Non-competes in the Electronic Workplace: Solicitation in the Age of Social Media

Presented by:

Covenants Not to Compete and Trade Secrets Subcommittee

Editors-in-Chief:
David J. Carr, Ice Miller LLP, Indianapolis, Indiana
Arnold Pedowitz, Pedowitz & Meister, LLP,New York, NY
Eric A. Tate, Morrison, Foerster LLP, San Francisco, CA

Contributors:
James M. Shore, Stoel Rives LLP, Seattle, WA
David Kight, Spencer Fane Britt & Browne, LLP, Kansas City, MO
Denise Portnoy, Spencer Fane Britt & Browne, LLP, Overland Park, KS
Christina H. Bost Seaton, Troutman Sanders LLP, New York, NY
Christopher J. Harristhal, Larkin Hoffman Daly & Lindgren Ltd., Minneapolis, MN
Katherine J. Donohue, Butzel Long, PC, Detroit, MI
Bernhard J. Fuhs, Butzel Long, PC, Detroit, MI

Presented For:
ERR Committee of the ABA Section of Labor and Employment Law

Las Vegas, Nevada—March 28-31, 2012

TABLE OF CONTENTS

Page

SOLICITATION VIA SOCIAL MEDIA—CASE LAW

"Viral" today describes social media use itself. Facebook boasts over 800 million users;[1] LinkedIn[2]--over 120 million users. New professionals currently sign up at a rate faster than two new members per second.[3]

The workplace possesses no immunity from the rapid expansion of social networking. To the contrary, social media continues to experience significant growth in that context. Businesses use social media to advertise products. Professionals use social media to promote the services they provide. However, while social media offers numerous benefits to businesses and their employees, its presence in the workplace creates unique legal issues, and courts find themselves struggling to keep up.

Social networking allows employees to easily connect and communicate with co-workers and clients, and this feature creates concern for employers as it relates to restrictive covenants. Users of Facebook, LinkedIn, and other social media sites may find themselves in violation of non-solicitation or non-competition agreements with former employers.

Routine LinkedIn or Facebook activities, such as connecting with contacts and posting information about one's place of employment, can constitute serious violations of an employee's non-solicitation agreement. Many employers are uncertain how to deal with employees' use of

---

[1] Facebook Statistics, http://www.facebook.com/press/info.php?statistics (last visited on October 23, 2011).

[2] LinkedIn is a social networking website geared towards use by professionals looking to manage and expand their business network. LinkedIn users create a profile containing their business contact information, along with information on education, work history, and job skills. Users may search for other registered members and "connect" with them. Once users are connected, they have access to each other's business contact information and publicly indicate that they are professionally associated. Users can also designate their membership in professional groups or associations and indicate the employers for whom they work.

[3] LinkedIn, "About" page, *http://press.linkedin.com/about*(last visited on October 23, 2011).

Facebook, LinkedIn, and other social media to communicate with contacts in and outside of the company. Former employees using social media covered by agreements containing restrictive covenants do not always know what constitutes permitted social networking conduct after the cessation of the employment relationship.

To date, no large body of binding precedent exists as to employer and employee conduct with respect to social media. However, recent case law at least identifies some significant issues that arise from the interplay between social media use and restrictive covenants. In this ever changing field, wise employers and employees will anticipatorily address these issues to avoid being the next test case.

Connecting With Contacts On Social Media Websites May Violate Non-Solicitation And Non-Competition Agreements.

A recently filed lawsuit, *TEKsystems, Inc. v. Hammernick*, raised a novel legal question: can simply "connecting" with professional contacts through networking sites violate an agreement barring solicitation?[4] Brelyn Hammernick ("Hammernick") was employed as a recruiter for TEKsystems, Inc. ("TEKsystems"), an Information Technology staffing firm. On November 13, 2009, Hammernick left TEKsystems to work for Horizontal Integration, Inc., an IT-staffing firm that competes with TEKsystems. Four months later, TEKsystems sued Hammernick and Horizontal Integration. It alleged that Hammernick, on behalf of her new employer, unlawfully communicated with at least twenty TEKsystems contract employees. TEKsystems specifically alleged that Hammernick violated her employment agreement by "connecting" to the other employees via LinkedIn.

[4] Complaint, *TEKsystems, Inc. v. Hammernick*, 2010 WL 1624258 (D. Minn. dismissed Oct. 18, 2010) (No. 10-CV-00819).

Hammernick's employment agreement with TEKsystems included covenants not to compete, not to solicit and not to divulge confidential information. These agreements prohibited Hammernick from directly or indirectly approaching, contacting, soliciting, or inducing any person who had been a "Contract Employee" to" cease working for TEKsystems . . . refrain from beginning work for TEKsystems . . . [or] provide services to any individual, corporation or entity whose business is competitive with TEKsystems. " These restrictive covenants were silent with respect to using social media as method of solicitation, competition, or disclosure of information.

In addition to alleging that Hammernick improperly "connected" with contract employees, TEKsystems claims that Hammernick unlawfully sent messages to these individuals through the LinkedIn service. An exhibit to the complaint contains the following correspondence between Hammernick and a TEKsystems contract employee:

> Tom—
>
> Hey! Let me know if you are still looking for opportunities! I would love to have [you] come visit my new office and hear about some of the stuff we are working on!
>
> Let me know your thoughts!
>
> Brelyn
>
> ----------
>
> Hi Brelyn,
>
> Indeed I am still looking. I have time, though!
>
> Let's get together. Where are you working these days? Your profile still has you working at TEKsystems. BTW - my email address is lipidfish@gmail.com if you would prefer the non-LinkedIn route.
>
> Tom[5]

[5]Exhibit D, TEKsystems, Inc. v. Hammernick, 2010 WL 1624258 (D. Minn dismissed Oct. 18, 2010) (No. 10-CV-00819).

Although Hammernick's actual correspondence contains more conspicuous solicitation, the allegation that merely "connecting" to new contacts on LinkedIn constitutes solicitation stands as unique and far-reaching. Unfortunately, this issue failed to receive explicit court attention. On October 18, 2010, U.S. District Judge Patrick Schiltz approved a settlement dismissing the TEKsystems action.[6]

The allegations made in *TEKsystems*raise a number of additional unanswered questions about connecting on social networking sites. Will individuals have to "disconnect" LinkedIn contacts or "de-friend" Facebook friends who are colleagues, customers, clients, or former employers until the end of restrictive covenant periods?[7] What if a former employee leaves to work for a competitor, then updates his LinkedIn profile to reflect his new position?[8] What if LinkedIn automatically messages the former employee's contacts to announce his change in employment?[9] What if the employee had "connected" with his former employer's key customers just before quitting?[10]

Updates, Postings, And Messages On Social Media Websites May Constitute Solicitations.

Status updates, postings, and messages on social media sites may violate restrictive covenants, even though they are contained within an individual's existing social media contacts.

---

[6] Order for Permanent Injunction and Dismissal of Action, *TEKsystems, Inc. v. Hammernick*, 2010 WL 1624258 (D. Minn dismissed Oct. 18, 2010) (No. 10-CV-00819).

[7] Ed Frauenheim addresses these and other questions in his recent article: *You Can't Take Your Online Contacts with You—or Can You?*, CRAIN'S CLEVELAND BUSINESS (June 30, 2011), http://www.crainscleveland.com/article/20110630 (last visited October 23, 2011).

[8]Marisa Warren & Arnie Pedowitz, *Social Media, Trade Secrets, and Yes, the Sky is Falling*, ABA NATIONAL SYMPOSIUM ON TECHNOLOGY IN LABOR & EMPLOYMENT LAW (April 27-29, 2011), *available at*http://www2.americanbar.org/calendar/ll04271-national-symposium/Documents/a_03.pdf (last visited October 23, 2011).

[9] Id.

[10] Id.

Coface Collections North America, Inc. v. Newton presented these very issues.[11]William Newton ("Newton") voluntarily left his position as President of Coface in December 2008. Around January 5, 2011, Newton formed, and began actively operating, a new company, Newton, Clark & Associates, LLC ("Newton Clark"). Around this time, Newton updated his LinkedIn profile to reflect his new status as "Chairman of the Board" at "Newton Clark." On Facebook he stated that his "non-compete ends on 12/31/2010 and I have decided that the USA needs another excellent, employee oriented Commercial Collection Agency." The posts encouraged experienced professionals to contact Newton or Clark Pellegrin, also a former Coface employee, to apply for a position with Newton Clark.

Coface sought an injunction restricting Newton from owning, operating, or participating in any business "similar or competitive to" Coface. Coface argued that Newton's conduct violated several express terms of his employment agreement, including the restrictive covenant. The District Court granted the injunction and the Third Circuit affirmed.

As demonstrated by this case, updating profile information and posting comments on social media sites can provide evidence that an employee violated his or her restrictive covenants.

Passive Messages About Job Opportunities On Social Media Websites May Qualify As Solicitations.

Passive messages promoting job opportunities on social media sites or job postings to a public group of social media may also qualify as solicitations. In *Amway Global v. Woodward*, the court affirmed an arbitrator's award for a breach of a non-solicitation provision.[12] The court held that the record included evidence that would readily be characterized as solicitations. In

[11] 430 Fed.Appx. 162 (3rd Cir. 2011).

[12] 744 F. Supp. 2d 657 (E.D. Mich. 2010).

particular, the court focused on a blog entry in which a distributor announced his decision to join the competitor and gave his reasons for doing so, stating, "If you knew what I knew, you would do what I do."

The former employee argued that to the extent his former employer relied upon blogs and website postings to establish violations of the non-solicitation provision in the Rules of Conduct, such passive, untargeted communications fail as a matter of law to qualify as actionable solicitations. The court disagreed, deciding that the statement posted could be readily characterized as an invitation for the reader to follow the individual's lead and join the former employer's competitor. "Common sense dictates that it is the *substance* of the message conveyed, and not the medium through which it is transmitted, that determines whether a communication qualifies as a solicitation…Solicitations do not lose this character simply by virtue of being posted on the Internet." Contrarily, the dissent argued that the "passive placement" of a message that could potentially be viewed as an advertisement for a job opening should not qualify as solicitation because it did not entail "one-on-one importuning" and was not "directed at specific individuals."

Enhanced Network Solutions Group, Inc. v. Hypersonic Technologies Corporation dealt with a similar issue but reached a different result.[13] In that case, two companies entered into a SubContractor Agreement through which Enhanced Network Solutions Group, Inc. ("ENS") would acquire certain services from Hypersonic to serve ENS's own clients. Pursuant to the terms of the Agreement, the parties were to refrain from soliciting employees of the other parties. During the parties' contractual relationship, Hypersonic posted an open position for an outside

[13] 951 N.E.2d 265 (Ct. App. Ind. 2011).

sales representative on its LinkedIn web portal. The LinkedIn posting was available for viewing by the people who belonged to a certain group within LinkedIn.

After reading the job description, Robert Dobson, a field representative for ENS, noticed the job posting and informed Shawn Mettler, President of Hypersonic, that he was interested in applying for the position. Hypersonic's owner and Mettler met Dobson for lunch in April of 2010. Hypersonic offered Dobson employment and he accepted.

Hypersonic filed a complaint against ENS for declaratory judgment, seeking a decision as to the enforceability of the Agreement. The trial court issued an order concluding that Hypersonic did not solicit, induce, or attempt to solicit or induce Dobson to terminate his employment with ENS.

The appellate court, in reviewing the lower court's decision, noted that the Agreement did not define "solicit" and "induce." Based on the dictionary definitions of the words, the court concluded, Hypersonic did not improperly solicit or induce Dobson to terminate his position with ENS and accept a job opening at Hypersonic. As Dobson made the initial contact with Hypersonic after reading the job posting on a portal of LinkedIn, Dobson solicited Hypersonic, not the other way around. Dobson made all the major steps to initiate conversations about the position. Thus, the appellate court decided that Hypersonic did not breach the non-solicitation clause of the agreement.

Social Media May Impact Employers' Ability To Protect Confidential Information And Trade Secrets

Social Media use may impact employers' ability to protect confidential information. In order to qualify as a trade secret, information must be maintained in confidence, must have commercial value not generally known, and must not be readily ascertainable by proper means.

As a general rule, the more detailed and difficult to obtain the information, the more likely that the customer list will be considered a trade secret.

Otherwise confidential customer information may lose its protection through inclusion or connection to social media profiles. A company's customer list may qualify as a trade secret only if the company takes reasonable steps to protect the secrecy of that information. Employees who used sites like LinkedIn and Facebook provide public access about their contacts to persons to whom they are connected. These sites often provide information about how contacts know each other, business they have done together, and other details about the nature of the relationship. Employers would seem hard pressed to assert that customer lists and customer contact information remains "confidential and proprietary" when its employees provide access to that information via Facebook, LinkedIn or another similar social media accounts.

In *Sasqua Group, Inc. v. Courtney*, the court held that although an employer's customer list can qualify for trade secret protection, "the exponential proliferation of information made available through full-blown use of the Internet [presents] a different story."[14] Sasqua Group, Inc. ("Sasqua Group"), an executive search consulting firm that recruits and places professionals in the financial services industry, sought an injunction against Lori Courtney ("Courtney") former recruiter, alleging that Courtney misappropriated trade secrets. According to Sasqua, Courtney had access to its customer database prior to her departure, and the database was the "lifeblood" of its business. The database contained client contact information, individual candidate profiles, contact hiring preferences, employment backgrounds, descriptions of previous interactions with clients, resumes and other information.

[14] No. CV 10-528, 2010 WL 3613855 (E.D.N.Y. Aug. 2, 2010).

Courtney testified that "virtually all personnel in the capital markets industry . . . have their contact information on Bloomberg, LinkedIn, Facebook or other publicly available databases." During the hearing, Courtney was asked what she would do "if she had amnesia tomorrow, lost her blackberry" and "needed to identify" decision makers and prospective clients. She said she would use the internet and the vast amount of information available on it, which she claimed she could find through a five-minute search. Courtney explained that she could start with LinkedIn "because people put their whole profile on LinkedIn." She explained that if she wanted to find the decision maker at a particular company, she could simply enter the name of the company in the search box. Seconds later, she would have a list of employees, their positions, current title, prior jobs, undergraduate school, dates of attendance, experience, objectives, and even contact information. If she wanted more information, she could do a search on Google and she would have thousands of search results, many of which pointed to news stories recounting companies' hiring plans.

Based on Courtney's testimony, the court concluded that the information publicly available "exceeded the amount and level of detail contained in the Sasqua database." The clients, their contact information, and other data stood readily accessible and thus not protected in light of the public nature of the information and Sasqua's failure to take reasonable measures to protect the database in question, including putting in place a confidentiality agreement. Plainly, companies must be aware of what information their employees are putting on social media sites such as LinkedIn and Facebook, and take steps to protect the confidentiality of information they desire to protect. Failure to do so will find them holding an empty bag at trial.

With that said, there still may be an issue as to whether an employee's disclosure of such information on a social media site was permissible. *See, e.g., Masonite v. County of Mendocino*

Air Quality Mgmt. Dist., 42 Cal. App. 4th 436, 452 (1996) (employee can issue a waiver only within the scope of her employment); *Paley v. Du Pont Rayon Co.*, 71 F.2d 856, 858 (7th Cir. 1934) (employee's immediate supervisor could not waive company's right to employee's invention, because he lacked authority to do so). Indeed, employers may be able to preserve the trade secret status of such compromised information by taking prompt steps to address an unauthorized disclosure. *See, e.g.,By-Buk Co. v. Printed Cellophane Tape Co*., 163 Cal. App. 2d 157, 165 (1958) (remedial action may enable the company to "preserve [its] rights in the trade secret by preventing a public disclosure.").

In that regard, confidentiality agreements and social media policies can be important tools in avoiding the loss of trade secret status. In order to address the particular risk of proliferation of confidential information on social media, employers can maintain confidentiality agreements and social media policies that incorporate provisions explicitly regulating employee social media use as it pertains to confidential information. Although there may be concerns,in some contexts, about regulating employee social media use (*e.g.*, free speech, that are outside the scope of this paper), it is clear that employees have no less of a right to breach a confidentiality agreement through social media than they otherwise would if not using social media. *See, e.g.*, *Immunomedics, Inc. v. Doe*, 342 N.J. Super. 160, 167 (App. Div. 2001) ("[i]ndividuals choosing to harm another or violate an agreement through speech on the Internet cannot hope to shield their identity and avoid punishment through invocation of the First Amendment"). Ultimately, the fact that an improper disclosure may occur through a blog or other social medium does not somehow exempt that disclosure from the reach of a lawful confidentiality obligation.

PRE-LITIGATION INVESTIGATIONS INVOLVING SOCIAL MEDIA

As will be discussed in greater detail in Section 3 below, no question exists that social media may be responsive to traditional discovery requests during litigation. During the pre-litigation investigation phase, however, the answer to whether an employer has a right to investigate an employee's (or former employee's) social media profiles and usage stands as far less clear-cut. At its core, the issue before the court in such cases rests on whether the employee's right to privacy suffered violation, and if so, what remedy stands as appropriate for dealing with such a violation.

As a developing area of the law, few cases directly address the question. We can, however, look to cases involving an employer's pre-litigation investigation into an employee's email accounts for guidance as to how the courts may go.

The cases discussed below suggest that practitioners must pay close attention to employers' policies to determine the permissibility of monitoring of employees' social media accounts. If an employer's policy stands silent on this point, some cases (such as *Stengart v. Loving Care*, below) suggest that the employee has not impliedly authorized the employer to access the account. Accordingly, the employer lacks authorization to monitor the employee's social media account. Another factor that courts consider when determining implied authorization to access an employee's social media account: whether the employee saved his log-in information on his work computer. *See Pure Power Boot Camp v. Warrior Fitness Boot Camp*, below. If an employer receives log-in information from someone other than the owner of the social media profile, the employer must make sure both that the person giving the log-in information was himself a permitted user of the social media profile, and that the third party provided the log-in information to the employer willingly. *SeePietrylo v. Hillstone Restaurant Group*, below.

Finally, the ABA recently determined in Formal Opinion 11-459 (below) that attorneys are ethically required to, "as soon as practical…instruct [an] employee-client to avoid using a workplace device or system for sensitive or substantive communications, and perhaps for any attorney client communications…."

Please find set forth below an in-depth review of cases (as well as ABA Formal Opinions) that provide guidance as to whether, during the pre-litigation investigation phase, an employer possesses the right to investigate an employee's (or former employee's) social media profiles.

Pietrylo v. Hillstone Restaurant Group, No. 06-5754, 2009 U.S.Dist. LEXIS 88702 (D.N.J. Sept. 25, 2009)

The *Pietrylo* case offers one the few decisions directly addressing an employer's pre-litigation investigation into an employee's social media profile. Plaintiffs Pietrylo and Marino, employees of a Houston's restaurant, were terminated after Houston's managers gained access to the Spec-Tator, a private invitation-only chat group for Houston's employees on the social media network Myspace.com. Plaintiffs' complaint alleged (1) violations of the federal Wiretap Act (18 U.S.C. §§ 2510-22) (the "Wiretap Act"); (2) violations of the parallel New Jersey Wiretapping and Electronic Surveillance Control Act (N.J.S.A. 2A:156A-3, *et seq*.); (3) violations of the federal Stored Communications Act (18 U.S.C. §§ 2701-11) (the "Stored Communications Act"); (4) violations of the parallel provision of the New Jersey Act (N.J.S.A. 2A:156A-27); (5) wrongful termination in violation of a clear mandate of public policy; and (6) common law invasion of privacy. Plaintiffs voluntarily dismissed their wiretapping claims (their first and second claims) after discovery showed that Defendants did not "intercept" any electronic communications under the meaning of those acts.

At a jury trial, the jury returned a verdict in favor of Plaintiffs on their federal and state Stored Communications Act claims, finding that Defendant had, through its managers, knowingly or intentionally or purposefully accessed the Spec-Tator without authorization on five occasions. The jury found, however, that Defendant had not invaded the common law right of privacy. Since the jury found that Defendant had acted maliciously, it also awarded punitive damages. The jury awarded $2,500 and $903 in compensatory damages (lost wages) to Pietrylo and Marino, respectively. By stipulation of the parties, the award of punitive damages equaled four times the amount of punitive damages awarded by the jury.

Following the jury trial, Defendant moved for judgment as a matter of law pursuant to Fed. R. Civ. P. 50(b) or, in the alternative, for a new trial pursuant to Fed. R. Civ. P. 59.To prevail upon their claims under the Stored Communications Act, Plaintiffs were required to offer sufficient evidence to allow the jury to conclude that Houston's managers knowingly, intentionally, or purposefully accessed the Spec-Tator without authorization. Defendant argued that (1) there was no evidence that St. Jean, an invited member of Spec-Tator, did not authorize the Houston's managers to use her password to access the Spec-Tator; and (2) Plaintiffs presented no evidence that Houston's managers presented the requisite scienter for a violation of the Stored Communications Act. The Court denied Defendant's motion and upheld the jury verdict and the awards of compensatory and punitive damages.

On the issue of authorization, St. Jean had testified that "she felt she had to give her password [to a Houston's manager] because she worked at Houston's and for [that particular manager]." St. Jean also testified that "she would not have given [the manager] her password if he had not been a manager and that she would not have given her information to other co-workers." Finally, when asked whether she felt that something would happen to her if she did

not give the manager her password, she answered "I felt that I probably would have gotten into trouble." The Court found that the jury could reasonably infer from this testimony that St. Jean's purported "authorization" was coerced or provided under pressure, and accordingly, that Houston's access of the Spec-Tator was not, in fact, authorized.

On the issue of scienter, the Court found that the evidence presented to the jury showed that Houston's managers accessed the Spec-Tator on several different occasions, even though it was clear to them that St. Jean had reservations about having provided them with her log-on information. For example, one of the managers testified that he knew that St. Jean "was very uneasy with the fact that she had given me and the rest of the managers her password."

The Court also affirmed the jury's award of punitive damages, which are available under the Stored Communications Act (and its New Jersey equivalent) if the violation is "willful or intentional." Importantly, the Court found that:

> [a]lthough Houston's certainly does has a right and obligation to protect its employees and managers from harassment or humiliation, and to protect the core values of the restaurant, the jury's findings indicate that the jury did not believe that the method used by Houston's to protect those values was proper conduct, finding that Houston's knowingly accessed the stored communications without authorization five times…the jury had sufficiently evidence from which it could be inferred that Houston's acted maliciously in repeatedly accessing the Spec-Tator via St. Jean's password. St. Jean had testified, in sum and substance, that she did not feel free to deny her boss' request for her account and password…the inferences from her testimony could have been found by a reasonable jury to mean that she did not voluntarily consent [to give her password to Houston's managers].

Konop v. Hawaiian Airlines, Inc., 302 F.3d 868 (9th Cir. 2002)

While the *Konop* case pre-dates social media as we know it, it addresses an analogous situation, *i.e.*, access to an employee's private password-protected website discussing his employer and the terms and conditions of his workplace.In *Konop*, a pilot sued his employer, Hawaiian Airlines, alleging that the airline had viewed his secure website, upon which he had

posted entries critical of his employer, its officers, and the incumbent union. Konop controlled access to the website by requiring visitors to log-in with a username and password. Konop assigned a username to each of his colleagues, who then created their own passwords. Each person who logged in with a username had to also click a box to affirm that they agreed to abide by the website's terms and conditions, which specifically prohibited any members of Hawaiian Airlines' management from viewing the website, and which also prohibited users from disclosing the website's contents to anyone else.

Pilot Gene Wong, an approved user of Konop's website, was asked by Hawaiian Airlines' vice president, James Davis, for permission to use Wong's log-in information for Konop's website. Wong agreed and provided Davis with his log-in information. Davis told Wong that he was concerned about untruthful allegations that he believed Konop was making on the website. Another pilot, Gardner, also agreed to provide Davis with his log-in information. Later that day, Konop was contacted by the chairman of the union, who informed Konop that the Hawaiian Airlines' president, Bruce Nobles, had contacted him earlier in the day about the contents of Konop's website. Among other allegedly disparaging claims on Konop's website, Nobles was upset by Konop's accusations that Nobles was suspected of fraud.

Konop asserted federal claims pursuant to (1) the Wiretap Act (in particular, Title I of that Act, which is the Electronic Communications Privacy Act ("ECPA"); (2) the Stored Communications Act; (3) the Railway Labor Act (45 U.S.C. §§ 151-188) (the "Railway Labor Act"). He also alleged several state law tort claims, which were not at issue in this decision. Konop also alleged that Hawaiian airlines placed him on medical suspension in retaliation for his opposition to its proposed labor concessions, in violation of the Railway Labor Act. The Court, reviewing the decision below *de novo*, affirmed the decision below and concluded that the

Wiretap Act did not apply because Davis' conduct did not constitute an "interception" of an electronic communication in violation of the Wiretap Act.

The Court reversed the District Court's decision in favor of Hawaiian Airlines on Konop's claim pursuant to the Stored Communications Act. Section 2701(c)(2) allows a person to authorize a third-party's access to an electronic communication if the authorizing person is a "user" of the "service" and the communication to which access is granted is a communication "or of intended of that user." A "user" is "any person or entity who - (A) uses an electronic communications service; and (B) is duly authorized by the provider of such service to engage in such use." 18 U.S.C. § 2510(13). The Court reversed the District Court because there was no evidence that either Wong or Gardner was a "user" of Konop's website who could have authorized Davis' access to the website. The Court found that there was no evidence in the record that Wong had ever used Konop's website, and while there was some evidence that Gardner may have used the website, because the District Court had never made any findings as to whether Wong and Gardner had actually used Konop's website, they could not be users for purposes of the Stored Communications Act. The Court stated that finding otherwise would read the "user" requirement out of the Stored Communications Act.

As for the Railway Labor Act, the Court reversed the District Court's decision below to find that, *inter alia*, (a) Konop's claims were not grounded in the collective bargaining agreement, and therefore not subject to mandatory arbitration; (b) Konop's website constituted protected activity under the Railway Labor Act since there was no evidence that he forfeited his protection by "circulating defamatory or insulting material known to be false"; and (c) that Konop raised a triable issue of fact that, by accessing his website, Hawaiian Airlines

(1) interfered with his union organizing activity in violation of the Railway Labor Act; and (2) improperly assisted one union faction over another in violation of the Railway Labor Act.

Pure Power Boot Camp v. Warrior Fitness Boot Camp, 587 F.Supp.2d 548 (S.D.N.Y. 2008)

Plaintiffs Pure Power Boot Camp, *et al*. ("Pure Power") brought an action against defendants Warrior Fitness Boot Camp, *et al*. ("Warrior Fitness") seeking an injunction and damages, arising out of Defendants' alleged (1) theft of Plaintiffs' business model, customers, and internal documents; (2) breach of fiduciary duties; and (3) infringement upon Plaintiffs' trademarks, trade-dress, and copyrights. Plaintiffs alleged, *inter alia*, that Defendants stole Plaintiffs' client list and other items, destroyed a copy of one of the defendant's noncompete agreements, and opened a competing fitness center in direct violation of the noncompete agreement and using Pure Power's misappropriated information.

Defendants moved to preclude the use or disclosure of thirty-four emails sent or received by individual defendant Alexander Fell ("Fell"), who was a trainer who had worked for Pure Power until he was terminated, who then partnered with another former Pure Power trainer, Ruben Belliard ("Belliard") to form Warrior Fitness. The emails were obtained by Pure Power's principal and owner, Laura Brenner ("Brenner"). Defendants argued that Brenner's obtaining of the emails violated (1) the ECPA; (2) the Stored Communications Act; and (3) New York's wiretap law.

The evidence demonstrated that, after Fell and Belliard were no longer working at Pure Power, over the course of a week, Brenner accessed and printed emails from three of Fell's personal email accounts; *i.e.*, (1) his Hotmail account; (2) his Gmail account; and (3) his Warrior Fitness account. Brenner stated that she accessed Fell's Hotmail account because he left his

username and password information stored on Pure Power's computers. She also alleged that Fell gave his username and password to another Pure Power employee so that the employee could monitor an Ebay sale for him (which Fell denied). Brenner accessed Fell's Gmail account because the username and password were sent to Fell's Hotmail account. Brenner accessed his Warrior Fitness account by making a "lucky guess" at his password, which turned out to be the same password he used for his other email accounts. Plaintiffs relied heavily on the emails and considered them to be "critical" to their case.

Pure Power had an Employee Handbook stating that employees' did not have a right to privacy in "any matter stored in, created on, received from, or sent through or over the system [including] the use of personal e-mail accounts on Company equipment." The policy also stated that Pure Power "reserve[d] the right to review, monitor, access, retrieve, and delete any matter stored in, created on, received from, or sent through the system, for any reason, without the permission of any system user, and without notice." As there was no forensic review of Fell's computer by Plaintiffs, they could not determine what emails Fell actually received, sent through, read, or accessed from Plaintiffs' computers.

The Court found that both Brenner's accessing of Fell's emails, and her obtaining them for her own use, would violate the Stored Communications Act if these acts were done without authorization. Plaintiffs argued that the Pure Power email policy put Fell on notice that his emails could be viewed by Brenner, and, alternately, that his leaving his username and password for the Hotmail account on Pure Power's computer gave Brenner implied access to his accounts.

As to Plaintiffs' argument that its email policy put Fell on notice, the Court found that the Pure Power email policy was, by its own terms, limited to "Company equipment" and thus could not apply to emails stored on outside systems such as Microsoft (Hotmail) or Google (Gmail).

The Court also found that there was no evidence that the emails at issue were created on, sent through, or received from Pure Power's computers. The Court further found that there was no evidence that the Gmail or Warrior Fitness accounts were ever accessed from Pure Power's computers, or that those accounts had even existed when Fell worked for Pure Power.

The Court found that Plaintiffs' implied consent argument had no support in the law, because (1) Fell did not store the communications on Pure Power's computers, servers, or systems (they were on a third-party's server); (2) there was no evidence that Fell's personal accounts were used for Pure Power work, or that Pure Power paid or support Fell's maintenance of those accounts; (3) there was nothing in Pure Power's email policy that even suggested that if an employee simply viewed a single personal email from a third-party email account, over Pure Power's computers, then all of his personal emails on all of his email accounts would be subject to inspection; and (4) there was no evidence that the email policy was clearly communicated to employees, consistently enforced in such a manner that would have alerted employees to the possibility that their private email accounts could be accessed and viewed by their employer.

The Court found that Fell had a subjective belief that his emails were private, and that this belief was reasonable. Accordingly, the Court determined that Brenner's access to Fell's personal email accounts violated the Stored Communications Act, and precluded the emails from use in litigation, but not from impeachment purposes should Defendants open the door.

Shefts v. Petrakis, et al., 758 F.Supp.2d 620 (C.D.Ill. 2010)

Shefts, the founder of Access2Go, Inc. ("Access2Go"), a telecommunications company, served as Access2Go's President and CEO, as well as a 30% owner. Defendants Morgan, Petrakis, and Tandeski constituted the other owners of Access2Go.

Morgan, Petrakis, and Tandeski became concerned that Shefts was sexually harassing Access2Go employees and otherwise violating his fiduciary duties. Petrakis was appointed by

the Board, with Shefts' knowledge, to serve as its "liaison of security." In that role, Petrakis purchased monitoring software, which was installed on all Access2Go employees' computers, including Shefts' computer. In addition, Petrakis had all emails sent or received by Shefts forwarded to a dummy account that Petrakis monitored. In addition, Access2Go's Blackberry Enterprise Server ("BES") software was updated to allow for the logging of text messages sent or received from any Blackberry registered to the server. In addition, the Board (including Shefts) ratified the adoption of an Employee Manual that provided, *inter alia*, that Access2Go had the "right to monitor electronic mail messages (including personal/private/instant messaging systems) and their content, as well as any and all use of the Internet and of computer equipment used to create, view, or access e-mail and Internet content."

Several months later, Shefts filed a Verified Complaint against Defendants, alleging violations of (1) ECPA; (2) the Stored Communications Act; (3) the Computer Fraud and Abuse Act, 18 U.S.C. § 1030 ("CFAA"); and (4) Illinois' wiretapping statute. At the same time, Shefts filed (and was granted) an *ex parte* motion seeking a TRO against Petrakis, as well as an *ex parte* motion seeking the seizure of computers in Defendants' offices. After the computers were seized, the parties appeared before the Court for a hearing wherein the parties agreed to have Shefts' forensic examiner image the computers' hard drives, but refrain from analyzing the images until the Court determined whether it would grant a preliminary injunction. At the preliminary injunction hearing, the parties agreed to allow a forensic examination, and met and conferred as to the limitations of such analysis. The decision addresses Shefts' motion for summary judgment.

The Court first denied Shefts' claim that Defendants violated the ECPA by intercepting SMS text messages sent and received on Shefts' blackberry. Although the Court found that an

"intercept" occurred when the BES software acquired and logged Shefts' text messages, it found that Shefts had impliedly consented to this text message logging because he was (1) involved in the purchase and installation of the BES server; (2) knew that emails sent on his Blackberry would be stored on the server; and (3) requested that his Blackberry be connected to the server at various points. The Court noted that Plaintiff was "a sophisticated businessman in the telecommunications industry", but found more compelling the fact that the Employee Manual made clear that communications were subject to archiving at all times.

Next, the Court denied Shefts' claim under the Illinois wiretapping statute. Shefts argued that Petrakis violated the statute by intercepting emails sent or received by Shefts using his personal Yahoo email account, his Blackberry, and his Access2Go email. The Court found that Shefts had no reasonable expectation of privacy in messages sent and received on Access2Go's equipment or using its servers because (1) Access2Go had an Employee Manual disclosing that all communications sent and received on Access2Go's equipment was subject to monitoring; and (2) Shefts was aware that Petrakis had been appointed "security liaison." The Court also denied Shefts' claim under the Stored Communications Act because the Employee Manual authorized Defendants to access and monitor Shefts' communications.

Thygeson v. U.S. Bancorp, et al., No. 03-467, 2004 U.S.Dist. LEXIS 18863 (D.Or. Sept. 15, 2004)

Thygeson, employed by Defendants for over eighteen years, suffered termination after the discovery of inappropriate materials on his work computer. Thygeson was not provided with severance benefits. Theygeson's complaint alleged that Defendants violated the Employee Retirement Income Security Act ("ERISA"), 29 U.S.C. §§ 1001-1461 by (1) wrongfully interfering with his severance benefits in violation of 29 U.S.C. § 1140; (2) breaching their fiduciary duties under 29 U.S.C. § 1104 by failing to notify him of how to apply for severance benefits and failing to respond to his inquiries; and (3) wrongfully denying him benefits to which

he was entitled in violation of 29 U.S.C. § 1132(a)(1)(B). In addition, Thygeson alleged a state law invasion of privacy claim.

In his 2001 performance evaluation, Thygeson, a regional manager, received several "needs improvement" ratings. The next year, his supervisor, Tim Evans ("Evans"), began receiving numerous complaints from sales representatives that reported to Thygeson. Evans was also informed that Thygeson was observed sleeping on the job. When Evens confronted Thygeson about this complaint, Thygeson told Evans that he suffered from "non-debilitating intermittent narcolepsy." Thygeson, however, failed to produce medical documentation for this alleged narcolepsy, after which Evans informed Thygeson in writing that his behavior was unacceptable. Evans began to monitor Thygeson closely, noticing that Thygeson spent a significant amount of time on his computer. Evans also received reports from some of Thygeson's subordinates that Thygeson was sending them emails with inappropriate attachments.

Evans had a report prepared showing Thygeson's internet activity over an extended period time, as Evans wanted to determine if Thygeson was using his office computer for business purposes. Evans also asked for a search to be made of Thygeson's network drive to determine whether Thygeson had saved any inappropriate pictures on the company's equipment.

In response to Evan's monitoring requests, he received a one-inch-thick report listing the addresses of internet sites that Thygeson had visited in the past twelve day period. Evans determined that Thygeson was visiting internet sites approximately four hours a day, and that Thygeson's job did not require such internet usage. Evans also was informed that a search of Thygeson's network drive located inappropriate emails containing pictures of nudity and sexually offensive jokes.

Evans contacted the human relations department to determine which steps to take. The human relations department determined that the material saved on Thygeson's network drive was inappropriate material in violation of Defendants' employment policies. The human relations department advised Evans that because Thygeson was a manager, he should be terminated for his conduct. Thygeson claimed that he did not engage in inappropriate behavior and that Defendants did not follow their typical disciplinary procedures. Defendants moved for summary judgment on all counts.

Considering Thygeson's disparate treatment claim under Section 1140, the Court found that Thygeson's evidence was sufficient to give rise to an inference of discriminatory motive because Thygeson submitted evidence that (1) Evans never told him he spent too much time on the internet or that he was accessing inappropriate materials, and he was never given a chance to explain his actions before being terminated, even though other employees were given notice in similarly circumstances, and only one of those employees was actually terminated; and (2) Evans was looking for a reason to fire him for poor performance that would allow him not to pay Thygeson severance. The Court ruled against Thygeson on his other two ERISA claims.

As for Thygeson's state-law invasion of privacy claims, the Court granted Defendants' summary judgment motion and dismissed the claims. Thygeson argued that he had a reasonable expectation of privacy in files that were stored on Defendants' server in his "personal" folders (which did not have password protection). The Court noted that Thygeson used his employer's computer and network for personal use, and saved personal information in a location that could be accessed by his employer, despite warnings in the Employee Handbook that personal use was prohibited and monitored. The Court also found that Thygeson did not have a right to privacy as to the websites that he visited while using his work computer. This was particularly the case

because the Employee Handbook stated that Defendants' computers were not for personal use and could be monitored, and because the information Defendants' collected was only the website addresses, rather than the actual content of the websites visited.

Smyth v. The Pillsbury Co., 914 F.Supp. 97 (E.D.Pa. 1996)

Plaintiff Smyth received emails on his work email, which he accessed and responded to from home. Shortly thereafter, Plaintiff was terminated for inappropriate and unprofessional comments contained in that email. Plaintiff sued Defendant, alleging that he was wrongfully discharged as regional operations manager. Defendant moved to dismiss, and its motion was granted.

Pennsylvania permits wrongful discharge to be brought by at-will employees only where the discharge violates a clear mandate of public policy. Plaintiff argued that his termination was in violation of public policy "which precludes an employer from terminating an employee in violation of the employee's right to privacy as embodied in Pennsylvania common law. "The Court did not find that Plaintiff had a reasonable expectation of privacy in email communications voluntarily made over the company email system, notwithstanding any assurances made by Defendant that such communications would not be intercepted by management.

Stengart v. Loving Care Agency, Inc., et al., 201 N.J. 300, 990 A.2d 650 (N.J. 2010)

Stengart was provided with a laptop computer to conduct company business. Stengart used this laptop to access her personal, password-protected Yahoo email account, through which she communicated with her attorney about her work situation. She never saved her username or password on the laptop. Shortly thereafter, she left her employment with Loving Care Agency, Inc. ("Loving Care") and returned the laptop. Several months later, she filed a complaint for employment discrimination. During discovery, Defendants' attorneys responded to Stengart's interrogatories, in part, by informing Stengart that it had obtained information from Stengart's

laptop that constituted email correspondence between Stengart and her attorney. Stengart brought an order to show cause for return of the emails and other relief. The trial court denied Stengart's application, and the intermediate appellate court reversed the trial court's determination.

Defendants' Electronic Communications Policy provided that the company reserved the right to review and access "all matters on the company's media systems and services at any time." The Court found that the policy did not address personal accounts at all, and accordingly that Stengart did not have express notice that messages sent or received on her Yahoo email were subject to monitoring.

The Court found that Stengart had a reasonable expectation of privacy in the emails that she exchanged with her attorney on her company-issued laptop because (1) she took steps to protect her privacy by using a personal, password-protected email account rather than her work email account and by not saving her email account's password on her work computer; (2) the Electronic Communications Policy did not directly put her on notice that Defendants would be monitoring emails sent via personal email accounts; (3) the emails themselves were not illegal or inappropriate material that were stored on Defendants' equipment such that they might harm the company in some way. The Court also found that Stengart had not waived the attorney-client privilege generally or as to those emails. Finally, the Court found that Defendants' attorneys' review and use of the privileged emails violated New Jersey Rule of Professional Conduct 4.4(b), which provides that "[a] lawyer who receives a document and has reasonable cause to believe that the document was inadvertently sent shall no read the document or, if he or she has begun to do so, shall stop reading the document, promptly notify the sender, and return the document to the sender."

Holmes v. Petrovich Development Co., LLC, 191 Cal.App.4th 1047 (3d Dist. 2011)

Holmes served as an executive assistant to Paul Petrovich, the principal of the Defendant. Shortly after her hiring, she informed Petrovich that she was pregnant and would be taking up to six weeks maternity leave starting early December. Several months later, Holmes informed Petrovich, over email, that she would, in fact, be beginning her maternity leave mid-November, and that she might remain on maternity leave for the maximum amount of time permitted by California law (four months). Petrovich replied to her email and expressed that he felt as though Holmes had not been completely honest with him, and that this change would make it difficult for him as a small business owner, but that he would, of course, abide by the law.

After several more emails back and forth along these lines, Holmes emailed an attorney from her company computer and email system to ask for a referral for a lawyer specializing in pregnancy discrimination law. That same day, the attorney emailed Holmes and advised Holmes that she should delete their attorney-client communications from her work computer. The next day Holmes met with the attorney, came back to the office, cleaned out her things, and informed Petrovich by email that she felt that she had "no alternative but to end [her] employment."

The next month, Holmes sued Defendants, alleging (1) sexual harassment; (2) retaliation; (3) wrongful termination in violation of public policy; (4) violation of the right to privacy; and (5) intentional infliction of emotional distress. Defendants moved for summary judgment, and the motion was granted by the trial court as to the sexual harassment, retaliation, and wrongful termination causes of action. At trial defendants prevailed on the right of privacy and intentional infliction of emotion distress causes of action.

Holmes appealed the summary judgment decision in favor of Defendants. In her appeal, Holmes contended that the trial court abused its discretion in, *inter alia*, (1) denying her motion

demanding the return of privileged documents; and (2) permitting the introduction of the documents at trial.

The Court found that Holmes' attorney-client communications sent on her work email account and via her work computer were not protected by the attorney-client privilege. Holmes was aware that her work computer was not a confidential manner by which to communicate with her attorney because the company's computer policy disclosed that company would monitor email and that she had no expectation of privacy in any messages sent by the company computer.

ABA Formal Opinion 11-459 (August 4, 2011)

This opinion provides that a lawyer sending or receiving substantive communications with a client via email or other electronic means must warn the client about the risk of sending or receiving such communications via a computer, other device, or email account, where there is a significant risk that a third-party may gain access. The opinion states that "as soon as practical...a lawyer typically should instruct [an] employee-client to avoid using a workplace device or system for sensitive or substantive communications, and perhaps for any attorney client communications…."

ABA Formal Opinion 11-460 (August 4, 2011)

This opinion disagrees with the *Stengart v. Loving Care* Court's decision that Defendants' attorneys' use of plaintiff's emails with her attorney constituted a violation of Rule 4.4(b). The opinion provides that if an employee communicates with his attorney on his work computer or other work-issued device, or via work email, neither Rule 4.4(b) nor any other Rule requires that the employer's lawyer notify opposing counsel of the receipt of the communication.

DISCOVERY ISSUES INVOLVING SOCIAL MEDIA

The following cases provide examples of how courts are addressing discovery in the context of social media. While the focus of the research was intended to be on cases involving

restrictive covenants, cases involving other contexts are discussed as well in order to give a more complete view of the developing law in this area.

SPOLIATION AND THE DUTY TO MAINTAIN

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

The court noted that Facebook took down some information posted by the defendant to satisfy the plaintiff's take-down request and therefore held it would be unjust to hold the defendant responsible for the failure to preserve the information. In discussing spoliation of evidence, the court further held that a defendant's changing his profile picture on Facebook was not spoliation of evidence to a degree requiring an adverse inference, notwithstanding that the profile picture in dispute displayed defendant's business colors (which was the primary issue in this trade dress infringement case), and that when an individual changes his profile picture, the picture attached to all previous messages and posts from this user changes to the new profile picture. The court found the spoliation unintentional, holding that it would not have been immediately clear to the defendant that changing his profile picture would undermine discoverable evidence. The court also recognized other cases in which public websites were found to be within the control of the parties who own them even though they are publicly available and therefore were, at times, within the discovering party's access. E.g., *Arteria Property Pty. Ltd. v. Universal Funding V.T.O., Inc.*, 2008 WL 4513696 (D.N.J. 2008) at *5. The court rejected the defendant's argument that the data was directly available to the plaintiff via the Internet, referring to the defendants' argument as "an attempt to 'pass the buck' to Plaintiff to print websites that Defendants are obligated to produce." The court ordered the defendant to coordinate with plaintiff's counsel to change the picture back to the infringing picture so that the plaintiff could print whatever posts it felt were relevant. Id at *4.

***Arteria Property Pty. Ltd. v. Universal Funding V.T.O., Inc.**, 2008 WL 4513696 (D.N.J. 2008)*

The court found that spoliation of evidence occurred where the defendants had reason to believe that they would be hauled into court, and failed to insure that electronic files in the form of the parties' website were not maintained. The court noted that the defendants controlled the content posted on their website and therefore had the power to delete the content, and that even though the website may have been maintained by a third party, the defendants still had the ultimate authority and thus control to add, delete or modify the website's content. The court therefore provided that an adverse inference instruction should be provided to the jury. It is worth noting that the court made the comment about the ultimate control over the content of the website in comparison to the irrelevance of the owner of the server on which the website resides.

Sanofi-aventis Deutschland GmbH v. Glenmark Pharmaceuticals, 2010 WL 2652412 (D.N.J. Jul. 01, 2010)

The court found that no viable basis for a spoliation claim existed where a party did not produce a responsive e-mail in addition to an e-mail that invited a response. The court reasoned that the lack of a response, supported by testimony from the recipient that he did not respond even though the first e-mail invited one, was enough to invalidate the assertion of spoliation.

PRIVACY AND RELEVANCY

Held v. Ferrellgas, Inc., No. 10-2393-EFM 2011 WL 3896513 (D. Kan. Aug. 31, 2011).

Court held in Title VII retaliation case that plaintiff's Facebook page information was relevant, where plaintiff "could not recall at his deposition whether he posted anything on Facebook" during his employment for defendant. The court, in compelling production of Facebook profile information, noted that the defendant was attempting to mitigate plaintiff's

privacy concerns, and was only seeking limited access by allowing the plaintiff himself to download and produce the information rather than requesting he provide all of his login information.

Muniz v. United Parcel Service, Inc., No. C-09-01987-CW 2011 WL 311374 (N.D.Cal.2011).

Defendant's efforts to subpoena plaintiff's attorney's Facebook postings in an effort to establish and/or refute the time spent by attorney in incurring fees was denied by the court. The court held that defendant's request for the attorney's electronic postings on listservs and social media networks that describe the 'work' or 'efforts' of the attorney were vague, overbroad, and called for production of irrelevant information.

Offenback v. L.M. Bowman, Inc., 2011 WL 2491371 (M.D. Pa. June 22, 2011)

Court conducted "in camera review of Plaintiff's Facebook and MySpace accounts in order to determine whether certain information contained within Plaintiff's accounts [was] properly subject to discovery in [the] case." The court ultimately ordered a number of photographs and postings to be produced in this personal injury action to show his physical activity, etc.

E.E.O.C. v. Simply Storage Mgmt., LLC, 270 F.R.D. 430 (S.D. Ind. 2010)

Employee was required to produce portions of social networking sites ("SNS") that were relevant to claim, despite potential expectations of privacy from having "locked" the profile from public access. The court stated "[d]iscovery of SNS requires the application of basic discovery principles in a novel context. . . the main challenge in this case is not one unique to electronically stored information generally or to social networking sites in particular. Rather, the challenge is to define appropriately broad limits-but limits nevertheless-on the discoverability of social communications . . . in a way that provides meaningful direction to the parties."

Bass ex rel. Bass v. Miss Porter's School, 2009 WL 3724968 (D. Conn. Oct. 27, 2009)

Court ordered plaintiff (1) to produce the Facebook documents that it deemed responsive to defendant, and (2) submit all of the Facebook documents to the court so that it could conduct an in camera review. After reviewing the documents and finding no meaningful distinction between the documents plaintiff deemed responsive and those she wished to withhold, the court ordered the plaintiff to produce all of the Facebook documents: "relevance of the content of Plaintiff's Facebook usage as to both liability and damages in this case is more in the eye of the beholder than subject to strict legal demarcations, and production should not be limited to Plaintiff's own determination of what may be 'reasonably calculated to lead to the discovery of admissible evidence.'"

Mackelprang v. Fidelity Nat. Title Agency of Nevada, Inc., 2007 WL 119149 (D. Nev. Jan. 9, 2007)

Court denied defendant's motion to compel plaintiff in a sexual harassment case to sign a consent and authorization form directing Myspace.com to produce private messages because defendant was "engaging in a fishing expedition." MySpace complied with the subpoena merely by providing a spreadsheet which confirmed the plaintiff was a user of two accounts at issue in the case. The defendant was allowed to discover private messages exchanged with third parties that contained information regarding her sexual harassment allegations or her alleged emotional distress, but not those messages that were irrelevant to her employment with the defendants.

McCann v. Harleysville Ins. Co. of N.Y., 78 A.D.3d 1524 (N.Y. App. Div. 2010)

In a personal injury action, the Court rejected defendant's request to access plaintiff's Facebook page in a personal injury case as an overly broad "'fishing expedition' into plaintiff's

Facebook account based on the mere hope of finding relevant evidence." The defendant failed to establish a factual predicate with respect to the relevancy of the evidence.

Romano v. Steelcase, 907 N.Y.S. 2d 650 (N.Y. S. 2010)

Court granted defendant "access to Plaintiff's current and historical Facebook and MySpace pages and accounts, including all deleted pages and related information" because "it is reasonable to infer from the limited postings on Plaintiff's public Facebook and MySpace profile pages [which differed from her deposition testimony and claims], that her private pages may contain materials and information that are relevant to her claims or that may lead to the disclosure of admissible evidence." The court also stated that the plaintiff has no reasonable expectation of privacy "notwithstanding her privacy settings" because Facebook and MySpace did not guarantee "complete privacy."

Zimmerman v. Weis Markets, Inc., 2011 WL 2065410 (Pa. Com. Pl. May 19, 2011)

Court granted motion to compel plaintiff in personal injury case to provide "all passwords, user names and login names for any and all MySpace and Facebook accounts." The court found the prospect of an in camera review to be an unfair burden on the court. The court relied on the liberal rules of discovery, the pursuit of truth, and a finding that the plaintiff had consented to the fact that her personal information would be shared with others, notwithstanding her privacy settings.

McMillen v. Hummingbird Speedway, Inc., 2010 WL 4403285 (Pa. Com. Pl. Sept. 9, 2010)

Court rejected personal injury plaintiff's arguments that Facebook and Myspace login information was confidential or privileged and ordering plaintiff to provide user names and passwords. Defendants argued that even the publicly available portions of the plaintiff's Facebook page showed that the plaintiff had exaggerated his claims, thereby providing a hook for the relevance of other materials.

Habib v. 116 Central Park South Condominium, Index No. 108434/2009 (NY S.Ct. 3/1/11)

In another recent New York case, the defendant condominium in a slip and fall case sought an order compelling the eighty-year-old plaintiff "to provide authorizations for Facebook, MySpace and/or Twitter" accounts that he maintained, in an apparent speculative belief that the plaintiff commented about his claim or injury on the networks. The court, however, refused to compel discovery into this tech-savvy octogenarian's social media usage, finding the defendant did "not offer a reasonable explanation as to why they believe that material information would appear on plaintiff's social network pages [and that without] the explanation, the requested authorization is a fishing expedition."

Patterson v. Turner Constr. Co., 2011 WL 5083155 (N.Y.A.D. Oct. 27, 2011)

In this personal injury action, the court found that "it is possible that not all Facebook communications are related to the events that gave rise to plaintiff's cause of action," and thus remanded for the court to take a closer look, in camera, at the plaintiff's Facebook information to determine what was relevant. Important to note was the court also held the plaintiff's postings on Facebook were "not shielded from discovery merely because plaintiff used the service's privacy settings to restrict access." This statement followed the N.Y. precedent established in Romano and other cases.

Abrams v. Pecile, 922 N.Y.S.2d 16 (N.Y.App. 2011)

The court reemphasized the standard of discovery requests, and that a party must show the method of discovery sought "is reasonably calculated to lead to the discovery of information bearing on the claims."

Caraballo v. City of New York, No. 103477/08 2011 WL 972547 (N.Y.Sup. March 4, 2011)

In this case, a defendant's motion to compel plaintiff to provide "authorization to access [the party's] 'current and historical [social networking] pages and accounts, including all deleted pages and related information'" was denied as overbroad. The court noted that the plaintiff did not testify in deposition as to the type of information posted or available on his social networking cites, and like the court in McCann, ultimately held the defendant "failed to establish a factual predicate with respect to the relevancy of the information the sites may contain."

Progressive Ins. Co. v. Herschberg, No. 000014/10 2011 WL 1991960 (N.Y.Sup. March 30, 2011)

The petitioner (insurance company) in this personal injury case sought an order to compel the respondent to provide "unlimited access to his Facebook account" after discovering public information on the account which the petitioner alleged showed the respondent was lying about the extent of his injuries. The court held such an order was overbroad and unwarranted at the time, due to the fact that there was no showing that the materials sought were not cumulative. The court did hold, however, that such evidence warranted a framed issue hearing.

THIRD PARTY DISCOVERY

Ledbetter v. Wal-Mart Stores, Inc., 2009 WL 1067018 (D. Colo. Apr. 12, 2009)

Court denied plaintiff's motion for a protective order regarding subpoenas issued to social networking sites where "the information sought within the four corners of the subpoenas issued to Facebook, My Space, Inc., and Meetup.Com is reasonably calculated to lead to the discovery of admissible evidence and is relevant to the issues in this case." The plaintiff objected on the grounds of spousal and physician-patient privileges but the court deemed them waived because of the filing of a lawsuit alleging mental and physical injuries.

DFSB Kollective Co. Ltd. v. Jenpoo, No. 11-1050 SC 2011 WL 2314161 (N.D. Cal. June 10, 2011)

Court found that plaintiff met burden in copyright infringement case for early limited discovery (pre FRCP 26f meet and confer), and allowed subpoena of many third party service providers, including Facebook, Twitter, Google, and YouTube, in order to establish the identity of certain unknown defendants which allegedly assisted defendant in infringement of plaintiff's copyrighted materials.

The court granted some of the third-party discovery following the elements laid out in *Gillespie v. Cibiletti*, 629 F.2d 637, 642 (9th Cir. 1980). The criteria for conducting discovery to identify a Doe defendant requires the moving party to: 1) identify the defendant with enough specificity to allow the court to determine whether the defendant is a real person or entity who could be sued in federal court; 2) recount the steps taken to locate the defendant; 3) show that its action could survive a motion to dismiss; and 4) file a request for discovery with the court identifying the persons or entities to which discovery process might be served and for which there is a reasonable likelihood that the discovery process will lead to identifying information. *Columbia Ins. Co. v. seescandy.com*, 185 F.R.D. 573, 578-80 (N.D. Cal. 1999). The court noted that the plaintiffs identified the defendants with specificity by providing specific email addresses, user IDs, and account numbers. Additionally, they hired investigators and presented to the court the results of those investigations. The plaintiffs also established that their complaint was likely to survive a motion to dismiss and with few exceptions, demonstrated a reasonable likelihood that discovery served on the third party's ISPs would yield identifying information. As the plaintiffs failed to explain how they came to suspect the holders of certain email addresses were related to a party, the court limited the scope of subpoenas pertaining to those email addresses.

Mancuso v. Florida Metropolitan University, Inc., No. 09-61984-CIV 2011 WL 310726 (S.D. Fla. Jan. 28, 2011).

Court denied plaintiff's motion to quash subpoenas of defendant seeking information on plaintiff's Facebook and MySpace activity. Defendant sought such information for determination of how much back pay plaintiff was entitled to in FLSA case, alleging that the time spent on such social networks during business hours should cause a reduction in back pay given. The court did not quash the subpoena's because the plaintiff's challenge to them was not filed in the court issuing the subpoena, and therefore the court did not have jurisdiction to rule on such subpoenas.

First, the court noted that a party generally does not have standing to challenge a subpoena served on a non-party, unless that party has a personal right or privilege with respect to the subject matter of the materials subpoenaed. The court went on to note that parties are often deemed to have a personal interest in their financial and telephone records sufficient to confer standing to challenge a subpoena directed to a third party. The court specifically cited a case in which an individual had standing to challenge a subpoena issued to social networking websites. *Crispin v. Christian Audiger*, Inc., 717 F. Supp. 2d 965 (C.D. Cal. 2010). The court also agreed that the substance of the text messages or telephone calls which were the subject of aspects of the subpoena were not relevant to the overtime claims or defenses and, therefore, modified the scope of the subpoena accordingly.

***Bower v. Bower**, No. 10-10405-NG 2011 WL 3702086 (D. Mass April 5, 2011)*

Court held that Stored Communications Act precluded service providers (Yahoo! and Google) from producing requested e-mails of defendant. While the service providers could produce requested e-mails if consent was present, the court reasoned that because defendant fled the country and chose not to show up at court, her consent could not be implied as there was no affirmative participation in the judicial process.

The court distinguished other cases in which courts found an implied agreement to consent in light of the affirmative participation in the judicial process, e.g., *Thayer v. Chizewski*, No. 07-CV-1290, 2009 WL 2957317 at *7 (N.D. Ill. September 11, 2009) (where plaintiff had given consent to AOL to divulge at least one email, and "has not indicated that he would object to the disclosure of all relevant emails that it is later determined exist, the court presumes that Mr. Thayer – as the plaintiff who initiated this litigation and put at issue his mental state, impression, and the reasonableness [of the defendant's actions] – has given his consent to AOL to divulge all responsive emails"); *see also Romano v. Steelcase*, 907 N.Y.S. 2d 650 (N.Y. Sup. 2010) (plaintiff in personal injury case ordered, without discussion of implied consent, to provide executed consent and authorization required by operators of Facebook and MySpace).

Chasten v. Franklin, 2010 WL 4065606 (N.D.Cal. Oct. 14, 2010)

In effort to obtain e-mails sent by a corrections facility officer in connection with an inmate's murder, plaintiff served a subpoena on Yahoo!. The corrections officer moved to quash the subpoena, alleging that production of the e-mails violated the Stored Communications Act. The court sided with the corrections officer and quashed the subpoena, noting that the SCA prohibits providers such as Yahoo! from knowingly divulging its customers' electronic communications, and that civil subpoenas to non-parties are not one of the enumerated exceptions designated by the SCA which would allow production. The court reasoned that "compliance with the subpoena would be 'an invasion … of the specific interests that the [SCA] seeks to protect."

Crispin v. Christian Audiger, Inc., 717 F. Supp. 2d 965 (C.D. Cal. 2010)

The court quashed subpoenas to MySpace and Facebook, finding that some of the contents on those sites is protected by the Stored Communications Act, noting that the user had selected certain privacy settings intending to limit access.

Rene v. G.F. Fishers, Inc., No. 1:11-cv-514-WTL-DKL, 2011 WL 4349473 (S.D. Ind. Sept. 16, 2011)

The Stored Communications Act, in addition to preventing social network service providers (i.e. Facebook) from knowingly producing the electronic communications of its customers, also prohibits "intentionally accessing without authorization a facility through which an electronic communication service is provided" and thereby obtaining access to an "electronic communication while it is in electronic storage." In this context, an employee sued her employer for violation of the SCA in obtaining her login information to her private e-mail and banking accounts through "keylogging" her work computer.[15] While the court noted there is a split of authority on whether opened e-mails or messages are "in electronic storage" and deserving of protection under the act, the court held that unopened messages were in "temporary, intermediate storage," and were protected. Additionally, the court held that the employee did not have to state whether the e-mails accessed by her employer were opened to make a sufficient pleading.

MISCELLANEOUS

Facebook's "Download Your Information" feature allows users to download everything the user ever posted on Facebook and all correspondences with friends: messages, Wall posts, photos, status updates and profile information." See Mark Zuckerburg, Giving You More

[15] Keylogger software allows information typed into a computer to be logged and sent to another computer or e-mail address.

Control, The Facebook Blog, (Oct. 6,2010, 2:13 PM),http://www.facebook.com/blog.php?post=434691727130

ETHICAL CONSIDERATIONS

NEW YORK STATE BAR ASSOCIATION

Committee on Professional Ethics

Opinion 843 (9/10/10)

Topic: Lawyer's access to public pages of another party's social networking site for the purpose of gathering information for client in pending litigation.

Digest: lawyer representing a client in pending litigation may access the public pages of another party's social networking website (such as Facebook or MySpace) for the purpose of obtaining possible impeachment material for use in the litigation.

Rules: 4.1; 4.2; 4.3; 5.3(b)(1); 8.4(c)

Found at

http://www.nysba.org/Content/ContentFolders/EthicsOpinions/Opinions825present/EO_843.pdf

UNITED STATES V. ADOBE SYSTEMS, INC.:

LIMITATIONS ON NON-SOLICITATION AGREEMENTS

Recently, the Department of Justice ("DOJ") announced a crack down on high tech companies' agreements not to solicit each other's employees, calling into question the enforceability of such provisions in other fields. In the case of *United States v. Adobe Systems,*

Inc., U.S. District Court, District of Columbia, 1:10-cv-01629 (2010), the DOJ established its intent to pursue those employers who agree not to solicit skilled employees of competitors.

A. "No Cold Calling" Agreements

High tech employers, long time competitors with each other over the limited labor pool of highly skilled technical employees, commonly utilize solicitation "cold calling:" initiating contact with another company's employee without the employee having first indicated an interest in being contacted. Although designated as "cold *calling*" because of its telephonic origins, recent social media developments have greatly expanded the means by which cold calling can occur, including solicitation via social media sites such as Facebook, Twitter, and Linkedin. As DOJ explains it:

> High tech labor is characterized by expertise and specialization. Defendants compete for high tech employees, and in particular specialized computer science and engineering talent on the basis of salaries, benefits, and career opportunities. In recent years, talented computer engineers and computer scientists have been in high demand.
>
> . . . Although [high tech companies] employ a variety of recruiting techniques, cold calling another firm's employees is a particularly effective method of competing for computer engineers and computer scientists. Cold calling involves communicating directly in any manner (including orally, in writing, telephonically, or electronically) with another firm's employee who has not otherwise applied for a job opening. Defendants frequently recruit employees by cold calling because other firms' employees have the specialized skills necessary for the vacant position and may be unresponsive to other methods of recruiting. For example, several [high tech companies] at times have received an extraordinary number of job applications per year. Yet these companies still cold called engineers and scientists at other high tech companies to fill certain positions.

U.S. v. Adobe Sys., Inc., Complaint, ¶¶ 12-13.[16]

[16] The complaint can be viewed at the DOJ's website: http://www.justice.gov/atr/cases/f262600/262654.htm (last visited Oct. 21, 2011).

Aware of the increasing ease with which valued high tech employees could be poached, certain companies entered into non-solicitation agreements focused specifically on the practice of cold calling. Between 2005 and 2007, six major technology companies entered into five substantively similar non-solicitation agreements, agreeing to refrain from cold calling each other's employees through direct and explicit communications. The parties to these non-solicitation agreements were: (1) Apple Inc. ("Apple") and Google Inc. ("Google"); (2) Apple and Adobe Systems, Inc. ("Adobe"); (3) Apple and Pixar; (4) Google and Intel Corp. ("Intel"); and (5) Google and Intuit, Inc. ("Intuit"). Pursuant to these agreements, the companies maintained "Do Not Cold Call" lists and actively enforced the prohibition against initiating unsolicited contacts with employees from the other companies. *See id.* at ¶¶ 15-32.

B. The *Adobe* Consent Decree

These "no cold call" agreements came to an abrupt end after the DOJ filed an antitrust action against Apple, Google, Adobe, Pixar, Intel and Intuit on September 24, 2010, alleging that the non-solicitation agreements stood as*per se* unlawful under Section 1 of the Sherman Antitrust Act ("Sherman Act"). Section 1 of the Sherman Act provides that "[e]very contract . . . or conspiracy, in restraint of trade or commerce among the several States . . . is declared to be illegal." 15 U.S.C. § 1. A violation of the Act stems from: "(1) the existence of a contract, combination, or conspiracy among two or more separate entities that (2) unreasonably restrains trade and (3) affects interstate or foreign commerce." *Jack Russell Terrier Network of N. Cal. V. Am. Kennel Club, Inc.*, 407 F.3d 1027, 1033 (9th Cir. 2005*).* *Per se* violations of the Act involve "certain agreements or practices which because of their pernicious effect on competition and lack of any redeeming virtue are conclusively presumed to be unreasonable and therefore illegal without elaborate inquiry as to the precise harm they have caused or the business excuse

for their use." *Nat'l Collegiate Athletic Ass'n v. Bd. of Regents of Univ. of Okla.*, 468 U.S. 85, 104 n. 27 (1984).

The DOJ's complaint against Apple, Google, Adobe, Pixar, Intel, and Intuit alleged just such a *per se* violation of the Act, claiming:

> Defendants compete for highly skilled technical employees . . . and solicit employees at other high tech companies to fill employment openings. Defendants' concerted behavior both reduced their ability to compete for employees and disrupted the normal price-setting mechanisms that apply in the labor setting. These no cold call agreements are facially anticompetitive because they eliminated a significant form of competition to attract high tech employees, and, overall, substantially diminished competition to the detriment of the affected employees who were likely deprived of competitively important information and access to better job opportunities.

U.S. v. Adobe Sys., Inc., Complaint, ¶ 2. In its competitive impact statement, filed in connection with the DOJ's proposed final judgment in the lawsuit, the DOJ further asserted:

> Antitrust analysis of downstream, customer-related restraints is equally applicable to upstream monopsony[17] restraints on employment opportunities. . . .
>
> There is no basis for distinguishing allocation agreements based on whether they involve input or output markets. Anticompetitive agreements in both input and output markets create allocative inefficiencies. Hence, naked restraints on cold calling customers, suppliers, or employees are similarly per se unlawful.

U.S. v. Adobe Sys., Inc., Competitive Impact Statement, § III.[18]

Corporations found to be in violation of Section 1 of the Sherman Act risk a staggering fine of up to 100 million dollars. 15 U.S.C. § 1. Perhaps unsurprisingly, the six companies

[17] A "monopsony" is "[a] market situation in which one buyer controls the market. . . . Monopsony is often thought of as the flip side of monopoly. A monopolist is a seller with no rivals; a monopsonist is a buyer with no rivals. . . . Monopsony injures efficient allocation by reducing the quantity of the input product or service below the efficient level." Black's Law Dictionary 1028 (8th ed. 2004).

[18] The competitive impact statement can be viewed at the DOJ's website: http://www.justice.gov/atr/cases/f262600/262650.htm (last visited Oct. 21, 2011).

named in the *Adobe* case chose to enter into a consent decree with the DOJ to avoid litigation of this issue.

The court approved the parties' proposed final judgment on March 18, 2011. Although the defendant corporations pointed out that their consent to the final judgment included no admission that their non-solicitation agreements violated the Sherman Act, they agreed to subject themselves to the following injunction:

> Each Defendant is enjoined from attempting to enter into, entering into, maintaining or enforcing any agreement with any other person to in any way refrain from, requesting that any person in any way refrain from, or pressuring any person in any way to refrain from soliciting, cold calling, recruiting, or otherwise competing for employees of the other person.

U.S. v. Adobe Sys., Inc., 2011 U.S. Dist. LEXIS 83756, *4-5 (D. D.C. March 18, 2011). Significantly, the defendant corporations stand enjoined from agreeing to refrain from practices much broader in scope than mere cold calling; the injunction encompasses all forms of solicitation and recruitment.

C. The Implications of *Adobe*

The *Adobe* consent decree presents no isolated case. In its September 24, 2010 press release addressing its commencement of the *Adobe* litigation, the DOJ emphasized: "Today's complaint arose out of a larger investigation by the Antitrust Division into employment practices by high tech firms. The division continues to investigate other similar no solicitation agreements."[19] Indeed, the DOJ filed a complaint in December 2010 against Pixar and Lucasfilm Ltd. ("Lucasfilm"), stemming from a similar non-solicitation agreement between the two corporations, competitors for the employment of highly skilled digital animators. In June

[19] This press release can be viewed at: http://www.justice.gov/atr/public/press_releases/2010/262648.htm (last visited Oct. 21, 2011).

2011, Pixar and Lucasfilm entered into a consent decree with the DOJ that mirrored the final judgment in the *Adobe* case.[20]Expect future cases in a similar vein.

In bringing these lawsuits, the DOJ argues that the impacted market consists of highly-skilled employees, rather than the typical market for products or services. The highly-skilled nature of the subject employees' work appears to have been significant to the DOJ in its claim that the non-solicitation agreements in *Adobe* and *Lucasfilm* restrained free trade. But the implications of *Adobe* likely extend beyond the high tech industry. Any market where employers directly compete for skilled laborers in an industry involving interstate commerce could be subject to the type of claims raised by the DOJ. For example, employers competing for highly-trained professionals in research and development or banking and finance should proceed with caution if considering a non-solicitation agreement with a direct competitor in the same market.

Neither, however, does *Adobe* represent the death toll of all non-solicitation agreements in such industries. The final judgment between the DOJ and the six defendant corporations clarified that certain non-solicitation agreements remain lawful under the Sherman Act. Specifically, non-solicitation agreements may withstand scrutiny and comply with the Consent Decree if:

1. contained within existing and future employment or severance agreements with the Defendant's employees;

2. reasonably necessary for mergers or acquisitions, consummated or unconsummated, investments, or divestures, including due diligence related thereto;

[20] The complaint and final judgment can be viewed at the DOJ's website: http://www.justice.gov/atr/cases/lucasfilm.html (last visited Oct. 21, 2011). *See also U.S. v. Lucasfilm Ltd.*, 2011 U.S. Dist. LEXIS 70171 (D. D.C. June 3, 2011).

> 3. reasonably necessary for contracts with consultants or recipients of consulting services, auditors, outsourcing vendors, recruiting agencies or providers of temporary employees or contract workers;
>
> 4. reasonably necessary for the settlement or compromise of legal disputes; or
>
> 5. reasonably necessary for (i) contracts with resellers or OEMs; (ii) contracts with providers or recipients of services other than those enumerated in paragraphs . . . 1-4 above; or (iii) the function of a legitimate collaboration agreement, such as joint development, technology integration, joint ventures, joint projects (including teaming agreements), and the shared use of facilities.

U.S. v. Adobe Sys., Inc., 2011 U.S. Dist. LEXIS 83756, *5-6. As the DOJ explained in its competitive impact statement: "[A]n agreement that would normally be condemned as a per se unlawful restraint on competition may nonetheless be lawful *if it is ancillary to a legitimate precompetitive venture and reasonably necessary to achieve the precompetitive benefits of the collaboration*." *U.S. v. Adobe Sys., Inc.*, Competitive Impact Statement, § III (emphasis added).

Key to the DOJ's assertion that the "no cold calling" agreements in *Adobe* violated the Sherman Act: the fact that the agreements were not ancillary to any legitimate collaborative projects between the parties. *See id.*

> Defendants' agreements were not tied to any specific collaboration, nor were they narrowly tailored to the scope of any specific collaboration. The agreements extended to all employees of the firms, including those who had little or nothing to do with the collaboration at issue. The agreements were not limited by geography, job function, product group, or time period. This overbreadth and other evidence demonstrated that the no cold calling agreements were not reasonably necessary for any collaboration and, hence, not ancillary.

Id.; see alsoU.S. v. Adobe Sys., Inc., Complaint, ¶ 16.

The DOJ also emphasized the fact that "employees were not informed of and did not agree to" the no cold calling agreements. *U.S. v. Adobe Sys., Inc.*, Complaint, ¶¶ 18, 22, 25, 28, 31. Notably, non-solicitation provisions ancillary to a legitimate employment or severance

agreement with an employee stand explicitly exempted from the *Adobe* injunction. *U.S. v. Adobe Sys., Inc.*, 2011 U.S. Dist. LEXIS 83756, *5. Presumably, directly contracting with the employee, rather than with another corporation competing for that employee's services, does not have the same impact of "diminish[ing] competition to the detriment of the affected employees" or "depriv[ing them] of competitively important information and access to better job opportunities" without their knowledge or consent. *U.S. v. Adobe Sys., Inc.*, Complaint, ¶ 14.

D. Conclusion

Easy access to a competitor's employees remains an increasing concern in the age of social media, and employers competing for highly-skilled employees may be tempted to pursue non-solicitation agreements with their direct competitors. However, *United States v. Adobe Systems, Inc.* demonstrates the need for caution in undertaking any such endeavor. Employers should beware the potential pitfalls associated with entering into a non-solicitation agreement with a competitor not ancillary to another legitimate collaboration – including the unwelcome possibility of a 100 million dollar penalty under the Sherman Act. 15 U.S.C. § 1. Consequently, the easy solicitation provided by social media must not tempt employers to illegal pre-emptive agreements with competitors.