Presented:
27th Annual Labor and Employment Law Institute

August 19-20, 2016
Houston, Texas

BIG DATA: LITIGATION TIPS AND TRENDS IN DATA PRIVACY AND SECURITY

Jason S. Boulette

Jason S. Boulette
Michael J. Golden
Steven H. Garrett
Boulette Golden & Marin L.L.P.
2801 Via Fortuna, Suite 530
Austin, TX 78746

jason@boulettegolden.com
512.732.8901
mike@boulettegolden.com
512.732.8902
steven@boulettegolden.com
512.732.9933

TABLE OF CONTENTS

I. INTRODUCTION

Businesses, governments, employers, ordinary citizens, and even attorneys are becoming ever more creative in how they use social media. This paper provides an overview of some of the potential ethical, legal, and evidentiary issues implicated when entities and their attorneys attempt to use social media for gain in dealing with their employees and litigation adversaries.[1]

II. THE DISCIPLINARY RULES AND SELF-HELP DISCOVERY

Social networks like Facebook, Twitter, LinkedIn, and others, and online forums all represent new opportunities for attorneys to conduct discovery cheaply. However, the use of "self-help" discovery instead of the formal discovery process could implicate an attorney's ethical obligations.

A. Early Developments

Blogs were the first example of social media to emerge as fertile ground for informal discovery.[2] Some examples of potential uses of blogs or more "modern" forms of social media for informal discovery purposes include monitoring an opposing party's posts for useful tidbits of information or searching for potential witnesses to support a case.[3]

In this context questions under Rules 4.2 and 4.3 of the Model Rules of Professional Conduct (the "Model Rules") and Rules 4.02 and 4.03 of the Texas Disciplinary Rules of Professional Conduct first

---

[1] The author is an employment attorney and thus approaches most legal issues from the point of view of an employer's relationship with an employee, governmental agency, judge, or jury.

[2] *See, e.g., Goupil v. Cattell*, 2007 WL 1041117 (D.N.H. 2007) (slip copy) (defendant moving to set aside criminal conviction after discovering that the jury foreman had been composing a blog before, during, and after the trial that included the foreman's negative impression of criminal defendants); *Mark Hanby Ministries, Inc. v. Lubet*, 2007 WL 1004169, *6-8 (E.D. Tenn. 2007) (slip copy) (analyzing whether blog postings, among other things, provided sufficient basis for exercise of jurisdiction); *Healix Infusion Therapy, Inc. v. Helix Health LLC*, 2008 WL 1883546 (S.D. Tex. April 25, 2008) (slip copy) (same); *Pitbull Productions, Inc. v. Universal Netmedia, Inc.*, 2008 WL 1700196, *6 (S.D.N.Y. April 4, 2008) (slip copy) (same); *cf. Lorraine v. Markel American Ins. Co.*, 2007 WL 1300739, *39-55 (D. Md. 2007) (analyzing a variety of hearsay exceptions as they relate to blogs and other electronically stored utterances).

[3] *See, e.g., X17, Inc. v. Lavandeira*, 2007 WL 790061, *4 (C.D. Cal. 2007) (not reported in F.Supp.2d) (excluding as hearsay blog entries identifying defendant as the source of allegedly infringing photographs); *Cingular Wireless, LLC v. Hispanic Solutions, Inc.*, 2006 WL 3490802, *1 (N.D. Ga. 2006.) (slip copy) (plaintiff relying on "certain 'blog' chat" to support allegations that defendant made unsolicited phone calls to the mobile phones of plaintiff's customers); *McCabe v. Basham*, 450 F.Supp.2d 916, 924 (N.D. Iowa 2006) (in suit alleging nationwide conspiracy to suppress dissent, plaintiffs moving court to consider an anonymous blog entry from someone claiming the President shot him the bird at a rally in Pennsylvania).

arose. In particular, the use of blogs by litigators raised the issue of whether blogging constituted a "communication" for purposes of the Model Rules and Texas Rules and, if so, whether that communication runs afoul of the rules for communicating with a represented or unrepresented party.

B. The Model Rules and the Texas Rules

According to the American Bar Association, 49 states have rules of professional conduct relating to lawyers that follow the format of the Model Rules.[4] Accordingly, analysis under the Model Rules serves as a useful guideline in addressing questions of lawyers' ethical responsibilities.[5]

The Model Rules and Texas Rules include two rules that generally govern communications by lawyers with persons other than their clients or potential clients. The first, Model Rule 4.2 and Texas Rule 4.02, addresses communication with persons who are represented by counsel, such as adverse parties in litigation:

> In representing a client, a lawyer shall not communicate about the subject of the representation with a person the lawyer knows to be represented by another lawyer in the matter, unless the lawyer has the consent of the other lawyer or is authorized to do so by law or a court order.[6]

The second, Model Rule 4.3 and Texas Rule 4.03, addresses communication with persons who are not represented by counsel:

> In dealing on behalf of a client with a person who is not represented by counsel, a lawyer shall not state or imply that the lawyer is disinterested. When the lawyer knows or reasonably should know that the unrepresented person misunderstands the lawyer's role in the matter the lawyer shall make reasonable efforts to correct the misunderstanding. The lawyer shall not give legal advice to an unrepresented person, other than the advice to secure counsel, if the lawyer knows or reasonably should know that the interests of such a

---

[4] http://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct.html. According to the ABA, only California has not adopted the format of the Model Rules.

[5] Despite the adoption of the form of the Model Rules and their comments in most states, there may be some variation on a state-by-state basis regarding any particular rule or comment. Therefore, the applicable state's version of the rules of professional conduct should be consulted when reviewing questions pertaining to any particular situation.

[6] MODEL R. OF PROF. CONDUCT 4.2; *see also*, TEX. DISCIPLINARY R. PROF. CONDUCT 4.02(a) ("In representing a client, a lawyer shall not communicate or cause or encourage another to communicate about the subject of the representation with a person, organization or entity of government the lawyer knows to be represented by another lawyer regarding that subject, unless the lawyer has the consent of the other lawyer or is authorized by law to do so.").

person are or have a reasonable possibility of being in conflict with the interests of the client.[7]

In other contexts, courts and State and local bar associations have indicated that the rules regarding professional conduct of attorneys apply to online activity.[8] With the background of these professional standards of conduct in mind, this article addresses application of these standards to issues that arise in social media-related discovery.

1. Determining Whether Social Media Constitutes a "Communication"

Use of social media by a lawyer for informal discovery could take several forms. A lawyer might, for example, passively review an opposing party's social media content. Alternatively, the lawyer could take a more active role and post his or her own social media content in an attempt to elicit relevant information regarding his or her opponent or the underlying dispute. Moreover, this activity might all take place on the lawyer's own social media account (*e.g.*, the lawyer's Twitter account), on a social media outlet associated with the opposing party (*e.g.*, the plaintiff's Facebook wall, depending on settings and friend status), or on the social media outlet of a third-party (*e.g.*, an industry message board). As is discussed below, these different uses of interactive websites in informal discovery raise different issues under the Model Rules and Texas Rules.

a. Passive Review

Model Rule 4.2 and Texas Rule 4.02 states that a lawyer shall not "communicate" about the subject of his or her representation with a person the lawyer knows to be represented. The passive review of a

---

[7] MODEL R. OF PROF. CONDUCT 4.3; *see also*, TEX. DISCIPLINARY R. PROF. CONDUCT 4.03 ("In dealing on behalf of a client with a person who is not represented by counsel, a lawyer shall not state or imply that the lawyer is disinterested. When the lawyer knows or reasonably should know that the unrepresented person misunderstands the lawyer's role in the matter, the lawyer shall make reasonable efforts to correct the misunderstanding.").

[8] *See, e.g.*, South Carolina Ethics Opinion 09-10 http://www.scbar.org/MemberResources/EthicsAdvisoryOpinions/OpinionView/ArticleId/107/Ethics-Advisory-Opinion-09-10.aspx (stating that "Lawyers are responsible for all communications they place or disseminate, or ask to be placed or disseminated for them, regarding their law practice." And opining that if a lawyer "claims" a listing on a lawyer review website he or she is responsible for all information contained there); *United States v. Khan*, 538 F. Supp. 2d 929 (E.D.N.Y. 2007) (cautioning an attorney to review the postings on his website in light of New York's Disciplinary Rules and to "comport himself in a manner that adheres to these rules"). In addition, the court commented that the attorney's online postings also may be subject to the codes of professional conduct of other states. *Id.*

party's social media content is unlikely to be construed as a "communication," because there is no direct interaction between the party who posted the information and the lawyer reviewing it.[9] Rather, this use of a social media seems to be more comparable to a review of an unprivileged document voluntarily produced by the party.

b. Affirmative Posting

By contrast, an attorney who affirmatively and independently posts content in an attempt to gather information relevant to the subject matter of a dispute risks violating Model Rule 4.2 and Texas Rule 4.02. In assessing this risk, it is important to consider, among other things, whether the affirmative post by the attorney is an original post or a response to pre-existing post. It is also important to consider whether the post by the attorney is on the attorney's social media outlet or on someone else's.

i. Original Posting

In contrast to a passive review of online content, an attorney who initiates an original post seeking to elicit a response from a represented party appears to fall squarely within the Rules' prohibition against communicating with a represented party about the subject matter of representation without the consent of opposing counsel. In short, the initiation of an original post by an attorney appears to be a "communication" with the represented party.[10] Consider the following hypothetical. A plaintiff's lawyer posts to an online forum related to a company-defendant in search of current employees of the company-defendant who might be able to corroborate the plaintiff's version of events, thereby circumventing the company's lawyers. This active, affirmative act of posting in a forum known to be frequented by representatives of the employer-defendant (including managerial representatives) is likely to run afoul of Model Rule 4.2 and Texas Rule 4.02 because (1) a lawyer, (2) is initiating communication with persons who may be representatives of the

---

[9] Oregon Ethics Opinion 2013-189 at https://www.osbar.org/_docs/ethics/2013-189.pdf construed Oregon Rule of Professional Conduct 4.2 and earlier Oregon Ethics Opinion 2005-164 to conclude that reviewing someone's publically available information is not "communicating" and is more akin to reading a magazine article by or about the adversary.

[10] In San Diego County Bar Association Legal Ethics Opinion 2011-2 https://www.sdcba.org/index.cfm?pg=LEC2011-2 the Bar Association opined that lawyers were prohibited from making friend requests on Facebook to represented parties and that this prohibition extended to high-ranking employees of corporations. The opinion explicitly references Model Rule 4.2 in its reasoning despite California not actually adopting the Model Rules.

company, (3) requesting information about the subject matter of his representation, (4) with knowledge that the company is represented in the matter; and (5) without the permission of opposing counsel.[11]

ii. Responsive Posting

If passive review appears to fall outside the scope of Model Rule 4.2 and Texas Rule 4.02 and an original posting appears to fall within the scope of Model Rule 4.2 and Texas Rule 4.02, the question remains of whether a responsive posting triggers these Rules. Comment 3 to Rule 4.2 of the Model Rules states,

> The Rule applies even though the represented person initiates or consents to the communication. A lawyer must immediately terminate communication with a person if, after commencing communication, the lawyer learns that the person is one with whom communication is not permitted by this Rule.[12]

According to Comment 3, Model Rule 4.2 governs all communications with represented parties, whether initiated by the lawyer or not. Stated differently, according to the comment, Model Rule 4.2 applies any time the lawyer knows the party is represented by counsel.[13]

The Texas rules do not include a comment similar to Comment 3 of the Model Rules.[14] Nevertheless, a cautious practitioner should not read this omission as an explicit invitation to "communicate … about the subject matter of the representation with a person … the lawyer knows is represented by another lawyer regarding that subject."[15] As the Fifth Circuit Court of Appeals has explained, testimony that a represented criminal defendant met with one of his co-defendant's counsel "establishes the facial elements of a violation of Rule 4.02(a)."[16] Although the Fifth Circuit ultimately reversed the lower court's order that the co-defendant's lawyer be disbarred, it did so on the basis of Rule 4.02(d), which specifically provides that a lawyer may provide a represented party advice regarding the subject matter of the

---

[11] *See* MODEL R. OF PROF. CONDUCT 4.2; TEX. DISCIPLINARY R. PROF. CONDUCT 4.02(a).
[12] MODEL R. OF PROF. CONDUCT 4.2, cmt. 3.
[13] *Id.*
[14] *See* TEX. DISCIPLINARY R. PROF. CONDUCT 4.02, cmts.
[15] TEX. DISCIPLINARY R. PROF. CONDUCT 4.02(a).
[16] *In re Medrano*, 956 F.2d 101, 103-05 (5th Cir. 1992).

representation at the party's request (*i.e.*, provide a second opinion) without violating Rule 4.02(a).[17] The fact that the Fifth Circuit explicitly noted the meeting standing alone establishes the "facial elements of a violation" of Rule 4.02(a) and was *overruling a lower court's order of disbarment* counsels against speaking with a represented party regarding the subject matter of the representation, even if the represented party is the one who initiated the communication.

2. Determining Whether the Lawyer "Knows" A Social Media User Is Represented

Even if an attorney's post constitutes a "communication," there may yet be a question about whether the lawyer knew the party was represented.[18] Consider the question of a corporate-defendant:

> In the case of a represented organization, this Rule prohibits communications with a constituent of the organization who supervises, directs or regularly consults with the organization's lawyer concerning the matter or has authority to obligate the organization with respect to the matter or whose act or omission in connection with the matter may be imputed to the organization for purposes of civil or criminal liability.[19]

Given the inherently indeterminate scope of a corporate party, an attorney using social media to solicit information regarding a dispute must be careful to ensure that his or her efforts do not solicit responses from an employee of the corporate party who "supervises, directs or regularly consults with the organization's lawyer concerning the matter" or "has authority to obligate the organization with respect to the matter" or "whose act or omission in connection with the matter may be imputed to the organization for purposes of civil or criminal liability." Without such safeguards, the attorney runs the risk of violating Model Rule 4.2, if any such person responds to the post. This is particularly true with respect to the Model

---

[17] Id.

[18] *See* MODEL R. OF PROF. CONDUCT 4.2 (only prohibiting communication with a person known to be represented); *see also*, TEX. DISCIPLINARY R. PROF. CONDUCT 4.02(a) (same).

[19] MODEL R. OF PROF. CONDUCT 4.2, cmt. 7. The comment to the Texas Rule, although somewhat differently worded, is largely the same. TEX. DISCIPLINARY R. PROF. CONDUCT 4.02, cmt. 4 ("In the case of an organization or entity of government, this Rule prohibits communications by a lawyer for one party concerning the subject of the representation with persons having a managerial responsibility on behalf of the organization that relates to the subject of the representation and with those persons presently employed by such organization or entity whose act or omission may make the organization or entity vicariously liable for the matter at issue, without the consent of the lawyer for the organization or entity of government involved."). Nevertheless, this comment has been the subject of widely varying interpretations. *See* David Hricik, *The Ethics of Blogging, Blawging, Chatting, List-Serving and Just Kabitzing in Public Places*, p. 4-6 (2006), http://ssrn.com/abstract=917180. It should also be noted that, where a state's rule and the Model Rule differ, a federal court may attempt to apply a "national" ethics standard by analyzing the issue under both the applicable state rule *and* the Model Rule in an attempt to harmonize the two. *See id.* at p. 6.

Rule, which does not draw a distinction between communications initiated by the attorney and communications initiated by the represented party.[20] (Note, however, that neither the Model Rule nor the Texas Rule requires the consent of the organization for communications with *former* employees of the organization.)[21]

3. Reminding a Social Media User of the Lawyer's Role

Model Rule 4.3 requires an employer to advise an unrepresented individual of his or her role as an advocate:

> In dealing on behalf of a client with a person who is not represented by counsel, a lawyer shall not state or imply that the lawyer is disinterested. When the lawyer knows or reasonably should know that the unrepresented person misunderstands the lawyer's role in the matter, the lawyer shall make reasonable efforts to correct the misunderstanding. The lawyer shall not give legal advice to an unrepresented person, other than the advice to secure counsel, if the lawyer knows or reasonably should know that the interests of such a person are or have a reasonable possibility of being in conflict with the interests of the client.[22]

Accordingly, even if a lawyer does not run afoul Model Rule 4.2 and is speaking with a person who is not known to be represented, the Model Rules and Texas Rules still impose a duty on the lawyer to make certain not to imply that he or she is disinterested and to correct any confusion the unrepresented party may have regarding the nature of the lawyer's interests.[23]

C. Statutory Concerns

Not surprisingly, employers and their attorneys have figured out that reviewing an employee's email and network activity use occasionally yields astonishing findings. As these potential treasure troves

---

[20] MODEL R. OF PROF. CONDUCT 4.2, cmt. 3.
[21] MODEL R. OF PROF. CONDUCT 4.2, cmt. 7; TEX. DISCIPLINARY R. PROF. CONDUCT 4.02, cmt. 4.
[22] MODEL R. OF PROF. CONDUCT 4.3; *see also* TEX. DISCIPLINARY R. PROF. CONDUCT 4.03.
[23] A surprising number of ethics opinions have been written on the issue of whether an attorney or his or her agent may solicit a friend request without being 100% forthcoming about the lawyer or agent's identity and purpose. *See* Oregon Ethics Opinion 2013-189, https://www.osbar.org/_docs/ethics/2013-189.pdf; Kentucky Bar Ethics Opinion KBA E-434, http://www.kybar.org/documents/ethics_opinions/kba_e-434.pdf; New York State Bar Opinion # 843 http://www.nysba.org/CustomTemplates/Content.aspx?id=5162; New York City Bar Association Formal Opinion 2010-2, http://www.nycbar.org/pdf/report/uploads/20071997-FormalOpinion2010-2.pdf; Philadelphia Bar Association Opinion 2009-02, http://www.philadelphiabar.org/WebObjects/PBAReadOnly.woa/Contents/WebServerResources/CMSResources/Opinion_2009-2.pdf; and San Diego County Bar Association Legal Ethics Opinion 2011-2, https://www.sdcba.org/index.cfm?pg=LEC2011-2

of information are searched with ever-increasing regularity (with some companies making the forensic analysis of a departing employee's machine a regular part of the exit process), employees have started getting creative in their efforts to limit what an employer may do with such information once discovered and, in some instances, bringing counter-claims based on the employer's attempt at self-help discovery.

1. The Stored Communications Act

The Stored Communications Act ("SCA") is perhaps the single most significant piece of federal legislation of which lawyers representing employers should be aware of when attempting to use technology to conduct informal discovery. Applicable to public and private entities alike, the SCA makes it an offense to intentionally access without authorization a facility through which an electronic communication service is provided and thereby obtain access to a wire or electronic communication while it is in electronic storage in such system.[24] The SCA excepts from liability "conduct authorized ... by a user of that service with respect to a communication of or intended for that user."[25] Attorneys have found that the SCA sometimes provides a potent basis for challenging an opposing counsel's ability to access their client's online activities.

a. *Ehling v. Monmouth-Ocean Hosp. Serv. Corp*

In *Ehling v. Monmouth-Ocean,*[26] Ehling was the president of the Union that represented nurses at her employer hospital. Ehling maintained a Facebook page and configured her privacy settings so that only her friends were able to view the wall where she posted comments and other content.[27] One of Ehling's co-worker friends took screenshots of Ehling's postings, including one that captured a post following the shootings at the Washington D.C. Holocaust Museum on June 10, 2009, that said:

> An 88 yr old sociopath white supremacist opened fire in the Wash D.C. Holocaust Museum this morning and killed an innocent guard (leaving children). Other guards opened fire. The 88 yr old was shot. He survived. I blame the DC paramedics. I want to say 2 things to the DC medics. 1. WHAT WERE YOU THINKING? and 2. This was your opportunity to really make a difference! WTF!!!! And to the other guards .... go to target practice.[28]

---

[24] 18 U.S.C. § 2701(a)(1).
[25] 18 U.S.C. § 2701(c)(2).
[26] *Ehling v. Monmouth-Ocean Hosp. Serv. Corp*., 961 F. Supp. 2d 659 (D.N.J. 2013).
[27] 961 F.Supp. 2d 659, 662-663.
[28] *Id.* at 663.

The co-worker shared this and other screenshots with Monmouth-Ocean management (unsolicited) without Ehling's permission, and Ehling was soon suspended with pay.[29] Ehling eventually returns, only to be terminated following a spate of poor performance, absenteeism, and failure to follow procedures. Ehling promptly filed a lawsuit alleging, among other things, a violation of the SCA.[30]

On Monmouth-Ocean's motion for summary judgment, the district court first found non-public Facebook wall posts *are* covered by the SCA.[31] The district court then held, however, that the co-worker's access and subsequent forwarding to management of the Facebook wall posts did not violate the SCA because the co-worker was an "authorized user" and thus permitted to forward the content.[32]

Specifically, the court found the co-worker was a "user" of her Facebook posts, who then authorized the company's "access" to the posts free of any coercion:

> The authorized user exception applies where (1) access to the communication was "authorized," (2) "by a user of that service," (3) with respect to a communication … intended for that user." Access is not authorized if the "purported 'authorization' was coerced or provided under pressure." In this case, all three elements of the authorized user exception are present.[33]

In other words, once the co-worker accessed Ehling's Facebook page with Ehling's permission, he became a "user" who could then "authorize" access to her page (by showing it to management).[34] The court noted there was no suggestion that the co-worker had been coerced into sharing the Facebook posts with management.[35]

b. *Konop v. Hawaiian Airlines*

A different result was reached in *Konop v. Hawaiian Airlines*.[36] Konop, a pilot, created and maintained a website where he posted bulletins critical of his employer, its officers, and the incumbent

---

[29] *Id.* She also filed an NLRB charge and the NLRB found that the hospital's action did not violate the NLRA.
[30] *Id*. at 665.
[31] *Id.* at 669.
[32] *Id.* at 671.
[33] *Id.* 669-670.
[34] *Id*.
[35] *Id*.
[36] 302 F.3d 868 (9th Cir. 2002).

union.[37] Konop controlled access to his website by requiring visitors to log in with a user name and password.[38] Only certain people, mostly pilots and other employees of Hawaiian, were eligible to access the website.[39] The website allowed access when a person entered the name of an eligible person, created a password, and clicked the "SUBMIT" button on the screen, indicating acceptance of the terms and conditions of use, which prohibited any member of Hawaiian's management from viewing the website and prohibited users from disclosing the website's contents to anyone else.[40]

Hawaiian's vice president obtained permission from two eligible persons to use their names to access the website. Neither of them had previously accessed the website. Konop then received a call from the union chairman who told Konop that Hawaiian's president was upset by disparaging statements published on the website. Konop filed suit alleging claims under the SCA arising from the vice-president's viewing and use of the secure website. The Ninth Circuit held that the eligible employees who granted the vice-president access to the website were not "users" with authority to consent to the vice-president's access, because they had not in fact previously used the website, even though they were eligible to do so. Accordingly, the court reversed the lower court's grant of summary judgment on Konop's claims.[41]

c. *Pietrylo v. Hillstone Restaurant Group*

Likewise, *Pietrylo v. Hillstone Restaurant Group*, reached a result different from *Ehling*.[42] In *Pietrylo*, Brian Pietrylo ("Pietrylo") and Doreen Marino ("Marino") were servers at the Houston's restaurant in Hackensack, New Jersey.[43] Pietrylo created a group on MySpace called the "Spec-Tator."[44] The stated purpose of the group was to "vent about any BS we deal with out [sic] work without any outside eyes spying in on us. This group is entirely private, and can only be joined by invitation. … Let the s* *t

---

[37] *Id.* at 872.
[38] *Id.*
[39] *Id.*
[40] *Id.* at 872-73.
[41] *Id.* at 881.
[42] *See Pietrylo v. Hillstone Rest. Grp.*, No.06-5754, 2009 WL 3128420 (D.N.J. Sept. 25, 2009) (denying motion for new trial after jury found managers' access of employee Facebook group violated the Stored Communications Act); *Pietrylo v. Hillstone Rest. Grp.*, No.06-5754, 2008 WL 6085437 (D.N.J. July 25, 2008).
[43] *Id*.
[44] *Id*.

talking begin."[45] Pietrylo invited past and present employees of Houston's to join the group.[46] Once a member was invited to join the group and accepted the invitation, the member could access the Spec-Tator whenever they wished to read postings or add new postings.[47]

Among others, Pietrylo invited Karen St. Jean, a greeter at Houston's, to join the group.[48] St. Jean accepted the invitation and became an authorized member of the group.[49] One night, while dining at the home of TiJean Rodriguez, a Houston's manager, St. Jean accessed the group through her MySpace profile on Rodriguez's home computer and showed Rodriguez the Spec-Tator.[50] At some point thereafter, Robert Anton, a Houston's manager, asked St. Jean to provide the password to access the Spec-Tator, which she did.[51] St. Jean testified she was never explicitly threatened with any adverse employment action.[52] Nevertheless, St. Jean stated she gave her password to members of management because they were members of management and she thought she "would have gotten in some sort of trouble" if she did not.[53]

Anton used the password provided by St. Jean to access the Spec-Tator from St. Jean's MySpace page and printed copies of the contents of the Spec-Tator.[54] The postings included sexual remarks about Houston's management and customers, jokes about some of the specifications Houston's had established for customer service and quality, references to violence and illegal drug use, and a copy of a new wine test that was to be given to the employees.[55] After Robert Marano, a regional supervisor of operations for Houston's, reviewed the postings, he terminated Pietrylo and Marino.[56]

---

[45] *Id*.
[46] *Id*.
[47] *Id*.
[48] *Pietrylo v. Hillstone Rest. Grp.*, No.06-5754, 2008 WL 6085437 (D.N.J. July 25, 2008).
[49] *Id*.
[50] *Id*.
[51] *Id*.
[52] *Id*.
[53] *Id*.
[54] *Pietrylo v. Hillstone Rest. Grp.*, No.06-5754, 2008 WL 6085437 (D.N.J. July 25, 2008).
[55] *Id*. at *2.
[56] *Id*.

Pietrylo and Marino sued Hillstone for violations of the SCA.[57] In reviewing their claims, the court turned its attention to whether St. Jean authorized the review of the postings to the Spec-Tator group by Houston's management.[58] St. Jean testified that if she did not give the password to the manager who asked for it, "I knew that something was going to happen. I didn't think that I was going to get fired, but I knew that I was going to get in trouble or something was going to happen if I didn't do it."[59] St. Jean also testified that no one told her she would be fired and that "[i]t wasn't an overwhelming feeling, but I knew. It sounds bad, but I didn't want to lose my job.... I didn't want to lose my job for not cooperating with them."[60] When asked if she was "following orders" in giving Houston's management her password, St. Jean stated, "I wasn't following orders. They asked me and I didn't know what else to do so I just gave it to them."[61] When asked if she felt pressured into giving her password, St. Jean explained, "No and yes," but later explained that she believed Houston's "would have kept on pressuring me and I'm not good under pressure."[62] St. Jean acknowledged that she "pretty much thought after I gave him [Anton] the password all the managers were going to see it."[63]

After summarizing this testimony, the court held St. Jean's provision of her password to Anton would not constitute "authorization," if it was given under "duress."[64] The court then held that St. Jean's testimony demonstrated that there was a fact issue as to whether her consent was given voluntarily or under "duress."[65] A jury then found that Hillstone had in fact violated the SCA, and the court denied Hillstone's motion for judgment as a matter of law, explaining that the jury could have concluded that St. Jean's consent did not constitute an effective authorization under the SCA.[66]

---

[57] Stored Communications Act, 18 U.S.C. §§ 2701-11 (2010); New Jersey State Act, N.J. STAT. ANN. §2A: 156A-27 (West 2010); Pietrylo, No. ,2008 WL 6085437 at *3.
[58] *Pietrylo*, 2008 WL 6085437 at *3-4.
[59] *Id*. at *4.
[60] *Id*.
[61] *Id*.
[62] *Id*.
[63] *Id*.
[64] *Pietrylo v. Hillstone Rest. Grp*., No.06-5754, 2008 WL 6085437, *4 (D.N.J. July 25, 2008).
[65] *Id*.
[66] *Pietrylo*, 2009 WL 3128420 at *2-3.

Setting aside the entertaining fact pattern, the significance of the *Pietrylo* decision is the court's holding that an at-will employee's consent does not necessarily constitute "authorization" for purposes of the SCA, which appears to be at odds with cases recognizing, for example, that an at-will employee can consent to something as meaningful as a mandatory arbitration program merely by continuing to work after receiving notice of the program.[67] Moreover, from a practical standpoint, the *Pietrylo* court's wholesale failure to provide any guidance whatsoever regarding when an employer may safely rely on a consent given by an at-will employee and when an employer must instead be concerned that the employee harbors some unstated, secret reservations about providing consent that will later be held to have destroyed the effectiveness of the consent is troubling, to say the least.[68]

This issue was not presented directly in *Ehling*, because there was no suggestion whatsoever that the co-worker had been coerced in any way into sharing Ehling's Facebook posts.[69] Notably, Ehling actually specifically distinguished Pietrylo on this ground, and given the holdings of *Konop* and *Pietrylo*, employers are well advised to consider restraint when reviewing an employee's obviously personal and confidential communications without the employee's specific consent.

d. *Pure Power Boot Camp, Inc. v. Warrior Fitness Boot Camp, Inc.*

The employer in *Pure Power Boot Camp, Inc. v. Warrior Fitness Boot Camp, Inc.* accessed the employee's web-based email accounts, because the employee had "auto-saved" the username and passwords for one account on the employer's computers, the employer obtained the username and password for another account from the first account, and the employer then guessed the password for a third account would be the same as the other two.[70] The court found that, even though the passwords were stored on the employer's computers and some of the emails retrieved from the account may have been read by the

---

[67] *Compare Id., with In re* Halliburton Co., 80 S.W.3d 566, 569 (Tex. 2002) (citing Hathaway v. General Mills, Inc., 711 S.W.2d 227 (Tex.1986)).
[68] *See Pietrylo.*, 2008 WL 6085437 at *3-4 (finding a fact issue on whether consent was freely given, where employee voluntarily disclosed online group to one manager, was never threatened with adverse action for refusing to share her user id or password, and never expressed any concern over providing such information when asked).
[69] *Ehling*, 961 F. Supp. 2d at 670 (D.N.J. 2013).
[70] *Pure Power Boot Camp, Inc. v. Warrior Fitness Boot Camp*, Inc. 759 F.Supp.2d 471 (S.D.N.Y. Dec. 22, 2010).

employee while at work, there was no evidence that the emails were downloaded onto the employer's computer.[71] The court noted that the employer did not examine its own computer memory to determine which emails were accessed at work, but instead logged directly into the web-based email accounts to view and print the emails.[72] The court concluded that both the unauthorized access to the electronic communication services and the unauthorized procurement of the emails while they were in storage on those service providers' systems were violations of the SCA.[73]

2. The Electronic Communications Privacy Act

Any discussion of laws relating to possible limits on self-help discovery must at least mention the potential application of the Electronic Communications Privacy Act (ECPA).[74] The ECPA creates criminal sanctions and a civil cause of action against persons who "intercept" electronic communications.[75] In the context of unauthorized access to e-mail, there is a general consensus among courts that emails no longer in transit cannot be "intercepted."[76] As one court explained, "The general reasoning behind these decisions is that based on the statutory definition and distinction between 'wire communication' and 'electronic communication,' the latter of which conspicuously does not include electronic storage, Congress intended for electronic communications in storage to be handled solely by the Stored Communications Act."[77]

Given the nature of email, social media, microblogs, and other emerging technologies, it seems likely the SCA will be of greater relevance than the ECPA. Indeed, in *Pure Power Boot Camp, Inc. v.*

---

[71] *Pure Power Boot Camp, Inc. v. Warrior Fitness Boot Camp, Inc*., 587 F.Supp.2d 548, 555 (S.D.N.Y. 2008).
[72] *Id.* at 556.
[73] *Id.*
[74] 18 U.S.C. §§ 2510-2511.
[75] *Id.*
[76] *Steve Jackson Games, Inc. v. United States Secret Serv.*, 36 F.3d 457, 460-64 (5th Cir.1994); *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 873, 876-79 (9th Cir.2002) (noting that accessing a secure website did not constitute an "interception" of an electronic communication under the ECPA and narrowly defining interception as "contemporaneous interception"); *Fraser v. Nationwide Mut. Ins. Co.*, 352 F.3d 107, 115 (3rd Cir.2003) (holding that the defendant did not "intercept" the plaintiff's e-mail by accessing e-mail stored on its central file server, because "an 'intercept' under the ECPA must occur contemporaneously with transmission"); *United States v. Steiger*, 318 F.3d 1039, 1048-49 (11th Cir.2003) (declining to suppress evidence obtained by a hacker from defendant's computer under the ECPA, because "a contemporaneous interception is required to implicate the [ECPA] with respect to electronic communications").
[77] *Bailey v. Bailey*, No. 07 Civ. 11672, 2008 WL 324156, *4 (E.D.Mich. Feb. 6, 2008).

Warrior Fitness Boot Camp, Inc. the court specifically held that the employer did not violate the ECPA by retrieving the former employee's emails, even though it did violate the SCA, because the employer did not access and print the employee's e-mails contemporaneously with their transmission.[78]

3. The Computer Fraud and Abuse Act

Employer-side self-help discovery typically implicates the Stored Communication Act because employers often own the mediums of communication. Conversely when employees conduct self-help discovery by obtaining documents from their employer this can implicate the Federal Computer Fraud and Abuse Act ("CFAA"). Cases under CFAA[79] suggest the twenty-five year old law may provide an avenue for relief in a federal venue and, under the right circumstances, the force of a federal criminal prosecution.

Enacted in 1986, the CFAA prohibits anyone from accessing a protected computer without authority or by exceeding authorized access for purposes of obtaining information, causing damage, or perpetrating fraud.[80] Although the CFAA is a criminal statute, it also provides a private right of action.[81] The interesting issue raised in cases tied to employment has been whether misuse of information by an employee was transformed into unauthorized use or use exceeding authorized access for purposes of the CFAA.[82]

In *United States v. John*, the Fifth Circuit held that an employee of Citigroup exceeded her authorized access to her employer's computers when she accessed confidential customer information in violation of her employer's computer use restrictions and used that information to commit fraud.[83] Likewise, in *International Airport* Centers, *LLC v. Citrin*, the Seventh Circuit reasoned that, regardless of whether an employee once held authorization to use company computers, that employee loses authorization

---

[78] *Pure Power Boot Camp, Inc. v. Warrior Fitness Boot Camp, Inc*., 587 F.Supp.2d 548, 557-58 (S.D.N.Y. 2008).
[79] 18 U.S.C. § 1030(a)(1)-(7) (2004).
[80] *Id*.
[81] *EF Cultural Travel BV v. Explorica, Inc*., 274 F.3d 577, 581 (1st Cir. 2001) (referring to the private right of action under 18 U.S.C. § 1030(g)).
[82] *United States v. Nosal*, 2011 WL 1585600, at *2-3 (9th Cir. Apr. 28, 2011).
[83] *United States v. John*, 597 F.3d 263 (5th Cir. 2010).

when the employee violates a state law duty of loyalty. In essence, the employee's attempts to perpetrate a fraud on the company terminated the employee's authority to access company resources.[84]

In April 2011, the Ninth Circuit briefly joined this line of reasoning in its initial decision in *United States v. Nosal*.[85] In *Nosal*, the Ninth Circuit initially held that an employee exceeds his or her authorized access to an employer's computer under the CFAA when the employee's access violates the employer's access restrictions.[86] As the Court noted, "as long as the employee has knowledge of the employer's limitations on [] authorization, the employee 'exceeds authorized access' when the employee violates those limitations."[87]

The defendant in *Nosal* was an executive for Korn/Ferry International, an executive search firm. After he left the company, he allegedly engaged three Korn/Ferry employees to start a competing search firm.[88] The former Korn/Ferry employees obtained trade secrets and other proprietary information by accessing information contained on Korn/Ferry computers by using their user accounts.[89] The employees had signed agreements that expressly restricted the use and disclosure of Korn/Ferry's proprietary information to "legitimate Korn/Ferry business."[90] The agreements also stated: "You need specific authority

---

[84] *International Airport Centers, LLC v. Citrin*, 440 F.3d 418 (7th Cir. 2006). Other courts have also joined this broader interpretation of the CFAA. *See EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577, 583–[84] (1st Cir. 2001) (holding that an employee likely exceeded his authorized access when he disclosed information in violation of a confidentiality agreement the employee voluntarily signed); *United States v. John*, 597 F.3d 263 (5th Cir. 2010) (holding that an employee of Citigroup exceeded her authorized access when she accessed confidential customer information in violation of her employer's computer use restrictions and used that information to commit fraud); *United States v. Batti*, 631 F.3d 371, 379 (6th Cir. 2011) (although not addressing the issue of whether the employee's use was authorized or exceeded authority, the Court upheld a terminated employee's conviction and an award of restitution to his former company under the CFAA where the employee accessed the computer system to steal confidential data); *International Airport Centers, LLC v. Citrin*, 440 F.3d 418 (7th Cir.2006) (holding that an employee loses authorization to use a computer even absent an express policy against fraudulent use when the employee violates a state law duty of loyalty because, based on common law agency principles, the employee's actions terminated the employer-employee relationship "and with it his authority to access the [computer]."); *United States v. Rodriguez*, 628 F.3d 1258, 1263 (11th Cir. 2010) (upholding the conviction of a former employee who used the employer's databases to obtain personal information about people he knew).

[85] *United States v. Nosal*, 2011 WL 1585600 (9th Cir. Apr. 28, 2011).

[86] *Id*. at *4.

[87] *Id*.

[88] *Id*. at *2-3.

[89] *Id*. at *2.

[90] *Id*. at *2.

to access any Korn/Ferry system or information and to do so without relevant authority can lead to disciplinary action or criminal prosecution."[91]

In its initial *Nosal* opinion, the Ninth Circuit distinguished its holding in *LVRC Holdings L.L.C. v. Brekka*, an earlier employment-based CFAA case, in which the court had held that the employee was not subject to liability under the CFAA, because the employee was not acting without authorization when he emailed several confidential documents to his personal email address.[92] In *Brekka*, the court relied on the fact that the employee was not notified by his employer of any restrictions on his access to company computers, such that the employee "had no way to know whether—or when—his access would have become unauthorized."[93] Under *Brekka*, if a company gives an employee "unfettered access" to company computers (*i.e.*, does not have an agreement with the employee restricting use or employee guidelines setting out authorized use and unauthorized use), that employee cannot be held to have exceeded authorized access or even be held to have acted without authorization for purposes of the CFAA.[94]

The Ninth Circuit's initial *Nosal* opinion also explicitly rejected the defendant's argument that a broad interpretation of CFAA would criminalize too much employee computer behavior:

> We do not dismiss lightly Nosal's argument that our decision will make criminals out of millions of employees who might use their work computers for personal use, for example, to access their personal email accounts or to check the latest college basketball scores. But subsection (a)(4) does not criminalize the mere violation of an employer's use restrictions. Rather, an employee violates this subsection if the employee (1) violates an employer's restriction on computer access, (2) with an intent to defraud, and (3) by that action "furthers the intended fraud and obtains anything of value." 18 U.S.C. § 1030(a)(4) (emphasis added). The requirements of a fraudulent intent and of an action that furthers the intended fraud distinguish this case from the Orwellian situation that Nosal seeks to invoke. Simply using a work computer in a manner that violates an employer's use restrictions, without more, is not a crime under § 1030(a)(4).[95]

---

[91] *Id*. at *2.
[92] *LVRC Holdings L.L.C. v. Brekka*, 581 F.3d 1127, 1129-30 (9th Cir. 2009).
[93] *Nosal*, at *5.
[94] *Id*. at *6.
[95] *Id*, at *7.

Following its initial decision, however, the full Ninth Circuit took the question up for rehearing *en banc* and laid out the competing interpretations of the CFAA being offered by Nosal and the government as follows:

> The CFAA defines "exceeds authorized access" as "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter." 18 U.S.C. § 1030(e)(6). This language can be read either of two ways: First, as Nosal suggests and the district court held, it could refer to someone who's authorized to access only certain data or files but accesses unauthorized data or files—what is colloquially known as "hacking." For example, assume an employee is permitted to access only product information on the company's computer but accesses customer data: He would "exceed [ ] authorized access" if he looks at the customer lists. Second, as the government proposes, the language could refer to someone who has unrestricted physical access to a computer, but is limited in the use to which he can put the information. For example, an employee may be authorized to access customer lists in order to do his job but not to send them to a competitor.[96]

Ultimately, the full Ninth Circuit adopted Nosal's interpretation as being more consistent with the CFAA's purpose, rejecting the government's more sweeping interpretation:

> While the CFAA is susceptible to the government's broad interpretation, we find Nosal's narrower one more plausible. Congress enacted the CFAA in 1984 primarily to address the growing problem of computer hacking, recognizing that, "[i]n intentionally trespassing into someone else's computer files, the offender obtains at the very least information as to how to break into that computer system." The government agrees that the CFAA was concerned with hacking, which is why it also prohibits accessing a computer "without authorization." According to the government, that prohibition applies to hackers, so the "exceeds authorized access" prohibition must apply to people who are authorized to use the computer, but do so for an unauthorized purpose. But it is possible to read both prohibitions as applying to hackers: "[W]ithout authorization" would apply to outside hackers (individuals who have no authorized access to the computer at all) and "exceeds authorized access" would apply to inside hackers (individuals whose initial access to a computer is authorized but who access unauthorized information or files). This is a perfectly plausible construction of the statutory language that maintains the CFAA's focus on hacking rather than turning it into a sweeping Internet-policing mandate.
>
> The government's construction of the statute would expand its scope far beyond computer hacking to criminalize any unauthorized use of information obtained from a computer. This would make criminals of large groups of people who would have little reason to suspect they are committing a federal crime. While ignorance of the law is no excuse, we can properly be skeptical as to whether Congress, in 1984, meant to criminalize conduct beyond that which is inherently wrongful, such as breaking into a computer.[97]

---

[96] *U.S. v. Nosal*, 676 F.3d 854, 856-57 (9th Cir. 2012) (en banc).
[97] *U.S. v. Nosal*, 676 F.3d 854, 858-59 (9th Cir. 2012) (en banc) (citations and footnotes omitted).

In short, in the Ninth Circuit, the CFAA does not apply to the wrongful misappropriation of information, if the employee was otherwise authorized the access the information for legitimate purposes.

The Fourth Circuit court of appeals was faced with a similar question in *WEC Carolina Energy Solutions LLC v. Miller*.[98] In that case, Miller allegedly downloaded several confidential files, which he was permitted to access for legitimate purposes, and then emailed them to his personal email address shortly before quitting to join the competition.[99] WEC sued Miller, his assistant (who was alleged to have assisted him), and the competitor for, among other things, violations of CFAA. Miller responded by filing a 12(b)(6) motion to dismiss.

After reviewing the competing approaches of the Fifth and Seventh Circuit, on the one hand, and the Ninth Circuit, on the other, the Fourth Circuit adopted the Ninth Circuit's view of the meaning of "exceeds authorized access":

> With respect to the phrase, "without authorization," the CFAA does not define "authorization." Nevertheless, the Oxford English Dictionary defines "authorization" as "formal warrant, or sanction. Regarding the phrase "exceeds authorized access," the CFAA defines it as follows: "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter."
>
> Recognizing that the distinction between these terms is arguably minute, we nevertheless conclude based on the "ordinary, contemporary, common meaning" of "authorization," that an employee is authorized to access a computer when his employer approves or sanctions his admission to that computer. Thus, he accesses a computer "without authorization" when he gains admission to a computer without approval. Similarly, we conclude that an employee "exceeds authorized access" when he has approval to access a computer, but uses his access to obtain or alter information that falls outside the bounds of his approved access. Notably, neither of these definitions extends to the improper use of information validly accessed.[100]

D. The Constitution

For public employers, the highly publicized case involving the sexual text messages of an Ontario, California, SWAT police sergeant provides a good example of the issues implicated when

---

[98] *WEC Carolina Energy Solutions LLC v. Miller*, 687 F.3d 199, 204 (4th Cir. 2012) (citations omitted).
[99] *Id.* at 202.
[100] *WEC Carolina Energy Solutions LLC v. Miller*, 687 F.3d 199, 204 (4th Cir. 2012) (citations omitted).

a government employer uses technology to enforce its policies.[101] In *Quon v. City of Ontario*, the Ontario Police Department (the "OPD") distributed text-message capable pagers to its officers, including Sergeant Jeff Quon.[102] The City had no official policy directed to text-messaging by users of the pagers. However, the City did have a general "Computer Usage, Internet and E-mail Policy" (the "Policy") applicable to all employees. The Policy stated that "[t]he use of City-owned computers and all associated equipment, software, programs, networks, Internet, e-mail and other systems operating on these computers is limited to City of Ontario related business. The use of these tools for personal benefit is a significant violation of City of Ontario Policy." Each pager was allotted 25,000 characters, after which the City was required to pay overage charges. Lieutenant Duke was responsible for procuring payment for overages. Quon went over the monthly character limit "three or four times" and paid the City for the overages.

In August 2002, Quon and another officer again exceeded the 25,000 character limit. Lieutenant Duke then let it be known that he was "tired of being a bill collector with guys going over the allotted amount of characters on their text pagers." In response, Chief Scharf ordered Lieutenant Duke to "request the transcripts of those pagers for auditing purposes."[103] Chief Scharf asked Lieutenant Duke "to determine if the messages were exclusively work related, thereby requiring an increase in the number of characters officers were permitted, which had occurred in the past, or if they were using the pagers for personal matters.[104] One of the officers whose transcripts [he] requested was plaintiff Jeff Quon.[105] After receiving the transcripts, Lieutenant Duke conducted an audit and reported the results to Chief Scharf, who reported them to Quon's

---

[101] *See Quon v. City of Ontario, et al.*, 529 F.3d 892 (9th Cir. 2009), *reversed and remanded, City of Ontario et al. v. Quon*, 560 U.S. 746 (2010).
[102] *Quon v. City of Ontario, et al.*, 529 F.3d 892, 895 (9th Cir. 2009).
[103] *Id.* at 898.
[104] *Id.*
[105] *Id.*

supervisor and then referred the matter to internal affairs "to determine if someone was wasting ... City time not doing work when they should be."[106] According to the investigation, the transcripts revealed that Quon "had exceeded his monthly allotted characters by 15,158 characters," and that many of these messages were personal and often sexual.

In deciding the appeal, the Ninth Circuit noted that the nature of a public employee's expectation of privacy is unsettled.[107] Although the principle was discussed extensively in *O'Conner v. Ortega*, the approaches of the plurality and Justice Scalia's concurrence diverged.[108] All members of the Court agreed that, "Individuals do not lose Fourth Amendment rights merely because they work for the government instead of a private employer," and a majority further agreed that the warrant and probable-cause requirements are impracticable for government employers.[109] The *O'Connor* plurality then concluded the correct analysis has two steps. Step one requires a case-by-case analysis of the operational realities of the workplace to determine whether an employee's Fourth Amendment rights are implicated, as some government offices may be so open to fellow employees or the public that no expectation of privacy is reasonable.[110] If the employee had a legitimate privacy expectation, step two requires the court to determine whether the employer's intrusion on that expectation "for noninvestigatory, work-related purposes, as well as for investigations of work-related misconduct," was reasonable under all the circumstances.[111] In contrast, Scalia's concurrence advocated a different approach. Scalia would assume "that the offices of government employees ... are covered by Fourth Amendment protections as a general matter" and dispense

---

[106] *Id.*
[107] *Quon v. City of Ontario et al.*, 529 F.3d 892, 904 (9th Cir. 2008) ("The extent to which the Fourth Amendment provides protection for the contents of electronic communications in the Internet age is an open question. The recently minted standard of electronic communication via e-mails, text messages, and other means opens a new frontier in Fourth Amendment jurisprudence that has been little explored.").
[108] 480 U.S. 709, 711 (1987) (plurality opinion); *see also id.*, at 731 (SCALIA, J., concurring in judgment); *id.*, at 737 (Blackmun, J., dissenting).
[109] *Id.*, at 725, 107 S.Ct. 1492 (plurality opinion) (quoting *New Jersey v. T.L. O.*, 469 U.S. 325, 351, 105 S.Ct. 733, 83 L.Ed.2d 720 (1985)) (Blackmun, J., concurring in judgment); 480 U.S., at 732, 107 S.Ct. 1492 (opinion of SCALIA, J.) (quoting same).
[110] *Id.* at 718.
[111] *Id.*, at 725-726.

with a case by case analysis into the operational realities of the workplace.[112] Further, Scalia's analysis of reasonableness would hold that "that government searches to retrieve work-related materials or to investigate violations of workplace rules-searches of the sort that are regarded as reasonable and normal in the private-employer context-do not violate the Fourth Amendment."[113]

Ultimately, the Supreme Court declined to settle the question of workplace privacy expectations for employees and instead found that, even if Quon had a legally recognizable expectation of privacy, the City's intrusion into such privacy was reasonable.[114] Under the approach espoused by Justice Scalia, the search was reasonable, because the employer had a legitimate reason for the search and the search was not excessively intrusive in light of that reason.[115] As for the *O'Connor* plurality approach, the Court reasoned as follows:

> Under the approach of the *O'Connor* plurality, when conducted for a "noninvestigatory, work-related purpos[e]" or for the "investigatio[n] of work-related misconduct," a government employer's warrantless search is reasonable if it is " 'justified at its inception' " and if " 'the measures adopted are reasonably related to the objectives of the search and not excessively intrusive in light of' " the circumstances giving rise to the search. . . .The search was justified at its inception because there were "reasonable grounds for suspecting that the search [was] necessary for a noninvestigatory work-related purpose." As a jury found, Chief Scharf ordered the search in order to determine whether the character limit on the City's contract with Arch Wireless was sufficient to meet the City's needs. This was, as the Ninth Circuit noted, a "legitimate work-related rationale." . . . As for the scope of the search, reviewing the transcripts was reasonable because it was an efficient and expedient way to determine whether Quon's overages were the result of work-related messaging or personal use.
>
> The review was also not "'excessively intrusive.'" Although Quon had gone over his monthly allotment a number of times, OPD requested transcripts for only the months of August and September 2002. . . . And it is worth noting that during his internal affairs investigation, McMahon redacted all messages Quon sent while off duty, a measure which reduced the intrusiveness of any further review of the transcripts.
>
> Furthermore, and again on the assumption that Quon had a reasonable expectation of privacy in the contents of his messages, the extent of an expectation is relevant to assessing whether the search was too intrusive. Even if he could assume some level of privacy would inhere in his messages, it would not have been reasonable for Quon to conclude that his messages were in all circumstances immune from scrutiny. Quon was told that his

---

[112] *Id.*, at 732.
[113] *Id.*
[114] *City of Ontario et al v. Quon.*, 560 U.S. 746, 761-762 (2010).
[115] *Id.* at 2633.

> messages were subject to auditing. . . . Under the circumstances, a reasonable employee would be aware that sound management principles might require the audit of messages to determine whether the pager was being appropriately used. . . . OPD's audit of messages on Quon's employer-provided pager was not nearly as intrusive as a search of his personal e-mail account or pager, or a wiretap on his home phone line, would have been. That the search did reveal intimate details of Quon's life does not make it unreasonable, for under the circumstances a reasonable employer would not expect that such a review would intrude on such matters. The search was permissible in its scope.[116]

E. Public Policy

1. The Evolving Privacy Concept

In the 1965 case of *Griswold v. Connecticut,* the United States Supreme Court recognized (or created) a constitutional right to privacy and, on the basis of that right, struck down a state statute prohibiting the use of contraceptives:

> The foregoing cases suggest that specific guarantees in the Bill of Rights have penumbras, formed by emanations from those guarantees that help give them life and substance. Various guarantees create zones of privacy. The right of association contained in the penumbra of the First Amendment is one, as we have seen. The Third Amendment in its prohibition against the quartering of soldiers 'in any house' in time of peace without the consent of the owner is another facet of that privacy. The Fourth Amendment explicitly affirms the 'right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures.' The Fifth Amendment in its Self-Incrimination Clause enables the citizen to create a zone of privacy which government may not force him to surrender to his detriment. The Ninth Amendment provides: 'The enumeration in the Constitution, of certain rights, shall not be construed to deny or disparage others retained by the people.' The Fourth and Fifth Amendments were described in *Boyd v. United States,* as protection against all governmental invasions 'of the sanctity of a man's home and the privacies of life.' We recently referred in *Map v. Ohio* to the Fourth Amendment as creating a 'right to privacy, no less important than any other right carefully and particularly reserved to the people.' We have had many controversies over these penumbral rights of 'privacy and repose.' These cases bear witness that the right of privacy which presses for recognition here is a legitimate one.[117]

While the debate over reproductive rights continues, emerging technologies are creating new and equally complex questions regarding the extent to which the "penumbral rights of 'privacy and repose'" protect personal information and under what circumstances and to what extent the government and private parties may gather, analyze, and use such information. In 2010, the Supreme Court was called upon to

---

[116] *Id.* at 2630-2632 (internal citations and quotations omitted).
[117] *Griswold v. Connecticut,* 381 U.S. 479, 484 (1965).

address whether a public employee has a right of privacy in text messages he sent from his work-issued pager,[118] and in 2011, the Supreme Court addressed whether an employee of a government contractor had an informational right to privacy that would preclude a requirement that he fill out a government background check inquiring into drug use and treatment.[119]

Notably, in both cases, the Court declined to rule on whether an applicable right to privacy existed, and instead decided the cases based on the reasonableness of the inquiries at issue. The Court explained its approach to the issue as follows:

> Rapid changes in the dynamics of communication and information transmission are evident not just in the technology itself but in what society accepts as proper behavior. . . . At present, it is uncertain how workplace norms, and the law's treatment of them, will evolve. . . .Cell phone and text message communications are so pervasive that some persons may consider them to be essential means or necessary instruments for self-expression, even self-identification. That might strengthen the case for an expectation of privacy. On the other hand, the ubiquity of those devices has made them generally affordable, so one could counter that employees who need cell phones or similar devices for personal matters can purchase and pay for their own. And employer policies concerning communications will of course shape the reasonable expectations of their employees, especially to the extent that such policies are clearly communicated. A broad holding concerning employees' privacy expectations vis-à-vis employer-provided technological equipment might have implications for future cases that cannot be predicted. It is preferable to dispose of this case on narrower grounds.[120]

As the Court acknowledged, technology and behavior surrounding technology are dynamically evolving in our society. Moreover, although the Court's decisions regarding Constitutional privacy are of direct applicability only to public employers, private employers would do well to heed the arc of such cases, as public policy issues related to "privacy" continue to press in on the private sector, particularly where the attorney-client relationship is involved, as is discussed below.

---

[118] *City of Ontario, Cal. v. Quon*, 130 S. Ct. 2619, 2625 (2010).
[119] *See National Aeronautics and Space Administration v. Nelson*, 131 S.Ct. 746, 756-57 (2011) ("we will assume for present purposes that the Government's challenged inquiries implicate a privacy interest of constitutional significance"); *City of Ontario, Cal. v. Quon*, 130 S. Ct. 2619, 2630 (2010) ("For present purposes we assume several propositions *arguendo:* First, Quon had a reasonable expectation of privacy in the text messages sent on the pager provided to him by the City").
[120] *City of Ontario, Cal. v. Quon*, 130 S. Ct. 2619, 2630 (2010).

2. *Stengart v. Loving* Care *Agency*

For example, in *Stengart v. Loving Care Agency*, the New Jersey Supreme Court has held that an employer's broadly worded IT policy advising employees that the employer reserved the right to review communications made via the employer's information systems and further advising employees that they had no expectation of privacy in email messages or internet usage did not permit the employer's lawyers to review otherwise confidential communications between an employee and her lawyer that were made using a personal, password protected, web-based email service that the employee accessed via the company's information technology resources.[121]

Marina Stengart ("Stengart") worked for Loving Care Agency.[122] In December 2007, Stengart used her laptop to access a personal, password-protected e-mail account on Yahoo's website and communicate with her attorney about her situation at work.[123] Shortly thereafter, Stengart quit, returned her laptop to the company, and brought claims for constructive discharge, hostile work environment, retaliation, and harassment based on sex, religion, and national origin..[124] Stengart did not save her Yahoo password on her work computer.[125]

In or about April 2008, Loving Care engaged a forensic expert to create an image of Stengart's hard drive.[126] Among the items retrieved were temporary Internet files containing the contents of seven or eight e-mails Stengart had exchanged with her lawyer via her Yahoo account.[127] Loving Care's outside counsel reviewed the messages but did not inform Stengart's counsel that they had them until months later and then only in response to written interrogatories from Stengart.[128]

---

[121] *Stengart v. Loving Care Agency, Inc*., 990 A.2d 650, 657 (N.J. 2010).
[122] *Id*. at 656.
[123] *Id*.
[124] *Id.*
[125] *Id*.
[126] *Id*.
[127] *Stengart v. Loving Care Agency, Inc*., 990 A.2d 650, 656 (N.J. 2010).
[128] *Id*.

The New Jersey Supreme Court concluded that the broad language of Loving Care's IT policy did not specifically address personal, web-based email accounts, did not warn employees that the contents of their hard drives could be retrieved forensically, and created an ambiguity about whether personal email was personal or company property by acknowledging that "occasional personal use" of email was permitted.[129] The court further found that Stengart and her counsel intended for the emails to be confidential, that Stengart had a reasonable expectation that the emails would be confidential, and that Stengart had not waived the attorney-client privilege with respect to same.[130]

Anticipating employers' likely reaction to the holding, the New Jersey Supreme Court went on to hold that a clearly written policy that specifically purported to permit an employer to review such messages would be against public policy and thus unenforceable:

> Our conclusion that Stengart had an expectation of privacy in e-mails with her lawyer does not mean that employers cannot monitor or regulate the use of workplace computers. Companies can adopt lawful policies relating to computer use to protect the assets, reputation, and productivity of a business and to ensure compliance with legitimate corporate policies. And employers can enforce such policies. They may discipline employees and, when appropriate, terminate them, for violating proper workplace rules that are not inconsistent with a clear mandate of public policy. For example, an employee who spends long stretches of the workday getting personal, confidential legal advice from a private lawyer may be disciplined for violating a policy permitting only occasional personal use of the Internet. But employers have no need or basis to read the specific contents of personal, privileged, attorney-client communications in order to enforce corporate policy. Because of the important public policy concerns underlying the attorney-client privilege, even a more clearly written company manual—that is, a policy that banned all personal computer use and provided unambiguous notice that an employer could retrieve and read an employee's attorney-client communications, if accessed on a personal, password-protected e-mail account using the company's computer system—would not be enforceable.[131]

3. *Holmes v. Petrovich Development* Company

On the other hand, in *Holmes v. Petrovich Development Company*, a California Court of Appeals held it was not error to deny a motion for the return of and to admit over objection at trial emails written by

---

[129] *Id*. at 658.

[130] It should be noted that the New Jersey Supreme Court held that the company's lawyers should have notified Stengart's lawyer, once they realized they were in possession of confidential communications between Stengart and the lawyer. *Stengart*, 990 A.2d 650, 659-60, 664-66.

[131] *Id*. at 324-25 (citations omitted).

an employee to her attorney from her company email account using her company computer.[132] Gina Holmes was an executive assistant working for Paul Petrovich at Petrovich Development Company, LLC.[133] The company had a technology resource policy that (1) stated technology resources should only be used for company business; (2) prohibited employees from sending or receiving personal emails; (3) warned that employees who use technology resources to create or maintain personal information or messages had no right of privacy; (4) stated that "email is not private communication, because others may be able to read or access the message"; and (5) spelled out that the company may inspect all messages at any time for any reason at its discretion and would periodically monitor its technology resources for compliance with company policy.[134]

Holmes and Petrovich exchanged several emails regarding a conflict between them about Holmes's upcoming maternity leave.[135] At the end of the exchange, it appeared the conflict had been resolved and both parties agreed to move forward with their working relationship.[136] However, after mentioning the conflict to her doctor, Holmes decided to contact an attorney about the situation.[137] Holmes exchanged emails with an attorney using her company computer and company email address.[138] The next day Holmes met with the attorney for, and afterwards emailed her resignation to Petrovich.[139]

Holmes filed suit for sexual harassment, retaliation, wrongful termination, violation of the right to privacy, and intentional infliction of emotional distress.[140] During the course of the case, Holmes filed a motion requesting the emails she exchanged with her attorney from her work computer be returned on the grounds of attorney-client privilege. She also objected to the emails being presented at trial. The trial court denied Holmes's motion and allowed the company to introduce the emails at trial, holding the emails were

---

[132] *Holmes v. Petrovich Development Co., LLC*, 119 Cal.Rptr.3d 878,893-99 (Cal.App. (3d Dist.) 2011).
[133] *Id.* at 883.
[134] *Id.* at 883.
[135] *Id.* at 884-86.
[136] *Id.*
[137] *Id.* at 886-87.
[138] *Id.* at 886-87, 896.
[139] *Id.* at 887.
[140] *Id.* at 882.

not privileged. The California Appellate Court affirmed the trial court's rulings, finding the emails were not "confidential communications" between client and lawyer, because Holmes used a company computer after being told that the computer was solely for company business, that she was prohibited from using the computer for personal email, that the computer would be monitored, and that employees had no right of privacy.[141] As the court explained, [Holmes] used defendants' computer, after being expressly advised this was a means that was not private and was accessible by Petrovich, the very person about whom Holmes contacted her lawyer and whom Holmes sued. This is akin to consulting her attorney in one of defendants' conference rooms, in a loud voice, with the door open, yet unreasonably expecting that the conversation overheard by Petrovich would be privileged.[142]

III. FORMAL DISCOVERY

A. Early Development

Early informal discovery of social media centered around the earliest form of social media, blogs. Starbucks, for example, sought blog-related discovery in connection with its defense against a Fair Labor Standards Act collective action.[143] More specifically, Starbucks sought discovery of any "internet handles" used by any of the plaintiffs in making any posting about Starbucks.[144] Starbucks argued such information would lead to the discovery of internet postings it believed the plaintiffs had made regarding the number of hours they worked and the nature of their duties.[145] The court denied the request until such time as Starbucks has established that the plaintiffs had made such postings.[146]

---

[141] *Id.* at 883. The court distinguished this case from *Stengart*, because *Stengart* involved "the use of a personal web-based e-mail account accessed from an employer's computer where the use of such an account was not clearly covered by the company's policy and the e-mails contained a standard hallmark warning that the communications were personal, confidential, attorney-client communications." *Id.* at 896.
[142] *Id.* at 896.
[143] *See Pendlebury v. Starbucks Coffee Co.*, 2005 WL 2105024 (S.D. Fla. 2005).
[144] *Id.* at *3.
[145] *Id*.
[146] *Id.*

B. Continuing Application

1. Production of Electronic Communications

Employers may find a plaintiff's social media interactions to be a useful source of evidence in opposing an employee's claim for emotional distress damages resulting from alleged workplace harassment. First, however, employers must use the discovery process to gain access to the employee's social networking site profiles and communications.

2. *Palma v. Metro PCS Wireless, Inc.*

Employers are especially apt to do this in FLSA cases where the date and time someone posted a comment or sent a message can provide clues about whether that employee was on or off the clock. For example, in *Palma v. Metro PCS Wireless, Inc.*, the defendant employer in this FLSA collective action sought "all posts to Plaintiff's social media accounts from 2010 to the present that relate to 'any job descriptions or similar statements about this case or job duties and responsibilities or hours worked which Plaintiffs posted on LinkedIn, Facebook or other social media sites.'"[147] The court holds that "social media content is neither privileged nor protected by any right of privacy."[148] But ultimately denies the Defendant's request for production.

The Court held that Defendant's "speculation" was not sufficient to have the Plaintiffs review all of their social media postings for the last four years and determine which were relevant.[149] In cases where blanket social media communications are requested it is important to limit the requests just as an attorney would for non-electronic communications.

3. *Keller v. Nat'l Farmers Union*

This approach to discovery was also rejected in *Keller v. Nat'l Farmers Union*.[150] In *Keller* the defendant insurer in an automobile accident case requested that the Plaintiff "Please produce a full printout

---

[147] *Palma v. Metro PCS Wireless, Inc*., 8:13-CV-698-T-33MAP, 2014 WL 1877578 (M.D. Fla. Apr. 29, 2014).
[148] *Id.* at *1.
[149] *Id.* at *2.
[150] *Keller v. Nat'l Farmers Union Prop. & Cas. Co*., CV 12-72-M-DLC-JCL, 2013 WL 27731 (D. Mont. Jan. 2, 2013).

of all [social media website pages and all photographs posted there] from August 26, 2008 to the present."[151] The court acknowledges that even though the information was "private" and was not available to the public it was not protected from discovery.[152] Despite not being protected from discovery, this court also did not compel production.

The *Keller* court reasoned that the party seeking discovery must make a threshold showing that publically available information on those sites undermines the opposing party's claims before the requesting party is able to obtain it.[153] The court's reasoning would be that this would protect against fishing expeditions and would enforce the requirement that the discovery be reasonably calculated to lead to the discovery of admissible evidence.[154]

4. *EEOC v. Simple Storage Management*

A federal district court in Indiana recently allowed an employer limited discovery into sexual harassment claimants' social networking communication.[155] In that case, the EEOC responded to an interrogatory that, as a result of the alleged sexually hostile work environment, two of the claimants suffered anxiety, depression, and post traumatic stress disorder for which they sought medical treatment.[156] The employer then sought production of all social networking site content, photographs, and videos of those two claimants for the relevant time period.[157] The EEOC, while conceding social media content that directly addressed the matters alleged in the complaint was relevant, objected to production of *all* social networking site content (and to similar deposition questioning) on the grounds that the requests were overbroad, not

---

[151] *Keller* 2013 WL 27731 at *3 (D. Mont. Jan. 2, 2013).
[152] *Id.* at *4.
[153] *Id.* at *4.
[154] *Id.* Similarly, investigation of internet postings on blogs and their authors is particularly on the rise in defamation cases. More specifically, plaintiffs are increasingly using third-party subpoenas to seek the identity of anonymous bloggers who post allegedly defamatory statements. *See, e.g., Krinsky v. Doe6*, 159 Cal.App.4th 1154, 1168-73 (2008); *In re Does 1-10*, 242 S.W.3d 805 (Tex.App.—Texarkana 2007); *Klehr Harrison Harvey Branzburg & Ellers, LLP v. JPA Development, Inc.*, 2006 WL 37020, * (Pa. Com. Pl. 2006) (collecting cases).
[155] *EEOC v. Simply Storage Management, LLC*, 270 F.R.D. 430 (S.D. Ind. 2010). Whether social networking posts are discoverable has also been addressed outside the context of employment cases, with conflicting results. *Compare Romano v. Steelcase Inc.*, 907 N.Y.S.2d 650 (N.Y.Super. 2010) (granting access) *with Crispin v. Christian Audigier, Inc.*, 717 F.Supp.2d 965 (C.D. Cal. 2010).
[156] *Id.* at 433.
[157] *Id.* at 432.

relevant, unduly burdensome because they improperly infringe on claimants' privacy, and would harass and embarrass the claimants.[158] The employer claimed discovery of the material was proper, because the discovery responses placed the emotional health of such claimants at issue, thereby implicating all their social communications.[159]

In striking a balance between the positions of the parties, the court noted at the outset that social networking communication is not immune from discovery merely because the communications have been "locked" by privacy controls on the social network site.[160] While acknowledging the validity of privacy concerns, the court held such concerns were appropriately addressed through a protective order.[161] The court further held that social networking communication and content must be produced when it is relevant to a claim or defense in a case.[162] With regard to the limitations of relevance in addressing an emotional distress claim, the court held—on the one hand—that claims of distress, depression, or similar injuries do not automatically render all social networking communications relevant, but—on the other hand—that restricting discovery to communications directly addressing the allegations of the complaint was too narrow.[163] Accordingly, the court granted the employer discovery of (1) the claimants' social networking communications "that reveal, refer, or relate to any emotion, feeling, or mental state, as well as communications that reveal, refer, or relate to events that could reasonably be expected to produce a significant emotion, feeling, or mental state"; (2) third-party communications to the claimants that placed the claimants' own communications in context; and (3) pictures and video of the claimants taken during the relevant time period and posted on the claimants' profiles.[164]

Since social media communication contains generally unfiltered reflections of the emotional state of individuals, it will have an ever increasing role to play in litigation between employers and employees

---

[158] *Id.* at 432.
[159] *Id.* at 432-33.
[160] *Id.* at 434.
[161] *Id.*
[162] *Id.*
[163] *Id.*
[164] *Id.* at 436.

with regard to claimed emotional distress. As demonstrated by the Indiana court's analysis, courts are still developing the parameters of the relevance of social media to employment cases. Employers and their counsel should not overlook social media as a source of evidence in employment litigation.

5. *Negro v. Superior Court*

The Stored Communication Act ("SCA") also presents obstacles to formal discovery. In a recent California state case the court grappled with the limits that the SCA places on civil discovery. In *Negro v. Superior Court* a Florida district court case resulted in a subpoena to Google being issued from a California court for the emails of Matteo Negro a defendant in the underlying Florida litigation.[165] Initially the subpoena was ineffective because Negro did not provide his consent to the disclosure as required by the SCA to permit the disclosure of the emails which are stored communications under the SCA.[166]

By the time the California appellate court reviewed the case, the Florida court had ordered Negro to provide his consent and he complied with the order to do so.[167] The California appellate court issued a writ directing the lower California court to issue a new order requiring Google to produce the emails.[168] Negro challenged the California court's order arguing that his consent was compelled because it was only done in order to comply with the Florida court's order.[169]

The appellate court made three significant findings of interest to a larger audience. The first is that the emails are protected by the SCA.[170] The second is that the user's consent to disclosure is required before the subpoena could be enforced.[171] The third is that a trial court can "compel" that consent through an order enforced by the threat of contempt and the consent granted under these circumstances satisfies the SCA.[172]

---

[165] *Negro v. Superior Court*, 2014 WL 5341926 (Cal. Ct. App. Oct. 21, 2014).
[166] *Id.* at *7.
[167] *Id.* at *8.
[168] *Id.* at *16.
[169] *Id.* at *9-10.
[170] *Id.* at *4.
[171] *Id.*
[172] *Id.* at *12 ("He seeks to have the best of both worlds by complying with the court's order while denying that his decision to do so should be given legal effect. We reject this contention and hold that the consent expressly given by him pursuant to court order constituted "lawful consent" under the SCA.").

So, for savvy practitioners seeking third-party discovery from large, well-heeled companies that store electronic communications under the SCA making sure that a consent from the party the communications were created by will prevent a dispute later.

6. Electronic Information on Employer-Owned Computers

In any dispute between an employer and an employee or former employee, electronic information on the employee's work computers may be highly probative. However, in many cases, employees use their workstations for personal use, as well as for work purposes. Accordingly, compelling discovery of such information can be complex.

For example, a California Court of Appeals granted a writ of mandamus overruling a lower court's decision that a former employee was not required to produce a home workstation provided to the employee by the employer.[173] Robert Zieminski was an executive of TBG Insurance Services Corporation who was given two computers owned by TBG to use for work purposes, one at the office and one at home.[174] In connection with these computers Zieminski signed TBG's electronic equipment policy which stated the computers would be used only for business purposes and would not be used for personal benefit or for improper, derogatory, defamatory, obscene, or other inappropriate purposes.[175] Zieminski was terminated from his employment when pornographic sites had been repeatedly accessed on Zieminski's work computer.[176] Zieminski claimed such sites accidentally popped up on his workstation and that he was actually terminated as a pretext to prevent his stock holdings in the company from vesting.[177] He sued for wrongful termination.[178]

TBG's attorneys asked Zieminski's attorneys to return the home computer owned by TBG and not to delete anything stored on the computer's hard drive.[179] Zieminski refused, saying he would either

---

[173] *TBG Insurance Services Corp. v. Superior Court*, 96 Cal.App.4th 443 (Cal.App. (2d Dist.) 2002).
[174] *Id.* at 446.
[175] *Id.*
[176] *Id.*
[177] *Id.*
[178] *Id.*
[179] *Id.*

purchase the computer from TBG or return it after deleting personal information on the computer that was "subject to the right of privacy."[180] Upon TBG's motion to compel, Zieminski argued he had a right to privacy under the California constitution, it was understood the home computer was a perk to senior executives, and the computer was used by his wife and children and contained significant personal data.[181] The trial court denied the motion to compel, because TBG already had significant evidence from the work computer and the "merely corroborative" evidence contained on the home computer did not outweigh the privacy interest in the personal information contained therein.[182]

The appellate court disagreed. Initially, the court noted the test for discovery is not admissibility but relevance.[183] The home computer was "indisputably relevant" and whether or not it was cumulative could not render it undiscoverable.[184] The issue to be addressed was whether Zieminski had a protectable privacy interest in the information contained on the home computer.[185] The appellate court found Zieminski did not have a reasonable expectation of privacy in the home computer, because community norms in the modern workplace diminish an employee's reasonable expectation of privacy, TBG gave Zieminski advanced notice through its policy statement that his use of the computer may be monitored, and Zieminski agreed to TBG's policy, thereby voluntarily waiving whatever right of privacy he might otherwise have had.[186] In conclusion, the court noted appropriate protective orders could protect unnecessary copying and dissemination of financial and other information contained on the computer that was not relevant to the case. [187]

---

[180] *Id.* at 446-47.
[181] *Id.* at 447.
[182] *Id.* at 447-48.
[183] *Id.* at 448.
[184] *Id.*
[185] *Id.* at 449.
[186] *Id.* at 449-454.
[187] *Id.* at 454.

IV. ADMISSIBILITY

In *Tienda v. State*, the Texas Court of Criminal Appeals held that the existing rules of evidence provide the relevant framework for determining the admissibility of social media such that no special rule is required for dealing with same.[188]

Tienda involved a gang-related murder trial, in which the State introduced postings taken from MySpace as statements made by the defendant.[189] The State elicited testimony from the victim's sister about the MySpace profile and its connection to the defendant, as well as testimony from a detective on how gangs use Myspace.[190] The State also introduced evidence of multiple pictures "tagged" to the profile that showed a person displaying gang-related tattoos and hand-signs, as well as posts written by the profile that revealed knowledge of the murder. The defendant's counsel objected strenuously and elicited testimony from the detective about how easy it would be for someone to create a fake MySpace profile.[191]

On review, the Criminal Court of Appeals explained that "as with the authentication of any kind of proffered evidence, the best or most appropriate method for authenticating electronic evidence will often depend upon the nature of the evidence and the circumstances of the particular case."[192] The Court then held that the State had presented enough circumstantial evidence of authenticity to submit the posts to the jury who, as the finders of fact, could determine if the evidence was authentic or not.[193]

In *Parker v. State*, the Delaware Supreme Court compared the Texas approach in *Tienda* with a more stringent approach used by Maryland in *Griffin v. State*.[194] Under the Maryland approach, social media evidence may only be authenticated through "the testimony of the creator, documentation of the internet history or hard drive of the purported creator's computer, or information obtained directly from the social

---

[188] *Tienda v. State*, 358 S.W.3d 633 (Tex. Crim. App. 2012).
[189] *Tienda*, 358 S.W.3d at 636.
[190] *Id.*
[191] *Id.*
[192] *Id.* at 640.
[193] *Id.* at 647.
[194] *Parker v. State*, 85 A.3d 682, 684 (Del. 2014) (the post that was at issue in this case stated "bet tht [sic] bitch didnt [sic] think [I] was going to see her ass ... bet she wont [sic] inbox me no more, # caughtthatbitch").

networking site."[195] Unless the proponent can demonstrate the authenticity of the social media post to the trial judge using these exacting requirements, the social media evidence will not be admitted in Maryland and the jury cannot use it in their factual determination.[196] Stated differently, in Maryland, social media evidence is only authenticated and admissible where the proponent can convince the trial judge that the social media post was not falsified or created by another user.[197]

After considering the two approaches, the Delaware Supreme Court concluded that the Texas approach better conforms to the requirements of Rule 104 and Rule 901 of the Delaware Rules of Evidence, under which the jury ultimately must decide the authenticity of social media evidence.[198] The Delaware Supreme Court described its reasoning as follows:

> Social media has been defined as "forms of electronic communications ... through which users create online communities to share information, ideas, personal messages, and other content (as videos)." Through these sites, users can create a personal profile, which usually includes the user's name, location, and often a picture of the user. On many sites such as Facebook or Twitter, a user will post content—which can include text, pictures, or videos—to that user's profile page delivering it to the author's subscribers. Often these posts will include relevant evidence for a trial, including party admissions, inculpatory or exculpatory photos, or online communication between users. But there is a genuine concern that such evidence could be faked or forged, leading some courts to impose a high bar for the admissibility of such social media evidence. Other courts have applied a more traditional standard, "determining the admissibility of social media evidence based on whether there was sufficient evidence of authenticity for a reasonable jury to conclude that the evidence was authentic." This approach recognizes that the risk of forgery exists with any evidence and the rules provide for the jury to ultimately resolve issues of fact.[199]

Given the heightened concerns associated with the admissibility of evidence in a criminal trial, it seems likely that a similar approach to social media admissibility will prevail in civil employment law matters.

---

[195] *Parker*, 85 A.3d at 683.
[196] *Id.* at 683.
[197] *Id*.
[198] *Id.*
[199] *Parker*, 85 A.3d at 685-6 (footnotes and citations omitted).

V. CONCLUSION

Social media offers a wealth of opportunities for the savvy entity or attorney, but mining it without restriction or heed for the growing body of patchwork limitations and restrictions can lead to disaster. Attorneys in particular are well advised to be intimately familiar with their obligations under the applicable rules of professional conduct and for the limits existing statutes (like the SCA) and emerging trends (like those involving electronic attorney-client communications) before undertaking self-help discovery of social media and other electronic data. Identifying and addressing potential points and limits may or may not be a simple matter, but being aware that they exist is far better than pretending they do not.

This paper is not intended as legal advice.