



CACJ REMEMBERS SUSAN B. JORDAN

June 21, 1941–May 29, 2009

Page 12

TIPS & TECHNIQUES

Page 21

**The Internet and
Social Networks as Evidence**

By Charles M. Sevilla



Page 43

**The NAS Report
Strengthening Forensic Science in the
United States: A Path Forward**

By Jennifer Friedman

CACJ

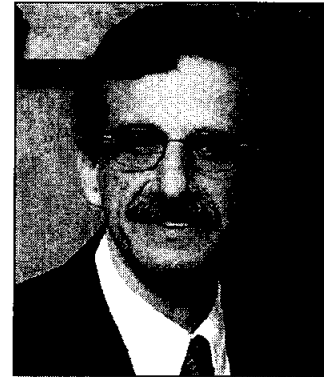
FORUM

California Attorneys
for Criminal Justice
2009 ♦ Volume 36, No. 2

TIPS & TECHNIQUES

The Internet and Social Networks: Emerging Investigative, Evidentiary, Ethical and Legal Issues

By Charles Sevilla*



CACJ Past President Charles M. Sevilla is now in private practice in San Diego.

When drug enforcement agents began investigating Ryan R[], they looked him up on MySpace. The first thing they reportedly found was a photograph of R[] standing in a room, surrounded by marijuana plants. His name — viewable to anyone with a MySpace account — was “1cashcrop,” and he declared his heroes are, “The Farmers from Humboldt who give to the people ...” On Tuesday, the 29-year-old R[] was one of 15 suspects arrested in a countywide raid conducted by Humboldt County Drug Task Force agents investigating an alleged commercial marijuana growing ring. And, according to drug task force Commander Jack Nelsen, those photos will likely be used as evidence against him in court.¹

A wide-spread, surging phenomena of social networking has taken hold of peoples’ communications. Estimates are that over 80% of young people have an internet presence on a social network. Facebook² and MySpace.com, the two most popular, boast of sixty million registered participants each.³

The social networks are extremely popular and heavily used. In one month, Facebook gets over one billion hits on its sites. MySpace states that the average user spends about

400 minutes a month on their site.⁴ Each participant invites “friends” to regularly connect to his/her site. For example, President Barack Obama has over one million friends on his MySpace profile. See <http://www.myspace.com/barackobama>. In order to look for any person or entity on Facebook, you have to join. In searching a profile of a defendant’s defense fund site, I joined and created a private profile (see below).

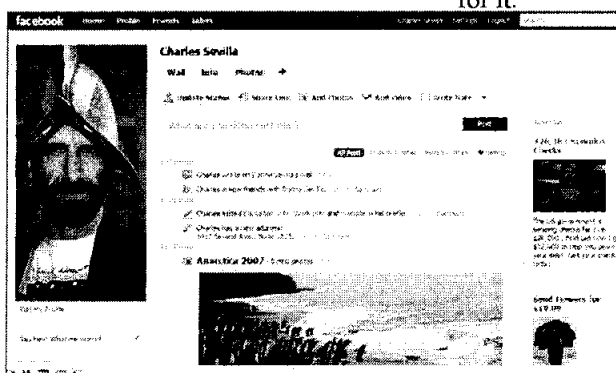
Young and old participate and the cyberworld of social networks is one of the most popular means of social interaction. At the same time, these networks are providing law enforcement and private investigators with leads on developing important information about suspects, jurors, employment and college applicants, and witnesses. Although by no means restricted to the young, the vast majority of users are between 14 and 30. Members of these networks post

personal information publicly. Others post the bulk of their information privately so that only invited “friends” may view and participate in communications. Communications may involve friends emailing or just posting comments on the host’s site (called posting on the “wall.”) The host’s site, or profile, may, and often does, include detailed personal information about himself/herself. This personal information has made the networks routine sources for investigation of witnesses.

A. Examples of Forensic Use of Social Internet Services

Law enforcement investigators now routinely check these networks (or just Google the name of the person) for information about suspects, witnesses and jurors.⁵ Stories abound where young people place incriminating information on the networks and pay a huge adverse consequence for it.

- When the son of a former state politician was recently arrested for a stabbing murder in San Diego, MySpace entries were provided to the police to help track the alleged killers. At the bail hearing, the defense presented numer-



ous testimonials on the character of one of the defendants. The prosecution responded by showing the court pictures from the defendant's MySpace page showing a frog being stabbed and another with an uplifted knife aimed at a kitten. A picture is worth a 1,000 words.⁶

- When police shot and killed a young black man in St. Petersburg, Florida (a 17 year old with no criminal record) the following appeared in the local paper to besmirch the young man's name based solely upon his internet postings:

Though he had had no brushes with the law before a police officer fatally shot him this weekend, Javon Dawson had taken on the persona of a street thug on his MySpace page. On Saturday night, Dawson, 17, was spotted firing a gun into the air outside the Shining Light Masonic Lodge, where there was a graduation party. He got into a confrontation with St. Petersburg police officer Terrence Nemeth, with Nemeth telling him to put down the weapon, and Dawson running off, pointing his gun at Nemeth as he fled before Nemeth fired, police said. On his MySpace page, Dawson takes on the persona of a violence-prone street thug in his featured video. With music blaring in the background and with Dawson caught mostly in silhouette, he talks threateningly to his imaginary audience. Repeatedly spouting profanities and a racial epithet used commonly among African-American gangsters, Dawson throws punches as a sign of his street bravado. He then picks up a gun or a facsimile of one and points it at the camera, threatening to use it unless the imaginary person he is talking to doesn't back down.⁷

- Then there are those who post photos of their stolen loot on the internet:

Detectives in Hillsborough, Florida, arrested seven people after the suspects posed with suspected stolen guns, jewelry, laptop computers, and TVs posted on the popular social-networking site MySpace.com. The detectives had been investigating a residential burglary in Apollo Beach, when they discovered that some of the suspects were posing for pictures with the stolen property and then displayed it all on their MySpace page.⁸

- Here's the case of a closet pot grower who came out of the closet on the internet:

A teen in Sheboygan, Wisconsin, who was arrested after cops found his pictures of potted marijuana plants and drug paraphernalia posted on the ubiquitous social-networking website was sentenced to 30 days in jail. The teen, identified as 18-year-old Moua Yang, pleaded no contest on May 25 Sheboygan County Circuit Court to felony marijuana manufacturing and misdemeanor possession of drug paraphernalia. Police monitoring for gang activity traced the information to him from said

website. According to authorities, a label on the picture of potted cannabis plants read: "My Mary Jane thats growin in my closet right now."⁹

- Police often find evidence of probation or parole violations via the net:

The Texas Attorney General's office has arrested seven convicted sex offenders who violated their parole conditions by creating MySpace profiles. Officials used the information they were given after the repeated demands they placed on the social networking site. MySpace has found itself walking a thin line between helping catch crooks and protecting users' privacy.¹⁰

Wikipedia lists many other examples of the investigative use of these sites. See http://en.wikipedia.org/wiki/Use_of_social_network_websites_in_investigations.

Their numbers grow both in sites and membership almost daily as indicated in the chart below from the *Webworker Daily*, February 10, 2009 (found at <http://webworkerdaily.com/2009/02/10/social-networks-leapfrog-each-other-in-latest-metrics/>).

Social Networks Leapfrog Each Other in Latest Metrics

February 10th, 2009 (4:40pm) [Samuel Dean](#) [No Comments](#)

Compete.com is out with its [latest metrics on audiences for social networks](#), and web workers may find some surprises in the who's hot and who's not roundup. The top 10 list is seen below, and a full list of the Top 25 is available below the fold. As you would expect, Facebook and MySpace are easily the top two in terms of both unique visitors and monthly visits, but Facebook has surged past MySpace recently with nearly 69 million unique visitors.

Top 25 Social Networks Re-Rank (Ranked by Monthly Visits, Jan '09)

Rank	Site	UV	Monthly Visits	Previous Rank
1	facebook.com	68,557,534	1,191,373,339	2
2	myspace.com	68,635,600	810,163,536	1
3	twitter.com	5,979,062	54,218,731	22
4	myspace.com	7,646,425	63,286,874	16
5	linkedin.com	11,274,160	42,744,438	9
6	logged.com	4,448,915	38,630,827	10
7	classmatters.com	17,226,524	35,219,210	3
8	myyearbook.com	3,312,868	33,121,821	4
9	livejournal.com	4,720,720	25,221,354	6
10	livejournal.com	8,047,491	22,993,608	13

The defense has the same opportunities to search the net and the social networks for information to impeach prosecution witnesses. To fail to investigate is to miss out on potentially devastating impeachment evidence.

B. Lessons to Learn

One of the first inquiries of clients and witnesses should be whether they have a social network account. They should be informed that anything embarrassing (or worse) on the network will inevitably be inspected by law enforcement or the other side in a civil suit. Consider this: "Online hangouts like Facebook and MySpace have offered crime-solving help to detectives and become a resource for employers vetting job applicants. Now the sites are proving fruitful for prosecutors, who have used damaging Internet photos of defendants to cast doubt on their character during sentencing hearings and argue for harsher punishment."¹¹

Attorneys and investigators should routinely search the networks for information about clients and witnesses. Rest assured the other side will. And one cannot assume that even the smartest client will not post harmful things on the internet. The January 27, 2009 issue of the *Los Angeles Times* reports on a Stanford Law School grad who reportedly bragged on the internet that she paid her way through law school as an "escort." This resulted in a search warrant, a prosecution for tax evasion, a felony guilty plea and \$313,134 in penalties and other sanctions.

1. Investigation Cautions. Every investigator working for counsel needs to be informed of the practical, legal and ethical boundaries of internet searches. As the investigator is the attorney's agent, counsel has a duty to make sure the investigator is not violating ethical prohibitions or the law. It does a client no good to have to be defending oneself or the investigator in the context of the criminal case.

One practical suggestion about internet searches: there are a number of

web-based "background" check services that conduct for fee searches. In a recent study done by the Wall Street Journal,¹² the journalist hired four such services to check out a volunteer subject's background. One service, InfoRegistry, could find no data. Intelius responded with some basic information about the test subject including date of birth, recent home addresses and contact information of neighbors. But it also turned up bad information such as three civil judgments for a Chapter 7 bankruptcy (the subject had never filed for bankruptcy) and cities where the subject never lived. Another firm, NetDetective, also produced some correct and incorrect data on the subject. US Search provided detailed address information dating back 30 years, but also provided inaccurate data. The moral of the story: what you get isn't all accurate and must be independently verified.

Investigators must be aware that people post fraudulent profiles and other data about others on the internet. So care must be taken to insure that anything to be used in a court proceeding is accurate. In *Barnes v. Yahoo!, Inc.*, __ F.3d __ (9th Cir. No. 05-36189 05/07/09), Barnes' ex-boyfriend created an unauthorized fake public profile of her on Yahoo. The profile included nude photos and suggestions she was open to sexual adventures.¹³

This phenomena is known as "cybersmearing," another reason to be wary when conducting an internet

search on a witness or client. In *Krinsky v. Doe*, 159 Cal. App. 4th 1154 (2008), anonymous cybersmearers were sued unsuccessfully by a defamed doctor. The case is interesting in describing the procedures the doctor had to overcome to sue the anonymous defamers — the ISP (internet service provider) was subpoenaed to reveal the alleged defamer's identity. The latter elected not to come forward, so then the plaintiff had to deal with formidable First Amendment hurdles before the court would compel the revelation of the identity of the smearers. Surprisingly, despite the smears, she failed to clear that hurdle.¹⁴

On the other hand, there is a contrary phenomena known as "sock puppeting." This is defined as "the act of creating a fake online identity to praise, defend or create the illusion of support for one's self, allies or company."¹⁵ Here, the actual poster of material sends out to internet targets a flattering self-portrait of him or herself (or business) under a phony identity. Wikipedia has a number of notorious examples where authors, politicians and business persons have posted self-laudatory promotional material under false identities. See "Sockpuppet (Internet)" on Wikipedia.

2. Ethical/legal issues. Then there are ethical issues: what do you recommend to a client with an embarrassing Facebook or MySpace.com profile? Is this "evidence" that cannot be taken down at counsel's suggestion without running afoul of ethical mandates?¹⁶ If

Problems in Washington State?

Washington attorney accepting referrals in:



Criminal Defense

Felonies, Misdemeanors,
Restoring Civil Rights,
Expungement of Criminal Record



Over 15 years of experience.

Law Office of Michael Schwartz, Inc.

524 Tacoma Avenue South, Tacoma, WA 98402

Phone: (253)272-7161 Fax: (253)272-7178

Email: mschwartz@callatg.com

it is evidentiary material on the site, the issue will be difficult as destruction of evidence is a crime in every jurisdiction.¹⁷ But when is it “evidentiary” or merely politically incorrect and embarrassing? The client will need advice and it may be as simple as having them read an article like this one.

Take the recent Massachusetts case involving lawyer Kevin Plante.¹⁸ According to Plante (and his civil suit), his firm had taken possession of a major client’s computer and found evidence of child pornography on it. He advised the partners they were obligated to report the material to law enforcement as possession of child porn is a crime. The firm did not care for that advice and sought advice outside the firm. But that advice supported Plante. Nevertheless, the firm ordered Plante to find a company that could permanently erase the images from the computer. Plante refused and was fired. The next day he reported the matter to the FBI which seized the computer. Plante sued for wrongful termination. The firm defends the suit as coming from a disgruntled ex-employee and argued that the entire matter was covered by the attorney-client privilege. The case was dismissed in the trial court but that decision was reversed on appeal, the latter holding his claim stated a basis for wrongful termination.

The Plante case illustrates the problems of attorneys or investigators accepting possession of any e-media from a client without knowing exactly what is received.

How about instructing an investigator to “befriend” an adverse witness on Facebook? Assume the investigator truthfully identifies himself or herself but does not reveal that the purpose of the “friendship” is to gather information about the witness on a pending case. An advisory opinion issued in March 2009 by the Philadelphia Bar Association Professional Guidance Committee states that an attorney cannot ethically ask a third party (read investigator) to ‘friend’ a witness on a social network. (Opinion 09-2.) The

reason: the contact is deceptive and such conduct is prohibited under the Pennsylvania Rules of Professional Conduct:

Turning to the ethical substance of the inquiry, the Committee believes that the proposed course of conduct contemplated by the inquirer would violate Rule 8.4(c) because the planned communication by the third party with the witness is deceptive. It omits a highly material fact, namely, that the third party who asks to be allowed access to the witness’s pages is doing so only because he or she is intent on obtaining information and sharing it with a lawyer for use in a lawsuit to impeach the testimony of the witness. The omission would purposefully conceal that fact from the witness for the purpose of inducing the witness to allow access, when she may not do so if she knew the third person was associated with the inquirer and the true purpose of the access was to obtain information for the purpose of impeaching her testimony.

Not only can one run afoul of state bar associations, but the prosecutor’s office may take an interest in defense social network investigation. So may the offended social network owner. If the latter has made his or her profile restricted and a defense investigator gains access to it by slight of hand, there may be a privacy invasion suit in the future.¹⁹

3. The Drew case example. Investigators and attorneys thinking of befriending a person of interest on a social network using a ruse should take heed of the case of *U.S. v. Lori Drew*, the so-called “cyber bully” case tried in federal court in Los Angeles late last year. There, Ms. Drew, who resided in a St. Louis suburb, created a phony MySpace profile of a young boy who befriended a young neighbor girl on MySpace. The young girl lived only a few houses away from Drew, but because MySpace’s office was in Beverly Hills, the cyber transmission

went from Drew’s home near St. Louis to Los Angeles and back to the young girl’s home a few doors away.

Because the email traffic between the two turned ugly, the young girl committed suicide and Drew ended up being prosecuted by the U.S. Attorney in Los Angeles for a violation of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030. The Act states that whoever intentionally accesses a computer without authorization or exceeds authorized access and thereby obtains information from any protected computer is guilty of a federal crime (assuming interstate/foreign communications were involved.) Punishment can be a misdemeanor or a felony for up to five years in prison if the offense was committed in furtherance of a crime or a tortious act.

In *Drew*, the government theory of “exceeding” authorized access was this: MySpace, like all social networks, has a detailed description of its “terms of service.” These are similar to the End User License Agreements (EULA) we are so familiar with when beginning use of a program. Most of us ignore them, scroll to the bottom, say “I agree,” and activate the service. With MySpace, several of the terms of service are: the user must agree to provide truthful registration information, must refrain from using MySpace to abuse or harm others and must not solicit information from persons under 18. Violation of these terms was deemed by the government to mean Drew exceeded the authorized access to the young girl’s MySpace profile. In this sense, the MySpace terms of service were elevated to violations of the federal criminal statute.

In Drew’s case, the government charged felony conspiracy and substantive felonies for several of the MySpace contacts with the girl. The basis of the felony was that Drew committed a tortious act — the intentional infliction of mental distress. Thanks to the hard work of Dean Steward, Drew’s defense counsel, she was acquitted of the felonies and convicted of several misdemeanors.

As this article goes to press, the trial judge in the case is still pondering whether this prosecution theory is valid and has continued the case until July 2, 2009 for further review. See *San Diego Union Tribune*, p. A-4, May 19, 2009, "Sentencing Delayed in Web Hoax Case." For the moment at least, the *Drew* case is a cautionary tale. Investigators using the social network to gain information from a person of interest should think about what they are doing and consult ahead of time with counsel in the case. While there is nothing wrong with looking at publicly posted information, things get precarious when going beyond that.

4. In criminal cases, what are your discovery obligations? In California for example, Penal Code § 1054.8 states that witnesses' whose names have been disclosed in discovery cannot be questioned without the defense interviewer complying with the disclosure requirements of the statute.²⁰ This law has obvious implications when contacting such witnesses via a social network or email. The investigative ruse of befriending a prosecution witness online through a false identity has obvious problems with such statutes.²¹

5. You've got it, now prove it. There are many evidentiary issues associated with introducing e-matter as evidence, the first and foremost being authentication. What if the alleged author denies authorship on the stand? How difficult is it to nail down the authorship to get the material admitted? Assuming the witness denies authorship despite being shown a print out of their profile (complete with network assigned registration/membership number), how may the attorney use the evidence to impeach? This may involve subpoenaing the social network provider. See <http://www.search.org/programs/high-tech/isp/>, an exhaustive listing of the contact information on all of the relevant sites, and more. Subpoenaing the social network can be a time-consuming effort. Assistant Monterey Public Defender Donald Landis has informatively written of his experi-

ences dealing with MySpace.com and trying to subpoena MySpace profiles.²²

Authenticating paperless e-evidence may not be easy, but with some thought about it, it certainly can be done. In *Lorraine v. Markel Am. Ins. Co.*, 241 F.R.D. 534, 546 (D. Md. 2007), the court exhaustively explores the issues involved in authentication of ESI (electronically stored information) and is well worth reading should you face the issue of attempting to authenticate text messages, emails, or web postings.²³

C. Interview checklist about social networks and e-media

When interviewing clients or witnesses, the following questions are suggested as starters. If the answer to any is "yes," then the details need to be explored. This list is more expansive than questioning just about social networks, but one needs to know about the client/witness's complete cyber presence. But beware about taking possession of anything without knowing exactly what it is. See fn. 16 *supra*.

Cases have allowed law enforcement to seize and search computers as part of any search warrant operation even if there is no mention of the computer as evidence to be seized. They are seized as "dominion and control" evidence to tie the defendant to the place searched.²⁴ Further, quasi-agent hackers provide law enforcement with data from illicit invasions of home computers that eventually lead to prosecutions, convictions and sentences.²⁵ Thus, defense counsel needs to know what e-media the client possesses, or possessed, to provide informed counseling.

The following list of questions, while not comprehensive, should provide a start for inquiring of the person's cyber profile. The introduction to these questions might start with:

"Because the internet could be a source of much public information about yourself, I need to know what presence, if any, you have there. You should know that law enforcement

routinely checks every available resource on the internet to discover information about persons of interest. This has often led to persons being criminally prosecuted simply based upon what they have placed on the internet, or even what their friends have posted about them. To properly advise you, I need to know what you have posted and if there are legal issues to consider."

1. Do you have a profile on a social network like Facebook, Twitter or MySpace. In your name? How many profiles? Is it open to the public? What is posted? Where do you post your communications? Have you commented on articles, blogs, pictures, or other people's social media sites?
2. Do you have a website? How long have you had it? When did you first launch the site?²⁶
3. Do you have a blog?²⁷
4. Do you post material on YouTube?²⁸
5. Do you buy or sell on EBay, Craig's List, or similar services?²⁹
6. Do you have a Flip Video or other recorder? Does your cell phone have video?³⁰ Where is the content stored? Do you upload any of it to the net?
7. Do you email from a computer, Blackberry, I-Touch? Do you use Skype? Instant Message?³¹
8. Do you text message from your cell phone?
9. Do you use Limewire or similar peer-to-peer programs?³²
10. On what media do you store files, photos? Your PC, Mac, laptop, PDA, DVD, CD, Compaq Flash cards,³³ or do you backup files to an internet site like Mozy?

D. A Final Word

Defense counsel has to be alert to the many issues raised by rise of the social networks as a major source of human communication. As noted, the network profiles may provide easy to obtain sources of both harmful and helpful evidence and investigative leads. Further, an ever increasing variety of e-gadgets are marketed to store and send e-material.

Attorneys can and should ask the starter questions in the checklist to acquire rudimentary information from clients and witnesses. Further, exploration of the internet to find what may be there requires not only someone adept in the ways of cyberspace, but also one fully aware of the legal and ethics boundaries concerning the privacy rights of others – even though the boundaries are not yet clearly established.

ENDNOTES

¹“(Un)anonymous on the Internet: Social networking sites offer tool for law enforcement,” Sean Garmire, *The Times-Standard* (7/21/2008), http://www.times-standard.com/localnews.ci_9946604.

² **Facebook** is a social networking website launched on February 4, 2004. The free-access website is privately owned and operated by Facebook, Inc. The website’s name refers to the paper facebook depicting members of a campus community that some American colleges and preparatory schools give to incoming students, faculty, and staff as a way to get to know other people on campus. Mark Zuckerberg founded Facebook.

³ See general list of the most popular social networks in Wikipedia found at http://en.wikipedia.org/wiki/Social_network_service (May 20, 2009).

⁴ **MySpace.com** is the a very popular social networking website offering an interactive, user-submitted network of friends, personal profiles, blogs, groups, photos, music and videos for teenagers and adults internationally. Its headquarters are in Beverly Hills, California, USA, where it shares an office building with its immediate owner, Fox Interactive Media; which is owned by News Corporation, which has its headquarters in New York City. The 100 millionth account was created on August 6, 2006 in the Netherlands and a news story claimed 106 million accounts on September 8, 2006, and the site reportedly attracts 230,000 new registrations per day. It too receives almost one billion hits on its site a day.

⁵ See, e.g., “Appeal of \$12.6 million verdict alleges juror sent ‘tweets’ biased against company,” *San Diego Union*, March 14, 2009, p. A5, noting that a juror sent biased messages against the defendant company on Twitter.com during the trial. See also March 18, 2009 article, “As Jurors Turn to Web, Mistrials Are Pop-

ping Up,” *New York Times*, http://www.nytimes.com/2009/03/18/us/18juries.html?_r=1&hp=&p. Jurors are now routinely instructed not to use the internet (CalCrim 201), but it may be that stronger and more frequent instructions are necessary during the trial.

⁶ *Los Angeles Times*, December 10, 2008, “Esteban Nunez released from jail after posting \$1 million bail,” found at <http://latimesblogs.latimes.com/lanow/2008/12/esteban-nunez-t.html>.

⁷ See “Teen Shot By St. Pete Police Took Thug Persona On MySpace,” Stephen Thompson, *The Tampa Tribune* (June 10, 2008), <http://www2.tbo.com/content/2008/jun/10/teen-shot-st-pete-police-took-thug-persona-his-web/?imw=Y>.

⁸ See “Thieves Post Pictures Of Stolen Items On MySpace,” (November 22, 2006) at <http://www.dumbcrooks.com/thieves-post-pictures-of-stolen-items-onmyspace>.

⁹ See “Wisconsin Teen Gets Jail After Posting Homegrown Pot Pictures Online,” (May 27, 2007) at <http://www.dumbcrooks.com/wisconsin-teen-gets-jail-after-posting-homegrown-pot-pictures-online>.

¹⁰ See *Ecommerce Times*, Fred J. Aun, “Sex Offenders Nabbed After Violating Parole on MySpace,” (June 15 2007) <http://www.ecommercetimes.com/story/57873.html>.

¹¹ See “Drinking, Driving And Facebook Don’t Mix: Web Networking Photos Come Back To Bite Defendants,” July 18, 2008, www.cbsnews.com/stories/2008/07/18/tech/main4272846.shtml?source=RSSattr=SciTech_42.

¹² Jane Hodges, “Investigating Online Private Eyes” (May 21, 2009), found at http://online.wsj.com/article_email/SB124286773775841705-1MyQjAxM-DI5NDIyMjgyNjI3Wj.html#.

¹³ Barnes asked Yahoo to take down the profile. Yahoo did not respond to several of her requests. Later, it assured her it would be done, but nothing happened. Barnes sued Yahoo. The Circuit found that when Yahoo assured Barnes the material would be removed it could be liable under breach of contract and promissory estoppel principles.

¹⁴ Given what was said about Lisa Krinsky, one can see that the First Amendment protection is high indeed. Cybersmearers regularly made “scathing verbal attacks” against her and other company officers including references to them as “a management consisting of boobs, losers and

crooks.” One post said of Krinsky, “I will reciprocate felatoin [sic] with Lisa even though she has fat thighs, a fake medical degree, ‘queefs’ and has poor feminine hygiene.” (159 Cal. App. 4th 1159.) These comments were deemed protected speech despite being “crude, satirical hyperbole which, while reflecting the immaturity of the speaker, [they] constitute protected opinion under the First Amendment. It hardly need be said that this conclusion should not be interpreted to condone Doe 6’s rude and childish posts [which were]... intemperate, insulting, and often disgusting remarks.” (*Id.*, at 1178.)

¹⁵ Brad Stone and Matt Richtel “The Hand That Controls the Sock Puppet Could Get Slapped,” *New York Times* (July 16, 2007) at <http://www.nytimes.com/2007/07/16/technology/16blog.html>.

¹⁶ See, e.g., *People v. Meredith*, 29 Cal.3d 682 (1981)(counsel cannot deprive the prosecutor of evidence of a crime found and retrieved by a defense investigator during the defense investigation).

¹⁷ E.g., Calif. Penal Code § 135 states: “Every person who, knowing that any book, paper, record, instrument in writing, or other matter or thing, is about to be produced in evidence upon any trial, inquiry, or investigation whatever, authorized by law, willfully destroys or conceals the same, with intent thereby to prevent it from being produced, is guilty of a misdemeanor.”

¹⁸ What follows is taken from an article by David E. Frank, “Court: filed lawyer can sue Boston firm,” *Massachusetts Lawyers Weekly* (May 4, 2009) at <http://www.mass-lawyersweekly.com/index.cfm/archive/view/id/448126>.

¹⁹ Compare the situation in *Susan S. v. Israels*, 55 Cal.App.4th 1290 (1997), where the Court of Appeal upheld a tort liability suit against a criminal defense lawyer for his unauthorized reading of the crime victim’s confidential mental health records. The records had been mistakenly sent to the attorney in response to his subpoena. The appellate court held such records fell under the person’s constitutional right to privacy and should have been submitted to the trial court for *in camera review* instead of being examined by the attorney. If restricted network profiles are deemed private and are infiltrated to secure information, a similar lawsuit vulnerability is certainly possible.

²⁰ The statute reads “(a) No prosecuting attorney, attorney for the defendant, or investigator for either the prosecution or

the defendant shall **interview, question, or speak to a victim or witness** whose name has been disclosed by the opposing party pursuant to Section 1054.1 or 1054.3 without first clearly identifying himself or herself, identifying the full name of the agency by whom he or she is employed, and identifying whether he or she represents, or has been retained by, the prosecution or the defendant. If the interview takes place in person, the party shall also show the victim or witness a business card, official badge, or other form of official identification before commencing the interview or questioning.”

²¹ Compare this to the legal problems Hewlett Packard lawyers, investigators, and consultants encountered when authorizing “pretexting” – where one pretends to be the person investigated to gain unauthorized access to their telephone records. Stephen Lawson, “Charges against HP’s Dunn dropped,” *Networkworld, IDG News Service*, (March 14, 2007) <http://www.networkworld.com/news/2007/031407-charges-against-dunn.html>.

²² See “MySpace.com: Discovery Issues in the 21st Century,” *California Defender*, p. 37-39 (Winter 2008-2009).

²³ See cases cited therein: *U.S. v. Siddiqui*, 235 F.3d 1318, 1322-23 (11th Cir. 2000) (authentication of an e-mail); *U.S. v. Safavian*, 435 F. Supp. 2d 36, 40 (D.D.C. 2006) (same); *In Re F.P. a Minor*, 878 A.2d 91, 94 (Pa. Super. Ct. 2005) (transcripts of instant messaging conversation authenticated based on defendant’s screen name, use of defendant’s first name, and content of threatening message, which other witnesses had corroborated); *Perfect 10, Inc. v. Cybernet Ventures, Inc.*, 213 F. Supp. 2d 1146, 1153-54 (C.D. Cal. 2002) (admitting website postings as evidence due to circumstantial indicia of authenticity, including dates and presence of identifying web addresses).

²⁴ Two California cases have held that computers may be seized in home searches pursuant to warrant even if not mentioned in the warrant. They can be seized to establish “dominion and control” of the premises. *People v. Varghese*, 162 Cal. App. 4th 1084, 1100 (2008); *People v. Balint*, 138 Cal.App.4th 200, 205 (2006).

These courts held that the “computer is the functional equivalent of a filing cabinet and a reasonable place to seek information concerning the dominion and control of the place searched.” *Varghese, supra* at 1101. In the latter case, the court allowed the “dominion and control” of the residence theory to justify the computer seizure even though the laptop was found in a car outside the house.

²⁵ E.g., *U.S. v. Steiger*, 318 F.3d 1039, 1043-1044 (11th Cir. 2003) (The hacker stated: “How did I get access to his PC? I used the well known Trojan horse named Subseven. . . . I made it undetectable so av [anti-virus] softwares [sic] couldnt [sic] see it and bind it with a fake program;” this led to a search warrant, prosecution and a 235 month sentence for possession of child porn); *U.S. v. Jarrett*, 338 F.3d 339 (4th Cir. 2003) (same hacker held not a state agent despite trial court finding otherwise because hacker used same FBI agent as in *Steiger* who said “give us more” and promised no prosecution for his crimes.)

²⁶ This needs to be asked because the content of websites as they appeared at different times may be able to be reproduced. The Internet Archive Company may retrieve copies of the website as it appeared at relevant dates though use of its “wayback machine.” See discussion in *Lorraine v. Markel Am. Ins. Co.*, 241 F.R.D. 534, 553 (D. Md. 2007).

²⁷ A blog (a contraction of the term web log) is a website, usually maintained by an individual, with regular entries of commentary, descriptions of events, or other material such as graphics or video or personal online diaries. There are tens of millions of blogs.

²⁸ With the advent of devices like Flipvideo and cell phone recorders, persons can post video content on YouTube or their social network within seconds of the video being taken. YouTube is a video sharing website where users can upload, view and share video clips. It was created in mid-February 2005 by three former PayPal employees. In October 2006, Google acquired the company for \$1.65 billion in Google stock.

²⁹ These sites are used for the buy/sell of legitimate goods, but also illicit ones. One site notes the site has been used for

many crimes including prostitution, selling bogus stock and even to sell babies. See “Major NY Craigslist Prostitution Bust,” *Trench Reynolds Crime News* (May 21, 2009) at <http://crimene.ws/category/craigscrimelist/>.

³⁰ Cellular Seizure Investigation [CSI] Sticks, often used by law enforcement, can plug into a cell phone and quickly pull any e-mail, instant & text messages, dialed numbers, phone books, photos, and even deleted files that have not been overwritten.

³¹ See *Quon v. Arch Wireless Operating Co.*, 529 F.3d 892, 905 (9th Cir. 2008) (“e-mail . . . users have no expectation of privacy in the to/from addresses of their messages . . . because they should know that this information is provided to and used by Internet service providers for the specific purpose of directing the routing of information.” *U.S. v. Forrester*, 512 F.3d 500, 510 (9th Cir. 2008). . . . Thus, we have extended the pen register and outside-of-envelope rationales to the ‘to/from’ line of e-mails. But we have not ruled on whether persons have a reasonable expectation of privacy in the content of e-mails.”)

³² Peer to peer programs like “Limewire” mean that the user may open his/her computer to others so they can download music or photos on the hosts computer. The host then searches to find others who have the music, photos, etc. of interest for his/her download. If used, it means the person’s computer is open to all including law enforcement. See *U.S. v. Ganoe*, 583 F.3d 1117 (9th Cir. 2008) (being on a file sharing program is an open invitation for all to “come on in” and there is no right of privacy violation if others do search one’s computer.)

³³ Note that those who travel across international borders run the risk of a border search of any of this equipment. See *U.S. v. Arnold*, 523 F.3d 941, 942 (9th Cir. 2008), where the question was posed: “We must decide whether customs officers at Los Angeles International Airport may examine the electronic contents of a passenger’s laptop computer without reasonable suspicion.” Answer: yes. *Accord People v. Endacott*, 164 Cal. App. 4th 1346, 1350 (2008). ▲