Chapter 2
THE IMPACT OF SOCIAL NETWORKING IN CRIMINAL CASES

David H. Angeli
Avalyn Taylor

Table of Contents

I. INTRODUCTION ........................................................................................................ 2-1
II. UNITED STATES v. DREW AND NEW SOCIAL NETWORKING “CRIMES” .... 2-2
III. SOCIAL NETWORKING AND CRIMINAL LAW ................................................... 2-3

A. Criminal Investigations .......................................................................................... 2-3
  1. Social Networking Sites as Investigatory Tools ........................................ 2-3
  2. Is There a “Reasonable Expectation of Privacy” in Social Networking Information? ................................................................. 2-4
  3. DOJ Releases Internal Documents on Social Networking Investigations .................................................................................. 2-6
  4. Ethical Issues Raised by Going Undercover on Social Networking Sites ....................................................................................... 2-8
     a. Philadelphia Bar Association Opinion 2009-02 .............................. 2-8
     b. New York State Bar Committee on Professional Ethics Opinion 843 ......................................................................................... 2-9
B. Discovery ............................................................................................................... 2-9
  1. The Stored Communications Act, the Computer Fraud & Abuse Act, and Subpoenaing Social Networking Sites ........................................... 2-10
     a. The Stored Communications Act................................................... 2-10
     b. The Computer Fraud & Abuse Act................................................. 2-12
2. Case Law on “Relevance”—Varying Approaches ................................. 2-13

3. Duty to Preserve—Legal and Ethical Obligations............................. 2-14

C. Trial ................................................................................................................. 2-15

1. The Admissibility of Social Networking Evidence ............................ 2-15
   a. Authenticity ............................................................................................... 2-15
   b. Other Reasons for Exclusion ....... .................................................. 2-17

2. Social Networking and Juries ............................................................. 2-18
   a. Jury Selection .......................................................................... 2-18
   b. Posting from the Jury Box—Grounds for Mistrial? ............... 2-18

D. Sentencing ....................................................................................................... 2-19

CONCLUSION ....................................................................................................................... 2-20
Chapter 2

THE IMPACT OF SOCIAL NETWORKING IN CRIMINAL CASES

David H. Angeli
Avalyn Taylor

I. INTRODUCTION

A recent episode of the PBS radio series “This American Life” featured a story on comedian Joe Lipari’s recent encounter with law enforcement, based on a Facebook “status update” that he posted after an exasperating trip to the Apple store in Manhattan.1 Frustrated by an hours-long wait at the store to have his iPhone serviced, he returned home and, while watching the popular cult movie “Fight Club,” vented his frustration by “updating his status” on the social networking website Facebook. Inspired by a scene from “Fight Club,” he wrote, “Joe Lipari might walk into an Apple store on Fifth Avenue with an Armalite AR-10 gas powered semi-automatic weapon and pump round after round into one of those smug, fruity little concierges”—a near verbatim quote from the movie. Thinking not much about the posting, other than that his friends would get a kick out of the movie reference, Lipari was completely unaware of the Pandora’s box he had opened.

Within an hour of his Facebook posting, armed police officers were searching Lipari’s apartment and interrogating him. Apparently, one of Lipari’s Facebook “friends” reported the update to the N.Y.P.D., who interpreted it as a potential terrorist threat. Eventually, he was charged with two felonies for making terrorist threats and falsely reporting an incident. Although the case is currently in adjournment and is expected to be dropped, this incident illustrates both the utility of social networking websites for law enforcement and the potential dangers that these websites may pose for unwitting users—or actual criminals.

It goes without saying that social networking websites like Facebook and MySpace have become an integral part of today’s popular culture. Facebook alone has over 500 million “active” users, defined as users who have returned to the site within the past 30 days.2 Of these users, half log on to the website at least once a day.3 Further, gone are the days when these websites were only the domain of Gen-Yers. Increasingly, older Americans and professionals are utilizing these websites for both personal and professional networking, information sharing, and entertainment. According to a study by the Pew Research Center, social networking among internet users ages 50-64 grew by 88 percent between April 2009 and May 2010.4 Lawyers have also increasingly embraced social networking. In a 2010 American Bar Association survey, fifty-six percent of lawyers surveyed said that they are members of at least one online social network, compared to only fifteen percent in 2008.5
Much like the widespread expansion of the use of e-mail in the 1990s, social networking has fundamentally and permanently altered the legal landscape in nearly every area of civil and criminal law. This article examines the myriad ways in which social networking has influenced the field of criminal law at every stage in a criminal proceeding—from the budding criminalization of certain online activities, to investigation, to trial, and to sentencing. It also identifies and discusses ethical issues—for both prosecutors and the defense bar—that may arise as these issues become increasingly relevant in this new electronic frontier.

II. **UNITED STATES v. DREW AND NEW SOCIAL NETWORKING “CRIMES”**

The Communications Decency Act of 1996 currently exempts websites and internet service providers from liability relating to information posted by third party users, even if it is used for criminal purposes. It also protects them from liability for refusing to disclose the identities of anonymous posters who use the websites for criminal or fraudulent activities. 47 U.S.C. § 230(c). However, despite the legal protections that exist for social networking providers, a recent federal case in California reveals the growing trend of social networking users being held criminally responsible for their actions.

In *United States v. Drew*, 249 F.R.D. 449 (C.D. Cal. 2009), a jury convicted a Missouri woman who had created a false MySpace entry of violating the Computer Fraud and Abuse Act (CFAA), a statute that had formerly been used exclusively to prosecute computer hackers. The defendant, Lori Drew, had created a fake MySpace profile of a teenage boy, “Josh,” and used it to “friend” and develop an online relationship with one of her daughter’s friends, teenager Megan Meier.6 After several months of online correspondence, “Josh” lashed out at Meier. Shortly after receiving a message from “Josh” that the world would be a better place without her, Meier committed suicide. *Id.* at 452.

The incident generated significant media attention and public outrage, but Missouri officials determined that Drew had broken no state laws and declined to press charges.7 However, in a move that the New York Times dubbed “highly unusual,” the U.S. Attorney in Los Angeles, where MySpace is headquartered, asserted jurisdiction over the case and charged Drew with three felony violations of the CFAA.8 Prosecutors argued that Drew’s creation of the false profile in violation of MySpace’s Terms of Service, in itself, constituted the “unauthorized use” of a computer used in interstate commerce, a felony under the statute. *Id.* at 461. Although the jury reduced the felony charges to misdemeanors, it ultimately convicted Drew of the charges. *Id.* at 453.

However, amid significant legal criticism in response to the conviction,9 a federal district court granted Drew’s motion for judgment of acquittal. Striking down Drew’s conviction under the void for vagueness doctrine, the court reasoned that the interpretation of the CFAA posited by the government would make any intentional violation of an Internet website’s terms and conditions a crime, “transforming [the CFAA] into an overwhelmingly overbroad enactment that
would convert a multitude of otherwise innocent Internet users into misdemeanant criminals.” *Id.* at 466. It also held that the “clickwrap” agreements that the users of social networking websites enter into are not sufficient to put users on notice of potential criminal liability. *Id.* at 463-65.

Although Lori Drew was ultimately acquitted, her story raises important questions about whether criminal laws should be revamped to address the ever-changing ways in which people use Internet technologies. The *Drew* case is part of a growing trend among legislatures and prosecutors to criminalize “cyberbullying” and hate speech. To date, seven states have passed anti-cyberbullying laws that include criminal penalties, and legislation is pending in several others. In Congress, Representative Linda Sanchez has introduced a bill entitled the “Megan Meier Cyberbullying Prevention Act,” which would amend the federal criminal code to make it a crime, punishable by up to two years in prison, to “[transmit] in interstate or foreign commerce any communication, with the intent to coerce, intimidate, harass, or cause substantial emotional distress to a person.” This trend in criminalizing cyberbullying may be invigorated after the recent tragic suicide of Rutgers University freshman Tyler Clemente, who jumped off the George Washington bridge after his roommate allegedly posted a live Internet feed of him having sex with another man—and Twittered about it.

III. SOCIAL NETWORKING AND CRIMINAL LAW

As social media sites have permeated nearly every aspect of many people’s lives, they have also become an important tool for law enforcement to investigate criminal activities and, consequently, the Achilles heel of many criminal defendants in the United States justice system. The following section discusses some of the ways in which social networking information has influenced criminal investigations, as well as the ethical issues raised by the growing trend of “going undercover” on social networking websites.

A. Criminal Investigations

It should come as no surprise that social networking sites have become important sources of information for both prosecutors and defense attorneys in researching criminal defendants, witnesses, and other key players in criminal cases. Further, as Joe Lipari’s story illustrates, the information that individuals post on social networking sites, in itself, can bring them into the focus of law enforcement. Although the law is still developing in this area, government agents routinely search these websites to obtain information on criminal suspects, often without search warrants.

1. Social Networking Sites as Investigatory Tools

There are countless examples of law enforcement officials using social networking websites to target and research suspected criminals. These websites are especially useful in police investigatory work because of the wealth of personal information available on the sites—
including individuals’ social networks, photographs, likes and dislikes, and whereabouts. Sites such as MySpace and Facebook also allow users to update their “status,” which often provides law enforcement with useful information about a suspect’s state of mind at a given time. Such information may enable law enforcement to establish probable cause to search a suspect’s residence, or may lead to information about a suspect’s motives or accomplices. The following are just a few examples of ways that investigators have used social networking websites to identify and gather evidence:

- Police used a photograph of a defendant on MySpace to enable a witness to make a pretrial identification of the defendant based on the tattoos visible in the MySpace picture, after the witness was unable to identify the defendant in a pretrial lineup.14

- Police in Massachusetts located and arrested three men accused of sexual assault of a woman who had met the men on MySpace, based on the usernames and account information that MySpace provided to police.15

- In La Crosse, Wisconsin, police issued tickets to at least eight minors for underage drinking based on photographs the teens posted on social media websites.16

- In the prosecution of University of Texas student Laura Hall for assisting her friend in the dismemberment of the body of a fellow student who the friend had murdered, prosecutors introduced information from Hall’s Facebook profile to show her motive for involvement, including movies, quotations, and music lyrics which suggested a penchant for extreme violence. (For example, Ms. Hall had listed as her favorite quotation, “You’re part music and part blood, part thinker and part killer. And if you can find all of that within you and control it, then you deserve to be set apart.”)17

Additionally, many law enforcement officials routinely create assumed identities on social networking websites to gain access to information on criminal suspects. For example, one Massachusetts police chief maintains an undercover Facebook persona, changing the site’s photo daily, in order to gain information on potential suspects.18 He views this practice as no different “than putting on a pizza guy uniform and knocking on the door.”19 However, doing so violates such websites’ user agreements—for example, Facebook’s Terms of Service prohibit the use of false accounts, and the site has refused to make an exception for law enforcement purposes.20

2. Is there a Reasonable Expectation of Privacy in Social Networking Information?

“What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection.” United States v. Katz, 389 U.S. 347, 351 (1976).
An important question that must be answered in analyzing the role of social networking information in criminal law is whether the government’s “search” of social networking information—including photographs, messages, and personal information—violates the Fourth Amendment’s prohibition on unreasonable searches. For Fourth Amendment protections to attach, social networking users must have a reasonable expectation of privacy in information they post and receive on social networking websites. *Katz*, 389 U.S. 347, 351 (1976). Although the law is still developing in this area, other cases in the electronic media area suggest that a defendant making such an argument may face an uphill battle.

**COMMENT:** If the Facebook user has not proactively set her privacy settings to “private,” her profile information—including her wall posts (messages friends write on the profile page), status updates, and photographs—is available for viewing by any other member of Facebook. If a person changes her privacy settings to “private,” only “friends” or “networks” (friends of friends) of the user may view most of her profile—including the information listed above. This article refers to such information as “private” profile information.

*However*, and importantly, some “basic information” remains “public”—visible to all Internet users—even when a user changes her privacy settings to private. This includes the user’s name, profile picture, gender, and friends and networks (including groups that person belongs to, such as alumni associations or political groups). Other information—including a person’s interests, likes and dislikes, relationship status, and contact information—is also set as a default to be viewable by all Internet users, but may be set to private. Finally, activating an account’s privacy settings may not actually mean that social networking users are restricting access to their accounts. Research has shown that many people accept “friend” requests from nearly anyone who asks them, whether or not they know the prospective “friend.”

As noted above, the *Katz* rule suggests that “public” information on a user’s profile may not be afforded any constitutional privacy protections. However, the issue becomes more complex if, for example, the user places privacy protections on her profile, or the government accesses, without a warrant, information from an e-mail message sent via a social networking site. Similar issues arise if the individual’s site is privacy protected, but the site is accessed by the government through a third party—such as an informant—who the user has authorized to view his profile.

Courts will likely look to Fourth Amendment jurisprudence governing searches of other electronic information to determine whether a reasonable expectation of privacy exists in “private” social networking information. In this regard, the Sixth Circuit has held that members of a “private” online bulletin board have no reasonable expectation of privacy in their “user information,” including their names, birthdates, and passwords. *Guest v. Leis*, 255 F.3d 325 (6th
Cir. 2001). The court reasoned that the users of the site had no reasonable expectation of privacy in their user information because “they communicated it to the systems operators.” Id. at 336. Further, in United States v. Gines-Perez, 214 F.Supp.2d 205 (D.P.R. 2002), the court determined that a defendant had no reasonable expectation of privacy in a photograph of himself placed on an allegedly private website that was used to identify him for arrest. The court held that by its very nature, information about oneself placed on the Internet ceases to be private, stating:

A person who places information on the information superhighway clearly subjects said information to being accessed by every conceivable interested party. Simply expressed, if privacy is sought, then public communication mediums such as the Internet are not adequate forums without protective measures.

Id. at 225.

Recently, in City of Ontario v. Quon, 130 S.Ct. 2619 (2010), a unanimous Supreme Court declined to rule on whether an employee had a reasonable expectation of privacy in the content of text messages on his government employer-issued cell phone, but ruled nonetheless that a search of these communications was reasonable. The Court recognized that expectations of privacy have changed in our Internet-focused world, stating, “[c]ell phone and text message communications are so pervasive that some persons may consider them to be essential means or necessary instruments for self-expression, even self-identification. That might strengthen the case for an expectation of privacy.” Id. at 1230. Although the Court ultimately declined to address the privacy expectation issue, the fact that that it found the search to be reasonable may indicate a reluctance to expand the Fourth Amendment’s protections to shared information on the Internet.

Further, in a number of settings, courts have found no reasonable expectation of privacy in e-mail messages and inboxes.23 Thus, even with privacy protections in place, the government’s search of a user’s “private” information on a social networking website may be deemed “reasonable” under the Fourth Amendment.

PRACTICE TIP: Despite the fact that the law in this area is not yet fully developed, there is little doubt that individuals have a greater expectation of privacy in material that they have proactively protected via social networking privacy settings, so attorneys should, as a matter of course, advise their clients and witnesses to change their privacy preferences to the most restrictive settings.

3. DOJ Releases Internal Documents on Social Networking Investigations

In March 2010, in response to a Freedom of Information Act request by the Electronic Frontier Foundation, the Department of Justice (“DOJ”) released an internal PowerPoint presentation entitled “Obtaining and Using Evidence from Social Networking Sites.”24 Though
thin on details and partially redacted, the 33-page document sheds some light on the government’s recognition of both the utility of social networking sites for investigations and the potential legal problems that may arise.

The presentation, which was intended to educate law enforcement officials about social networking sites and their potential utility in investigations, began with an overview of the most popular social networking websites (Facebook, MySpace, Twitter, and LinkedIn) and their features. The presentation then focused on how and why investigators should use these tools. In one slide, the presentation poses the question, “Why go undercover on Facebook, MySpace, etc.?” and lists the following reasons:

- Communicate with suspects/targets
- Gain access to non-public info
- Map social relationships/networks

The presentation also notes that most social networking sites’ terms of service contain exceptions for emergency disclosures to law enforcement, and that all of them contain exceptions to respond to legal process.

Interestingly, there are numerous references in the DOJ presentation to the potential legal issues presented by violating a website’s terms of service during investigations. In a slide entitled “Going Undercover,” the presentation mentions United States v. Drew (discussed in Section II, supra), which explores whether a violation of a website’s terms of service is “unauthorized activity.” 249 F.R.D. 449 (C.D. Ca. 2009). Another slide entitled “Legal and Practical Issues: Undercover Operations,” poses the question, “[i]f agents violate terms of service, is that ‘otherwise illegal activity?’” Though not explained, the reference to “otherwise illegal activity” presumably refers to the provision in the Attorney General’s Guidelines Regarding the Use of Confidential Informants which requires that confidential informants receive special authorization before participating in otherwise illegal activity.28 It is unclear whether this presentation was given before or after the Drew case was decided that same year.29 In any event, the presentation makes clear DOJ officials’ awareness of the potential legal problems posed by law enforcement officials going “undercover” on social networking websites.

Although the Drew court held that the violation of a social networking site’s terms of service is not, ipso facto, a crime, numerous ethical issues come into play when an attorney or his agent goes undercover online. For example, while not necessary a crime, is it an ethical violation to create false personas on Facebook or another social networking website in order to obtain information on defendants or witnesses?
4. Ethical Issues Raised by Going Undercover on Social Networking Sites

As mentioned above, it has become standard practice, not only for prosecutors, but for all types of attorneys, to use social networking websites to research their clients, witnesses, and other key parties to litigation. Although it might seem to some that information posted online for public consumption is “fair game,” attorneys—including prosecutors—who use false pretenses to gather social networking information run the risk of violating their ethical obligations.

To date, two State Bar ethics committees have issued opinions—reaching different conclusions—on the issue of whether “undercover” social networking activity is a violation of state ethics rules. Although these opinions did not arise in the course of criminal proceedings, they nevertheless raise important ethical considerations that should be considered by both prosecutors and defense counsel in obtaining information from social networking sites.

a. Philadelphia Bar Association Opinion 2009-02

Recently, the Ethics Committee of the Philadelphia Bar Association considered whether it was a violation of the Pennsylvania Code of Conduct for a third party, at the request of an attorney, to “friend” a witness unknown to him in order for the lawyer to gain access to that person’s profile information. The committee found that doing so would violate Pennsylvania Rule 8.4 (prohibiting lawyers from “engag[ing] in conduct involving dishonesty, fraud, deceit or misrepresentation”) because “[i]t 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.” It also found that doing so would violate Rules 4.1 (Truthfulness in Statements to Others) and 5.3 (Responsibilities Regarding Nonlawyer Assistants).

The Committee considered it immaterial that, by accepting friend requests from strangers, some people make themselves vulnerable to having their personal information accessed by third parties for litigation or investigatory purposes, stating:

Even if, by allowing virtually all would-be “friends” onto her Facebook and MySpace pages, the witness is exposing herself to risks like that in this case, excusing the deceit on that basis would be improper. Deception is deception, regardless of the victim’s wariness in her interactions on the internet and susceptibility to being deceived.
b. New York State Bar Committee on Professional Ethics Opinion 843

Shortly after the release of the Philadelphia Bar Association opinion, the Professional Ethics Committee of the New York State Bar reached a slightly different conclusion on similar but not identical facts. The committee considered whether it was a violation of New York’s ethics rules for an attorney to obtain information on a person’s social networking profile that is publicly available to all users of the network. The committee concluded that such activity did not violate the state’s ethics rules, reasoning that “[o]btaining information about a party available in the Facebook or MySpace profile is similar to obtaining information that is available in publicly accessible online or print media, or through a subscription research service such as Nexis or Factiva, and that is plainly permitted.”

In its opinion, the committee stated that its decision was limited to information that was available to all users on a social networking site, as opposed to only the user’s “friends.” The committee implied—but did not explicitly state—that “friending” a party or witness in order to obtain information might violate ethical rules. Further, it stated that if an attorney “friends” a represented party, he would violate Rule 4.2 (the “no contact” rule). Finally, it stated that a “key difference” between that case and the one at issue in the Philadelphia Bar Opinion was that the New York case concerned a party, whereas in Philadelphia, the attorney wanted to use Facebook to obtain information on a witness. (The committee did not specifically discuss whether or, if so, how this difference affected its analysis).

PRACTICE TIP: Although some jurisdictions (i.e., New York) may allow attorneys to use social networking websites for research purposes, it is, of course, never permissible to contact a represented party without obtaining opposing counsel’s consent. Thus, if a prosecutor or an investigator (at the prosecutor’s request) were to “friend” a represented defendant, he or she would likely be found to have violated rules analogous to Model Rule of Professional Conduct 4.2.

B. Discovery

Social networking information is increasingly sought in discovery in both civil and criminal cases. As discussed above, law enforcement officials routinely utilize social networking information in investigations. Defense attorneys also mine social networking sites for background, exculpatory material, and impeachment information on third-party witnesses. For example, a Tucson, Arizona defense attorney successfully obtained an acquittal for his client, who was accused of assault, by introducing a video from the state’s key witness’s MySpace page that actually showed the witness starting the brawl at issue.

Facebook has been served with so many subpoenas for information on its sites that it has adopted a formal “Subpoena Policy” that is available on its website. According to the company’s General Counsel, the site receives information requests almost daily from law
enforcement and civil litigators. Defense attorneys are also increasingly seeking material from these websites relating to non-party witnesses. In the civil context, courts have largely held that information contained on social networking websites is discoverable as long as there is some showing of relevance.

PRACTICE TIP: Assume that whatever information your client or witnesses have on social networking sites will surface in discovery. Be sure to ask clients and witnesses what social networking material they have posted online, and validate the answers they give you.

In federal criminal cases, defense attorneys seeking to compel the production of information from social networking sites may invoke Rule 17(c) of the Federal Rules of Criminal Procedure to subpoena that information from either the sites themselves or the social networking account holders. The following section discusses the special issues that arise when subpoenaing information from social networking providers.

1. The Stored Communications Act, Computer Fraud & Abuse Act, and Subpoenaing Social Networking Sites

Even if information on Facebook or another social networking website is discoverable, attorneys seeking information from these sites may not be able to obtain it directly from the social networking providers. This is because such requests are subject to (1) the Stored Communications Act (“SCA”), the provision of the Electronic Communications Privacy Act applicable to Internet Service Providers (ISPs) and other electronic service providers and (2) the Computer Fraud & Abuse Act, which provides a cause of action against one who “intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer if the conduct involved an interstate or foreign communication.”

a. The Stored Communications Act

The SCA sets forth the conditions under which “providers of electronic storage information” may release both the content of communications and “user information” to third parties. Electronic communication service providers are prohibited from divulging customer records unless an exception applies. The SCA does allow for the release of “basic user information”—such as the user’s name and IP address—to third parties.

“[T]here is no exception to this statutory prohibition against disclosure pursuant to a civil discovery subpoena.” J.T. Shannon Lumber Co. v. Gilco Lumber, Inc., Civ. A. No. 2:07-CV-119, 2008 WL 3833216, at *1 (N.D. Miss. Aug. 14, 2008); see also In re Subpoena Duces Tecum to AOL, LLC, 550 F.Supp.2d 606, 611 (E.D. Va. 2008) (“Applying the clear and
unambiguous language of § 2702 to this case, AOL, a corporation that provides electronic communication services to the public, may not divulge the contents of [its customers’] electronic communications to [the requesting party] because the statutory language of the Privacy Act does not include an exception for the disclosure of electronic communications pursuant to civil discovery subpoenas.”); *O’Grady v. Superior Court*, 44 Cal. Rptr. 3d 72, 89 (2006) (holding that “the Act makes no exception for civil discovery”). And the SCA provides a cause of action against anyone who “intentionally accesses [such information] without authorization.”

To date, only one court has directly ruled on the application of the Stored Communications Act to social networking providers. (A number of cases, some of which are cited above, have dealt with the analogous situation of subpoenas directed to ISPs for the production of e-mails and related information.) Earlier this year, in *Crispin v. Audigier*, 2010 WL 2293238 (C.D. Cal. 2010), the court granted a motion to quash a subpoena directed at Facebook and MySpace, ruling that these sites were electronic communication service providers subject to the provisions of the SPA and, as such, could not release content information (versus user account information) to third parties. The district court overruled a magistrate judge’s determination that the act did not apply because the communications were for public display. *Id.* at *9. (The magistrate erroneously believed that all messages sent through these websites were public information, like “Wall Postings.”) The district court reasoned that, because these sites allow individuals to send messages, they are similar to e-mail service providers and are thus subject to the SCA. *Id.*

Although *Crispin* held that social networking sites are subject to the SCA, the statute provides an exception pursuant to which prosecutors and law enforcement can obtain user information to investigate criminal activity. One provision allows ISPs to release the content of communications to law enforcement if the communication “appears to pertain to the commission of a crime.” *Id.* Another allows disclosure if “the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency.” The SCA also permits government entities, when acting in their civil or criminal enforcement capacities, to obtain certain information pursuant to “an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena” served by the government entity. *Id.* However, even in situations in which a government entity is acting in its regulatory or enforcement capacity, it may not properly issue civil discovery subpoenas demanding the production of materials protected by the SCA. *See FTC v. Netscape Comms. Corp.*, 196 F.R.D. 559 (N.D. Cal. 2000) (holding that the “government entity” exception does not apply in the context of civil discovery subpoenas).

For criminal law purposes, it is important to note that, even if social networking sites are subject to the SCA, courts must still determine the degree of privacy protection that must be given to different types of data on social networking sites. For example, the SCA currently
requires law enforcement to obtain a warrant to access communications that have been stored by the provider for less than 180 days. However, for older messages, a subpoena or court order is sufficient. This distinction is important because law enforcement must make a showing of probable cause to obtain a warrant, which requires a greater showing than a subpoena or court order. Further, because Crispin and other decisions have held that a greater degree of protection exists for private messages and posts than ones that are in public view (such as Wall posts), more stringent procedures may be required for law enforcement to obtain the former.

Finally, asserting a constitutional right to obtain potentially exculpatory information contained on these websites, some criminal defendants have argued that a social networking provider’s refusal to release this information is an unconstitutional violation of the defendants’ Sixth Amendment rights. For example, in one California case, a defendant in a sexual assault case served subpoenas on MySpace and Facebook, seeking to compel them to release messages from the alleged victims of the assault which he believed were exculpatory. However, the court refused to compel the information, and no published opinions have further considered that argument.

PRACTICE TIP: Because most social networking sites will generally only release “user information” (the account holder’s name, address, and email and ISP address), even if served with a subpoena, defense attorneys seeking to obtain social networking information may have more success issuing subpoenas directly to third party witnesses, rather than the sites themselves. If the third party witness no longer has access to this information, the subpoena or court order may direct them to give their consent to the social networking sites to release the stored information, which would fall under a “voluntary disclosure” exception of the SCA. Additionally, in criminal cases attorneys may seek exculpatory information directly from the government through asserting their rights to obtain Brady and Giglio materials (potentially exculpatory information in the possession of the government).

b. The Computer Fraud & Abuse Act

The Computer Fraud & Abuse Act provides a cause of action against one who “intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer if the conduct involved an interstate or foreign communication.” A party may recover damages even if the unauthorized access relates to a third party’s computer—the civil remedy extends to “[a]ny person who suffers damage or loss by reason of a violation of this section.” Serving subpoenas on third parties for information relating to their subscribers may well implicate the statute. See, e.g., Theofel v. Farey-Jones, 359 F.3d 1066, 1078 (9th Cir. 2003).

In Theofel—where the defendants served subpoenas on ISPs, seeking e-mails—the Ninth Circuit upheld the district court’s finding that the subpoena, on its face, “was massively
overbroad’ and “patently unlawful.”’ 359 F.3d at 1071-72. The district court had “soundly roasted” the defendants, granting plaintiffs’ motion to quash “and sock[ing] defendants with over $9,000 in sanctions.” Id. The Ninth Circuit characterized the subpoena as “not merely technically deficient, nor a borderline case over which reasonable legal minds might disagree.” Id. at 1074. Rather, the Ninth Circuit concluded that the subpoena “transparently and egregiously violated the Federal Rules, and defendants acted in bad faith and with gross negligence in drafting and deploying it.” Id. (internal quotation marks omitted).

Again, the precise contours of the Computer Fraud & Abuse Act, and its application to social networking sites, remains to be determined. But counsel seeking to obtain information from those sites must be mindful of the statute and its implications.

2. Case Law on “Relevance” – Varying Approaches

Even if material on social networking sites is otherwise discoverable, litigants seeking to discover social networking information must still prove its relevance. In criminal litigation, parties seeking to obtain information from non-party witnesses under Rule 17(c) of the Federal Rules of Criminal Procedure must show that the information sought is “relevant, admissible, and requested with specificity.” United States v. Nixon, 418 U.S. 683, 700 (1974).

Several civil cases have addressed whether social networking information is “relevant” for discovery purposes. Those cases may be useful in predicting how courts might rule on this issue in the criminal context. In Makelprang v. Fidelity National Title Agency, 2007 WL 119149 (D. Nev. 2007), the defendant in a sexual harassment lawsuit moved to compel the production of messages sent to and from the plaintiff’s MySpace account. The defendant believed that the plaintiff had willingly sent e-mails of a sexual nature to coworkers, including the defendant, casting doubt on the veracity of her harassment claim. Id. The court refused to compel the production of the e-mails sent via MySpace, reasoning that the defendants could do no more than speculate about the contents of the e-mail communications. Instead, the court ordered that the defendants narrow their request to relevant e-mails, which might include messages sent via MySpace, but refused to compel the production of other MySpace information (wall postings, photographs, etc.). Id. at *8.

In contrast, in the Canadian case Leduc v. Roman, [2009] CanLII 6838 ON S.C. (Can.), the defendant in a tort case sought discovery of information from Facebook in order to discredit the plaintiff’s claims that the accident at issue had negatively impacted his quality of life. The defense was unable to gain access to the plaintiff’s Facebook page due to the privacy settings on the account, so it could not determine whether the page contained information relevant to the litigation. Regardless, the court ordered production of the materials, holding that the Facebook profile is similar to “categories of documents,” the relevance of which sometimes cannot be ascertained until after a preliminary production is made. The court held that it was “reasonable to infer” that plaintiff’s profile information was “likely” to contain information about how he
was able to lead his life after the accident, because “[Facebook] is a device by which users share
with others information about who they are, what they like, what they do, and where they go.”
Id. at ¶¶ 31-34. Notably, the court held that the same duty of production of relevant material
existed for individuals whose accounts were privacy-protected as those with public profiles. Id.
at ¶ 32.

Finally, some courts have ordered in-camera reviews of social networking materials so
the court could determine relevance before requiring the production of the materials. See, e.g.,
an in camera review of Facebook documents to determine which of the documents were relevant
and therefore discoverable).

**PRACTICE TIP:** Effective discovery requires extensive informal Internet research on
social networking sites—look for social networking information on witnesses, parties,
experts, close relatives, and co-defendants. Even if this information is not admissible at
trial, it can be used to gather information for impeachment or cross examination.

3. **Duty to Preserve – Legal and Ethical Obligations**

What is a criminal defense attorney to do, if, during his initial meeting with a client, the
client informs him that there are numerous photographs on his Facebook profile of him taking
drugs, brandishing weapons, or engaging in other illegal activities? Should the lawyer advise the
client to delete the Facebook page? Although some attorneys have publicly advocated that
approach,50 lawyers who choose this course of action may run afoul of both their ethical
obligations and the law.

Under Rule 3.4 of the Model Rules of Professional Conduct (Fairness to Opposing Party
and Counsel), lawyers may not “unlawfully . . . destroy or conceal a document or other material
having potential evidentiary value,” nor may they counsel any other person to do so. (emphasis
added.) The commentary to the rule makes clear that the prohibition “applies to evidentiary
material generally, including computerized information,” and to information that has potential
evidentiary value to “a pending proceeding or one whose commencement can be foreseen.”
(emphasis added.) Moreover, under both Oregon and federal law, destroying evidence relevant
to pending litigation—or causing someone else to do so—is a criminal offense.51

For these reasons, lawyers should exercise great caution when advising clients about the
possibility of deleting potentially relevant social networking materials. However, as noted
above, attorneys may ethically advise their clients to change the privacy settings on their
accounts so that they are not publicly available. And defense counsel can (and should) advise
their clients immediately to cease posting new information on social networking sites.
C. Trial

Social networking has also influenced many aspects of the trial stage of a criminal proceeding. This section focuses on the manner in which courts have handled the introduction of social networking information into evidence and the numerous ways in which social networking sites have impacted juries.

1. The Admissibility of Social Networking Evidence

Even if evidence is discoverable, parties seeking to use information garnered from social networking websites may nonetheless encounter admissibility issues at trial if the evidence cannot be properly authenticated. Other rules of evidence—e.g., those prohibiting hearsay, character evidence, and unduly prejudicial evidence—may also bar its introduction.

a. Authenticity

Those seeking to introduce evidence from a social networking site—from either the prosecution or defense—must obviously establish that the evidence is authentic, i.e., that it is what the proponent claims it to be. Because anyone with an e-mail address may create a social networking profile, there is significant potential for users to create false personas or pretend to be someone else on the sites, creating serious authenticity problems if that information is then sought to be introduced at trial.

Numerous cases have analyzed the ways in which social networking information sought to be introduced as evidence must be authenticated, and the decisions have varied widely on this issue, as the cases below illustrate.

In *Griffin v. State*, 192 Md. App. 518 (Md. App. 2010), the Maryland Court of Appeals considered whether the trial court erred in admitting a print-out from the defendant’s girlfriend’s MySpace profile, over objection from the defense that the print-out had not been authenticated. The undated profile page contained a message which read, “FREE BOOZY! Just remember, snitches get stitches!” *Id.* at 524. The State sought to introduce the profile page for the limited purpose of corroborating the change in testimony from an eyewitness to the crime, who had originally testified in the first trial (which ended in a mistrial) that he had not seen the defendant at the crime scene, but in the second trial named the defendant as the shooter. *Id.* The witness explained that he had not testified against the defendant at the first trial because the defendant’s girlfriend had threatened him, a claim that was arguably supported by the MySpace post.

The court held that the trial court had not erred in admitting the printout, because there was sufficient circumstantial evidence on and relating to the MySpace profile page to confirm that it indeed belonged to the defendant’s girlfriend. *Id.* at 530. The court noted that the page contained a photograph of the defendant’s girlfriend as the profile picture, her date of birth, and
references to her children and her boyfriend “Boozy.” The court also noted that the girlfriend had testified that “Boozy” was the nickname her boyfriend sometimes went by. *Id.* Finally, the court emphasized that the admission of the page was accompanied by a detailed jury instruction from the judge that it should only be used for the limited purpose of corroborating the eyewitness’s change in testimony.

However, in *Commonwealth v. Williams*, 456 Mass. 857 (Mass. 2010), the Massachusetts Supreme Court came to a very different conclusion on similar facts. The court held that the trial court had erred in allowing a witness to testify about the content of MySpace messages sent to her by the defendant’s brother, which she claimed threatened her in the event she testified against the defendant. The testimony was admitted over a hearsay objection by the defense. *Id.* at 867. That ruling was reversed on appeal because the messages had not been properly authenticated:

> Although it appears that the sender of the messages was using Williams’s MySpace Web “page,” there is no testimony . . . regarding how secure such a Web page is, who can access a MySpace Web page, whether codes are needed for such access, etc. . . . Here, while the foundational testimony established that the messages were sent by someone with access to Williams’s MySpace Web page, it did not identify the person who actually sent the communication. Nor was there expert testimony that no one other than Williams could communicate from that Web page.

*Id.* at 869. It is noteworthy that here—unlike in the *Griffin* case—the court required that the party offering the social networking evidence authenticate that such evidence was actually posted by the person claimed, and not just that a particular social networking account belonged to that person. These disparate rulings illustrate how courts are still grappling with how to apply the rules of evidence to social networking information.

**PRACTICE TIPS:** Keep in mind the following tips to establish the authenticity of information from social networking websites:

1) Provide testimony from the person who obtained the copy of the Web page, stating when and how it was copied and affirming that the copy is accurate.

2) Offer evidence that the purported author of a profile or message actually wrote it, which may include:
   - an admission by the author;
   - testimony of a witness who observed the creation of the online content;
   - content on the profile page that connects it to the author; or
   - by stipulation.
b. Other Reasons for Exclusion

Social networking information may be subject to exclusion based on other evidentiary rules, including information that reveals evidence of prior criminal convictions, is impermissible character evidence, is inadmissible hearsay, or is unduly prejudicial.

All written evidence on social networking websites—including status updates, messages, and photograph captions—are hearsay if offered to prove the truth of the matter asserted. Exemptions (non-hearsay) and exceptions (admissible hearsay) pursuant to which such evidence may nonetheless be admitted include: present state of mind (e.g., a status update moments before a shooting in which a defendant expresses anger toward the victim); admission of a party-opponent (e.g., a status update or message bragging about having committed a crime); or as impeachment material (e.g., a witness claiming a belief in nonviolence is shown in a Facebook photograph brandishing a gun). Further, if a criminal defendant has not “opened the door” to the introduction of character evidence, social networking information should not be admissible to cast negative light on the defendant’s character. Finally, attorneys should look for references on social networking sites to a defendant’s prior convictions, such as mentions of “doing time” or previous trials, which may be inadmissible.

In criminal sexual assault cases, defense attorneys may encounter rules against using social networking evidence to cast doubt on the veracity of the victim’s story. For example, Oregon’s Rape Shield Statute, OEC 412, prohibits the introduction of evidence relating to a sexual assault victim’s reputation, character, or past sexual behavior. Thus, for example, it would not be permissible to admit Facebook photographs of a victim scantily clad or intoxicated in order to prove that the sexual encounter was consensual. Similarly, in State v. Corwin, 295 SW 3d 573 (Mo. App. S.D. 2009), a trial court refused to allow a defendant in a rape case to admit evidence of the victim’s Facebook status updates—which referred to nights of hard partying and unexplained bruises—to impeach her testimony. The court of appeals upheld the exclusion, holding that the Facebook entries, which were posted nine months after the alleged incident, were not relevant to the charges. Id.

Finally, even if evidence is excluded at or before trial, attorneys should be mindful that if information on their clients’ social networking sites is not privacy protected, any user of that site—including potential or current jurors—may view it. As one commentator observed, “[t]he . . . availability [of social networking information] to the average juror even if excluded at trial undercuts . . . traditional protections [in criminal trials] and the policies they support.”53 Thus, avoiding jury bias is another reason why attorneys should counsel their clients to change the privacy settings on their accounts so they are not easily accessible to all users.
**PRACTICE TIP:** Attorneys who know that they will have an admissibility objection to content on a social networking website should consider addressing it prior to trial with a motion in limine, in order to avoid potential jury bias from the introduction of such evidence even if it is later excluded.

2. **Social Networking and Juries**

According to the Pew Research Center, nearly half of American Internet users ages 50-64 are members of at least one social networking site, with an even higher percentage of use among younger Americans. Thus, attorneys should expect for many of their jurors to be social networking users, for better or for worse. In some respects, this can be very helpful to attorneys and litigants—especially if the social networking sites enable attorneys to research their jury pool. However, these sites may serve as tempting mechanisms for jurors to obtain and distribute outside information about ongoing trials, potentially undermining a defendant’s Sixth Amendment rights to an impartial jury and compulsory process.

a. **Jury Selection**

Just as social networking websites have become useful tools for researching parties and witnesses, attorneys and jury consultants have also increasingly turned to them to gather information about potential jurors. For instance, numerous jury consultants have used sites such as Facebook and MySpace to determine whether jurors answered truthfully on their juror questionnaires. For example, one consultant, for example, reported a juror answering on his questionnaire that he had no political affiliation, but his Facebook and MySpace pages revealed that he belonged to “fringe right-wing conservative groups.”

As mentioned above (see “Comment,” supra p. 2-5), even if a person has activated his or her account privacy preferences to the most private settings, the “basic information” (gender, profile picture, friend list, and likes and dislikes), as well as Facebook groups that person belongs to (such as alumni associations, political groups, and sports fan clubs) remain open for viewing to any member of the network. Thus, even if a juror has activated her privacy settings, these sites may still reveal essential information about potential jurors during *voir dire*.

b. **Posting from the Jury Box – Grounds for Mistrial?**

Jurors, often armed with smart phones that enable them to go online with a simple click, may—perhaps inadvertently—impede a defendant’s right to a fair trial by social networking. For example, in the mail and wire fraud trial of former Philadelphia politician Vincent Fumo, a juror repeatedly issued Twitter postings and Facebook status updates regarding the trial. See *U.S. v. Fumo*, 639 F.Supp.2d 544 (E.D. Pa. 2009). For example, one post issued shortly before the verdict stated, “Stay tuned for a big announcement on Monday everyone!” *Id.* at 559 n.11.
Despite Fumo’s argument that these posts impeded his right to a fair trial, especially because numerous other jurors were aware of the Tweeting, the judge denied Fumo’s motion for a mistrial because of the general nature of the posts. He noted that the juror had not revealed any specific facts relating to the trial, and thus concluded that the posts “were nothing more than harmless ramblings having no prejudicial effect” and were “so vague as to be virtually meaningless.” Id. at 554. However, because of the dangers illustrated by cases like these, some courts have imposed restrictions on juror Internet use in the courtroom, and, in at least one case, throughout the entire trial.56

Additionally, many jurisdictions have begun including specific provisions in their jury instructions to warn jurors about their use of social networking websites and other Internet sources during trials. For example, one Multnomah County jury instruction stated, “Do not discuss this case during the trial with anyone, including any of the attorneys, parties, witnesses, your friends, or members of your family. ‘No discussion’ also means no emailing, text messaging, tweeting, blogging or any other form of communication.”57 It also reminded jurors not to use the Internet to research the case during the trial, stating, “[i]n our daily lives we may be used to looking for information on-line and to ‘Google’ something as a matter of routine. . . . You must resist that temptation for our system of justice to work as it should.”58 This type of instruction is becoming progressively more common.

In some cases, judges have declared mistrials based on jurors’ improper Internet use. In a federal drug case in Florida, a judge found out, after one juror came forward and confessed, that a total of nine jurors had been doing research about the case on the Internet. Accordingly, the judge declared a mistrial, stating that he felt he had no other choice.59 In light of the temptation among jurors to use the Internet during trials, criminal attorneys should craft jury instructions to explicitly preclude this type of behavior. Further, should a juror’s social networking or Internet activities come to light during or after a trial, attorneys should consider moving for a mistrial.

D. Sentencing

Social networking has also influenced the final stage of many criminal proceedings, sentencing. Prosecutors have successfully introduced such material as evidence of “relevant conduct” to justify sentencing increases or at revocation hearings to show likely violations of probation.

In State v. Altajir, 123 Conn.App. 674, 2010 WL 3489049 (Conn. App. 2010), photographs from a defendant’s Facebook page were used to support the inference that a defendant had violated the terms of her probation. At the probation revocation hearing for a defendant who had been convicted of involuntary manslaughter in a drunk driving accident, the state sought to introduce photographs from the defendant’s Facebook page depicting the defendant drinking alcohol and attending parties. Id. Although these activities were not a violation of her probation, per se, the state argued that “inferences could be drawn [from the
photographs] that the defendant possibly could have been drinking and driving and . . . she had
not reformed, nor . . . learned from her mistakes.” Id. The judge admitted some of the
photographs, and ultimately revoked the defendant’s probation, stating in his ruling, “I'm looking
at these pictures, and all I can think of is, where is the remorse?” Id. On appeal, the defendant
argued that her due process rights were violated because the trial court substantially relied on the
unauthenticated Facebook photographs in its decision. Id. at *6. However, the appellate court
decided that this claim because it determined that, as an evidentiary rather than
constitutional issue, it did not merit review, and affirmed the judgment on other grounds. Id.

Similarly, in United States v. Villanueva, 315 Fed.Appx. 845 (11th Cir. 2009), the
Eleventh Circuit affirmed the sentencing enhancements of a convicted felon for being in
possession of a firearm, based upon the discovery of both MySpace photographs and a YouTube
video of the defendant brandishing several different firearms. Although the defendant argued
that the guns in the photographs were plastic pellet guns, and that there was no way of knowing
when the photographs and video were taken, the court upheld the trial court’s finding that they
depicted actual weapons and were taken after the defendant’s conviction. Id. Further, the court
upheld the finding that the photographs and video featured the defendant holding different
firearms, which justified a two-count sentencing increase for the possession of three or more
firearms. Id. at 849.

One commentator recently noted that information taken from social networking websites
may also serve as a mitigating, rather than incriminating, factor in sentencing, and that defense
attorneys should consider using this information to display “humanizing portrait[s]” of criminal
defendants.60 The commentator also noted that social media sites can and have played an
important role in generating positive letters to include in the pre-sentence report. For example,
he mentioned the case of a Pennsylvania official who, after pleading guilty to federal corruption
charges, sent a message to his 1,270 Facebook friends asking them to write the judge to
encourage leniency in his sentence.61 He ultimately received a sentence below the applicable
Guidelines range.62

As with the other stages of criminal proceedings, the use of social media information in
sentencing reinforces the practice points made above: ensure that clients change their privacy
settings to the most restrictive settings, and—once under criminal investigation—cease social
networking activity. Further, defense attorneys may consider using these sites to advocate for
lesser sentences.

CONCLUSION

As ever-increasing numbers of Americans join the online social media bandwagon, the
impact of social media on the American legal system will undoubtedly expand. In the arena of
criminal law, social networking has already made a significant mark. Additionally, the rise of
this technology has raised numerous ethical issues that bar committees and courts are only beginning to address.

The case of United States v. Drew, which was ultimately dismissed, demonstrates that prosecutors are searching for new tools to hold individuals who engage in harassment or bullying over social networking sites legally responsible for such actions. It also demonstrated that, although the violation of online user agreements is not yet in itself a crime, state legislatures, which have already begun a movement toward enacting anti-cyberbullying statutes, might seek to criminalize certain social networking behavior in addition to harassment. This may include the criminalization of behavior such as the creation of false profiles or unauthorized use of another person’s profile.

Along with the increased potential that a person’s social networking activities might give rise to criminal liability, social networking information has become an important tool for law enforcement officials. As demonstrated by the cases discussed above, officials have used social networking websites for everything from enabling witness identifications of suspects to investigating gang affiliations to going undercover to gather evidence against suspected criminals. Further, defense attorneys are routinely mining these sites for information on their clients, witnesses, and other key players.

Government searches of social networking data, depending on the location of the data, may not require a search warrant because some courts have held that no reasonable expectation of privacy exists in information that users voluntarily place on the Internet. However, some courts have held that Internet users have a greater expectation of privacy in information that is only viewable by one or a few people (such as a message sent via a social networking site), rather than visible to many (such as a Wall posting). With respect to such “private” information, the government probably must make some showing in order to obtain information from a social networking provider. However, because the Stored Communications Act is likely applicable to social networking providers, the government may be held to a lower standard for searches of this information than probable cause.

Judges have been generally willing to order the production of social networking information in the discovery process. However, a party seeking to request production of this information must be prepared to at least make some threshold showing of relevance, although the exact standard will vary from court to court. Finally, one court has interpreted the Stored Communications Act to apply to social networking site providers, therefore they cannot be compelled to release the content of user’s messages to third parties. Further, the Computer Fraud and Abuse Act protects social networking sites from civil liability for material placed on their sites by third party users. That statute may also be interpreted to create a civil cause of action from the unauthorized release of social networking information.
During trial, social networking information will generally be admitted into evidence as long as it is authenticated and not contrary to any other rules of evidence. Courts have varied regarding the degree to which information from social networking websites must be authenticated to be admissible, but at a minimum some evidence seems to be required to demonstrate a linkage between the account holder and the person at issue. Information posted on social networking sites has also been utilized by prosecutors to justify sentencing increases or revocations of probation.

In the jury box, social networking may interfere with a criminal defendant’s right to a fair trial by serving as a tempting medium by which jurors can share confidential trial information with the outside world. Additionally, the wide degree of availability of information on the sites can enable jurors to gain information—such as on prior convictions—about defendants, even if it has been excluded. Finally, social networking information is gaining popularity as an important tool for researching potential jurors in voir dire.

As these issues continue to gain relevance in today’s “brave new world,” attorneys should be aware of both the utility and downfalls of social networking information for their clients. Further, they should take great care to uphold their own ethical obligations while tweeting, posting, blogging, and clicking.

---


6 In Facebook terminology, to “friend” someone is to make an online request for them to become a Facebook friend.


See, e.g., Kendall K. Hayden, *The Attorney and Social Media: How Social Media is Changing the Law*, 73 TEX. B.J. 188, 191 (quoting a prosecutor as stating, “I am always aware of what social networking sites my victims or witnesses belong to. I make it a practice to discuss and examine the contents of their profiles before trial.”)


Sarah Randag, *Police Use Social Networking to Target Underage Drinkers*, ABA JOURNAL ONLINE (Nov. 25, 2009).


*Id.*, (quoting Harvard, MA police chief Edward Denmark).


According to Facebook’s Privacy policy,

"Certain information is visible to everyone because it's essential to helping people find and connect with you on Facebook. Name and profile picture are visible to everyone so real world friends can recognize you, and so we can display them when you write on someone's Wall. Gender is public so we can correctly display your gender (for example, "Add her as a friend"). Networks are visible to everyone so you can see who else is part of your network (and will have access to your information) before choosing "Friends and Networks" for any of your privacy settings. Other information in this section, including hometown and interests, is visible by default to help friends and other people you have things in common with connect with you.


*State v. Townsend*, 147 Wash. 2d 666 (Wash. 2002) (holding that a defendant did not have a reasonable expectation of privacy in email messages he sent to an undercover police officer posing online as a fictitious child); *United States v. Hart*, 2009 WL 2552347, *22* (W.D.Ky. 2009) (noting that the expectation of privacy in email communications is “not a yet fully-formed area of law” and holding that criminal defendant did not have a reasonable expectation of privacy in the content of email messages stored by the Yahoo! server, because he had agreed to Yahoo!’s Terms of Service said that the website could disclose the communications in order to comply with the legal process).


*Id.* at Slide 32.

*Id.* at Slide 30. For example, Facebook has a page entitled “Safety for Law Enforcers” which states,

Facebook works with law enforcement to the extent required by law and where appropriate to ensure the safety of Facebook users. We have developed materials, including a Law Enforcement Handbook, to help officials understand Facebook and ways to request information to aid in their investigations. At the same time, we take the privacy of our users very seriously, and respect the balance between law enforcement's need for information and the rights of our users. We ensure that applicable laws and their limitations on access to any Facebook user data are respected and enforced.


DOJ PowerPoint, *supra* note 24, at Slide 32.


There is a citation within the DOJ PowerPoint to a website that was “last accessed” Aug. 12, 2009, which makes it clear that it was authored after that date. The opinion granting the motion for judgment of acquittal in *United States v. Drew* was released Aug. 29, 2009.


Id. at 3.

Id. The Committee declined to address the separate issue of whether information obtained by the lawyer’s agent could be used in litigation, stating that such a determination was a matter of substantive and evidentiary law to be decided by the applicable court.


18 U.S.C. § 2702(c).


18 U.S.C. § 1030(g).

See, e.g., Molly McDonough, *First Thing Lawyer Tells New Clients: Shut Down Facebook Account*, ABA Journal (Feb. 9, 2010) (quoting a criminal defense lawyer as saying that the first thing he tells new clients is to shut down their Facebook pages).


Matthew Mastromauro, *Pre-Trial Prejudice 2.0: How Youtube Generated News Coverage is Set to Complicate the Concepts of Pre-Trial Prejudice Doctrine and Endanger Sixth Amendment Fair Trial Rights* at n.163, 10 J. High Tech. L. 289 (2010).


Id. (quoting jury consultant Robert Hirschhorn of Cathy E. Bennett & Associates of Lewisville, Texas).


Id.

61 Id.
62 Id.