

ABA Section of Litigation

ABA Annual Meeting

August 8-12, 2013 / San Francisco, CA



*ABA Section of Litigation, 2013 ABA Annual Meeting, August 8-12, 2013:
“Social Media Evidence—How to Find It and How to Use It”*

Social Media Evidence—How to Find It and How to Use It

Moderators:

Gary L. Beaver
Nexsen Pruet, LLC
Greensboro, NC

Mark A. Romance
Richman Greer
Miami, FL

Speakers:

Steven Brower
Buchalter Nemer
Irvine, CA

Amy Longo
O’Melveny & Myers LLP
Los Angeles, CA

Cecil A. Lynn III
Littler Mendelson P.C.
Phoenix, AZ

SOCIAL MEDIA EVIDENCE – How To Find It And How To Use It

by Gary L. Beaver, Steven Brower, Amy Longo, Cecil Lynn, and Mark Romance

I. The Importance and Forms of Social Media

The growth of social media use has been exponential. Over 70% of the people in the U.S. are using social media of one form or another (over 50% on Facebook alone). You have probably never even heard of one of the most widely used social media websites –Qzone – it is a Chinese social media similar to Facebook with over 500 million monthly users.

There are many forms of social media. Litigation attorneys must do their best to keep up with what the public is doing on social media in order to know where to look for evidence. The numbers below are estimated number of users though some or even many may not be active users. The numbers were obtained from various websites and we cannot vouch for their accuracy. They are provided to provide a sense of the important role of social media today.

Personal interaction/ friendship: Facebook (about 1 billion monthly users); Twitter (500 million); Qzone (500 million); Google-plus (340 million); Tagged (330 million); WeChat (300 million); Badoo (170 million); Netlog (90 million); MyLife (60 million); Tango (mobile video chat – 80 million); Sonico (focused on Latin American users; 55 million); Stumbleupon (30 million); Bebo (30 million); MySpace (25 million unique monthly users).

Business: LinkedIn (200 million users); Branchout (30 million).

Dating sites: match; zoosk; meetup; eharmony; spark; datehookup; okcupid; spark; gofishdating; mingle2; connectingsingles; howaboutwe; flirt; howaboutwe. Some are a bit more focused: christiandating; christianmingle; jdate (for Jewish faith); blackplanet (for African-Americans); ourtime (over 50 years old); professionalsinglesover40; and for those who are not satisfied with chasing Nigerian fortunes on the internet some Sugar Daddy dating sites – findrichguys.com and seekingmillionaire.com.

Photo and video-sharing and editing: Youtube (800 million); Instagram (90 million/ 4 billion photos); Dropbox (100 million); Flickr (75 million); Imgur (50 million); Pinterest (25 million; over 90% are women).

Videos/ audio: YouTube (800 million; 4 billion views per day); Soundcloud (180 million); Socialcam (50 million); Viddy (40 million).

Blogs: Sina Weibo (Chinese; 400 million); Tumblr (over 75 million multimedia blogs and 150 million users); personal blogs (for example, see on the internet the story of the young woman fired from a nonprofit for her graphic sex blog “The Beautiful Kind” created on her own time).

Coupons: Groupon (40 million); Living Social.

Entertainment: Shazam (share movies, TV shows, music; 250 million users and 5 billion tags); Steam (gaming; 50 million).

Shopping preferences: Paypal (117 million); Ebay (100 million); Pinterest (50 million and rising rapidly; only 3 years old; 80% or more of users are women); Foursquare (local businesses and restaurants – 25 million).

Communications: QQ (Chinese instant messaging; 700 million); Skype (280 million); Orsbo (200 million); Viber (140 million); Voxer (70 million); Kakao Talk (70 million); Kik Messenger (mobile instant messaging; 30 million).

News: Reddit (40 million; 37 billion).

Directions: Waze (34 million).

Travel: WAYN (20 million).

There are additional sources of valuable information such as comments on websites' bulletin boards, note storage (Evernote: 45 million users). You will have to use searches on internet search engines and traditional discovery methods to discover such information.

A review of many reported cases indicates that the likeliest sources of relevant information are Facebook, Twitter, and MySpace. While LinkedIn has become immensely popular, it is work-oriented and postings are less likely to reveal the bad acts and true character of the posters.

Facebook. Your public postings on Facebook go to anyone in the world unless you have placed access restrictions on your Facebook page. Note also that Facebook updates access controls and often defaults new features to “public view” which necessitates frequent checking of preferred settings and options to maintain desired levels of privacy.

Twitter. Twitter posts differ from Facebook posts. Twitter users post “tweets” of up to 140 characters, can monitor, follow, and repost others' tweets, and can permit or forbid access to their own tweets. Twitter is more like a private electronic bulletin board which is only seen by persons who sign up to be on the board. If you follow someone on Twitter, Twitter will send them an email notifying them that you are following them using your Twitter account name. Despite this difference, tweets on Twitter are usually discoverable.

MySpace. After dominating from about 2005 to 2008, MySpace appears to have lost the battle for No.1 to Facebook in the personal message arena. However, it has had more success in discovering and promoting new music artists. MySpace is in the process of reinventing itself by focusing on interaction about entertainment, including music, movies, celebrities, and TV.

II. Privacy Protection

A. Federal Statutory Privacy Protection. A number of federal statutory schemes govern the possession and use of individuals' private data. Included:

1. The Federal Trade Commission Act (FTC Act), 15 U.S. C. § 25, generally prohibits unfair and deceptive acts and practices affecting commerce. The FTC has brought a number of cases under the FTC Act in instances where companies have failed to comply with

their own privacy policies. These types of actions have generally arisen in two circumstances: (1) where the company promised a specific level of data security to its customers, only to have its data compromised because it did not in fact deliver the promised level of security, and; (2) where the company promised not to sell or otherwise disclose customer information to third parties, only to do so when a sale of the information turned out to be financially attractive to the company;

2. The Financial Services Modernization Act, also known as the Gramm-Leach Bliley Act (GLBA), 15U.S.C. §§ 6801-6809, requires financial institutions to issue privacy notices to their customers giving them the opportunity to opt-out of sharing personally identifiable financial information with outside companies;

3. The Health Insurance Portability and Accountability Act of 1996 (HIPAA), includes provisions designed to encourage electronic transactions and also creates an opt-in framework for the use and disclosure of protected health information. There are hefty criminal and civil penalties available to punish violators;

4. The Children's Online Privacy Protection Act (COPPA), 15 U.S.C. §§ 6501-08 and 16 C.F.R. Part 312, applies to online business collecting information from children under the age of 13;

5. The Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. § 1232g and 34 C.F.R. § 99, and the Protection of Pupil Rights Amendment (PPRA), 20 U.S.C. § 1232h and 34 C.F.R. § 98, govern student records. Institutions that receive federal funds must comply with FERPA or lose their federal funding. Specifically, the statute and its regulations cover public and private institutions that "provide education services or instruction" and receive any kind of federal funding. *See* 34 C.F.R. § 99.3.

6. The Fair Credit Reporting Act (FCRA), 15 U.S.C. §§ 1681 *et seq.*, applies to data collected by consumer reporting agencies;

7. The primary statute affecting discovery of social media is the Stored Communications Act (SCA), 18 USC §§ 2707-2711, which is part of the Electronic Communications Privacy Act enacted in 1986. This is a pre-Internet statute. See Section D below for more about the SCA.

B. State data privacy laws. The 50 individual states have their own privacy laws and standards. Many states have laws governing privacy for social security numbers; some have laws governing website privacy policies. Some states, like California, have constitutional provisions as well as numerous privacy statutes (*see, e.g.*, California Constitution, Sec. 1, California Invasion of Privacy Act and Song-Beverly Credit Card Act). California also has a new Privacy Enforcement and Protection Unit. In addition, under California law, businesses are required to comply with the following state code provisions:

1. Disposal of Customer Records (Calif. Civil Code § 1798.79.8) - Requires businesses to shred, erase, or otherwise modify personal information when disposing of customer records under their control.

2. Security of Personal Information (Calif. Civil Code § 1798.81.5) - This law requires specified businesses to use safeguards to ensure the security of Californians' personal information (defined as name plus SSN, driver's license/state ID, financial account number) and to contractually require third parties to do the same. It does not apply to businesses that are subject to certain other information security laws.

If you seek social media information from an entity in another state, review that state's data privacy laws to ensure that you do not run afoul of them. Do not count on the target of your discovery request to know the applicable laws and assert the required protections.

C. International data privacy laws may be more restrictive than those in the United States though there are decisions in other countries, including the United Kingdom and France, that allow employers to discipline employees for making social media comments that are detrimental to the employer and its image. The Baker Hostetler law firm has an accessible International Compendium of Data Privacy Laws on its website. It is organized by country and runs about 200 pages long. If you have an issue regarding social media evidence posted by someone outside the United States, then you ought to examine the laws that apply in that country as well as the laws in the country in which you are trying to obtain the information.

In addition to the laws enacted by individual countries, there are international organizations' laws that might apply. For example, EU Directive 9546 was created to regulate movement of personal data across the borders of the EU countries and to establish security guidelines for storing, transmitting, and processing personal information. It has 33 articles in 8 chapters and took effect in October 1998. Other European Commission (EC) enactments also affect privacy such as the e-Privacy Directive applicable to the communications sector and Framework Decision 2008/977/JHA applicable to police and criminal matters. The EC is also expected to unify data protection in the EU with a single law called the General Data Protection Regulation. A proposal was published on January 25, 2012, and is planned for adoption in 2014, to take effect in 2016 (to allow for the transition).

D. Common Law Protections. In addition to the specific federal statutes described above, common law causes of action provide private remedies where sensitive information is improperly disclosed. Three common law privacy causes of action that can be brought in the wake of improper disclosure of private information include the torts of intrusion upon seclusion; public disclosure of private facts; and misappropriation of personality. Generally they entail the following:

1. intrusion upon seclusion is a tort where a given intentional intrusion (in circumstances where there is a reasonable expectation of privacy) would be highly offensive to a reasonable person, but does not include conduct that is simply offensive, insensitive or intrusive in the normal sense;

2. public disclosure of private facts is a tort which occurs when private personal information (such as health information, etc.) is "published" in a manner that would be highly offensive to a reasonable person. This tort results in liability for the owner of the database in which the information is stored and for the publisher. California recently expanded this tort in

Ignat v. Yum! Brands, Inc., 214 Cal.App.4th 808, 154 Cal.Rptr.3d 275 (2013) (did not involve social media evidence); and

3. misappropriation is a tort where someone else's name or personality is used for gain without consent.

In Roberts v. Careflite, 2012 WL 4662962 (Tex. Ct. App. 2012), Roberts, a paramedic, had commented on Facebook that she had wanted to slap a patient who needed restraining. The post was communicated to a company compliance officer who gave Roberts a calm warning. Rather than take heed, Roberts again let her anger show in another post and was soon thereafter fired. She challenged the firing by asserting two invasion of privacy torts – public disclosure of private facts and intrusion upon her seclusion. She lost on summary judgment.

In R.S. v. Minnewaska Area Sch. Dist. No. 2149, 894 F.Supp.2d 1128 (D.Minn. 2012), the court allowed a claim for invasion of privacy claim to go forward but dismissed a claim for intentional infliction of emotional distress.

In Lawlor v. North American Corp., 983 N.E.2d 414 (Ill. 2012), the Illinois Supreme Court affirmed a lower court holding that defendant was vicariously liable for “invasion upon seclusion” when its hired investigators obtained her phone records by pretending to be her, i.e., “pretexting.”

E. Social Media and the Stored Communications Act

Congress passed the SCA because “the Internet presented a host of potential privacy breaches that the Fourth Amendment does not address.” *See Quon v. Arch Wireless Operating Co., Inc.*, 529 F.3d 892, 900 (9th Cir. 2008). The SCA governs the circumstances under which electronic data service and storage providers may disclose customers’ data. It provides that whoever (1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or (2) intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system shall be punished as provided in subsection (b) of this section. 18 U.S.C. § 2701. The SCA precludes certain “providers” of communication services from divulging private communications to certain entities and individuals.

- The SCA defines an electronic communications service provider (“ECS”) as “any service that provides the user thereof the ability to send or receive wire or electronic communication.” 18 USC §2510[15].
- An ECS provider is only prohibited from divulging “the contents of a communication while in electronic storage by that service.”
- “Electronic storage” is defined as “any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof” or alternatively “any storage of such communication by an [ECS] for purposes of backup protection of such communication.”

- The SCA defines a remote computing service provider (“RCS”) as “the provision to the public of computer storage or processing services by means of an electronic communications system.”
- RCS providers are prohibited from “knowingly divulg[ing] to any person or entity the contents of any communication which is carried or maintained on that service.”

Standing under SCA to prevent production. Ordinarily a party has no standing to move to quash a subpoena issued to a nonparty unless the objecting party claims some personal right or privilege with regard to the information sought. Under the SCA, the party has a personal right with regard to stored emails and other electronically stored information. *See Crispin v. Christian Audigier*, 717 F.Supp.2d 965, 974 (C.D. Cal. 2010) (discovery sought from Facebook, MySpace, and others); *Chasten v. Franklin*, 2010 WL 4065606, at *1 (N.D. Cal. 2010) (Yahoo! email account); *J.T. Shannon Lumber Co. v. Gilco Lumber, Inc.*, 2008 WL 3833216, at *1 (N.D.Miss. Aug. 14, 2008) (emails).

In *People v. Harris*, 36 Misc.3d 613, 945 N.Y.S.2d 505 (2012), prosecutors sent subpoenas to Twitter for Harris’s tweets during a 3.5 month period. The court denied Harris’s motion to quash and ordered Twitter to produce for in camera inspection because Harris lacked standing to quash under the SCA. Twitter then moved to quash arguing that denying users standing put Twitter to the hard choice of producing or moving to quash to protect users’ rights. The court rejected Twitter’s arguments and held in a second opinion (36 Mis.3d 868, 949 N.Y.S.2d 590) that “[t]here can be no reasonable expectation of privacy in a tweet sent around the world.” The court also rejected Fourth Amendment and NY state law arguments and, on the basis of the SCA, modified the earlier order to produce by holding that under the SCA, ECS information under 180 days old may only be disclosed pursuant to a search warrant.

Application of the SCA by the courts. The majority of courts hold that internet service providers and social media websites are ECS providers bound by the SCA to not produce postings and emails of their subscribers/ registrants in response to a civil subpoena. Instead, the party seeking discovery must use Rule 34 requests to the opposing party to obtain the postings. To obtain social media postings a non-party witness one the best practice is to serve a subpoena on the non-party, not the social media ISP.

- In *Crispin v. Christian Audigier*, 717 F.Supp.2d at 97, the court quashed defendants’ subpoenas duces tecum on third-party businesses, including Media Temple, Facebook, and MySpace, because the social media sites were considered electronic communication services (ECS) under the SCA. The court held that the social media sites were ECS providers under the SCA with respect to wall posting and comments and that such communications were electronic storage and inherently private. In the alternative, the court held that Facebook and MySpace were remote computing services (RCS providers) under the SCA with respect to wall posting and comments. Therefore, Facebook and MySpace could not divulge the contents of any communication carried or maintained on that service (for RCS providers) nor divulge the contents of communication in electronic storage (for ECS providers). The court quashed subpoenas to Media Temple, Facebook, and

MySpace to the extent that they sought private messaging. With respect to the subpoenas seeking Facebook wall posts and MySpace comments, the court vacated the lower court's decision for an insufficient evidentiary record regarding privacy settings of the social media accounts at issue.

- Flagg v. City of Detroit, 252 F.R.D. 346 (E.D. Mich. 2008). Court held that SCA did not preclude discovery of city's relevant, non-privileged text messages stored by a non-party service provider. City had "control" over the text messages pursuant to contract between City and provider. Plaintiff had served 2 subpoenas on the service provider and City moved to quash. Court established a discovery protocol by which magistrate judges would make initial review of produced emails. Then City moved to block discovery under the SCA. Provider also moved to quash the subpoenas or for protection against SCA liability. Court held that plaintiff could get the information but must use Rule 34 request directed at the City to do so. Other courts agreed with the Flagg court. *See, e.g., Barnes v. CUS Nashville, LLC*, 2010 WL 2196591 (M.D. Tenn. 2010).
- Chasten v. Hubbard, 2010 WL 4065606 (N.D. Cal. Oct. 14, 2010) (civil subpoena to a non-party is not among the SCA's Section 2702(b)'s "unambiguous exceptions;" quashed subpoena to Yahoo! for emails).
- In Juror Number One v. Superior Court, 206 Cal.App. 4th 854, 142 Cal.Rptr.3d 151 (2012), the court noted that protection under the SCA applies only to attempts by the court or real parties in interest to compel the social media provider to disclose information, not to compel the person who posted the material to disclose.
- Mintz v. Mark Bartelstein & Assocs., 2012 WL 3553351 (C.D. Cal. Aug. 14, 2012) (subpoena to AT&T for cell and text message information quashed; court noted defendants could get information from plaintiff by Rule 34 request).

F. Constitutional Protections. You should prepare yourself for arguments for privacy protection under the First, Fourth, Fifth, and Ninth Amendments, which will be made to try to block your discovery efforts.

- Poor parenting rewarded. In R.S. v. Minnewaska Area Sch. Dist. No. 2149, 894 F.Supp.2d 1128 (D. Minn. 2012), the court upheld a student's First Amendment right to post rude comments about a school hall monitor on Facebook. The court also held that, under the Fourth Amendment, the student had a reasonable expectation of privacy to her private Facebook information and messages. Similarly, in Layshock v. Hermitage Sch. Dist., 650 F.3d 205, 207-08 (3d Cir. 2011) and J.S. ex re. Snyder v. Blue Mountain Sch. Dist., 650 F.3d 915, 920-21(3d Cir. 2011), the courts overturned punishments of students who had made nasty comments about school administrators through a "parody profile" on MySpace.
- Choose your "friends wisely." In U.S. v. Mereglido, 2012 WL 3264501

(S.D.N.Y. Aug. 10, 2012), there was no Fourth Amendment violation in gaining access to defendant's Facebook profile through one of his Facebook "friends."

- City of Ontario v. Quon, 130 S.Ct. 2619 (2010). A government employee's expectation of privacy in his text messages sent through a government-issued pager were insufficient to overcome a government search of the pager messages that revealed inappropriate messaging.
- In a criminal case, People v. Harris, 36 Misc.3d 613, 945 N.Y.S.2d 505 (2012), the court rejected a Fourth Amendment argument and allowed discovery of defendant's tweets. The same result occurred in a civil case, Romano v. Steelcase, Inc., 907 N.Y.S.2d 650 (2010).
- Internet subscribers' First Amendment right to speak anonymously is not enough to bar discovery of their subscriber identity information. See U.S. v. Hambrick, 2000 WL 1062039, at *4 (4th Cir. Aug. 3, 2000); Cinetel Films, Inc. v. Does 1-1,052 (853 F.Supp.2d 545, 555-56 (D. Md. 2012) (by sharing the identity information with the ISP, the subscriber loses his/her reasonable expectation of privacy).

G. Social Media Website Terms of Service.

Always check the Terms of Service for the social media website as they may have an impact on your approach to obtaining the information or even the target of your discovery demands. For example, Twitter's Terms of Service clearly state that a Twitter user provides Twitter a license to distribute to anyone at any time whatever the user tweets. In People v. Harris, a criminal prosecution of an Occupy Wall Street protestor, the prosecutor served a subpoena on Twitter. The court denied defendant's motion to quash (36 Misc.3d 613, 945 N.Y.S.2d 505 (2012)) because he lacked standing. Twitter then moved to quash; the court again denied (36 Misc.3d 868, 949 N.Y.S.2d 590 (2012)) and held that the defendant had no proprietary interest or expectation of privacy in his tweets and that by submitting tweets he had granted Twitter an unlimited license to use and distribute the tweets. Similar results have occurred in civil cases regarding the Terms of Service for other social media. See, e.g., Tompkins v. Detroit Metro. Airport, 2012 WL 179320, at *2 (E.D.Mich. Jan. 18, 2012); EEOC v. Simply Storage Mgmt., LLC, 270 F.R.D. 430, 434 (S.D. Ind. 2010); Beye v. Horizon Blue Cross Blue Shield of New Jersey, 2:06-cv-05337 (D. N.J. 2007); see also Patterson v. Turner Constr. Co., 931 N.Y.S.2d 311, 312 (N.Y.App.Div. 2011); Romano v. Educational & Institutional Coop Servs., Inc., 907 N.Y.S.2d 650 (N.Y.App.Div. Sept. 21, 2010).

IV. Ethical Considerations/ Restrictions

A. Generally, attorneys may access and review public portions of a party's or non-party's social networking sites without ethical implications. However, trying to get past privacy protections or misrepresenting any facts to access social media information will land you in hot water.

1. See NYSBA Opin. 843 (2010): A lawyer can view the public portions of

a non-client party's Facebook or MySpace pages in order to obtain material for use in litigation, provided the lawyer does not "friend" the party or direct a third party to do so. Because the lawyer is not interacting with the party in a deceptive manner, there is no violation of NY Rule of Professional Conduct 8.4(c), which prohibits attorneys from engaging in fraud, deceit or misrepresentation

B. To the extent a lawyer or his or her agent however makes contact with the owner of the profile, ethical issues can arise.

1. Jury Research.

a. Attorneys are expected to investigate potential jury members, including through online research. *See Johnson v. McCullough*, 306 S.W.3d 551, 558-59 (Mo. 2010) (affirming grant of new trial on grounds of juror nondisclosure during voir dire). *Accord* NYCLA Committee on Prof. Ethics Formal Opin. 743 (2011) (lawyers may conduct social media research in publicly available profiles on prospective and actual jurors, but may not friend, email, tweet or otherwise communicate with jurors, nor engage in deceptive conduct).

b. However, attorneys may not communicate with jurors through social media websites, and may not use agents to do so either. *See* New York City Bar Assoc. Formal Opin. 2012-02 (2012). Rule 3.5 of the NY Rules of Professional Conduct prohibit communications between lawyers and jurors or members of the venire. If a potential or sitting juror receives a friend request or otherwise learns of an attorney's viewing or attempted viewing of the juror's social media content, this would violate Rule 3.5.

c. Any type of deceptive conduct to communicate with a juror through social media would violate Rule 8.4.

2. Communications with a Represented Party. These are usually barred under Model Rule of Professional Conduct 4.2. That the communications are made through social media does not change the rule. Looking at a public website of a represented party is not considered a communication. It is touchier with Facebook

a. An attorney may not send a friend request to a high ranking employee of a corporate opposing party to obtain information for the litigation without running afoul of the rule prohibiting communications with represented parties about the subject of the representation, according to the San Diego County Bar Legal Ethics Committee. SDCBA Legal Ethics Opin. 2011-2.

- The Committee rejected the notion that the friend request itself did not concern the subject of the representation, finding that the motive was to obtain information about the litigation, in violation of Cal. Rules of Professional Conduct Rule 2-100.
- The Committee also found that sending this type of friend request would be deceptive conduct in violation of Cal. Bus. & Prof. Code Section 6068(d).

3. Communicating with a Witness

a. An attorney may not engage someone to friend a deponent for purposes of gathering information useful to the attorney's client, without violating the rule against deceptive conduct. *See* Philadelphia Bar Assoc. Prof. Guidance Comm. Opin. 2009-2 (2009). That Committee issued the opinion in response to an attorney who asked if he could have a third person friend an 18-year old adverse witness who was known to allow access to, i.e., "friend," anyone who asked.

b. Compare New York City Bar Assoc. Comm. on Prof. Ethics Formal Opin. 2010-2 which advises that an attorney may "truthfully" friend an unrepresented party, though may not engage in deceptive conduct directly or indirectly, to obtain social media information. In early June 2013, an Ohio prosecutor was fired for posing as an ex-girlfriend of a murder defendant to chat on Facebook with the defendant's female alibi witnesses in an effort to have them change their story.

4. Communications with judges. ABA Formal Opinion 462 provides that judges may participate in electronic social networking but in doing so "must comply with the relevant provisions of the Code of Judicial Conduct and avoid any conduct that would undermine the judge's independence, integrity, or impartiality, or create an appearance of impropriety." You may want to avoid "friending" any judges that you might appear before so as not to create a possible reason for recusal.

C. Self-publicity. ABA Model Rule 3.6 limits what a lawyer can say about his or her own cases. The rule says that you cannot say anything that "will have a substantial likelihood of materially prejudicing an adjudicative proceeding in the matter." There are other rules that may bar what you say about your case while it is pending. In May 2013, after a mediation session, a New York attorney posted a photo of himself smiling with his client with a caption stating "Pic After Making A \$43 Million Dollar Demand at Mediation." The defendant moved for sanctions alleging that the attorney violated Florida confidentiality provisions prohibiting revealing mediation communications (prohibitions that many states have). The judge did not impose sanctions but we are sure that the NY attorney experienced some distress until the court ruled. Take care in discussing your cases on social media. A former Illinois assistant public defender had her law license suspended for 60 days because her blog postings were detailed enough that authorities found that readers could ascertain the identities of the clients and thereby client confidences would be exposed.

V. Social Media In The Employment Context

A. Impact of the National Labor Relations Act.

Section 7 of the National Labor Relations Act prohibits retaliation against nonsupervisory employees for engaging in "concerted activities . . . for mutual aid or protection. . ." 29 U.S.C. §§ 151-169. "Concerted activity" is employees acting "together to try to improve their pay and working conditions or fix job-related problems." Complaining among co-workers on social media like Facebook may be protected "concerted activity." This federal law applies to union and nonunion employers and is enforced by the National Labor Relations Board. *See Hispanics United of Buffalo, Inc. and Carla Ortiz*, 359 N.L.R.B. No.37 (Dec. 14, 2012); *cf. Tasker*

Healthcare Group d/b/a Skinsmart Dermatology, a May 8, 2013 decision by the NLRB Division of Advice that an employee's Facebook comments that her employer was full of sh[*]t" and challenging the employer to "FIRE ME . . . Make my day" were not protected when the employer accepted the challenge and canned her.

Employers must be careful in reacting to negative comments made about employees. Obviously, if a comment is a concerted activity, an attempt to use it at trial against a fired employee will not go well and will help establish the fired employee's argument that he or she was fired improperly. When representing companies in such disputes, look closely at the company written social media policy if the company has one. The written policy itself may be too broad and create problems in supporting an adverse action against the employee.

B. Employers' efforts to investigate social media use and requiring or requesting passwords to social media websites.

There are reasons for and against employers investigating the use of social media by their job applicants and employees.

Personal traits of the job applicants and employees. Anyone want to hire a substance abuser? How about a virulent racist? Social media evidence can show a more accurate picture of someone's character than what one sees in a job interview or in the workplace when that employee believes someone is watching.

After 20 years with CNN, Octavia Nasr was fired as CNN's senior Middle East editor for tweeting praise for a Lebanese cleric who was a leader of Hezbollah and widely known to hate Americans.

A police reporter for The Arizona Daily Star was fired for Twitter comments making jokes about not enough murder in Tucson: "What?!?! No overnight homicide . . . You're slacking, Tucson" and "You stay homicidal, Tucson". His bosses did not get the joke (come on, where is their sense of Ferrell humor?), nor did the NLRB.

A job applicant at Cisco Systems tweeted after an interview that she would hate the job but love the "fatty paycheck." Someone reported it to Cisco and the applicant not only did not get the job but became widely known on the internet as "Cisco Fatty."

A Scottish politician was removed by the Labour Party as a candidate for office on its ticket for tweeting offensive and profane insults about political opponents and ridiculing the elderly as "coffin dodgers."

Negative comments about the business, customers, and clients. This is a concern in several ways. First, if the employees are trashing the business online in public social media postings, the business's reputation may suffer resulting in loss of business. Second, if the employee has a bad view of the business, its products, its policies, its operations, its managers, and fellow employees, that employee may not be giving the employer his or her best efforts. Third, such comments may negatively affect the morale and cooperation within the business's work force.

A Paterson, New Jersey school teacher was fired after posting on Facebook that she was not a teacher but rather “a warden for future criminals.” The kids’ parents and the school superintendent found her bad attitude outweighed her master’s degree and teaching certifications. The court agreed with them when she appealed.

Postings that reflect badly on the employer. This includes personal photos or statements that may mar the reputation or image of the employer.

In St. Louis, a single mother was fired from her job with a non-profit after her “sex blog,” which included graphic sexual photos obscuring her face, was discovered. She had kept the blog secret until she accidentally disclosed publicly her real name while creating a Twitter profile. Her employer’s senior management suggested supervisors search the internet from time-to-time concerning employees. She was fired the day after her sex blog was discovered due to a perceived risk to the nonprofit’s public image.

A research attorney for a Kansas appeals court was fired after tweeting during a supreme court ethics hearing about the former state attorney general who was facing the ethics charges. She referred to him as a “naughty, naughty boy” and a “douchebag” and predicted he would be disbarred for 7 years. Her apology acknowledging that she should not have tweeted because the comments might be a reflection on the Kansas courts did not save her job.

With this parade of horrors that employee social media postings can cause, why should business owners and managers not look for social media commentary by their employees and job applicants?

First, the social media statements may be protected by the National Labor Relations Act as described above so that learning of them may be of little use other than to cause ill feelings between management and employees. Not all complaints will be protected. A woman in Phoenix posted on Facebook that “I wish I could get fired some days, it would be easier to be at home than to have to go through this.” She got her wish the next day. In that case, she may not have even been commenting about the job; she posted the comment on the first anniversary of her mother’s death. However, her employer read it as making negative comments about her workplace. Had she actually been complaining about the job and being specific about the complaints (not receiving overtime pay, harsh language by supervisors, bad work conditions, etc.) she may have merited the NLRA “water cooler” protection. A woman in Michigan was fired after years of working as a cashier at a large store when managers discovered her Facebook comments complaining about the store. She has filed a claim with the NLRB.

Second, suppose what is found is information concerning an applicant’s or employee’s religion, age, marital status, pregnancy, other medical condition, or disability. The employer’s knowledge of that disability or condition may create an obstacle to taking adverse employment actions against the employee even if the employee richly deserves them or in refusing to hire the job applicant. You may have a perfectly legitimate basis for the employment action but may create an argument for the disgruntled applicant or fired employee to assert that you acted against them on an improper basis.

Third, if the business managers use improper methods to obtain the social media

evidence, then the business may be exposed to liability. In Pietrylo v. Hillstone Restaurant Group, 2009 WL 3128420 (D. N.J. Sept. 25, 2009), two employees fired for bad-mouthing the restaurant on a private, employee-only MySpace page sued the former employer claiming the managers had gotten access to the negative comments by threatening another employee to obtain an email address and password. A jury found the managers had violated the SCA and the New Jersey Wire Tapping & Electronic Surveillance Act but held that defendants had not committed common law violations of privacy because plaintiffs had no reasonable expectation of privacy in the MySpace group. The jury only awarded a total of \$3,403 in compensatory and punitive damages.

Sometimes the information about the social media postings is brought to the employer. In Lineberry v. Richards, 2013 WL 438689 (E.D. Mich. Feb. 5, 2013), employees brought Facebook photos to their employer showing that Lineberry, who was out on FMLA leave based on an on-the-job back injury, was riding in a motorboat while on vacation in Mexico and holding two grandchildren at once. So what is an employer to do with such evidence? In that instance, Lineberry was fired for misusing her FMLA leave. She sued company managers and the company for retaliation for exercising FMLA rights and not reinstating her. The court granted summary judgment to the defendants based on the photos and Lineberry's "lies" about using a wheelchair while on vacation. The employer dropped its counterclaim to recover the FMLA short-term disability benefits that Lineberry had received. One should never underestimate the resentment of co-workers who see a co-employee receive undeserved benefits while they are working. *See also Jaszczyszyn v. Advantage Health Physician Network*, 2012 WL 5416616 (6th Cir. Nov. 7, 2012)(court affirmed summary judgment for employer that fired worker for fraudulent use of FMLA leave where Facebook photos provided by co-employee to supervisor showed plaintiff at a festival while off work due to claimed complete incapacitation).

Fourth, requiring disclosure of social media passwords or access to personal social media material and firing an employee for use of social media can lead to negative publicity and subsequent loss of market share or other negative consequences. In 2009, the city of Bozeman, Montana required job applicants to provide their social media login information. The city discontinued the practice after a public outcry. Similarly, in 2010, a Maryland state agency required social media login information from job applicants and rejected some applicants based on social media evidence the agency found. The agency stopped requiring that information after the ACLU made a video about it that went viral.

C. Laws preventing requiring disclosure of social media user names and passwords.

At the time this was written, eleven states had prohibited employers from demanding social media user names and passwords from employees and job applicants. They are: Maryland (effective May 2012); Michigan (effective December 2012); Illinois (effective 1/1/13); California (effective January 2013), Utah (effective May 2013), New Mexico (effective July 2013), Washington (enacted May 2013), Arkansas (enacted April 2013), Oregon (effective 1/1/14), Colorado (enacted 5/11/13) and Nevada (effective 10/1/13). Other states were proposing similar legislation, including Massachusetts, Minnesota, Missouri, Nebraska, New York, Ohio, Pennsylvania, South Carolina, and Texas.

The federal government has not yet imposed such prohibitions. The federal “Password Protection Act of 2012” was considered in the U.S. Senate in May 2012 but not brought to a vote. The House of Representatives considered the “Social Networking Online Protection Act (SNOA)” in May 2012 but did not vote on it. SNOA was recently reintroduced. In addition, some Congressman asked the EEOC in May 2012 to investigate whether demanding passwords violated federal law.

Some states have gone farther. California, in keeping with its Constitutional protection of privacy, has barred colleges and universities from demanding user names and passwords from students, prospective students, and student groups. Other states are considering doing the same.

VI. Methods/Techniques to Obtain Social Media Discovery

At the beginning of a case, be sure to notify the opposing party or counsel to preserve the party’s social media information. Also tell your own client to preserve all social media accounts. All parties are obligated to preserve evidence that they reasonably should know is relevant to the lawsuit. Zubulake v. Warburg, 220 F.R.D. 212 (S.D. N.Y. 2003). If a party closes a social media account, the information may be lost forever. If that deleted information was potentially relevant, the consequences for the deleting party are not good. In Gatto v. United Air Lines, Ltd., 2013 WL 1285285 (D. N.J. March 25, 2013), the plaintiff deleted his Facebook account after the defendant sought it. The court punished the plaintiff with an adverse instruction to the jury.

The usual methods of discovery can be used – informal requests, written interrogatories and document production requests to parties, and subpoenas to non-parties. You will find sample written interrogatories and document production requests at Appendix A. A special problem occurs with regard to information posted on the internet by persons who do not identify themselves (usually on purpose). In conjunction with the discussion below, you will find at Appendix C sample filings used to pierce the anonymity of an internet poster in a case in a California federal court.

A. Discovering anonymous internet posters. Not surprisingly, those who defame or infringe trademarks and copyrights are not keen on having others know their true identities. Thus, your first major obstacle in a lawsuit involving such internet abuses is finding out whodunit. An author’s decision to remain anonymous raises freedom of speech concerns under the First Amendment. McIntyre v. Ohio Elections Comm’n, 514 U.S. 334, 115 S.Ct. 1511 (1995). The court must balance a party’s need to discover the identity of the anonymous actor against that actor’s free speech rights. Remember, though, that defamatory statements do not merit constitutional protection. Beauharnais v. Illinois, 343 U.S. 250, 266, 72 S.Ct. 725 (1952).

As in other areas of the law, where the anonymous act was done by the claimant’s business competitor for commercial reasons, the First Amendment protection may be reduced – it certainly is in the Ninth Circuit. See In re Anonymous Online Speakers, 611 F.3d 653 (9th Cir. 2010). In S103, Inc. v. Bodybuilding.com, LLC, 2011 WL 2565618 (9th Cir. June 29, 2011), the court reversed denial of the plaintiff’s motion to compel and held that the district court should have required in camera disclosure of the posters’ identities to determine if they were commercial competitors of the plaintiff and, therefore, the nature of the speech, because

commercial speech merits reduced protection. On the other side of the coin, on April 4, 2013, the Michigan Court of Appeals reversed a trial court's denial of a motion for protective order when the Thomas M. Cooley Law School sued an anonymous former student who denigrated the school on his blog even though the law school had already learned the defendant's identity. The law school sought the identity information through a subpoena to Weebly. The court ruled that First Amendment might protect the comments and the blogger's identity and the lower court misapplied the law in making those determinations.

In some jurisdictions, unidentified individual Doe defendants may not have standing to quash or modify a subpoena served on an ISP. See Cinetel Films, Inc. v. Does 1-1,052 (853 F.Supp.2d 545, 555-56 (D. Md. 2012)).

The courts have taken several approaches to addressing the First Amendment balance. They include:

1. In Dendrite Int'l v. Doe, 775 A.2d 756 (N.J. Ct. App. 2001), the court modified an earlier holding in Columbia Ins. Co. v. Seescandy.com, 185 F.R.D. 573 (N.D. Cal. 1999), to require that the plaintiff: (1) give the poster notice / a reasonable opportunity to oppose the disclosure; (2) identify with exactness the defamatory statements; (3) show assertion of a *prima facie* claim and sufficient evidence to support each element. If that is done, the court then (4) balances First Amendment protection for anonymous speech against the strength of the *prima facie* case and the need for the defendant's identity. The court in Doe v. Cahill, 884 A.2d 451 (Del. 2005), modified the Dendrite test to require only factors 1 and 3 and altered factor 3 to requiring *prima facie* evidence sufficient to defeat a motion for summary judgment and held factors 2 and 4 were unnecessary because they were subsumed within factor 3. The Dendrite-Cahill factors are used in some fashion by many courts.
2. In In re Subpoena Duces Tecum to America Online Inc., 52 Va. Cir. 26, 37 (2000), the court required the plaintiff to demonstrate a good faith basis for defamation, materiality of the identifications sought, and that the only way to discover the identity is through the ISP.
3. In Sony Music Entertainment Inc. v. Doe, 326 F.Supp.2d 556, (S.D. N.Y.2004), the court considered five factors in a copyright infringement case: (1) a concrete showing of a *prima facie* claim of actionable harm; (2) specificity of the discovery request; (3) absence of alternative means to obtain the subpoenaed information; (4) a central need for the subpoenaed information to advance the claim; and (5) the party's expectation of privacy.
4. In In re Indiana Newspapers, Inc., 963 N.E.2d 534 (Ind. Ct. App. 2012), the court altered the third prong of Dendrite to require "prima facie evidence to support only those elements of the cause of action that are not dependent on the commenter's identity."

B. Principles/Trends In Cases Involving Discovery Of Social Media Evidence

- **Discovery requests/subpoenas for social media evidence should be drawn narrowly.**

- **Tie your discovery requests to information already in hand that shows that the request is seeking evidence that likely exists and, therefore, not a fishing expedition.**

Courts normally hold that the posted social media information is discoverable because any privilege or privacy protection was waived by sharing the content. However, most courts will require some showing of relevance and not allow discovery of all or a broad scope of material. Usually, the discovering party must show information that at least suggests the existence of relevant information at the social media account before the court will order production or access to the information.

In EEOC v. Simply Storage Mgmt., LLC, 270 F.R.D. 430 (S.D. Ind. 2010), the court allowed broad discovery of plaintiffs' Facebook and MySpace accounts through Rule 34 document requests directed at the two claimants though the court had concerns that the requests may be seeking too much.

In Reid v. Ingerman Smith LLP, 2012 WL 6720752 (E.D. N.Y. Dec. 27, 2012) a legal secretary sued her former law firm employer for same-sex harassment and sought damages for emotional distress. The law firm obtained her private Facebook postings by showing the court that her public postings contradicted her claims of mental anguish.

In Howell v. The Buckeye Ranch, Inc., 2013 WL 1282518 (S.D. Ohio Oct.1, 2012), the court denied a motion to compel production of plaintiff's user names and password for each social media site she used. The request was deemed overbroad because it was not limited to seeking only social media information relevant to the limited purposes identified by the defendants – plaintiff's emotional state and whether the alleged sexual harassment had occurred.

In Thompson v. Autoliv ASP, Inc., 2012 WL 234928, at *1 (D. Nev. June 20, 2012), the plaintiff sought damages from a massive stroke, including for physical injury, hedonic damages, and damages for emotional distress and depression. The defendant found wall posts and photos on plaintiff's Facebook page undermining her claims. The defendant belatedly changed the privacy settings and then produced only redacted material that supported her injury claims while opposing defendant's document requests for complete, unredacted copies of plaintiff's Facebook and other social networking sites accounts. The court ordered all Facebook and MySpace information for more than a 5-year period produced without requiring an *in camera* review relying heavily on the relevant information defendant had already found online.

Likewise, in Zimmerman v. Weis Markets, Inc., 2011 WL 2065410 (Pa. Ct. of Common Pleas May 19, 2011), the court ordered production of all passwords, user names, and log-in names for all of his MySpace and Facebook accounts. Plaintiff claimed that injuries to his leg in a forklift accident caused serious, permanent health impairment and that scarring caused embarrassment so that he never wore shorts. The plaintiff undermined his claims with photos of his injuries from motorcycle accidents before and after the forklift accident, photos showing him wearing shorts, and claims that he enjoyed "bike stunts." Reminds one of the joke with the punchline "who you going to believe, me or your lying eyes."

In contrast, the court in Mailhoit v. Home Depot U.S.A., Inc., 2012 WL 3939063 (C.D. Cal. Sept.7, 2012), rejected the approach in Simply Storage and held that the discovery requests

were much too broad in light of the defendant's failure to satisfy Rule 34(b)(1)(A)'s requirement for "reasonable particularity" and Rule 26(b)(1)'s requirement that the information be relevant or would lead to admissible evidence. The court rejected requests for "any profiles, postings or messages" from any social media site for a 7-year period that could reveal the plaintiff's emotions, feelings, or mental state and for "any pictures of Plaintiff" during that same time period and posted on her profile or tagged to her profile.

Similarly, in Tompkins v. Detroit Metropolitan Airport, 278 F.R.D. 387 (E.D. Mich. 2012), the court held that a "request for the entire Facebook account, which may well contain voluminous personal materials having nothing to do with this case, is overly broad." The court did not find that plaintiff's public postings opened the door to more expansive discovery as was the case in Thompson because the public information was consistent with the plaintiff's claims.

In Mackleprang v. Fidelity Nat. Title Agency of Nevada, Inc., 2007 WL 119149 (D. Nev. Jan. 9, 2007), the defendants obtained public information from MySpace for two accounts held by plaintiff. The defendants sought an order requiring defendant to provide her private messages in those accounts in search for sexually oriented messages that might disprove her claim of emotional harm from sexual harassment. The court denied the motion to compel because (1) the plaintiff opened the MySpace accounts after she left defendant's employment so not relevant to show she welcomed defendant's sexual advances and (2) the probative value did not outweigh the unfair prejudice with regard to her emotional distress claim as it would not provide evidence that plaintiff welcomed defendants' alleged sexual conduct.

- **Compulsion efforts are better targeted at the users of the social media, not at the social media providers.**

ISPs are not responsible for defamatory or derogatory postings under the Communications Decency Act. 47 U.S.C. § 230(c)(1) (2008). You have to go after the poster of the comments.

In Barnes v. CUS Nashville, LLC, 2010 WL 2196591 (M.D. Tenn. May 27, 2010), the court relied on the SCA and Flagg to set aside the magistrate judge's show cause order directed at Facebook to turn over postings by a nonparty witness.

In Romano v. Steelcase, Inc., 907 N.Y.S.2d 650 (2010), material on plaintiff's public Facebook and MySpace pages showed her living an active lifestyle and traveling though she claimed her injuries prevented such activity. The court held that the private pages had information relevant and material to the claims and defenses and ordered plaintiff to provide an authorization to defendant to access plaintiff's private pages. *See also* McMillen v. Hummingbird Speedway, Inc., 2010 WL 4403285 (Pa. Ct. of Common Pleas Sept. 9, 2010) (ordered plaintiff to produce Facebook and MySpace user names and passwords because public parts showed plaintiff enjoying fishing and the Daytona 500 in contradiction to claimed injuries); Ledbetter v. Wal-Mart Stores, Inc., 2009 WL 1067018, at *2 (D. Colo. Apr. 21, 2009) (court noted that SCA barred social media sites from producing information but rejected plaintiff's privacy arguments and ordered plaintiff to produce contents of Facebook, MySpace, and Meetup.com accounts because public information on those accounts contradicted claims of physical and psychological injuries).

In a criminal case, targeting the social media provider may not be as difficult. In People v. Harris, described earlier, the New York court denied repeated motions to quash by Twitter and ordered Twitter to produce tweets by an Occupy Wall Street protestor for in camera review

Sometimes the court shortcuts the process. In Glazer v. Fireman's Fund Ins. Co., 2012 WL 1197167 (S.D.N.Y. April 5, 2012), the defendant served a subpoena duces tecum on LivePerson, a psychic hotline seeking plaintiff's communications. The court sidestepped the SCA and Terms & Conditions issues by directing plaintiff to open a new LivePerson account to obtain all prior chats, including those she deleted, and then producing them. In Bower v. Bower, 2011 WL 1326643 (D.Mass. Apr. 5, 2011), the court relied on the SCA to deny a motion to compel Yahoo! and Google postings made by a fugitive defendant who fled to Egypt with his children but did all but order the plaintiff to make a Rule 34 document request of the absent defendant so that the court could sanction him when he failed to respond. Presumably, the sanction would assist in obtaining the information from Yahoo! and Google.

Not all courts refuse discovery directed to social media sites. In Ledbetter v. Wal-Mart Stores, Inc., 2009 WL 1067018 (D.Colo. Apr. 21, 2009), the court denied plaintiffs' motion for protective order designed at halting production pursuant to subpoenas issued to Facebook, MySpace, and Meetup.com.

- **If you have evidence that the producing party has improperly withheld evidence, go to the court for sanctions and/or for more social media discovery.**

In Bass v. Miss Porter's School, 2009 WL 3724968 (D. Conn. Oct. 27, 2009), the court's *in camera* inspection showed plaintiff withheld relevant Facebook material so the court ordered production of her entire Facebook page.

- **Consider closely who "owns" the social media link. You may have more than one potential discovery target.**

For example, controversies have erupted over the ownership of LinkedIn profiles after an employee creates a LinkedIn profile on the employer's computer and then leaves the company. In Eagle v. Morgan, 2013 WL 943350 (E.D. Pa. 2013), the plaintiff was president of a company acquired by another company. She was terminated. Prior to leaving she let another employee access her LinkedIn profile and update it. After she left, the other employee changed the password and put her own photo and name on it. Eagle prevailed on state law claims of unauthorized use of name, invasion of privacy, and misappropriation of publicity. However, the court awarded no damages holding she suffered no economic loss. If Eagle's LinkedIn account had been in issue in a lawsuit against the company by someone other than Eagle should that plaintiff serve the company with a discovery request or Eagle with a subpoena?

A similar situation occurred in PhoneDog v. Kravitz, 2012 WL 273323 (N.D. Cal. Jan. 30, 2012), where Kravitz developed a Twitter account with 17,000 followers while employed by PhoneDog and at PhoneDog's request and continued to use the account after resigning from PhoneDog. PhoneDog asked for control of the Twitter account and when it did not get it, sued for conversion, misappropriation of trade secrets, and more. Kravitz asserted that Twitter actually owns the account under its Terms of Service. The court did not grant Kravitz's motion

to dismiss. The case later settled on confidential terms with Kravitz keeping sole custody of the Twitter profile. One can see at least 3 possible discovery targets if you needed access to information in that Twitter account for your lawsuit.

In Maremont v. Susan Fredman Design Group, Ltd., 2011 WL 6101949 (N.D. Ill. Dec. 7, 2011), Maremont, after leaving defendant's employ, sued for damages when the employer sent out Tweets and Facebook posts on Maremont's personal Twitter and Facebook accounts while she was out recuperating from a severe accident.

- ***In Camera* Review By The Court May Be Needed.**

The court in EEOC v. Original Honeybaked Ham Company of Georgia, Inc., 2012 WL 5430974 (D. Colo. Nov. 7, 2012), ordered access to all plaintiff's social media accounts for a special master. After both sides stated positions on what was collected, the court would instruct the special master on what would be produced to the court for *in camera* review. Other cases involving court's *in camera* review of social media evidence include: Reid, supra; Glazer, supra; Bass, supra; Simply Storage, supra.

Note that a court may find that no *in camera* inspection is necessary in the absence of privilege claims. See Tompson v. Autoliv, supra.

- **If The Request Is Too Broad, The Court May Limit It Or Deny It Altogether.**

In In re Air Crash, 2011 WL 6370180 (W.D.N.Y. Dec. 20, 2011), the court ordered production of 5 years of electronic communications, including social media, but only to the extent it related to issues of (a) decedent's domicile on date of airplane crash or (b) each claimant's loss of support claims.

In Kregg v. Maldonado, 98 App.Div.3d 1289, 2012 NY Slip Op. 6454 (N.Y. App. Div. Sept. 28, 2012), the defendants tried to compel production of the "entire contents" of all social media accounts maintained by or for the plaintiff (Facebook and MySpace accounts were known to exist). The court overruled the trial court and held that the discovery requests were "overbroad" and "a fishing expedition" and denied motion to compel without prejudice to service of a revised narrowly-tailored discovery request. Likewise, in McCann v. Harleysville Insurance Company of New York, 78 A.D.3d 1524, 910 N.Y.S.2d 614 (2010), the lower court denied a motion to compel plaintiff to provide "an authorization for plaintiff's Facebook account" but allowed defendant to make a revised, more limited discovery demand. The court then denied a motion to compel the same again because though the "defendant specified the type of evidence sought, it failed to establish a factual predicate with respect to the relevancy of the evidence" and was trying to engage in "a fishing expedition" in plaintiff's Facebook account.

In Squeo v. Norwalk Hosp. Ass'n, 2011 WL 7029761 (Conn. Super. Dec. 16, 2011), the parents of the decedent plaintiff (death by suicide) cooperated in providing access to the decedent's Facebook and MySpace accounts. The court denied a motion to also compel a forensic examination of the parents' computer (decedent used it infrequently) because overbroad ("sweeping in scope and unlimited in time") and the privacy interests outweighed allowing discovery that might find relevant documents but would inevitably produce irrelevant, private

information.

VII. Use of Social Media Evidence in Lawsuits

One of the first places to look for assistance in understanding the law governing the use of electronic records as evidence in court is Lorraine v. Markel American Ins. Co., 241 F.R.D. 534 (D. Md. 2007), in which Magistrate Judge Paul Grimm issued an 101-page order setting forth the issues and which rules and cases were applicable. The opinion is a primer on how to use electronic evidence in court.

A. Evidentiary uses and issues.

1. **Authentication.** FRE 901 establishes the requirements for authentication or identification as a condition precedent to the admissibility of non-testimonial evidence. FRE 901(b) gives examples of how authentication can be accomplished. Generally, the proponent of the internet printout must provide testimony by live witness or affidavit that the printout is what it purports to be. See In re Carrsow-Franklin, 456 B.R. 753, 756-57 (Bankr.D.S.C. 2011) (noting that blogs are not self-authenticating and rejecting blog evidence due to failure to present authentication testimony) and cases cited there. The Lorraine case gives an excellent discussion of how Rule FRE 901 works with FRE 104 and the necessity for the court to decide authentication as a preliminary question. However, if the evidence is not relevant to begin with, it cannot be authenticated because it cannot meet the requirements under FRE 104 and 401.

These evidentiary rules do not appear to be consistently applied between the criminal and civil contexts. Some state criminal courts appear to fail to apply or misapply the evidentiary rules. For example, in Griffin v. State, 419 Md. 343, 19 A.3d 415 (Md. Ct. App. 2011), the court overturned conviction for felonies including second-degree murder because MySpace pages of defendant's girlfriend on which there were threats ("snitches get stitches") against a key witness lacked a proper foundation as they were not properly authenticated. The court analyzed a Maryland rule of evidence that was, in part, similar to FRE 901 and looked at decisions in other states. The court held that the prosecutor's effort to authenticate through the police investigator rather than the girlfriend, who testified at trial, was insufficient. The court noted that the prosecution could also have searched the computer of the person who allegedly created the profile and the posting or sought information from the social media website. The Griffin opinion appears to be based more on the court's skepticism about admitting internet evidence in general. The court focused on the fact that the evidence may have been created by someone other than its putative creator, even in the absence of any evidence that this in fact happened, and then excluded the evidence on the grounds that there was inaccurate authentication. The reasoning in Griffin conflicts with FRE 104 and 901 and Lorraine in which Judge Grimm stated that authentication "as a condition precedent to admissibility is satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims . . . This is not a particularly high barrier to overcome . . . as [a] party seeking to admit an exhibit need only make a prima facie showing that it is what he or she claims it to be . . . [and] '[t]he court need not find that the evidence is necessarily what the proponent claims, but only that there is sufficient evidence that the *jury* might ultimately do so.'" 241 F.R.D. at 541-42 (internal citation omitted).

In People v. Clevestine, 68 A.D.3d 1448, 891 N.Y.S.2d 511 (2009), the court held that MySpace messages were properly admitted in a rape case. Defendant asserted that someone else accessed his account and posted the messages. Both victims testified that they had engaged in MySpace instant messaging with defendant about sexual activities, a police investigator retrieved the messages from the hard drive of the computer of the victims, and a MySpace employee testified that the messages had been between the victims and users of accounts created by the defendant. The court applied New York case law on authentication without any reference to evidentiary rules.

2. **Identification.** Photos from social media sites have been used to help identify and incriminate criminal defendants. In Bradley v. Texas, No. 14-10-01167-CR (Tex. Ct. App. 2012), a robbery victim found photos of the two robbers on Facebook. Bradley was one of them and he was holding two guns in one photo, including a gun that looked like the one used in the robbery. The victim emailed the photos to the investigating detective and they were used in photo arrays through which the victim identified the robbers. The court held that even if the array was suggestive, there was ample other evidence of identification that occurred prior to the use of the array. *See also* Rene v. State, 376 S.W.3d 302 (Tex. Ct. App. 2012) (prosecution used MySpace photos of defendant showing him with gang signs, tattoos, a pistol, and a large amount of cash).

3. **Relevance.** Obviously, the social media evidence has to be relevant to issues in the case. *See* FRE 401. The courts routinely decide relevance of such evidence. *See, e.g., Bass, supra; Ledbetter, supra; Engman v. City of Ontario*, 2011 WL 2463178*10-11 (C.D.Cal. June 20, 2011) (excluding information on plaintiff's MySpace page); B.M. v. D.M., 2011 WL 1420917, at *5 (N.Y. Sup. Ct. Apr. 7, 2011) (admissions in blog were relevant and admissible). If a party fails to produce relevant evidence in discovery, the consequences can be severe. In Lester v. Alliance Concrete Co., a Virginia state court reduced a jury award by over \$4 million dollars and ordered the plaintiff and his counsel to pay the defendants over \$700,000 in fees and expenses because of deliberate deletion of Facebook photos responsive to discovery requests.

4. **Other evidentiary issues.** Of course, hearsay objections may arise when using electronic evidence. *See* Miles v. Raycom Media, Inc., 2010 WL 4791764 *3 n.1 (S.D.Miss. Nov. 18, 2010) (unsworn statements made on Facebook page by nonparties were inadmissible under FRE 801). You may have multiple layers of hearsay involved and have to rely upon several hearsay exceptions. Judge Grimm provides an extensive discussion in Lorraine of hearsay in the context of electronically stored information. The procedural posture may affect how the court treats the information. In granting defendant's motion for summary judgment in Witt v. Franklin County Board of Education, 2013 WL 832152 (N.D.Ala. Feb. 28, 2013), the court considered three Facebook messages from nonparties offered by plaintiff because plaintiff could have reduced them to admissible form at trial by calling the witnesses.

You may also often be faced with objections concerning unfair prejudice under FRE 403 and 404. *See, e.g., Quagliarello v. Dewees*, 2011 WL 3438090 *2-4 (E.D.Pa. Aug.4, 2011) (allowing some but not all photos from plaintiff's MySpace page because relevance to emotional distress claim outweighs unfair prejudice); State v. Townsend, 208 N.C. App. 571, 706 S.E.2d 841 (2010) (court denied request to allow testimony about Facebook and MySpace

postings because probative value substantially outweighed by danger of unfair prejudice). Not all courts will use the same approach. Some commentators suggest that statements on Facebook and other social media are not considered statements of one's actual knowledge or belief but more in the nature of loose talk that do not merit admission as evidence. Those arguments seem to go to the weight to be given not the admissibility.

B. Investigating Prospective Jurors And Jurors.

Prospective jurors and jurors, like everyone else, have smartphones and use social media. If you practice in a jurisdiction where you have access to juror rolls and the case is worth the cost or you otherwise have time to research prospective jurors during a lengthy voir dire process (i.e., not in any federal court in which I have conducted voir dire), then searching for those prospective jurors' social media statements and photos could be of some assistance in deciding whether or not to keep them on the jury. You may well be obligated to conduct such research where you can and may be further obligated to disclose your research to the court under some circumstances. In Johnson v. McCullough, 306 S.W.3d 551, 559 (Mo. 2010), the court held that a 'party must use reasonable efforts to examine the litigation history on Case.net of those jurors selected but not empanelled and present to the trial court any relevant information prior to trial.'

Lawyers are prohibited from communicating directly with jurors outside of the in-court processes. Lawyers are not barred from investigating jurors and potential jurors online and are doing so regularly. The prohibition can come into play during such investigations. You cannot "friend" jurors and prospective jurors or use subterfuge or agents to "friend" jurors and prospective jurors in a case you are trying. Nor can you subscribe to a juror's Twitter account. Remember, if you decide to follow a potential juror on Twitter, Twitter will send the juror an email identifying your Twitter account name. You will have just made an *ex parte* communication to a juror. Becoming a "fan" on Twitter is akin to "friending" the juror on Facebook. Some bar associations specifically prohibit that action. For example, the New York County Law Association issued Formal Opinion No. 743 on May 18, 2011, against this practice.

C. Jurors' Use Of Social Media During Trial.

The judiciary is struggling with how to prevent jurors from using their technology, mobile or otherwise, to do independent investigation of matters before them in their capacity as jurors. In December 2009, the Judicial Conference Committee on Court Administration and Case Management (the "CACM") endorsed use of model jury instructions to prohibit jurors from using electronic technology to research or communicate about cases during jury duty.

Jurors use social media in a variety of ways. The Federal Judicial Center issued a 40-page report to the CACM on the issue on November 22, 2011. The report included the results of a survey of 952 federal district court judges, 508 of whom responded from all 94 districts. Thirty judges (about 6%) had detected use of social media during trial (23 judges reported) or jury deliberations (12 judges reported). The social media uses included Facebook and Google-plus (9 each), instant messaging (7), and Twitter and internet chat rooms (3 each). Three judges reported juror attempts to "friend" a participant in the case and three reported juror attempts to communicate directly with a participant in the case. None reported a juror divulging confidential information about a case but one reported a juror disclosing identifying information about other

jurors. Five reported jurors doing case-related research and four reported sharing general trial information. The FJC report included in its appendices seven variations of jury instructions concerning juror conduct used by the federal judges. These are a good source to fashion your own.

As a result of the FJC report, CCACM published in June 2012, revised model jury instructions on juror use of social media and technology during jury duty. In March 2013, the FJC issued the sixth edition of the Benchbook for U.S. District Court Judges. Section 6.06 provides “Preliminary jury instructions – civil case” which include specific instructions prohibiting jurors from conducting online research or using technology or social media to communicate with anyone about the case. The applicable portion appears at Appendix B. You can find the entire Benchbook at http://www.fjc.gov/library/fjc_catalog.nsf. Another source for jury instructions is Eric P. Robinson, *Jury Instructions for the Modern Age: A 50-State Survey of Jury Instructions on Internet and Social Media*, 1 Reynolds Courts & Media Law Journal 307 (2011). You should note that the author found that only one federal circuit and ten states explained why the jurors should not use the internet and social media during trial so exercise care in deciding which instructions to use.

The problem of “tweeting” (on Twitter) and texting from the courthouse is likely to grow. In Arkansas, a murder conviction and death sentence were reversed and remanded due to juror misconduct when a juror posted tweets in violation of court’s instructions. Dimas-Martinez v. State, 385 S.W.3d 238, 246-49 (Ark. 2011). Similarly, in April 2013, an Oregon state court judge sentenced a juror to two days in jail for texting during a trial contrary to instructions.

The increasing use of iPhones is likely to lead to an increase in juror efforts to do outside research. In September 2010, a Florida appellate court reversed a manslaughter conviction due to the jury foreman using an iPhone to search for the definition of “prudent.” You should ensure that the jury instructions specifically state a prohibition against jurors conducting outside research.

The problem of juror use of social media during trial is likely to continue and may even grow as more people become active on social media sites and obtain more advanced mobile IT devices. In U.S. v. Fumo, a high-profile, 5-month-long, criminal trial of a Pennsylvania state senator and another person, a juror posted messages on Facebook and Twitter about the trial (he also had a blog or two). A local TV station reported the postings. The court (U.S. District Court for the Eastern District of Pennsylvania) denied the convicted defendants’ motion to disqualify and remove the juror finding that the juror’s internet postings/ messages were vague and that there was no evidence that the juror was not impartial. The court also denied a post-trial motion for a new trial finding that the evidence did not show that the juror had been influenced in his deliberations by such activities. The Third Circuit affirmed because the juror’s statements were vague, “harmless ramblings.” 655 F.3d 288 (3d Cir. 2011).

When the possibility occurs of jurors engaging in social media communications about a trial during the trial, the presiding judge generally has inherent authority to investigate to ensure that the jury is not tainted by exposure to evidence outside of that presented at trial. The investigative methods by the court vary. In Commonwealth v. Werner, 81 Mass. App. Ct. 689, 967 N.E.2d 159 (Mass. Ct. App. 2012), the defendant was convicted of larceny but made a new

trial motion based on a juror posting comments on Facebook during the trial. The court denied the motion. In doing so, the court relied upon the sworn statements of the jurors without waiting for Facebook to provide materials subpoenaed from it. In Juror Number One v. Superior Court, 206 Cal.App.4th 854, 142 Cal.Rptr. 3d 151 (2012), the court quashed as overbroad a subpoena to a juror for all items that the juror posted on Facebook during the trial but ordered the juror to sign a consent form authorizing Facebook to release the material to the court for in camera review. The juror unsuccessfully opposed citing to the SCA, Fourth Amendment, Fifth Amendment, and privacy rights. The party seeking the information had first subpoenaed Facebook but when it moved to quash, subpoenaed the juror.

D. Recommendations regarding jurors:

- If voir dire is permitted, ask your jurors about their use of social media. Even if you do not disqualify the juror, if the case is high value, it may be worth monitoring the social media sites identified as being used. You may also choose to excuse a juror showing signs of an addiction to social media use (unless you are defending in a criminal case and want to have a possible basis to disrupt the prosecution of your client through a motion for mistrial or to disqualify a juror or to overturn a conviction).
- If your court or judge does not have a standard jury instruction concerning the use of social media and internet-based technology during trial, you should propose one. Make sure the jury instructions also tell the jurors not to communicate with one another through social media use.
- Go online and investigate your prospective jurors in advance of voir dire if that is possible but do not friend them on Facebook or follow them on Twitter. Disclose to the court any information that the court ought to know before seating the juror. During trial, if time and expense permit, have a paralegal go online to determine if any jurors are improperly communicating about the trial. If so, report to the court any violations of the court's instructions to the jury.

APPENDIX A

Case law makes clear that social media discovery directed to a party must be narrowly tailored to the issues relevant in the case. Below are some sample interrogatories and requests for production that may be useful in your case.

SAMPLE INTERROGATORIES TO PARTY

1. Please identify any home or other e-mail accounts (including those associated with social media sited, eg., jane.doe@facebook.com) that you maintained or used during the entire time that you claim is relevant to this case, including a listing of the specific e-mail addresses for all such accounts, when they were first established, and if they have been terminated, the date of termination.
2. Please identify any home or other Instant Messaging (“IM”) applications or services (*e.g.*, AOL Instant Messenger, Yahoo Messenger, MSN Messenger, Google Chat, Facebook Messenger, *etc.*) that you maintained or used during the entire time that you claim is relevant to this case, including a listing of the specific IM addresses or screen names for all such accounts, when they were first established, and if they have been terminated, the date of termination.
3. Please identify any chat rooms or social networking web-sites that you maintained an account with or used during the entire time that you claim is relevant to this case, including a listing of each such account, when they were first established, and if they have been terminated, the date of termination;
4. Please identify any Google+, MySpace, Facebook, Twitter, Meetup.com, Orkut, Flickr, Gather.com, Tumblr, Windows Live Spaces, MSN Spaces or similar social networking accounts that you maintained or used during the entire time that you claim is relevant to this case, including a listing of the specific screen names for all such accounts, when they were first established, and if they have been terminated, the date of termination.
5. Please identify any LinkedIn, Monster.com, CareerBuilder.com or similar job listing or professional networking accounts you maintained or used during the entire time that you claim is relevant to this case, including a listing of when they were first established, and if the account has been terminated, the date of termination;
6. Please identify any blogging or wiki provider or similar accounts that you maintained or used during the entire time that you claim is relevant to this case, including a listing of the specific screen names for all such accounts, when they were first established, and if the account has been terminated, the date of termination;
7. Please identify all personal ads you have placed on-line or in print, including a listing of where the ads were placed and when;
8. Please identify all online and internet personas or identities that you have assumed, including a listing of all such identities or personas and the date such identities and

personas were used, for what purpose and the names of the websites that such identities and personas were used.

9. For each of the websites and or services listed below, identify your usernames(s), the email address(es) associated with your account, and the approximate date you joined the website or service. If you have not joined a listed website or service, expressly state that you have never joined that particular website or service:

- | | | |
|----------------|----------------------|-------------------|
| • About.me | • Flixster | • Quora |
| • aNobil | • Food Spotting | • Rate Your Music |
| • AudioBoo | • Forrst | • Rebjä |
| • authorSTREAM | • Fotolog | • reddit |
| • Aviary | • foursquare | • Redux |
| • Badoo | • FriendFeed | • ResumeBucket |
| • Bambuser | • funnyordie | • Revver |
| • bebo | • fwhsp | • ryze |
| • behance.net | • Gather | • Seesmic |
| • Bit.ly | • Gdgt | • Setlist.fm |
| • BizNik | • GetGlue | • Shelfari |
| • blekko | • Github | • Skribit |
| • BlinkList | • Gogobot | • Skyrock |
| • Blip.fm | • Goodreads | • Slashdot |
| • blip.tv | • gowalla | • Slide |
| • blippr | • Hexday | • slideshare |
| • blippy | • hi5 | • SlideSix |
| • Blogger | • Howcast | • Snooth |
| • Blogmarks | • Hulu | • SocialShake |
| • blogTV | • ibibo | • SoundCloud |
| • brightkite | • identica | • Soup.lo |
| • Brizzly | • iLike | • Sphinn |
| • Buzznet | • iliketotallyloveit | • Squidoo |
| • cafemom | • ImageShack | • Steam |
| • Car Domain | • InsaneJournal | • StumbleUpon |
| • Chimp | • Instructables | • Technorati |

- claimid
- ColourLovers
- connect.me
- CopyTaste
- Current
- DailyBooth
- DailyMotion
- delicious
- deviantART
- Digg
- digo
- Disqus
- Doppir
- Dribbble
- Dropjack
- Ecademy
- eHow
- EightBit.Me
- epinions
- eSnips
- Etsy
- Facebook
- Families.com
- Fanpop
- Faves
- FFFFFound!
- Flavors.me
- Flickr
- Jaiku
- Jamendo
- Justin.tv
- Kaboodie
- Kongregate
- last.fm
- Linkedin
- Listorious
- LiveJournal
- Livevideo
- Mahalo
- Multiply
- My Name is
- myLot
- MySpace
- Netlog
- netvibes
- newsvine
- photobucket
- Picasa
- Picture Trail
- Plancast
- plaxo
- Plime
- Plurk
- Politics4all.com
- Posterous
- Qik
- ThisNext
- Tribe
- Tripit
- tumbir
- Twitpic
- Twitter
- UStream
- vi.sualize.us
- Viddler
- Vimeo
- VodPod
- Wakoopa
- Wefollow
- wikipedia
- Wishlistr
- WordPress
- WUAH
- Xanga
- XFire
- yfrog
- Yotify
- YouTube
- zeaLOG
- Zoomr

SAMPLE DOCUMENT REQUEST TO PARTY

1. Please provide copies of all instant messaging logs or transcripts associated with any accounts identified in response to Interrogatory No. ____.
2. Please provide copies of any contributions you have made to any online forum or Website or online service associated with any accounts identified in response to Interrogatory No. ____.
3. Please provide copies of any Documents or electronically stored information you have created and/or stored using any third party online service provider, including, but not limited to, Google+, MySpace, Facebook, Twitter, Meetup.com, Orkut, Flickr, Gather.com, Tumblr, Windows Live Spaces, MSN Spaces, LinkedIn, Monster.com, CareerBuilder.com, blogs, or wikis, associated with any accounts identified in response to Interrogatory No. ____.
4. Please provide an electronic copy of your complete Facebook history, including any and all profile information, postings, pictures, and data available pursuant to Facebook's "Download Your Own Information" feature.
5. For each Facebook account maintained by you, please produce your account data for the period of _____ through present. You may download and print your Facebook data by logging onto your Facebook account, selecting "Account Settings" under the "Account" tab on your homepage, clicking on the "learn more" link beside the "Download Your Information" tab, and following the directions on the "Download Your Information" page. [from *Held v. Ferrellgas, Inc.*, Case No. 2:10-cv-2393-EFM-GLR (D. Kan.)]

APPENDIX B

Federal Benchbook jury instructions prohibiting juror investigation, communication, and use of social media and technology

Conduct of the jury

Now a few words about your conduct as jurors.

You, as jurors, must decide this case based solely on the evidence presented here within the four walls of this courtroom. This means that during the trial you must not conduct any independent research about this case, the matters in the case, and the individuals or corporations involved in the case. In other words, you should not consult dictionaries or reference materials, search the internet, websites, or blogs, or use any other electronic tools to obtain information about this case or to help you decide the case. Please do not try to find out information from any source outside the confines of this courtroom.

Until you retire to deliberate, you may not discuss this case with anyone, even your fellow jurors. After you retire to deliberate, you may begin discussing the case with your fellow jurors, but you cannot discuss the case with anyone else until you have returned a verdict and the case is at an end.

I know that many of you use cell phones, Blackberries, the Internet, and other tools of technology. You also must not talk to anyone at any time about this case or use these tools to communicate electronically with anyone about the case. This includes your family and friends. You may not communicate with anyone about the case on your cell phone, through e-mail, Blackberry, iPhone, text messaging, or on Twitter, through any blog or website, including Facebook, Google+, My Space, LinkedIn, or YouTube. You may not use any similar technology of social media, even if I have not specifically mentioned it here. I expect you will inform me as soon as you become aware of another juror's violation of these instructions.¹ A juror who violates these restrictions jeopardizes the fairness of these proceedings, and a mistrial could result, which would require the entire trial process to start over.

Finally, do not form any opinion until all the evidence is in. Keep an open mind until you start your deliberations at the end of the case.

¹ Taken from "Proposed Model Jury Instructions: The Use of Electronic Technology to Conduct Research on or Communicate about a Case," prepared by the Judicial Conference Committee on Court Administration and Case Management (June 2012). *See* Memorandum, "Juror Use of Social Media" from Judge Julie A. Robinson, Chair, Committee on Court Administration and Case Management to all United States District Court Judges (Aug. 6, 2012), *available at* <http://jnet.ao.dcn/img/assets/7324/DIR12-074.pdf>. *See also* "Strategies for Preventing Jurors' Use of Social Media During Trials and Deliberations," *in* Jurors' Use of Social Media During Trials and Deliberations: A Report to the Judicial Conference Committee on Court Administration and Case Management 5-10 (Federal Judicial Center Nov. 22, 2011), *available at* [http://cwn.fjc.dcn/public/pdf.nsf/lookup/DunnJuror.pdf/\\$file/DunnJuror.pdf](http://cwn.fjc.dcn/public/pdf.nsf/lookup/DunnJuror.pdf/$file/DunnJuror.pdf).

APPENDIX C

BY FAX

11 JUN 14 PM 12:54
CLERK U.S. DISTRICT COURT
CENTRAL DISTRICT OF CALIF.
LOS ANGELES

FILED

1 BUCHALTER NEMER
2 A Professional Corporation
3 STEVEN BROWER (SBN: 93568)
4 Email: sbrower@buchalter.com
5 18400 Von Karman, Suite 800
6 Irvine, CA 92612
7 Telephone: (714) 549-5150
8 Facsimile: (949) 224-6410

9 Attorneys for Plaintiff Benjamin D. Chung, M.D.

10 UNITED STATES DISTRICT COURT
11 CENTRAL DISTRICT OF CALIFORNIA

CV 11-05023 ODW (EX)

12 Benjamin D. Chung, M.D.,

Case No. _____

13 Plaintiff,

Complaint for:

14 vs.

(1) Trade Libel

15 Does 1-10,

(2) Defamation

16 Defendants.

Demand for Jury Trial

17 Plaintiff Benjamin D. Chung, M.D. ("Dr. Chung" or "Plaintiff") alleges as
18 follows:

19 JURISDICTION AND VENUE

20 1. This action is for, *inter alia*, Trade Libel, in violation of the laws of
21 the United States. This Court has jurisdiction pursuant to 15 U.S.C. § 1121(a) and
22 28 U.S.C. §§ 1331 and 1338(a) in that this case arises under the laws of the United
23 States pursuant to the Lanham Act, 15 U.S.C. §§ 1051 *et seq.*

24 2. This Court has supplemental jurisdiction over the claims herein
25 arising under the laws of the State of California pursuant to 28 U.S.C. §§ 1338(b)
26 and 1367 in that said claims are so related to Plaintiff's federal claims that they
27 form part of the same case or controversy under Article III of the United States
28 Constitution.

BUCHALTER NEMER
A PROFESSIONAL CORPORATION
LOS ANGELES

8 4. Dr. Chung is an individual residing in the State of California who has
9 been and is licensed, in good standing, to practice medicine in the State of
10 California since October, 1990. He is currently Board Certified in
11 Gastroenterology and Internal Medicine. At all relevant times herein he resided and
12 practiced medicine primarily within the Central District.

6. Dr. Chung, in addition to many years he time expended in obtaining his professional credentials, including becoming Board Certified in gastroenterology and internal medicine, has expended over twenty years of his professional life in obtaining a positive reputation within his profession as a physician. These efforts have resulted in his creating a revenue source from his efforts as a physician.

BUCHALTER NEMER
A PROFESSIONAL CORPORATION
LOS ANGELES

1 harm to his reputation because they would seek to treat any patients who sought out
2 an alternative physician to Dr. Chung.

3 8. In or around February, 2011, Dr. Chung discovered a "review" posted
4 on a website known as Vitals.com. That posting, dated February 18, 2011
5 ("Offending Post"), states:

6 My father had an Advanced Directive which stated that he did not
7 want any aggressive treatments during his life as he was 90 years old
8 and had lived a long full life. This "doctor" performed over 10
9 colonoscopies on my father in less than 6 months and God only knows
10 how many stomach endoscopies. He is callous and ruthless and has no
11 bedside manner. I am reporting him to Medicare and the California
12 Medical Board. Apparently, this "doctor" has been known in
13 Riverside for many years to be one of the most fraudulent physicians
14 in practice. He performs countless procedures which are not medically
15 necessary, and this included multiple endoscopic procedures on my
16 father.

17 9. Upon information and belief, the Offending Post contains false and
18 disparaging statements of fact about the professional services provided by Dr.
19 Chung, including, but not limited to, a statement that he committed battery on a
20 patient, that he performs procedures which are not medically necessary and that he
21 has been known as "one of the most fraudulent physicians in practice."

22 10. Upon information and belief, the Offending Post was made with
23 either knowledge of falsity or with reckless disregard of its truth or falsity.

24 11. Upon information and belief, the Offending Post was published with
25 intent to harm Dr. Chung's medical practice or with knowledge that harm with
26 inevitably result, in combination with benefit to the Defendants

27 12. Upon information and belief, the Offending Post was placed on the
28 internet, by Defendants, with the intention that the Offending Post receives broad

1 exposure to patients and potential patients from a broad geographic area, such that
2 it affects interstate commerce.

3 13. Upon information and belief, Specific ("special") damages have been
4 suffered by Dr. Chung, which were directly caused by the Offending Post.

5 14. Upon information and belief, Defendants are profiting from the
6 Offending Post by having potential customers of Dr. Chung diverted to their
7 medical practice.

8 **FIRST CLAIM**

9 **TRADE LIBEL in violation of 15 USC 1125(a)(1)(B)**

10 15. Dr. Chung incorporates by reference paragraphs 1 to 14, as if set forth
11 in full.

12 16. Upon information and belief, Defendants' Offending Post was made
13 in interstate commerce in connection with goods or services, and is a false or
14 misleading representation of fact, which misrepresents the nature, characteristics,
15 and qualities of another person's goods, services, or commercial activities, in
16 violation of 15 USC 1125(a)(1)(B).

17 **SECOND CLAIM**

18 **DEFAMATION in violation of CA Civil Code §44**

19 17. Dr. Chung incorporates by reference paragraphs 1 to 14, as if set forth
20 in full.

21 18. Upon information and belief, the Offending Post is a false and
22 unprivileged publication by writing, which exposes Dr. Chung to hatred, contempt,
23 ridicule, or obloquy, or which causes Dr. Chung to be shunned, or avoided, or
24 which has a tendency to injure Dr. Chung in his occupation.

25 **PRAYER FOR RELIEF**

26 WHEREFORE, Dr. Chung prays for judgment against Defendants, and each
27 of them, as follows:
28

1 A. For a permanent injunction ordering Defendants, their agents, servants,
2 employees, attorneys, and all persons in active concert or participation with
3 Defendants to refrain from publishing the Offending Post;

4 B. For lost profits and costs incurred by Dr. Chung due to the Offending
5 Post;

6 C. For legal costs and fees incurred by Dr. Chung to attain the relief
7 requested herein; and

8 D. For such other and further relief as this Court deems just and proper.

9
10 DATED: June 14, 2011

BUCHALTER NEMER
A Professional Corporation

11
12 By: 

13 STEVEN BROWER
14 Attorneys for Plaintiff
15 Dr. Benjamin Chung
16
17
18
19
20
21
22
23
24
25
26
27
28

DEMAND FOR A JURY TRIAL

Pursuant to F.R.C.P. 38(b), Plaintiff Benjamin D. Chung, M.D. hereby demands a trial by jury in this action of any issues triable by jury.

DATED: June 14, 2011

BUCHALTER NEMER
A Professional Corporation

By: _____


STEVEN BROWER
Attorneys for Plaintiff
Dr. Benjamin Chung

**UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA**

NOTICE OF ASSIGNMENT TO UNITED STATES MAGISTRATE JUDGE FOR DISCOVERY

This case has been assigned to District Judge Otis D. Wright II and the assigned discovery Magistrate Judge is Charles Eick.

The case number on all documents filed with the Court should read as follows:

CV11- 5023 ODW (Ex)

Pursuant to General Order 05-07 of the United States District Court for the Central District of California, the Magistrate Judge has been designated to hear discovery related motions.

All discovery related motions should be noticed on the calendar of the Magistrate Judge

=====

NOTICE TO COUNSEL

A copy of this notice must be served with the summons and complaint on all defendants (if a removal action is filed, a copy of this notice must be served on all plaintiffs).

Subsequent documents must be filed at the following location:

☒ **Western Division**
312 N. Spring St., Rm. G-8
Los Angeles, CA 90012

☐ **Southern Division**
411 West Fourth St., Rm. 1-053
Santa Ana, CA 92701-4516

☐ **Eastern Division**
3470 Twelfth St., Rm. 134
Riverside, CA 92501

Failure to file at the proper location will result in your documents being returned to you.

ORIGINAL

BUCHALTER NEMER, A PROFESSIONAL CORPORATION
Steven Brower (SBN: 93568)
18400 Von Karman Avenue, Suite 800
Irvine, CA 92612
Phone: (714) 549-5150
Fax: (949) 224-6410

BY FAX

**UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA**

BENJAMIN D. CHUNG, M.D.

PLAINTIFF(S)

v.

DOES 1-10,

DEFENDANT(S).

CASE NUMBER

CV 11-05023 ODW (BX)

SUMMONS

TO: DEFENDANT(S): DOES 1-10

A lawsuit has been filed against you.

Within 21 days after service of this summons on you (not counting the day you received it), you must serve on the plaintiff an answer to the attached ☒ complaint ☐ amended complaint ☐ counterclaim ☐ cross-claim or a motion under Rule 12 of the Federal Rules of Civil Procedure. The answer or motion must be served on the plaintiff's attorney, Steven Brower, whose address is 18400 Von Karman Avenue, Suite 800, Irvine, CA 92612. If you fail to do so, judgment by default will be entered against you for the relief demanded in the complaint. You also must file your answer or motion with the court.

Clerk, U.S. District Court

Dated: JUN 14 2011

By: _____

Deputy Clerk

(Seal of the Court)

[Use 60 days if the defendant is the United States or a United States agency, or is an officer or employee of the United States. Allowed 60 days by Rule 12(a)(3).]

CV-01A (12/07)

SUMMONS

American LegalNet, Inc.
www.USBriefForms.com

UNITED STATES DISTRICT COURT, CENTRAL DISTRICT OF CALIFORNIA
CIVIL COVER SHEET

I (a) PLAINTIFFS (Check box if you are representing yourself <input type="checkbox"/>) BENJAMIN D. CHUNG, M.D.	DEFENDANTS DOES 1-10
(b) Attorneys (Firm Name, Address and Telephone Number. If you are representing yourself, provide same.) BUCHALTER NEMER, A PROFESSIONAL CORPORATION Steven Brower (SBN: 93568) 18400 Von Karman Avenue, Suite 800 Irvine, CA 92612 Phone: (714) 549-5150 Fax: (949) 224-6410.	Attorneys (If Known)

II. BASIS OF JURISDICTION (Place an X in one box only.) <input type="checkbox"/> 1 U.S. Government Plaintiff <input checked="" type="checkbox"/> 3 Federal Question (U.S. Government Not a Party) <input type="checkbox"/> 2 U.S. Government Defendant <input type="checkbox"/> 4 Diversity (Indicate Citizenship of Parties in Item III)	III. CITIZENSHIP OF PRINCIPAL PARTIES - For Diversity Cases Only (Place an X in one box for plaintiff and one for defendant.) <table style="width:100%;"> <tr> <td style="width:33%;">Citizen of This State</td> <td style="width:33%;">PTF DEF <input type="checkbox"/> 1 <input type="checkbox"/> 1</td> <td style="width:33%;">Incorporated or Principal Place of Business in this State</td> <td style="width:33%;">PTF DEF <input type="checkbox"/> 4 <input type="checkbox"/> 4</td> </tr> <tr> <td>Citizen of Another State</td> <td><input type="checkbox"/> 2 <input type="checkbox"/> 2</td> <td>Incorporated and Principal Place of Business in Another State</td> <td><input type="checkbox"/> 5 <input type="checkbox"/> 5</td> </tr> <tr> <td>Citizen or Subject of a Foreign Country</td> <td><input type="checkbox"/> 3 <input type="checkbox"/> 3</td> <td>Foreign Nation</td> <td><input type="checkbox"/> 6 <input type="checkbox"/> 6</td> </tr> </table>	Citizen of This State	PTF DEF <input type="checkbox"/> 1 <input type="checkbox"/> 1	Incorporated or Principal Place of Business in this State	PTF DEF <input type="checkbox"/> 4 <input type="checkbox"/> 4	Citizen of Another State	<input type="checkbox"/> 2 <input type="checkbox"/> 2	Incorporated and Principal Place of Business in Another State	<input type="checkbox"/> 5 <input type="checkbox"/> 5	Citizen or Subject of a Foreign Country	<input type="checkbox"/> 3 <input type="checkbox"/> 3	Foreign Nation	<input type="checkbox"/> 6 <input type="checkbox"/> 6
Citizen of This State	PTF DEF <input type="checkbox"/> 1 <input type="checkbox"/> 1	Incorporated or Principal Place of Business in this State	PTF DEF <input type="checkbox"/> 4 <input type="checkbox"/> 4										
Citizen of Another State	<input type="checkbox"/> 2 <input type="checkbox"/> 2	Incorporated and Principal Place of Business in Another State	<input type="checkbox"/> 5 <input type="checkbox"/> 5										
Citizen or Subject of a Foreign Country	<input type="checkbox"/> 3 <input type="checkbox"/> 3	Foreign Nation	<input type="checkbox"/> 6 <input type="checkbox"/> 6										

IV. ORIGIN (Place an X in one box only.)

☒ 1 Original Proceeding
 ☐ 2 Removed from State Court
 ☐ 3 Remanded from Appellate Court
 ☐ 4 Reinstated or Reopened
 ☐ 5 Transferred from another district (specify): _____
 ☐ 6 Multi-District Litigation
 ☐ 7 Appeal to District Judge from Magistrate Judge

V. REQUESTED IN COMPLAINT: JURY DEMAND: ☒ Yes ☐ No (Check 'Yes' only if demanded in complaint.)

CLASS ACTION under F.R.C.P. 23: ☐ Yes ☒ No **MONEY DEMANDED IN COMPLAINT:** \$ _____

VI. CAUSE OF ACTION (Cite the U. S. Civil Statute under which you are filing and write a brief statement of cause. Do not cite jurisdictional statutes unless diversity.)
15 USC 1051 - Lanham Act - False Advertising in Interstate Commerce

VII. NATURE OF SUIT (Place an X in one box only.)

OTHER STATUTES <input type="checkbox"/> 400 State Repportionment <input type="checkbox"/> 410 Antitrust <input type="checkbox"/> 420 Banks and Banking <input type="checkbox"/> 430 Commerce/ICC Rates/etc. <input type="checkbox"/> 460 Deportation <input type="checkbox"/> 470 Racketeer Influenced and Corrupt Organizations <input type="checkbox"/> 480 Consumer Credit <input type="checkbox"/> 490 Cable/Sat TV <input type="checkbox"/> 810 Selective Service <input type="checkbox"/> 840 Securities/Commodities Exchange <input type="checkbox"/> 875 Customer Challenge 12 USC 3410 <input type="checkbox"/> 890 Other Statutory Actions <input type="checkbox"/> 891 Agricultural Act <input type="checkbox"/> 892 Economic Stabilization Act <input type="checkbox"/> 893 Environmental Matters <input type="checkbox"/> 894 Energy Allocation Act <input type="checkbox"/> 895 Freedom of Info. Act <input type="checkbox"/> 900 Appeal of Fee Determination Under Equal Access to Justice <input type="checkbox"/> 950 Constitutionality of State Statutes	CONTRACT <input type="checkbox"/> 110 Insurance <input type="checkbox"/> 120 Marine <input type="checkbox"/> 130 Miller Act <input type="checkbox"/> 140 Negotiable Instrument <input type="checkbox"/> 150 Recovery of Overpayment & Enforcement of Judgment <input type="checkbox"/> 151 Medicare Act <input type="checkbox"/> 152 Recovery of Defaulted Student Loan (Excl. Veterans) <input type="checkbox"/> 153 Recovery of Overpayment of Veteran's Benefits <input type="checkbox"/> 160 Stockholders' Suits <input type="checkbox"/> 190 Other Contract <input type="checkbox"/> 195 Contract Product Liability <input type="checkbox"/> 196 Franchise REAL PROPERTY <input type="checkbox"/> 210 Land Condemnation <input type="checkbox"/> 220 Foreclosure <input type="checkbox"/> 230 Rent Lease & Ejectment <input type="checkbox"/> 240 Torts to Land <input type="checkbox"/> 245 Tort Product Liability <input type="checkbox"/> 290 All Other Real Property	TORTS PERSONAL INJURY <input type="checkbox"/> 310 Airplane <input type="checkbox"/> 315 Airplane Product Liability <input checked="" type="checkbox"/> 320 Assault, Libel & Slander <input type="checkbox"/> 330 Fed. Employers' Liability <input type="checkbox"/> 340 Marine <input type="checkbox"/> 345 Marine Product Liability <input type="checkbox"/> 350 Motor Vehicle <input type="checkbox"/> 355 Motor Vehicle Product Liability <input type="checkbox"/> 360 Other Personal Injury <input type="checkbox"/> 362 Personal Injury - Med Malpractice <input type="checkbox"/> 365 Personal Injury - Product Liability <input type="checkbox"/> 368 Asbestos Personal Injury Product Liability IMMIGRATION <input type="checkbox"/> 462 Naturalization Application <input type="checkbox"/> 463 Habeas Corpus - Alien Detainee <input type="checkbox"/> 465 Other Immigration Actions	TORTS PERSONAL PROPERTY <input type="checkbox"/> 370 Other Fraud <input type="checkbox"/> 371 Truth in Lending <input type="checkbox"/> 380 Other Personal Property Damage <input type="checkbox"/> 385 Property Damage - Product Liability BANKRUPTCY <input type="checkbox"/> 22 Appeal 28 USC 158 <input type="checkbox"/> 423 Withdrawal 28 USC 157 CIVIL RIGHTS <input type="checkbox"/> 441 Voting <input type="checkbox"/> 442 Employment <input type="checkbox"/> 443 Housing/Accommodations <input type="checkbox"/> 444 Welfare <input type="checkbox"/> 445 American with Disabilities - Employment <input type="checkbox"/> 446 American with Disabilities - Other <input type="checkbox"/> 440 Other Civil Rights	PRISONER PETITIONS <input type="checkbox"/> 510 Motions to Vacate Sentence Habeas Corpus <input type="checkbox"/> 530 General <input type="checkbox"/> 535 Death Penalty <input type="checkbox"/> 540 Mandamus/Other <input type="checkbox"/> 550 Civil Rights <input type="checkbox"/> 555 Prison Condition FORFEITURE / PENALTY <input type="checkbox"/> 610 Agriculture <input type="checkbox"/> 620 Other Food & Drug <input type="checkbox"/> 625 Drug Related Seizure of Property 21 USC 881 <input type="checkbox"/> 630 Liquor Laws <input type="checkbox"/> 640 R.R. & Truck <input type="checkbox"/> 650 Airline Regs <input type="checkbox"/> 660 Occupational Safety/Health <input type="checkbox"/> 690 Other	LABOR <input type="checkbox"/> 710 Fair Labor Standards Act <input type="checkbox"/> 720 Labor/Mgmt. Relations <input type="checkbox"/> 730 Labor/Mgmt. Reporting & Disclosure Act <input type="checkbox"/> 740 Railway Labor Act <input type="checkbox"/> 790 Other Labor Litigation <input type="checkbox"/> 791 Empl. Ret. Inc. Security Act PROPERTY RIGHTS <input type="checkbox"/> 820 Copyrights <input type="checkbox"/> 830 Patent <input type="checkbox"/> 840 Trademark SOCIAL SECURITY <input type="checkbox"/> 61 HIA (1395m) <input type="checkbox"/> 862 Black Lung (923) <input type="checkbox"/> 863 DIWC/DIWW 405(g) <input type="checkbox"/> 864 SSID Title XVI <input type="checkbox"/> 865 RSI (405(g)) FEDERAL TAX SUITS <input type="checkbox"/> 870 Taxes (U.S. Plaintiff or Defendant) <input type="checkbox"/> 871 IRS-Third Party 26 USC 7609
--	--	---	--	---	---

FOR OFFICE USE ONLY: Case Number: **CV11-05023**

AFTER COMPLETING THE FRONT SIDE OF FORM CV-71, COMPLETE THE INFORMATION REQUESTED BELOW.

CV-71 (05/08)

CIVIL COVER SHEET

 American LegalNet, Inc.
 www.FarmsWorkflow.com

Page 1 of 2

UNITED STATES DISTRICT COURT, CENTRAL DISTRICT OF CALIFORNIA
CIVIL COVER SHEETVIII(a). IDENTICAL CASES: Has this action been previously filed in this court and dismissed, remanded or closed? ☒ No ☐ Yes

If yes, list case number(s): _____

VIII(b). RELATED CASES: Have any cases been previously filed in this court that are related to the present case? ☒ No ☐ Yes

If yes, list case number(s): _____

Civil cases are deemed related if a previously filed case and the present case:

- (Check all boxes that apply)
- ☐ A. Arise from the same or closely related transactions, happenings, or events; or
- ☐ B. Call for determination of the same or substantially related or similar questions of law and fact; or
- ☐ C. For other reasons would entail substantial duplication of labor if heard by different judges; or
- ☐ D. Involve the same patent, trademark or copyright, and one of the factors identified above in a, b or c also is present.

IX. VENUE: (When completing the following information, use an additional sheet if necessary.)

- (a) List the County in this District: California County outside of this District: State if other than California; or Foreign Country, in which EACH named plaintiff resides.
- ☐ Check here if the government, its agencies or employees is a named plaintiff. If this box is checked, go to item (b).

County in this District:	California County outside of this District: State, if other than California; or Foreign Country
Los Angeles	

- (b) List the County in this District: California County outside of this District: State if other than California; or Foreign Country, in which EACH named defendant resides.
- ☐ Check here if the government, its agencies or employees is a named defendant. If this box is checked, go to item (c).

County in this District:	California County outside of this District: State, if other than California; or Foreign Country
Unknown	

- (c) List the County in this District: California County outside of this District: State if other than California; or Foreign Country, in which EACH claim arose.
- Note: In land condemnation cases, use the location of the tract of land involved.

County in this District:	California County outside of this District: State, if other than California; or Foreign Country
Los Angeles	

* Los Angeles, Orange, San Bernardino, Riverside, Ventura, Santa Barbara, or San Luis Obispo Counties

Note: In land condemnation cases, use the location of the tract of land involved

X. SIGNATURE OF ATTORNEY (OR PRO PER):

Steven Brower

Date June 14, 2011

Notice to Counsel/Parties: The CV-71 (JS-14) Civil Cover Sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law. This form, approved by the Judicial Conference of the United States in September 1974, is required pursuant to Local Rule 3-1 is not filed but is used by the Clerk of the Court for the purpose of statistics, venue and initiating the civil docket sheet. (For more detailed instructions, see separate instructions sheet.)

Key to Statistical codes relating to Social Security Cases:

Nature of Suit Code	Abbreviation	Substantive Statement of Cause of Action
861	HIA	All claims for health insurance benefits (Medicare) under Title 18, Part A, of the Social Security Act, as amended. Also, include claims by hospitals, skilled nursing facilities, etc., for certification as providers of services under the program. (42 U.S.C. 1935FF(b))
862	BL	All claims for "Black Lung" benefits under Title 4, Part B, of the Federal Coal Mine Health and Safety Act of 1969. (30 U.S.C. 923)
863	DIWC	All claims filed by insured workers for disability insurance benefits under Title 2 of the Social Security Act, as amended; plus all claims filed for child's insurance benefits based on disability. (42 U.S.C. 405(g))
863	DJWW	All claims filed for widows or widowers insurance benefits based on disability under Title 2 of the Social Security Act, as amended. (42 U.S.C. 405(g))
864	SSID	All claims for supplemental security income payments based upon disability filed under Title 16 of the Social Security Act, as amended.
865	RSI	All claims for retirement (old age) and survivors benefits under Title 2 of the Social Security Act, as amended. (42 U.S.C. (g))

CV-71 (05/08)

CIVIL COVER SHEET

Page 2 of 2

Amgen LegalNet, Inc.
www.FilingWorkshop.com

1 BUCHALTER NEMER
A Professional Corporation
2 STEVEN BROWER (SBN: 93568)
Email: sbrower@buchalter.com
3 18400 Von Karman, Suite 800
Irvine, CA 92612
4 Telephone: (714) 549-5150
Facsimile: (949) 224-6410
5

6 Attorneys for Plaintiff Benjamin D. Chung, M.D.
7

8 **UNITED STATES DISTRICT COURT**
9 **CENTRAL DISTRICT OF CALIFORNIA**
10

11 Benjamin D. Chung, M.D.,

Case No. 11-cv-05023 ODW (Ex)

12 Plaintiff,

**EX PARTE APPLICATION
(UNOPPOSED) FOR PERMISSION TO
CONDUCT LIMITED DISCOVERY
[FRCP 26(d)]; DECLARATION OF
STEVEN BROWER**

13 vs.

14 Does 1-10,

15 Defendants.
16

17 **SUMMARY OF REQUEST**

18 Plaintiff Benjamin D. Chung, M.D. ("Dr. Chung") hereby requests early
19 discovery (FRCP 26(d)) to serve a subpoena on the non-party operator of the
20 website where a defamatory comment was made about Dr. Chung, so that the
21 identity of the defendant(s) can, hopefully, be obtained.

22 **REQUEST**

23 Dr. Chung is a medical doctor, duly licensed in the State of California and
24 Board Certified in Gastroenterology and Internal Medicine. At all relevant times
25 herein he resided and practiced medicine primarily within the Central District.

26 As set forth in the Complaint, in or around February, 2011, Dr. Chung
27 discovered an anonymous "review" of himself posted on a website known as
28

1 Vitals.com. That posting, dated February 18, 2011 ("Offending Post"), in reference
2 to Dr. Chung states:

3 My father had an Advanced Directive which stated that he did not
4 want any aggressive treatments during his life as he was 90 years old
5 and had lived a long full life. This "doctor" performed over 10
6 colonoscopies on my father in less than 6 months and God only knows
7 how many stomach endoscopies. He is callous and ruthless and has no
8 bedside manner. I am reporting him to Medicare and the California
9 Medical Board. Apparently, this "doctor" has been known in
10 Riverside for many years to be one of the most fraudulent physicians
11 in practice. He performs countless procedures which are not medically
12 necessary, and this included multiple endoscopic procedures on my
13 father.

14 Dr. Chung contends that the Offending Post contains false and disparaging
15 statements of fact about the professional services provided by Dr. Chung, including,
16 but not limited to, a statement that he committed a criminal act (i.e. – battery) on a
17 patient, that he performs procedures which are not medically necessary and that he
18 has been known as "one of the most fraudulent physicians in practice."

19 Although the statement is phrased as though it comes from a family member
20 of a patient, Dr. Chung believes that the Offending Statement may have been posted
21 by another physician with malicious intent.

22 Prior to filing this case Dr. Chung, through his counsel, asked Vitals.com
23 about its policy regarding content and retention of identifying information about
24 authors. The response, a copy of which is attached hereto, indicated that Vitals.com
25 would provide the information, which it retains regarding the identification of the
26 person who wrote the comment, upon receipt of a subpoena.
27
28

1 The defendants in this matter are currently listed as "Does" because Dr.
2 Chung does not yet have information sufficient to identify the author of the
3 Offending Post.

4 FRCP 26(d) provides that a party may initiate discovery, prior to the 26(f)
5 meeting of counsel, upon Order of the Court. Dr. Chung would, therefore, request
6 this Court to authorize, pursuant to FRCP 26(d), discovery prior to the meeting of
7 counsel – specifically, to authorize Dr. Chung's counsel to issue a subpoena to
8 Vitals.com requesting information about the identity of the author of the Offending
9 Post.

10
11 DATED: June 22, 2011

BUCHALTER NEMER
A Professional Corporation

12
13 By: _____

14 STEVEN BROWER
Attorneys for Plaintiff
15 Dr. Benjamin Chung
16
17
18
19
20
21
22
23
24
25
26
27
28

DECLARATION OF STEVEN BROWER

I, Steven Brower, declare:

1. I am an attorney duly licensed to practice before the courts of the State of California. I am employed by Buchalter Nemer which is counsel of record to Dr. Chung. The facts stated herein are of my own personal knowledge and if called upon to testify I could and would competently do so.

2. Prior to the filing of this action I corresponded with Vitals.com in an effort to determine what information they retain regarding anonymous posts and how I could best get that information from them. Attached hereto as Exhibit "A" is a true and accurate copy of the email exchange in which they indicate that they do retain certain information and will produce the information in response to a subpoena.

I declare, under penalty of perjury, that the foregoing is true and correct.
Executed on June 22, 2011 at Mammoth Lakes, California.

_____/s/ by ECF

Steven Brower

Brower, Steven

From: VitalsSupport [support@vitals.com]
Sent: Wednesday, March 23, 2011 1:09 PM
To: Brower, Steven
Subject: Re: Corrections and Obtaining Information

Mr. Brower,

Thank you for contacting Vitals, we appreciate your feedback and we'll be happy to answer your questions regarding this matter.

Consumer ratings/comments are accepted into our system as statements of *opinion* and as such we are unable to evaluate them for any level of reported accuracy/inaccuracy, as we're sure you're aware, statements of opinion can not technically be validated or invalidated and we do not have any mechanism which would allow us to do so.

Even in a statement by a patient which alleges a factual account of medial care which a doctor may disagree with, we have no mechanism by which we can validate such statements and we opt not to attempt such evaluation.

It is our policy to not participate in the modification or removal of any ratings/comments where those ratings do not contain profanity, vulgarity, racism, sexism, threats of violence or other material which could be considered as inappropriate or explicit material.

If the rating in question contains any of the above violations of our terms of use/language policy please direct us to it, we will be more than willing to review it and act accordingly where we are able.

Please note that all doctors who register with our service obtain access to comment management tools that allow them at their discretion to remove up to two comments from their profile and the ability to respond to an unlimited number of comments in addition to that. If they have not already your client can register by visiting www.vitals.com/doctorjoin

While all users who visit Vitals must agree to our terms of use, there is no process by which a user "registers" for our service. The inclusion of any personally identifying information such as name, email, etc. is optional during the rating process, however we do record the date, time and IP address for every rating posted. While that information can not be distributed on request alone it is our policy to cooperate with any valid, lawfully issued subpoena requesting that data.

Subpoenas can be issued to "Custodian of Records for Vitals" and sent to:

MDx Medical Inc.
Attn: Legal Department
1200 Wall Street West
5th Floor
Lyndhurst, NJ
07071

6/22/2011

We hope that this information has been helpful. Please don't hesitate to let us know if you have any other questions.

Thank You.

Frank
Customer Care Manager
Vitals.com

On Wed, Mar 23, 2011 at 2:56 PM, Brower, Steven <sbrower@buchalter.com> wrote:

The purpose of this email is to determine your policy on a couple of related legal issues. I am willing to accept the responses (if so designated) on an "off the record - not for attribution" basis. My purpose here is not to play word games or to quote you - rather, I want to know, informally, whether these types of issues can, or cannot, be resolved without court intervention.

We represent a California doctor who is referred to on the vitals.com website. There is only one comment on his profile. It would appear that the comment includes untrue representations of fact, not merely disputed statements of opinion. What is your policy regarding correction/take down of false factual information?

Further, our client has reason to believe that the comment was not actually posted by a "patient's daughter" (which is what appears), but instead was posted by another physician for reasons unrelated to patient care. If the poster was *not* a registered user of your site, what is your policy regarding our obtaining the IP address, or whatever other potentially identifying information was retained by your system regarding the source of the post (it was posted in 2011).

Please feel free to call me to discuss this matter.

Steven Brower | Shareholder | **BuchalterNemer**, A Professional Corporation | 18400 Von Karman Avenue, Suite 800 | Irvine, CA 92612-0514 | Direct Dial: (714) 549-5150 | Cell Phone: (714) 244-6545 | Direct Fax: (949) 224-6410 | Switchboard: (949) 760-1121 | sbrower@buchalter.com | www.buchalter.com | [Bio](#)

Notice To Recipient: This e-mail is meant for only the intended recipient of the transmission, and may be a communication privileged by law. If you received this e-mail in error, any review, use, dissemination, distribution, or copying of this e-mail is strictly prohibited. Please notify us immediately of the error by return e-mail and please delete this message and any and all duplicates of this message from your system. Thank you in advance for your cooperation. For additional policies governing this e-mail, please see http://www.buchalter.com/bt/index.php?option=com_content&task=view&id=151&Itemid=129.

IRS Circular 230 Disclosure: In order to comply with requirements imposed by the Internal Revenue Service, we inform you that any U.S. tax advice contained in this communication (including any attachments) is not intended to be used, and cannot be used, for the purpose of (i) avoiding penalties under the Internal Revenue Code or (ii) promoting, marketing, or recommending to another party any transaction or matter addressed herein.

6/22/2011

6/22/2011

1 BUCHALTER NEMER
A Professional Corporation
2 STEVEN BROWER (SBN: 93568)
Email: sbrower@buchalter.com
3 18400 Von Karman, Suite 800
Irvine, CA 92612
4 Telephone: (714) 549-5150
Facsimile: (949) 224-6410
5

6 Attorneys for Plaintiff Benjamin D. Chung, M.D.
7

8 UNITED STATES DISTRICT COURT
9 CENTRAL DISTRICT OF CALIFORNIA
10

11 Benjamin D. Chung, M.D.,

12 Plaintiff,

13 vs.

14 Does 1-10,

15 Defendants.
16

Case No. 11-cv-05023 ODW (Ex)

**EX PARTE APPLICATION
(UNOPPOSED) FOR PERMISSION TO
OBTAIN CUSTOMER INFORMATION
FOR IP ADDRESS; DECLARATION
OF STEVEN BROWER**

17 **SUMMARY OF REQUEST**

18 Plaintiff Benjamin D. Chung, M.D. ("Dr. Chung") previously obtained an
19 Order from this court (Docket #6) allowing him to serve a subpoena to obtain
20 information from Vitals.com, which "hosted" the posting of the Offending Post.

21 Non-party Vitals.com promptly responded to the subpoena and provided
22 information about the source of the Offending Post. The information provided
23 included the IP address (a numeric address, not an email address) which was used
24 by the individual who published the Offending Post. Further research shows that
25 the IP Address was one of a large block of addresses owned by Charter
26 Communications, a major provider of internet services.

27 Charter has indicated that it will provide information about the identify of the
28 subscriber using that IP Address upon receipt of a subpoena accompanied by an

1 appropriate court order. Dr. Chung hereby requests an Order of this court
2 authorizing such further discovery.

3 **REQUEST**

4 Dr. Chung is a medical doctor, duly licensed in the State of California and
5 Board Certified in Gastroenterology and Internal Medicine. At all relevant times
6 herein he resided and practiced medicine primarily within the Central District.

7 As set forth in the Complaint, in or around February, 2011, Dr. Chung
8 discovered an anonymous "review" of himself posted on a website known as
9 Vitals.com. That posting, dated February 18, 2011 ("Offending Post"), in reference
10 to Dr. Chung states:

11 My father had an Advanced Directive which stated that he did not
12 want any aggressive treatments during his life as he was 90 years old
13 and had lived a long full life. This "doctor" performed over 10
14 colonoscopies on my father in less than 6 months and God only knows
15 how many stomach endoscopies. He is callous and ruthless and has no
16 bedside manner. I am reporting him to Medicare and the California
17 Medical Board. Apparently, this "doctor" has been known in
18 Riverside for many years to be one of the most fraudulent physicians
19 in practice. He performs countless procedures which are not medically
20 necessary, and this included multiple endoscopic procedures on my
21 father.

22 Dr. Chung contends that the Offending Post contains false and disparaging
23 statements of fact about the professional services provided by Dr. Chung, including,
24 but not limited to, a statement that he committed a criminal act (i.e. – battery) on a
25 patient, that he performs procedures which are not medically necessary and that he
26 has been known as "one of the most fraudulent physicians in practice."

27 Although the statement is phrased as though it comes from a family member
28 of a patient, Dr. Chung believes that the Offending Statement may have been posted

1 by another physician with malicious intent. (Vitals.com, after receiving the
2 subpoena, conducted a *sua sponte* review of the Offending Post. Because it
3 purports to be from a family member, and not from a patient, it violates the terms
4 and conditions of Vitals.com and Vitals.com has now removed the Offending Post.)

5 The defendants in this matter are currently listed as “Does” because Dr.
6 Chung does not yet have information sufficient to identify the author of the
7 Offending Post.

8 FRCP 26(d) provides that a party may initiate discovery, prior to the 26(f)
9 meeting of counsel, upon Order of the Court. Dr. Chung would, therefore, request
10 this Court to authorize, pursuant to FRCP 26(d), further discovery prior to the
11 meeting of counsel – specifically, to authorize Dr. Chung’s counsel to issue a
12 subpoena to Charter Communications requesting identification of the subscriber
13 associated with the IP Address provided by Vitals.com.

14 Disclosure of records regarding customers, by electronic communications
15 services, such as Charter Communications, are subject to the requirements in the
16 Stored Wire and Electronic Communications Act. The relevant section here is 18
17 USC § 2702, which provides in relevant part:

18 (a) Prohibitions – Except as provided in subsection (b) or (c) –

19 . . .

20 (c) Exceptions for Disclosure of Customer Records – A provider
21 described in subsection (a) may divulge a record or other information
22 pertaining to a subscriber to or a customer of such service (not
23 including the contents of communications covered by subsection (a)(1)
24 or (a)(2)) –

25 . . .

26 (6) to any person other than a governmental entity.
27
28

1 Dr. Chung seeks only the information about the identity and contact
2 information for the customer/subscriber using the IP Address, and not the contents
3 of any email. Therefore, pursuant to 2702(c)(6), his request is appropriate.

4
5 DATED: July 16, 2011

BUCHALTER NEMER
A Professional Corporation

6
7 By: _____

STEVEN BROWER
Attorneys for Plaintiff
Dr. Benjamin Chung

DECLARATION OF STEVEN BROWER

I, Steven Brower, declare:

1. I am an attorney duly licensed to practice before the courts of the State of California. I am employed by Buchalter Nemer which is counsel of record to Dr. Chung. The facts stated herein are of my own personal knowledge and if called upon to testify I could and would competently do so.

2. Pursuant to this court's prior order (Docket #6), I served a subpoena on Vitals.com. The response received from Vitals.com, in response to the subpoena, is attached hereto as Exhibit "A." That response includes a numeric IP Address which was used to publish the Offending Post.

3. I have determined (by use of an information tool referred to as "Whois") that the IP address is part of a "block" of addresses assigned to Charter Communications.

4. I have spoken with a paralegal in the subpoena unit of Charter Communications. I was advised that the best way to get expedited attention is to provide them (at a published fax number) with a subpoena accompanied by a Court Order.

5. This Order is being requested for a proper purpose, which is to obtain information about the person who published the Offending Post.

I declare, under penalty of perjury, that the foregoing is true and correct.
Executed on July 16, 2011 at Laguna Hills, California.

/s/ by ECF

Steven Brower

Steven Brower

From: VitalsSupport <support@vitals.com>
Sent: Friday, July 01, 2011 11:35 AM
To: Brower, Steven
Subject: Re: Subpoena re: Dr. Benjamin Chung
Attachments: Vitals Consumer Ratings Benjamin D Chung.pdf

Mr. Brower,

Attached you will find all of the data which we have related to the rating in question.

Additionally, in your initial correspondence you did not identify Dr. Chung and we were unable to review the rating in question.

Please note that the management of Vitals.com has determined that the rating/comment violates our terms of use (we do not permit ratings where the user indicates that they are not a patient) and they have removed it at their sole and appropriate discretion.

If you should need any further assistance, please feel free to email us at support@vitals.com

Thank you,

Customer Care

Vitals.com

On Fri, Jul 1, 2011 at 2:36 AM, Brower, Steven <sbrower@buchalter.com> wrote:

> We would appreciate receiving the information as soon as possible. As you
> saw, the Magistrate Judge specifically authorized us to obtain this
> information on an expedited basis.

>

>

> Steven Brower | Shareholder | BuchalterNemer, A Professional Corporation |
> 18400 Von Karman Avenue, Suite 800 | Irvine, CA 92612-0514 | Direct Dial:
> (714) 549-5150 | Cell Phone: (714) 244-6545 | Direct Fax: (949) 224-6410 |
> Switchboard: (949) 760-1121 | sbrower@buchalter.com | www.buchalter.com

>

>

>

> From: VitalsSupport [mailto:support@vitals.com]

> Sent: Tuesday, June 28, 2011 11:36 AM

> To: Brower, Steven

> Subject: Re: Subpoena re: Dr. Benjamin Chung

>

> Mr. Brower,

>

> Per your electronic transmission of this subpoena, which we are willing to

> accept by this method, would you/your client similarly be willing to accept
> the data requested in the subpoena via electronic transmission (fax/email),
> or do you need us to send physical copies?

>
> Customer Care
> Vitals.com

>
> On Fri, Jun 24, 2011 at 7:02 PM, Brower, Steven <sbrower@buchalter.com>
> wrote:

>>
>> Pursuant to your earlier email (which is part of the attached Ex
>> Parte Application), please find the following:

>>
>> 1. Subpoena for any information regarding the identity of a specified
>> post (see the application for details).

>>
>> 2. A copy of our ex parte application, which has the identifying
>> information (name of doctor, date of post, full text of post) and which also
>> has a copy of your earlier email stating that, in response to a valid
>> subpoena, you will provide the IP Address and any other information on file.

>>
>> 3. A copy of the Court Order which we obtained authorizing forthwith
>> service of this subpoena.

>>
>> If necessary we will pay to have you personally served on Monday. Of
>> course, we would prefer to avoid that expense and inconvenience and would
>> appreciate your email confirmation that you will respond without requiring
>> formal service.

>>
>> Steven Brower | Shareholder
>> Buchalter Nemer | 18400 Von Karman, Suite 800, Irvine, CA 92612
>> Direct: (714) 549-5150 | Fax: (949) 224-6410

>>
>> Notice To Recipient: This e-mail is meant for only the intended recipient
>> of the transmission, and may be a communication privileged by law. If you
>> received this e-mail in error, any review, use, dissemination, distribution,
>> or copying of this e-mail is strictly prohibited. Please notify us
>> immediately of the error by return e-mail and please delete this message and
>> any and all duplicates of this message from your system. Thank you in
>> advance for your cooperation. For additional policies governing this e-mail,
>> please see
>> http://www.buchalter.com/bt/index.php?option=com_content&task=view&id=151&Itemid=129.

>>
>> IRS Circular 230 Disclosure: In order to comply with requirements imposed
>> by the Internal Revenue Service, we inform you that any U.S. tax advice
>> contained in this communication (including any attachments) is not intended
>> to be used, and cannot be used, for the purpose of (i) avoiding penalties
>> under the Internal Revenue Code or (ii) promoting, marketing, or
>> recommending to another party any transaction or matter addressed herein.

>
> Notice To Recipient: This e-mail is meant for only the intended recipient of
> the transmission, and may be a communication privileged by law. If you
> received this e-mail in error, any review, use, dissemination, distribution,
> or copying of this e-mail is strictly prohibited. Please notify us
> immediately of the error by return e-mail and please delete this message and
> any and all duplicates of this message from your system. Thank you in
> advance for your cooperation. For additional policies governing this e-mail,
> please see
> http://www.buchalter.com/bt/index.php?option=com_content&task=view&id=151&Itemid=129.

>
> IRS Circular 230 Disclosure: In order to comply with requirements imposed by

- > the Internal Revenue Service, we inform you that any U.S. tax advice
- > contained in this communication (including any attachments) is not intended
- > to be used, and cannot be used, for the purpose of (i) avoiding penalties
- > under the Internal Revenue Code or (ii) promoting, marketing, or
- > recommending to another party any transaction or matter addressed herein.

<<Vitals Consumer Ratings Benjamin D Chung.pdf>>

Feedback Detail							
	Created	Is Deleted	IP Address	Status	Overall Rating	Reviewer	Email
658159	2011-02-19 22:58:43	Y [Edit]	66.214.142.200	A [Edit]	1		
Review Title		Comments	My father had an Advanced Directive which stated that he did not want any aggressive treatments during his life as he was 90 years old and had lived a long full life. This "doctor" performed over 10 colonoscopies on my father in less than 6 months and God-only-knows how many stomach endoscopies. He is callous and ruthless and has no bedside manner. I am reporting him to Medicare and the California Medical Board.Apparently this "doctor" has been known in Riverside for many years to be one of the most fraudulent physicians in practice. He performs countless procedures which are not medically necessary, and this included multiple endoscopic procedures on my father.			Response	
Question	Question						Response
81688	Following up as needed after my visit						1
81687	Spending enough time with me						1
81686	Bedside manner (caring)						1
81685	Accuracy in diagnosing a problem						1
81684	Courtesy and professionalism of office staff						1
81683	Waiting time during a visit						1
81682	Ease in getting an appointment						1

1
2
3
4
5
6
7
8 UNITED STATES DISTRICT COURT
9 CENTRAL DISTRICT OF CALIFORNIA
10

11 BENJAMIN D. CHUNG, M.D.,) NO. CV 11-5023-ODW (Ex)
12)
12 Plaintiff,)
13)
13 v.) ORDER
14)
14 DOES 1-10,)
15)
15 Defendants.)
16)
16 _____)
17

18 BACKGROUND AND PROCEEDINGS
19

20 Plaintiff, a gastroenterologist and internist, filed the
21 Complaint on June 14, 2011. The Complaint concerns an alleged
22 February, 2011 anonymous post on a website known as vitals.com.
23 The post, which purported to review Plaintiff's performance as a
24 physician, reportedly stated:
25

26 My father had a Advanced Directive which stated that he did
27 not want any aggressive treatments during his life as he was
28 90 years old and had lived a long full life. This "doctor"

1 performed over 10 colonoscopies on my father in less than
2 6 months and God knows how many stomach endoscopies. He is
3 callous and ruthless and has no bedside manner. I am
4 reporting him to Medicare and the California Medical Board.
5 Apparently, this "doctor" has been known in Riverside for
6 many years to be one of the most fraudulent physicians in
7 practice. He performs countless procedures which are not
8 medically necessary, and this included multiple endoscopic
9 procedures on my father.

10
11 The Complaint alleges a federal law claim for trade libel and a
12 state law claim for defamation against Defendants "Does 1-10." The
13 Complaint alleges on information and belief that Defendants Does 1-10,
14 the "authors, editors and/or publishers" of the post, are physicians
15 who compete with Plaintiff.

16
17 On June 22, 2011, Plaintiff filed an *ex parte* application for
18 permission to issue a subpoena to vitals.com requesting information
19 concerning the identity of the author of the post. The Court granted
20 this application by Minute Order filed June 23, 2011. Plaintiff
21 subsequently served a subpoena on vitals.com and learned that the post
22 originated from a particular numeric IP address owned by Charter
23 Communications, a provider of Internet services. By *ex parte*
24 application filed July 17, 2011, Plaintiff sought permission to serve
25 a subpoena on Charter Communications seeking the identity and contact
26 information for the customer/subscriber who used the particular
27 numeric IP address. The Court granted this application by Order filed
28 July 18, 2011, and Plaintiff subsequently served on Charter

1 Communications a subpoena issued from the United States District Court
2 for the Eastern District of Missouri.

3
4 On August 2, 2011, "Real Party in Interest" "John Doe" specially
5 appeared through counsel and filed a "Motion for an Order Quashing
6 Subpoena Duces Tecum and for a Protective Order" ("the Motion"). On
7 August 17, 2011, John Doe and Plaintiff filed a "Joint Stipulation
8 Pursuant to Local Rule 37-2.1." By the Motion, John Doe seeks to
9 prevent the disclosure of the subpoenaed subscriber information,
10 specifically John Doe's name, address, telephone number, and date of
11 birth. The Court heard oral argument on September 2, 2011.

12
13 Following oral argument, the Court invited John Doe and Plaintiff
14 to submit additional evidence pertaining to the Motion. On
15 September 9, 2011, John Doe submitted certain documents for *in camera*
16 review. Those documents are ordered filed *under seal* to preserve the
17 record. Also on September 9, 2011, Plaintiff submitted certain
18 documents for *under seal* filing. Those documents were ordered filed
19 *under seal* by Order dated September 12, 2011. The Court has reviewed
20 and considered all of the documents submitted on September 9, 2011,
21 all of the documents previously filed, and the September 2, 2011
22 arguments of counsel.

23 24 DISCUSSION

25
26 For the reasons discussed below, the Motion is denied. To the
27 extent the Motion seeks to quash or modify the subpoena, this denial
28 is without prejudice. To the extent the Motion seeks a protective

1 order or reconsideration of the Order filed July 18, 2011, this denial
2 is with prejudice.

3
4 The only court authorized to entertain a motion to quash or
5 modify a subpoena is the court from which the subpoena issued. See
6 S.E.C. v. CMKM Diamonds, Inc., ___ F.3d ___, 2011 WL 3795074 (9th Cir.
7 Aug. 26, 2011). The subpoena was issued from the United States
8 District Court for the Eastern District of Missouri. Therefore, to
9 the extent the Motion seeks to quash or modify this subpoena, the
10 Motion is denied without prejudice for lack of jurisdiction.

11
12 In the present circumstance, however, this Court retains
13 jurisdiction to issue a protective order concerning the subpoena.
14 See, e.g., Manufacturer Direct, LLC v. Directbuy, Inc., 2007 WL 496382
15 (N.D. Ind. Feb. 12, 2007); Wells v. GC Services, LP, 2007 WL 1068222
16 (N.D. Cal. Apr. 10, 2007); but see Multiquip, Inc. v. Water Management
17 Systems LLC, 2009 WL 5322946, at *1 n.1 (D. Idaho Dec. 29, 2009); see
18 also Schwarzer, Tashima and Wagstaffe, Federal Civil Procedure Before
19 Trial, § 11:1161 (2011) ("Protective orders are ordinarily sought from
20 the court in which the action is pending"). This Court also retains
21 jurisdiction to reconsider and modify interlocutory orders, including
22 the Order filed July 18, 2011. See generally Schwarzer, Tashima and
23 Wagstaffe, Federal Civil Procedure Before Trial, § 12:158 (2011).
24 Neither Plaintiff nor John Doe has objected to this Court's
25 consideration of the merits of the Motion.

26
27 John Doe argues that the "Stored Communications Act" prevents a
28 private party from subpoenaing subscriber information for use in a

1 civil action. See 18 U.S.C. § 2701 et seq. This argument must be
2 rejected. The Stored Communications Act distinguishes between
3 subscriber information and the contents of communications. See
4 18 U.S.C. § 2702. With regard to subscriber information, the Act does
5 not prohibit the disclosure of such information "to any person other
6 than a government entity." 18 U.S.C. § 2702(c)(6); see First Time
7 Videos, LLC v. Does 1-500, 2011 WL 3498227, at *4 (N.D. Ill. Aug. 9,
8 2011). Plaintiff is not a government entity.¹

9
10 John Doe also invokes the First Amendment.² There exists a First
11 Amendment right to speak anonymously. See, e.g., McIntyre v. Ohio
12 Elections Commission, 514 U.S. 334, 347, 357 (1995) (anonymous speech
13 "is not a pernicious, fraudulent practice, but an honorable tradition
14 of advocacy and of dissent. Anonymity is a shield from the tyranny of
15 the majority"). The First Amendment applies to speech on the
16 Internet. See Reno v. ACLU, 521 U.S. 844, 870 (1997).

17
18 The First Amendment right to speak anonymously comprehends a
19 "qualified privilege" of the speaker to remain anonymous. See, e.g.,
20 USA Technologies, Inc. v. Doe, 713 F. Supp. 2d 901, 906 (N.D. Cal.

21
22 ¹ As discussed at oral argument, the Cable Act, which
23 involves the transmission of video programming or other
24 programming services, has no application to the present dispute.
See 47 U.S.C. § 522.

25 ² John Doe does not appear to invoke the Fourth
26 Amendment. In any event, there exists no Fourth Amendment-
27 protected expectation of privacy in subscriber information
28 furnished to an Internet service provider. See, e.g., United
States v. Forrester, 512 F.3d 500 (9th Cir.), cert. denied, 129
S. Ct. 249 (2008); United States v. Perrine, 518 F.3d 1196 (10th
Cir. 2008).

2010). Particularly on the Internet, where the potential audience is vast and where a post can become virtually indelible, anonymous posts can be powerful vehicles for character assassination and unscrupulous business competition. Such posts can inflict grievous harm on innocent targets while leaving those targets without effective recourse. On the other hand, the right to speak anonymously on the Internet would essentially disappear if the target of any posted criticism could discover the identity of the poster merely by filing a meritless lawsuit and then subpoenaing the poster's Internet service provider.³

In an Order filed January 7, 2011, the Ninth Circuit discussed the "variety of standards" employed by federal district and state courts "to benchmark whether an anonymous speaker's identity should be revealed." In re Anonymous Online Speakers, 2011 WL 61635, at *5 (9th Cir. Jan. 7, 2011). The Ninth Circuit observed:

A number of courts have required plaintiffs to make at least a prima facie showing of the claim for which this plaintiff seeks the disclosure of the anonymous speaker's identity. .

. . The lowest bar that courts have used is the motion to dismiss or good faith standard. . . . Other courts have

³ Although the motion papers suggest that the subscriber might not be the author of the subject post (which would call into question the subscriber's standing to assert the author's First Amendment right), counsel for John Doe represented during the September 2, 2011 hearing that John Doe is both the subscriber of the subject IP address and the author of the subject post. The documents submitted by John Doe on September 9, 2011 confirm that John Doe is both the subscriber and the author.

1 relied on a standard that falls somewhere between the motion
2 to dismiss and the prima facie standards. . . . [T]he most
3 exacting standard . . . requires plaintiffs to be able to
4 survive a hypothetical motion for summary judgment . . .
5 Id. (citations omitted).

6
7 Without condemning or endorsing any of these standards, the Ninth
8 Circuit suggested that "the nature of the speech should be a driving
9 force in choosing a standard by which to balance the rights of
10 anonymous speakers in discovery disputes." Id. at *6. For example,
11 anonymous political speech usually should receive greater protection
12 than anonymous commercial speech. Id. In a recent unpublished
13 decision, the Ninth Circuit also suggested that the district court
14 sometimes should ascertain the anonymous speaker's identity, by *in*
15 *camera* review, before "settling upon a standard for disclosure." See
16 SI03, Inc. Bodybuilding.com, LLC, 2011 WL 2565618, at *1, n.1 (9th
17 Cir. June 29, 2011).

18
19 In the present case, this Court invited John Doe to disclose his
20 identity *in camera* (potentially to guide the Court's selection of an
21 appropriate "standard for disclosure"). The Court also invited
22 Plaintiff to submit evidence in support of Plaintiff's claims (in the
23 event the Court were to select the "prima facie" standard or the
24 "hypothetical motion for summary judgment" standard).

25
26 John Doe's submission indicates that a standard less exacting
27 than the "hypothetical motion for summary judgment" standard would be
28 appropriate in the present case. Ultimately, however, the issue of

1 the appropriate standard has become academic, because the application
2 of any of the standards requires the denial of the Motion.
3 Plaintiff's Complaint would survive a motion to dismiss, and there is
4 no evidence Plaintiff is pursuing the action in bad faith. With
5 respect to the defamation claim, Plaintiff's submission makes a prima
6 facie showing and a showing sufficient to survive a hypothetical
7 motion for summary judgment. Although the adequacy of Plaintiff's
8 showing with respect to the trade libel claim is less certain, the
9 showing (in conjunction with John Doe's submission) appears to warrant
10 additional discovery concerning the claim rather than the effective
11 denial of the claim. Moreover, even if the trade libel claim were
12 dismissed, as under a summary judgment standard, this Court still
13 would retain the discretion to exercise supplemental jurisdiction over
14 the defamation claim. See, e.g., Hunt Skansie Land LLC v. City of Gig
15 Harbor, 2010 WL 2650502, at *3 (W.D. Wash. July 1, 2010); see
16 generally 28 U.S.C. § 1367. Thus, the result of the present Motion
17 would remain the same. Plaintiff has demonstrated a need for the
18 discovery sufficient to counterbalance the infringement of John Doe's
19 qualified First Amendment right to speak anonymously. See In re
20 Anonymous Speakers, 2011 WL 61635, at *4.

21 ///

22 ///

23 ///

24 ///

25 ///

26 ///

27 ///

28 ///

