25, 2013).

[56] *See* Hilary N. Karasz, et. al., *Text Messaging to Communicate with Public Health Audiences*, Am. J. Public Health, available http://www.medscape.com/viewarticle/781061_2 (last visited April 10, 2014).

[57] Sue Thoms, *Lawsuit Against Spectrum Involving Facebook Comment Shows 'Perils' of Social Media, Attorney Says*, mLive, http://www.mlive.com/news/grand-rapids/index.ssf/2014/03/spectrum_doctors_facebook_comm.html (Mar. 18, 2014).

[58] Chelsea Conaboy, *For Doctors, Social Media a Tricky Case*, The Boston Globe, http://www.boston.com/lifestyle/health/articles/2011/04/20/for_doctors_social_media_a_tricky_case/?page=full (April 20, 2011).
[59] *Largest HIPAA Violation in History Happens on Facebook*, CNNiReport, http://ireport.cnn.com/docs/DOC-311690 (Aug. 9, 2009).

reality. Hello? Again...It's just a name out of millions and millions of names. If some people can't appreciate my humor than tough. And if you don't like it too bad because it's my wall and I'll post what I want to;"[60]

- Arizona physician group fined $100,000 and ordered to take corrective action based on its posting of clinical and surgical appointments for its patients on an Internet-based calendar that was publicly accessible[61]

As these cases illustrate, attorneys who represent covered entities should continually advise their clients about the potential perils of social media, texting, emailing, and other online activities with respect to HIPAA. In fact, prudent attorneys may advise their covered entities to have a policy governing online and social media usage if they do not have on already. Similarly, lawyers who are business associates need to take appropriate precautions to avoid severe penalties under HIPAA's Privacy or Security Rule, or worse, both.

The thanks of the AADC go out to Edie Ervin, Jamie Huffman Jones and Kathy McCarroll of Friday, Eldredge & Clark for drafting this article.



We welcome your articles and thoughts for future editions.

WE ARE BETTER TOGETHER: SUPPORT THE AADC

[60] Susan Abram, *Hospital Employee Allegedly Makes Fun of Patient's Medical Condition on Facebook; Officials Investigating*, Los Angeles Daily News, http://www.dailynews.com/20111229/hospital-employee-allegedly-makes-fun-of-patients-medical-condition-on-facebook-officials-investigating (Dec. 28, 2011)

[61] Howard Anderson, *Arizona Practice Gets $100k HIPAA Fine*, http://www.govinfosecurity.com/arizona-practice-gets-100k-hipaa-fine-a-4686 (April 18, 2012).