



NATIONAL ASSOCIATION OF CRIMINAL DEFENSE LAWYERS

[Close this Window](#)

 [Email](#) /  [Print](#)

If a client is in the crosshairs of a criminal investigation, chances are that law enforcement has already scoured Facebook, MySpace, Twitter, LinkedIn and other social networking sites to search for incriminating evidence. Several hundred million people have active Facebook and MySpace accounts.¹ Unlike traditional Web sites, where users are limited to passive viewing, social networking sites permit users to create personal profiles; post photographs, videos, and audio clips; write blog entries and status updates; send and receive private messages; and link to pages of others. Across the country, law enforcement agents and prosecutors are effectively mining these sites for inculpatory evidence. But evidence from social networking sites is not just for the prosecution. Evidence from these sites can also bolster the defense.

Government Uses of Social Networking Sites

A recently obtained document from the U.S. Department of Justice titled Obtaining and Using Evidence From Social Networking Sites highlights the "utility" of evidence from social networking sites for the prosecution.² In the government's view, the evidence can reveal personal communications, establish motives and personal relationships, provide location information, prove and disprove alibis, and establish a crime or criminal enterprise.³ Social networking evidence may also constitute "instrumentalities or fruits of crime."⁴ Through the use of subpoenas, search warrants, and undercover operations, law enforcement can easily obtain evidence from these sites, particularly given that many social networking companies readily cooperate with law enforcement.⁵

Numerous cases show that prosecutors are taking full advantage of social networking evidence and using it in every stage of the criminal process, including bail hearings,⁶ trials,⁷ sentencing hearings,⁸ and fugitive apprehension.⁹ For example, in a murder case, a Michigan appellate court upheld the trial court's admission of photos of the defendant from his MySpace page in which he was holding a gun and displaying a gang sign.¹⁰ In another case, police apprehended three men on sexual assault charges involving a woman they met on MySpace by obtaining their online usernames and accounts from the company.¹¹ The federal government even prosecuted one woman's use of a MySpace account as an alleged violation of the Computer Fraud and Abuse Act.¹²

Using Social Networking Evidence to Bolster the Defense

Defense counsel can learn a valuable lesson from law enforcement. Social networking sites are not only for the prosecution: they can also be a treasure trove of exculpatory evidence, impeachment material, and other helpful information for the defense. And like the prosecution, the defense can use this evidence at key phases of a case, such as jury selection, pretrial hearings, and during the trial itself, thereby leveling the playing field.¹³

Advising Clients About Their Use of Social Networking Sites

One of defense counsel's first tasks during an investigation or case is to learn whether the client has used any social networking sites and posted any harmful information on them. With the client's assistance, defense counsel should review the information on the client's past and current social networking accounts. Dated information may appear to be hidden; this could require use of a special search engine to access archived Web content.¹⁴ The client should also be advised about the dangers of using social networking sites and alerted that law enforcement is likely monitoring his accounts.¹⁵ A former Deputy District Attorney for Los Angeles County made this point quite clearly:

"As a prosecutor, the first thing I do when I get a case is to Google the victim, the suspect, and all the material witnesses. I run them all through Facebook, MySpace, Twitter, YouTube and see what I might get. I also do a 'Google image search' and see what pops up. Sometimes there's nothing, but other times I get the goods — pictures, status updates, and better yet, blogs and articles they've written.¹⁶"

Even the Justice Department instructs its prosecutors to advise witnesses to "think carefully about what they post" and "not to discuss cases on social networking sites."¹⁷ Thus, in most cases, the client should be advised to discontinue using social networking sites during a pending investigation or case.¹⁸

A more difficult issue involves whether anything can or should be done about existing, harmful information that a client has posted on a social networking site. If the information is deleted after the client learns of an investigation, the government likely will be able to retrieve it. In this situation, the prosecution may assert that the client obstructed justice by deleting incriminating information during a pending investigation.¹⁹ The government may also argue that the deletion of the information is evidence of the client's consciousness of guilt. Counsel should assume that the government knows about the evidence and, if not, it soon will.

Obtaining Evidence From Social Networking Sites

Defense attorneys face greater challenges than prosecutors in obtaining social networking evidence because they lack the authority to use many of law enforcement's investigatory techniques. In addition, social networking companies tend to cooperate with law enforcement's requests for information,²⁰ but defense requests have been opposed.²¹ Defense attorneys nevertheless have at least three sources from which they can obtain the evidence: the government, social networking companies and other non-parties, and the Internet.

There are two categories of evidence that defense counsel should seek from the government. The first is potentially harmful evidence that the government intends to offer against the defendant as part of its case-in-chief. The defense can obtain copies of this evidence by making a request under Fed. R. Crim. P. 16. Rule 16 requires the government to disclose (1) evidence that it intends to use in its case-in-chief, (2) items obtained from the defendant, and (3) relevant written and recorded statements of the defendant.²² However, if a defendant requests disclosure under Rule 16(a)(1)(E), then he is subject to providing reciprocal discovery under Rule 16(b)(1)(A).

The second category includes evidence that is material to the defense, including evidence that is favorable to the accused on either guilt or punishment.²³ Defense counsel can request the government to produce items that are "material to preparing the defense" under Rule 16(a)(1)(E).²⁴ Defense counsel also should request that the government produce evidence that is favorable to the defense under Brady and Giglio.²⁵

There is a strong likelihood that the government will have in its possession Brady and Giglio material regarding government witnesses, particularly since the Justice Department is advising its prosecutors to "research all witnesses on social networking sites."²⁶ And the government has candidly acknowledged that social networking pages pose "potential pitfalls for government witnesses."²⁷ They can even present similar problems for law enforcement officers who will testify at trial. According to a recent Los Angeles Sheriff's Department newsletter, some officers have posted self-descriptive materials on Facebook and MySpace, such as bragging about being a "rogue cop" and a "garbage man, because I pick up trash for a living."²⁸ These statements certainly qualify as impeachment material under Giglio.

Defense counsel can also request that the court issue subpoenas to social networking companies and non-party witnesses for the production of documents and data under Fed. R. Crim. P. 17. Rule 17(c)(1) provides that the court may order a witness to produce books, papers, documents, data, or other designated objects in court before trial or before they are to be offered in evidence.²⁹ A party seeking production of materials before trial under Rule 17(c) must show that the subpoenaed information is relevant, admissible, and requested with specificity.³⁰ While there is a paucity of reported cases involving the defense's use of a subpoena to obtain social networking evidence, this nevertheless could be a powerful tool for obtaining valuable evidence for the defense.³¹

In addition to directing discovery requests to the prosecution and requesting third-party subpoenas, defense counsel can obtain evidence from social networking sites by independent investigation using the Internet. As soon as possible in a case, defense counsel should search all social networking sites for publicly available information regarding both government and defense witnesses. Thereafter, counsel should perform routine checks of those accounts for any changes, and should conduct additional searches upon learning the identities of new witnesses. Counsel's investigation could yield helpful information that the government has not discovered and provide the defense with an advantage at trial.

Ethical Issues to Consider

Thorny ethical and legal issues can arise if, during an investigation of a social networking site, counsel (1) fails to disclose his true identity and relationship to a pending case; (2) uses third parties to gain access to information; or (3) uses a fictitious identity to obtain the information. While most jurisdictions have not yet addressed the limits of counsel's use of social networking sites to gather evidence, at least two bar committees have issued advisory opinions.³² At a minimum, defense counsel needs to be cautious, and should not attempt by any means to access a witness's online profile using a false name. Attorneys should seek counsel from the governing ethics boards of their local bar associations.

Jury Selection

Evidence from social networking sites can be useful to the defense during jury selection. Defense attorneys and trial consultants can obtain publicly available information about prospective jurors from social networking sites and Internet search engines.³³ In cases where juror questionnaires are available to counsel well before trial, there is ample time to conduct an effective search. Even when the identities of prospective jurors are disclosed for the first time at trial, defense counsel's staff and trial consultants should have sufficient time to gather valuable information.

Real-Time Trial Reporting on Social Networking Sites

Another possible issue that counsel may encounter involves the role of social networking sites in the real-time reporting of criminal trials from the courtroom, typically via live-feed Web sites like Twitter.³⁴ Real-time feeds and live blogging of trials can result in circumvention of sequestration orders by the government's witnesses, which happened in the recent criminal environmental trial of *United States v. W.R. Grace*.

In *Grace*, the court permitted the University of Montana Law School and School of Journalism to cover the trial in real time. Each day, students published detailed accounts of the trial testimony via Twitter and chronicled the trial's events on a weblog. Although

witnesses had been sequestered, the government's key witness nevertheless read about the trial testimony online, a fact that he admitted during cross-examination. The defense accused the witness of fabricating testimony based on his review of the real-time accounts of two other government witnesses' testimony. Indeed, the district court later struck the testimony of this witness against one of the defendants and issued a harsh jury instruction regarding his credibility.³⁵

Defense counsel should be aware of any live blogging or tweeting from the courtroom and alert the court to any problems this might cause. In making a request for witness sequestration, counsel should ask the court to prohibit witnesses from following online updates of the trial. During trial, the trial team must read any Twitter and real-time blog coverage of the case. This will assist counsel in determining whether a witness has based his testimony on online information concerning the testimony of another witness.

Conclusion

The explosion in the popularity of social networking sites has generated a wealth of evidence to be used in criminal cases. Comprehensive discovery of evidence from social networks is now imperative. The prosecution obtained an early lead. It's time for the defense to level the playing field and aggressively use this rich source of information at trial.

The authors wish to thank Rachel Z. Friedman and Allison S. Lukas, law students at Harvard Law School, for their helpful research and contributions to this article.

Notes

1. See Facebook Press Room, <http://facebook.com/press/info.php?statistics> (last visited July 6, 2010); MySpace Fact Sheet, <http://www.myspace.com/pressroom?url=/fact+sheet/> (last visited July 6, 2010).
2. In response to a request under the Freedom of Information Act by the Electronic Frontier Foundation, the U.S. Department of Justice, on March 3, 2010, produced an undated PowerPoint presentation authored by members of the Department's Computer Crime & Intellectual Property Section. The PowerPoint includes a data reference date of August 12, 2009, indicating that it was written after that date.
3. Obtaining and Using Evidence From Social Networking Sites, U.S. Department of Justice (Computer Crime & Intellectual Property Section, undated PowerPoint) at slide 9 (hereinafter "DOJ PowerPoint").
4. *Id.*
5. *Id.* at slide 8; see also Facebook Subpoena/Search Warrant Guide, <http://dto.net/docs/facebook-manual.pdf> (last visited July 6, 2010) (internal Facebook document dated February 2007, describing the procedure for requesting information from Facebook).
6. In a New York case involving charges of assault and unlawful possession of a firearm, the court increased the defendant's bail from \$5,000 to \$50,000 based on 10 pages of photos of the defendant found on a MySpace page. See Ken Strutin, Social Networking in a Self-Surveillance Society, *NEW YORK LAW JOURNAL*, March 10, 2009, citing MySpace Page Used Against Gang Suspect, *Buffalo News*, January 23, 2009. These pictures allegedly showed the defendant wearing gang clothing, displaying gang signs, and standing with others in gang colors. *Id.*
7. In sex offender cases, courts have admitted evidence of communications on social media sites between defendants and their under-aged victims. See, e.g., *State v. Bell*, 145 Ohio Misc. 2d 55, 67-69 (Com. Pl. 2008).
8. Photos of drunken or seemingly unremorseful DUI defendants, taken from their Facebook and MySpace pages, have reportedly influenced judges to impose longer prison sentences. See Philip K. Anthony and Christine Martin, Social Media Go to Court: Litigators Find There's More to Web 2.0 Than What Jurors Put on Their Facebook Profiles, *RECORDER* (San Francisco), February 20, 2009. In one case, images of a defendant holding a loaded weapon, taken and posted on his MySpace page after his conviction for a violent felony, were admitted as evidence to increase his sentence. See Daniel L. Brown and Aimee R. Kahn, Savvy Use of Social Networking Sites, *NEW YORK LAW JOURNAL*, September 8, 2009.
9. Laura Saunders, Is 'Friending' in Your Future? Better Pay Your Taxes First, *WALL ST. J.* (August 27, 2009) (discussing how tax authorities located a man accused of tax evasion from information that he posted on his MySpace page).
10. *People v. Liceaga*, 2009 Mich. App. LEXIS 160, *7-12 (Mich. Ct. App. Jan. 27, 2009).
11. Julie Masis, Is This Lawman Your Facebook Friend? Increasingly, Investigators Use Social Networking Web Sites for Police Work, *BOSTON GLOBE*, January 11, 2009.
12. See *United States v. Drew*, 259 F.R.D. 449 (C.D. Cal. 2009). In *Drew*, the defendant set up a fictitious MySpace profile, pretending to be a teenage boy, in violation of MySpace's terms of consent. She then used that profile to contact a classmate of her teenage daughter and instigate a romantic relationship. When the defendant abruptly ended the relationship, the young woman committed suicide. The defendant was charged with violating the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, for intentionally accessing a computer without proper authorization in furtherance of the commission of a criminal or tortious act. The jury acquitted the defendant on the felony charge, but convicted her of a misdemeanor violation. The district court vacated the conviction on the ground that the statute was void for vagueness as applied. *Id.* at 461-67.
13. Some defense attorneys have already followed the government's lead and successfully used evidence from social networking sites at trial. For example, in *People v. Rodriguez*, 19 Misc. 3d 830, *5 (N.Y. Crim. Ct. 2008), the court dismissed charges of harassment and endangering the welfare of a child based in part on the alleged victim's MySpace account activity, noting that she had made no efforts to block messages from the defendant or remove him from the list of friends granted access to her profile.
14. Several search engines, such as the Internet Archive: Wayback Machine (<http://www.archive.org/web/web.php>), are capable of locating old Web pages that have been altered or deleted.
15. See Gregory S. Spizer, Understanding of Social Media Intrinsic to Modern Legal Practice, 241 *LEGAL INTELLIGENCER* 93 (May 14, 2010).
16. See Robin Sax, Watch What You Say ... Online, *HUFFINGTON POST*, http://www.huffingtonpost.com/robin-sax/watch-what-you-say-online_b_217366.html (dated June 18, 2009, last visited June 19, 2009).
17. See DOJ PowerPoint, *supra* note 3, at slide 31.

18. The defense must also be prepared to oppose the admission of such evidence by the government. Counsel should consider filing a motion in limine to exclude the evidence, as well as objecting to its admission at trial. Objections could include lack of authentication, failure to identify the defendant as the author, relevancy, hearsay, and undue prejudice. See, e.g., *Griffin v. State*, 2010 WL 2105801 (Md. May 27, 2010) (discussing in detail authentication of evidence from social networking sites).
 19. See 18 U.S.C. § 1519; see also *United States v. Wortman*, 488 F.3d 752 (7th Cir. 2007) (defendant convicted of obstruction of justice for destroying incriminating evidence that belonged to her boyfriend after learning that he was under investigation by FBI).
 20. See DOJ PowerPoint, *supra* note 3, at slide 15.
 21. See, e.g., California Criminal Defense Law Firm Wallin & Klarich Seeks Court Order to Obtain Electronic Communications From Facebook, MySpace, PRWEB, <http://www.prweb.com/releases/facebook-myspace/court-order/prweb2675884.htm> (dated July 27, 2009, last visited July 6, 2010).
 22. See Fed. R. Crim. P. 16(a)(1)(B)(i) and 16(a)(1)(E)(ii) and (iii).
 23. One court has held that defense counsel's failure to investigate and pursue evidence from social networking sites could be ineffective assistance of counsel. See *Cannedy v. Adams*, 2009 WL 3711958 (C.D. Cal. Nov. 4, 2009).
 24. The scope of Rule 16 extends beyond items that are in the physical possession of the prosecutor; the government also must produce information in the possession of the federal agencies. See *United States v. W.R. Grace*, 401 F. Supp. 2d 1069, 1074 (D. Mt. 2005).
 25. While the government's constitutional obligations under Brady are self-executing and do not require a motion by the defense, defense counsel nevertheless should press for early disclosure of exculpatory evidence from social networking sites so that it can be effectively used in formulating the defense.
 26. See DOJ PowerPoint, *supra* note 3, at slide 15 (emphasis in original).
 27. *Id.*
 28. See San Diego District Attorney, Law Enforcement Legal Update, Easy Way to Destroy Your Credibility and Your Career, 14 LEGAL UPDATE 9 (August 13, 2009).
 29. In subpoenas directed to social networking companies, defense counsel should specifically seek production of (1) picture, audio and video files; (2) meta data; (3) information concerning certain URLs; (4) internet protocol address and other location identifiers; (5) Internet Service Provider address and Internet subscriber information; (6) abuse reports; (7) site terms of use; (8) social networking site profiles of witnesses and other individuals related to defendant; (9) business and personal activities of witnesses or the defendant; (10) frequency of postings/use; (11) social, business and other group affiliations on the Social Media platforms; and (12) evidence or any relevant information uploaded online to the Web site.
 30. See *United States v. Nixon*, 418 U.S. 683, 700 (1974).
 31. Memorandum and Order at 5, *United States v. Kernell*, No. 03-CR-142 (E.D. Tenn. March 17, 2010) (granting defendant's motion to authorize issuance of subpoena under Fed. R. Crim. P. 17(c) for information from 4chan's message boards).
 32. The Philadelphia Bar Association's Professional Guidance Committee issued an opinion prohibiting the use of deception by attorneys and their associates when contacting witnesses through online accounts. See Philadelphia Bar Association Professional Guidance Committee, Opinion 2009-02 (March 2009). The Committee proscribed counsel from contacting a person through online social media profiles without addressing the underlying purpose of the contact or disclosing an affiliation with the case. See *id.* Reaching a different conclusion, the New York County Lawyers' Association's Committee on Professional Ethics issued an opinion stating that attorneys may supervise non-attorney investigators who conceal or misstate their identity to gather evidence online, provided certain conditions are met. NYCLA Committee on Professional Ethics, Formal Opinion No. 737, Issued May 23, 2007. Those conditions include a showing that the evidence is "not reasonably available through other lawful means" and that the acts do not violate third-party rights and other ethical rules. *Id.* See also Ken Strutin, Evidence on Social Networking Sites, 8 INTERNET LAW & STRATEGY 3 (January 2010); Gregory S. Spizer, Understanding of Social Media Intrinsic to Modern Legal Practice, 241 LEGAL INTELLIGENCER 93 (May 14, 2010).
 33. See Molly McDonough, Trial Consultants Add Facebook/MySpace to Juror Research Toolbox, A.B.A.J. (Sept. 29, 2008).
 34. See Nadia White, UM's Grace Case Project, THE MONTANA LAWYER (April 2010).
 35. See Order, *United States v. W.R. Grace*, No. 05-07-M-DWM (D. Mont. April 28, 2009); Jury Instruction, *United States v. W.R. Grace*, No. 05-07-M-DWM (D. Mont. April 28, 2009). □
- © Thomas C. Frongillo and Daniel K. Gelb, 2010. All rights reserved.

National Association of Criminal Defense Lawyers (NACDL)
1660 L St., NW, 12th Floor, Washington, DC 20036
(202) 872-8600 • Fax (202) 872-8690 • assist@nacdl.org