Pace Law Review

Volume 31
Issue 1 *Social Networking and the Law*
Winter 2011

Article 6

January 2011

Social Media and the Vanishing Points of Ethical and Constitutional Boundaries

Ken Strutin
New York State Defenders Association

Social Media and the Vanishing Points of Ethical and Constitutional Boundaries

Ken Strutin*

Abstract

Social media are extraordinary communication and preservation tools brimming with fonts of incriminating, exculpating, and impeaching evidence. Legal professionals have already added online profiles, instant messaging, and videos to the list of information sources about their clients, their opponents, and their potential witnesses. Still, the bulk of legal authority and ethical guidance is rooted in precedent based on antecedent technologies, which has little resemblance to the emerging social centers of cyberspace. No guidelines for criminal defense discovery or investigation within networked social spaces can be found in existing statutes and ethics codes. One ethics committee has taken the lead on this issue in an opinion curtailing the limits of surreptitious witness investigation through Facebook. Defense counsel's duty to zealously and effectively represent their clients, the practical desire to avoid being sued for malpractice, and the promotion of the fair administration of justice all require a clear demarcation of the ethical and constitutional boundaries for accessing and using data from social networking sites. This Article will examine the dual nature of social media as a communication conduit and information warehouse, the meaning of privacy in this environment, and the ethical and legal dilemmas inherent in prosecuting and defending cases with this new breed of evidence.

---

* Director of Legal Information Services, New York State Defenders Association. J.D., Temple University School of Law, 1984; M.L.S. St. John's University, 1994; B.A., summa cum laude, St. John's University, 1981.

Introduction

Our brick and mortar world is receding into a virtual landscape. There is an online realm where hundreds of millions of people are conversing, networking, and logging the details of their lives. This new mode of human interaction does not fit neatly into any discovery statutes, case law precedents, or ethics codes. Indeed, the administration of justice is struggling to adapt to this emergent reality with little guidance. The social networking era, marked by the creation of instant communities and depots of personal information, is pushing legal practice towards the vanishing points for ethical and constitutional boundaries.

The virtual socialscape exists at right angles to the physical world, and so our perceptions must bend accordingly. In the first decade of this new century, people became accustomed to recording increasingly larger amounts of data about their lives and activities. Five hundred million Facebook users can't be wrong.[1] The creation and development of social media seems to satisfy a very deep biological need.[2] Another

---

1. WILLIE RASKIN, BILLY ROSE, & FRED FISHER, FIFTY MILLION FRENCHMEN (1927); *See* Scott Duke Harris, *Facebook Milestone: 500 Million Members; on to 1 Billion?*, SAN JOSE MERCURY NEWS, July 21, 2010, *available at* http://www.mercurynews.com/ci_ 15568209?nclick_check=1 ("If Facebook gallops ahead at its current pace, the 1 billion mark would indeed be reached in 2011. The online social network Mark Zuckerberg and a few Harvard classmates founded in 2004 went from zero to 250 million users in five years—and doubled that number over the past 12 months despite controversy regarding its privacy protocols."). Cecilia Kang, *Facebook to Hit 500 Million Users, But Meteoric Rise Has Come With Growing Pains*, WASH. POST BLOG (July 19, 2010, 5:00 PM), http://voices.washingtonpost.com/posttech/2010/07/facebook_hits_500_million_user.html ("The Silicon Valley Web site is now the biggest online trust of our vacation photos, electronic rolodexes, and recordings of how we felt about President Obama's candidacy for president, the ban on headscarves in France and the Lindsay Lohan's rollercoaster ride with sobriety. Seventy percent of users are outside the U.S., and one-quarter of all users are checking in and updating their pages from their cell phones.").

2. The explosive growth of social media is due to advances in technology, but its driving force might have originated in the depths of the mirror neuron response, i.e., the need to imitate. *See* Sandra Blakeslee, *Cells that Read Minds*, N.Y. TIMES, Jan. 10, 2006 ("The human brain has multiple mirror neuron systems that specialize in carrying out and understanding not just

important indicator of this subtle migration has been the growth of personal computer hard drives from megabytes to terabytes.[3] The amount of information people collect about their own lives, combined with the data scattered through countless government and commercial databases, are filling citizen libraries.[4] And the volume of information being

---

the actions of others but their intentions, the social meaning of their behavior and their emotions."); Shankar Vedantam, *How Brain's 'Mirrors' Aid Our Social Understanding*, WASH. POST, Sept. 25, 2006, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2006/09/24/AR2006092400718.html ("Three new studies published independently last week in the journal Current Biology have yielded new insights into 'mirror neurons' and point the way to two intriguing conclusions: The mirror system seems to be involved in the human capacity for language, and people with stronger mirror neuron responses to sounds seem to also have a larger capacity for empathy, suggesting the mirror system is part of the brain mechanisms that produce altruistic behavior."); *Use of Social Media in Fashion Industry*, THE VEDA BLOG (Mar. 16, 2010), http://www.vedainformatics.com/blogs/use-of-social-media-in-fashion-industry/ ("Recent research on social media indicates that there may be biological mechanisms that influence individuals who are active in the world of social media. This brain-to-brain link where one person's opinion, movement or behavior influenced the brain cells of others through interpersonal orchestration is known as mirror neurons.").

3. *See* Michael Kanellos, *Here Comes the Terabyte Hard Drive*, CNET NEWS (Jan. 4, 2007), http://news.cnet.com/2100-1041_3-6147409.html ("A terabyte is a trillion bytes, or a million megabytes, or 1,000 gigabytes, as measured by the hard-drive industry. (There are actually two conventions for calculating megabytes, but this is how the drive industry counts it.) As a reference, the print collection in the Library of Congress comes to about 10 terabytes of information, according to the *How Much Information* study from U.C. Berkeley. The report also found that 400,000 terabytes of e-mail get produced per year. About 50,000 trees would be necessary to create enough paper to hold a terabyte of information, according to the report. Who needs this sort of storage capacity? You will, eventually, said Doug Pickford, director of market and product strategy at Hitachi. Demand for data storage capacity at corporations continues to grow, and it shows no sign of abating. A single terabyte drive takes up less space than four 250GB drives, which lets IT managers conserve on computing room real estate. The drive can hold about 330,000 3MB photos or 250,000 MP3s, according to Hitachi's math.").

4. No doubt "citizen libraries" chronicling the lives of ordinary people will soon rival the bulk of Presidential Libraries. *Compare* PETER LYMAN & HAL R. VARIAN, HOW MUCH INFORMATION? 2003, at 2 (2003), http://www2.sims.berkeley.edu/research/projects/how-much-info-2003/printable_report.pdf ("According to the Population Reference Bureau, the world population is 6.3 billion, thus almost 800 MB of recorded information is produced per person each year. It would take about 30 feet of

consumed far outstrips the amount being stored.[5]

Profiles, tweets, and YouTube videos are the equivalent of pyramid building, an effort by individuals to defeat time and overcome their mortality by preserving a colossal monument to their lives, albeit measured in gigabytes instead of cubits. The data from this life logging[6] is creating a form of "micro-celebrity,"[7] memorializing actions and thoughts for indeterminate time periods and creating buzz for forums where

---

books to store the equivalent of 800 MB of information on paper."), *with About the Library*, LIBRARY OF CONGRESS, http://www.loc.gov/about/facts.html (last visited Aug. 26, 2010) ("Twelve Presidential Libraries maintain over 400 million pages of textual materials; nearly ten million photographs; over 15 million feet (5,000 km) of motion picture film; nearly 100,000 hours of disc, audiotape, and videotape recordings; and approximately half a million museum objects.").

5. *See* ROGER E. BOHN & JAMES E. SHORT, HOW MUCH INFORMATION? 2009 REPORT ON AMERICAN CONSUMERS 14 (2009), http://hmi.ucsd.edu/pdf/HMI_2009_ConsumerReport_Dec9_2009.pdf ("According to some estimates, the total amount of hard disk storage worldwide at the end of 2008 was roughly 200 exabytes. In other words, the 3.6 zettabytes of information used by Americans in their homes during 2008 was roughly 20 times more than what could be stored at one time on all the hard drives in the world.").

6. *See generally* Gary Wolf, *The Data-Driven Life*, N.Y. TIMES, Apr. 26, 2010 ("One of the reasons that self-tracking is spreading widely beyond the technical culture that gave birth to it is that we all have at least an inkling of what's going on out there in the cloud. Our search history, friend networks and status updates allow us to be analyzed by machines in ways we can't always anticipate or control. It's natural that we would want to reclaim some of this power: to look outward to the cloud, as well as inward toward the psyche, in our quest to figure ourselves out."); *Life-Logging and the Generation Gap over Privacy* (NPR Radio Feb. 14, 2007) ("Daily documentation has become routine as the tech-savvy [] connect with everyone, anyone, anytime. . . . Guests on the program talk[] about 'life-logging,' a system that documents every conversation, movement, and idea through a series of recording gadgets like GPS trackers and even brain scanners.")

7. *See* Clive Thompson, *Clive Thompson on the Age of Microcelebrity: Why Everyone's a Little Brad Pitt*, WIRED MAG., Nov. 27, 2007, *available at* http://www.wired.com/techbiz/people/magazine/15-12/st_thompson ("Microcelebrity is the phenomenon of being extremely well known not to millions but to a small group—a thousand people, or maybe only a few dozen. As [Do It Yourself] media reach ever deeper into our lives, it's happening to more and more of us. Got a Facebook account? A whackload of pictures on Flickr? Odds are there are complete strangers who know about you—and maybe even *talk* about you.").

"microfans" know and debate the intimate details of strangers outside the pale of news media. Additionally, the virtual socialscape is more than information creation and storage; it encompasses communication and interaction.[8] The administration of justice, the investigation of crimes, and the defense of the accused are being changed at the intersections with this virtual world.

This Article will examine the current state of social media, the cross-sections and currents that bring its users into the legal realm, and the existing laws and ethical rules that are guiding attorney conduct. Law and technology tend to develop along parallel lines. The principles and foundations of the legal system are over-layered by changes in society and electronic information sharing. It appears that social media and Internet behavior are leading the drive towards change.[9] Although there are no bodies of statutes and precedent to offer leadership in this area, the necessity of legal processes has already begun to bring some order to the untamed continent inhabited by Facebook, MySpace, YouTube, and Twitter.

In Part I, the panorama of online communities, which have inspired hundreds of millions to create profiles and publish the

---

8. The will to communicate, the need to express the details of our lives so that others can consume them, extends back to the dawn of consciousness. *See* Prakash Chakravarthi, *The History of Communications from Cave Drawings to Mail Messages*, IEES AES MAG., Apr. 1992, at 30 ("Crude drawings on rock and cave walls are the earliest methods of communication which we know. Though it was cumbersome and slow it helped to convey ideas and past events to other people.").

9. *See generally* Danah M. Boyd & Nicole B. Ellison, *Social Network Sites: Definition, History, and Scholarship*, J. COMPUTER-MEDIATED COMM. (Oct. 2007), http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html ("The rise of SNSs indicates a shift in the organization of online communities. While websites dedicated to communities of interest still exist and prosper, SNSs are primarily organized around people, not interests. Early public online communities such as Usenet and public discussion forums were structured by topics or according to topical hierarchies, but social network sites are structured as personal (or 'egocentric') networks, with the individual at the center of their own community. This more accurately mirrors unmediated social structures, where 'the world is composed of networks, not groups.' The introduction of SNS features has introduced a new organizational framework for online communities, and with it, a vibrant new research context.") (internal citation omitted).

unguarded moments of their personal existence for global audiences, will be explored. The definition of privacy and the meaning of access in online social centers will be examined in Part II. Part III will discuss the current methods of electronic discovery and their broadening applications to social media. Parts IV and V will analyze the importance of preserving social networking evidence both as an obligation for the prosecution and a necessity for the defense. Undercover investigation, pretexting online, and the ethical fallout of such practices in the socialscapes of Facebook and MySpace are reviewed in Part VI.

The parallel processes of traditional legal procedures and the line of technology that has revolutionized communication and information practices will be viewed through several notable legal developments. Facebook and MySpace have already come to play an incipient role in acquiring jurisdiction and initiating litigation in civil and criminal proceedings. These sites have provided law enforcement with information for arrest and search warrants, and laid the foundation for indictments, and in some cases convictions. On the civil side, courts have approved service of process through a defendant's online profile. In both arenas, the contents of online profiles and instant messages have played an important role as evidence at trial. But this is only the beginning. These media will eventually become a routine part of serving warrants and complaints, boilerplate discovery requests, evidence in all manner of proceedings, and ultimately, newly discovered evidence for post-conviction motions. For the criminal defendant, social media content might prove to be the DNA of newly discovered exonerating evidence.

I. Social Media, Social Networking, and Every Tweet in Between!

Social Networking provides a different avenue for familiar patterns of human behavior and public concern. For instance, "flash mobs," which are groups of young people connected by instant messaging alerts or e-vites, join in spontaneous activities. Since these "flash mobs" have led to some public

disturbances, they are now the object of law enforcement surveillance.[10] People in prison or on the run are also using Facebook and similar outlets.[11] The professional conduct of attorneys, prosecutors,[12] judges,[13] as well as the behavior of clients,[14] witnesses, and jurors[15] have all been touched by social media.

Depending on the perspective, social networking can complicate legal practice and due process in different ways. Criminal defense counsel have a constitutional obligation to effectively represent their clients and fully investigate their cases. Both civil and criminal practitioners face legal liability and ethical imperatives in handling the representation of a client.

The measure of professional competence in a society that interacts virtually necessitates asking questions such as: what Social Networking Sites (SNS) are people using to communicate and store information and how are they being utilized?[16] Will the information found on Social Networking

---

10. *See* Debra Cassens Weiss, *FBI to Monitor Social Media to Fight 'Flash Mobs' of Roving Teens*, A.B.A. J. (Mar. 25, 2010, 7:36 AM), http://www.abajournal.com/news/article/fbi_to_monitor_social_media_to_fight_flash_mobs_of_roving_teens.

11. *See, e.g.*, Debra Cassens Weiss, *Escaped Convict Captured After Telling of His Exploits on Facebook*, A.B.A. J. (Mar. 25, 2010, 10:58 AM), http://www.abajournal.com/news/article/escaped_convict_captured_after_telling_of_his_exploits_on_facebook/; Meg Handley, *How Prisoners Harass Their Victims Using Facebook*, TIME.COM (Feb. 18, 2010), http://www.time.com/time/business/article/0,8599,1964916,00.html.

12. *See, e.g.*, Rochelle Olson, *Hennepin County Prosecutor Accused of Anti-Somali Posting on Facebook*, STAR TRIBUNE, Feb. 17, 2010, *available at* http://www.startribune.com/local/84525452.html?page=1&c=y.

13. *See generally* Ken Strutin, *Pitfalls of Social Networking for Judges and Attorneys*, N.Y. L.J., Mar. 16, 2010, at 5 [hereinafter *Pitfalls*] (The author discusses ethics opinions and disciplinary decisions demarcating the lines for the behavior of judges and attorneys connecting through social media).

14. *See* Molly McDonough, *First Thing Lawyer Tells New Clients: Shut Down Facebook Account*, A.B.A. J., Feb. 9, 2010, *available at* http://www.abajournal.com/news/article/first_thing_lawyer_tells_new_clients_shut_down_facebook_account.

15. *See generally* Ken Strutin, *Juror Behavior in the Information Age*, LLRX.COM (Dec. 26, 2010), http://www.llrx.com/features/jurorbehavior.htm.

16. *See, e.g.*, Michael Liedtke, *Twitter Quitters Outnumber Tweeters*, ASSOCIATED PRESS, May 5, 2009 (60% stopped using Twitter after a month);

Sites be admissible?[17] Are there any privacy protections or barriers for materials stored on third-party sites?[18] Since almost everyone else is already using them—for example clients, witnesses, and jurors—digital contents are coming in as evidence of guilt, impeachment, and innocence. Therefore, knowledge and understanding of technology will help in investigation, discovery, and jury pool and venue challenges. A lawyer's professional responsibility ought to include staying abreast of this changing virtual environment.[19]

Defense counsel need to have the same level of knowledge about social networking that is required to intelligently handle forensic evidence, i.e., some basic understanding of the principles and mechanics of its operation.[20] The more detailed

---

Teddy Wayne, *Social Networking Eclipses E-mail*, N.Y. TIMES, May 18, 2009, at B3, *available at* http://www.nytimes.com/2009/05/18/technology/internet/18drill.html; Dave Rosenberg, *Twitters and Blogs: Post Once and Bail Out*, CNET NEWS (June 9, 2009), http://news.cnet.com/8301-13846_3-10260753-62.html (10% of users responsible for over 90% of tweets).

17. *See, e.g.*, *Law School Hosts Panel on 'Social Media as Evidence'*, UC DAVIS SCH. L. (Feb. 5, 2010), http://www.law.ucdavis.edu/news/news.aspx?id=2525 ("Now, thanks to Twitter, Facebook, text messaging and social media, a permanent record of the exact words exchanged often exists. This material can be introduced in court, complete with a time stamp showing when it happened.").

18. *See, e.g.*, Pete Cashmore, *Why Facebook's Privacy War Is Not Over*, CNN.COM (May 27, 2010, 4:16 PM), http://www.cnn.com/2010/TECH/social.media/05/27/facebook.privacy.war.cashmore/index.html ("If Facebook's mission is to build a 'more open and connected world' in which users 'share more,' doesn't this contradict the desire of some users to keep their information private?").

19. C*f.* The TJ Hooper, 60 F.2d 737, 740 (2d Cir. 1932) ("Indeed in most cases reasonable prudence is in fact common prudence; but strictly it is never its measure; a whole calling may have unduly lagged in the adoption of new and available devices. It never may set its own tests, however persuasive be its usages. Courts must in the end say what is required; there are precautions so imperative that even their universal disregard will not excuse their omission."); Smith v. Lewis, 530 P.2d 589, 593 (Cal. 1975) (An attorney's competence best measured by "such skill, prudence, and diligence as lawyers of ordinary skill and capacity commonly possess and exercise in the performance of the tasks which they undertake.").

20. *See generally* Debbie Ginsberg & Meg Kribble, *The Social Networking Titans: Facebook and MySpace*, LLRX.COM (Apr. 4, 2008), http://www.llrx.com/features/facebookmyspace.htm; Dave Roos, *How Social Networks Work*, HOWSTUFFWORKS.COM,

and nuanced issues will fall within the purview of expert or investigative assistance.[21] For example, computer forensics can uncover evidence found in digital storage media, sociologists can explain online behavior, and linguists can interpret the codes and subtly of chat and profile postings.[22]

The social media phenomenon is part of Web 2.0, i.e., the shifting of content from top-down publishing to user- and consumer-generated information; in other words, people powered publishing.[23] Social networking is a fast growing segment of this media. In essence, SNSs are "web-based

---

http://communication.howstuffworks.com/how-social-networks-work.htm (last visited July 28, 2010).

21. *See, e.g.*, *Applied Discovery Introduces New E-Discovery Consulting Service to Help Corporations Assess, Mitigate, and Manage Social Media Risks*, PR NEWSWIRE (June 3, 2010, 8:00 AM), http://www.prnewswire.com/news-releases/applied-discovery-introduces-new-e-discovery-consulting-service-to-help-corporations-assess-mitigate-and-manage-social-media-risks-95499699.html.

22. *See* Ken Strutin, *Internet Behavior and Expert Evidence*, N.Y. L.J., Nov. 4, 2008, at 5 ("Web-based criminal cases bring judges and jurors into contact with an enigmatic Internet culture. A clear understanding of cyber-behavior is crucial to assessing probable cause in a search warrant affidavit or the merits of a defense at trial. And misconceptions about Internet conduct, in some instances, may be explained or dispelled by expert evidence."); *see, e.g.*, Debra Cassens Weiss, *Twitter Expert Will Testify Against Courtney Love in Defamation Trial*, A.B.A. J. (Jan. 5, 2011, 7:31 AM), http://www.abajournal.com/news/article/twitter_expert_will_testify_against_courtney_love_in_defamation_trial/.

23. The need of members of a society to communicate, to extend their personal narratives into cyberspace and assume new personae online may have its origins in the beginnings of Western drama—when performances evolved from communal rituals involving everyone into plays performed exclusively by actors. According to one historian, more than 2,000 years ago, the seeds of modern drama started with the exploration of "new dimensions of experience" and the emergence of individual performers pretending to be other people, and finally, the separation of the audience from the performance where "one part of the community was addressing another part." *See* DANIEL J. BOORSTIN, THE CREATORS: A HISTORY OF HEROES OF THE IMAGINATION 207, 209 (1993). This fundamental transformation giving rise to personal expression, or "microtheater," is occurring anew online. *See, e.g.*, John Carroll & David Cameron, *Drama, Digital Pre-Text and Social Media*, 14 RES. IN DRAMA EDUC. 295 (2009) ("The techniques used for the development of the digital pre-text for this project are based on facilitator-generated online social networking and mobile media content. This approach generates the students' examination of mistaken identity as a platform for a classroom exploration of Shakespeare's *Twelfth Night*.")

services that allow individuals to (1) construct a public or semi-public profile within a bounded system, (2) articulate a list of other users with whom they share a connection, and (3) view and traverse their list of connections and those made by others within the system."[24]

The core ingredients of these sites are their individual user profiles (information storage and publication) and communication tools:

> While SNSs have implemented a wide variety of technical features, their backbone consists of visible profiles that display an articulated list of Friends who are also users of the system. Profiles are unique pages where one can 'type oneself into being.' After joining an SNS, an individual is asked to fill out forms containing a series of questions. The profile is generated using the answers to these questions, which typically include descriptors such as age, location, interests, and an 'about me' section. Most sites also encourage users to upload a profile photo. Some sites allow users to enhance their profiles by adding multimedia content or modifying their profile's look and feel. Others, such as Facebook, allow users to add modules ("Applications") that enhance their profile.[25]

For purposes of the penal law, the value of a communication/information source is measured by the need to control access to it.[26] Access to social media has been found to be important enough to be blocked as a condition of punishment. For example, Victor L, a juvenile delinquent and acknowledged gang member, pled guilty to a weapons offense

---

24. *See* Boyd & Ellison, *supra* note 9.

25. *Id.* (citations omitted).

26. *See generally* Ken Strutin, *No-Computer Sentencing*, N.Y. L.J., Jan. 11, 2005, at 5 (discussing the limits of banning access to the Internet, computers or even television as a condition of probation or post-release supervision).

in a California court.[27] He was sentenced to probation, which included interdicting access to MySpace.[28] Specifically, the terms of his probation limiting Internet usage stated: "The Minor shall not access or participate in any Social Networking Site, including but not limited to Myspace.com."[29] In a post-conviction proceeding, he challenged the condition, as well as several others, as vague and overbroad. However, the purpose behind this particular restriction was to "limit Victor's access to the Internet in ways designed to minimize the temptation to contact his gang friends or to otherwise use the computer for illegal purposes by requiring adult supervision whenever he goes online."[30] Therefore, the condition survived constitutional scrutiny, in contrast to other cases, with terms totally banning Internet use or access, which did not.[31]

The case of Victor L spearheads the judicial recognition of SNSs as communication media which can be monitored. Other cases involving social media have focused on its impact as

27. *In re* Victor L., 182 Cal. App. 4th 902, 908 (1st Dist. 2010).

28. *Id.* at 909.

29. *Id.* at 923.

30. *Id.* at 926.

31. Courts seem to be split on the appropriateness of lifetime or conditional Internet bans as a term of probation or supervised release. *Compare* United States v. Heckman, 592 F.3d 400, 409 (3d Cir. 2010) ("We do not hold that limited Internet bans of shorter duration can never be imposed as conditions of supervised release for this type of conduct, but when placed within the context of related precedents, the unconditional, lifetime ban imposed by the District Court in this case is so broad and insufficiently tailored as to constitute 'plain error.' We thus hold that this ban involved a 'greater deprivation of liberty than is reasonably necessary.' 18 U.S.C. § 3583(d)(2).") *with* United States v. Fortenberry, 350 F. App'x 906, 911 (5th Cir. 2009) ("Although we recognize the conditional ban on the internet usage for a lifetime is a harsh condition of supervised release, we cannot say that Fortenberry has demonstrated that imposition of the same was plainly erroneous."). *See generally* Robin Miller, *Validity of Condition of Probation, Supervised Release, or Parole Restricting Computer Use or Internet Access*, 4 A.L.R.6TH 1 (2005); David Kravetz, *U.S. Courts Split on Internet Bans*, WIRED MAG. (Jan. 12, 2010), *available at* http://www.wired.com/threatlevel/2010/01/courts-split-on-internet-bans/ ("[A]ppellate courts are all over the map when it comes to internet bans often imposed on defendants, especially sex deviants, once they have served their time. What's more, the courts appear to be accepting the internet as a basic freedom to which convicts, even the worst of the worst, usually should not be denied permanent access.").

evidence at trial, including its utilization during the commission of a crime,[32] creating a virtual crime scene,[33] and enhancing criminal sentences.[34]

II. The Illusion of Privacy

The tension in social networking investigations is in drawing the line between public and private information. While

---

32. *See, e.g.*, *Hoover Police Capture Two Suspected Facebook Bandits*, MYFOXAL.COM (July 31, 2009, 2:15 PM), http://www.myfoxal.com/global/story.asp?s=10825881 (In Alabama, burglars checked Facebook pages to see who was on vacation to lineup their targets); Chris Matyszczyk, *Facebook Break Leads to Burglary Suspect*, CNET NEWS (Sept. 17, 2009, 4:27 PM), http://news.cnet.com/8301-17852_3-10356117-71.html (In Virginia, a burglar checked his Facebook page in the victim's home during the break-in); *MySpace Pics Lead to Burglary Bust*, ABC-7.COM (Aug. 3, 2009, 6:22 PM), http://www.abc-7.com/Global/story.asp?S=10840135 (Burglars in Florida posted pictures online in which they were posing with the stolen goods). Notably, Louisiana has enacted a law punishing the "[u]nlawful posting of criminal activity for notoriety and publicity." LA. REV. STAT. ANN. § 14:107.4(A) ("It shall be unlawful for a person who is either a principal or accessory to a crime to obtain an image of the commission of the crime using any camera, videotape, photo-optical, photo-electric, or any other image recording device and to transfer that image obtained during the commission of the crime by the use of a computer online service, Internet service, or any other means of electronic communication, including but not limited to a local bulletin board service, Internet chat room, electronic mail, or online messaging service for the purpose of gaining notoriety, publicity, or the attention of the public.").

33. *See, e.g.*, Barbie Nadeau & Christopher Dickey, *Murder Most Wired*, NEWSWEEK, Dec. 3, 2007, at 51 (The investigation into the murder of a British college student in Italy wended its way through familiar social media such as Skype phone calls, photos, stories appearing on Facebook profiles, and a YouTube video); Nicholas Riccardi, *Criminal Charge Filed in Libel Case*, L.A. TIMES, Dec. 4, 2008, at A10, *available at* http://articles.latimes.com/2008/dec/04/nation/na-craigslist-libel4 (During a visitation dispute, a 40-year-old man allegedly posted comments about his former girlfriend on Craigslist Rants and Raves Forum. The state of Colorado charged him with criminal libel.).

34. *See, e.g.*, Eric Tucker, *Social Networking Puts the Bite on Defendants*, LAW.COM (July 22, 2008), http://www.law.com/jsp/lawtechnologynews/PubArticleLTN.jsp?id=1202423145595 (DWI defendants involved in crashes that resulted in serious injuries or death were disappointed to learn that pictures of themselves mocking or flaunting their actions, posted on Facebook or MySpace, had been provided to the court at sentencing.).

the scope of privacy expectations are being debated and argued in the courts, the public side of the online world is being archived and retransmitted without limit. The privacy dilemma lies at the center of a triangle formed by the private enclaves envisioned in the First, Fourth, and Fifth Amendments; service providers' terms of service agreements (TOS) and their definitions of privacy; and the meaning of "reasonableness" as expressed in the practices and habits of millions of online users.

The Wayback Machine,[35] which harvests much of the public side of the Internet, is almost two petabytes of data in size and growing at a rate of twenty terabytes per month.[36] The Library of Congress announced that it will be archiving all public tweets since Twitter started operation in March 2006.[37] The impetus behind Congress' effort was to gather legal blogs, websites of candidates for national office, and websites of Members of Congress and capture a snapshot of public life expressed through tweets to the tune of 167 terabytes. Presently, there are no legal or ethical[38] constraints on public

35. *About the Internet Archive*, INTERNET ARCHIVE, http://www.archive.org/about/about.php (last visited Aug. 13, 2010) ("The Internet Archive is a 501(c)(3) non-profit that was founded to build an Internet library. Its purposes include offering permanent access for researchers, historians, scholars, people with disabilities, and the general public to historical collections that exist in digital format.").

36. *See Frequently Asked Questions*, INTERNET ARCHIVE, http://www.archive.org/about/faqs.php (last visited Sept. 12, 2010) ("How large is the Wayback Machine? The Internet Archive Wayback Machine contains almost 2 petabytes of data and is currently growing at a rate of 20 terabytes per month. This eclipses the amount of text contained in the world's largest libraries, including the Library of Congress.").

37. Matt Raymond, *How Tweet It Is!: Library Acquires Entire Twitter Archive*, LIBR. CONG. BLOG (Apr. 14, 2010), http://blogs.loc.gov/loc/2010/04/how-tweet-it-is-library-acquires-entire-twitter-archive/.

38. *See* Oregon State Bar Legal Ethics Comm., Formal Op. 2005-164 (2005), http://www.osbar.org/_docs/ethics/2005-164.pdf ("Accessing an adversary's public Web site is no different from reading a magazine article or purchasing a book written by that adversary. Because the risks that Oregon RPC 4.2 seeks to avoid are not implicated by such activities, no Oregon RPC 4.2 violation would arise from such electronic access. A lawyer who reads information posted for general public consumption simply is not communicating with the represented owner of the Web site.").

web searching, which includes blogs or personal websites.

But how do privacy settings and terms of service affect the expectation of privacy in social media? The existence of privacy in social media is a key question under codes of ethics and discovery rules. If the expectation is that online profiles are as private as a person's home, desk drawer, or combination safe, then pretexting by private parties becomes problematic.[39] However, this protean media does not offer clarity in its definitions of privacy,[40] and those definitions change with advances in technology and public outcry.[41] Meanwhile, courts and ethics committees are relying on subjective expectations to define privacy in social space.[42]

---

39. *See generally* Douglas R. Richmond, *Deceptive Lawyering*, 74 U. CIN. L. REV. 577 (2005); Ken Strutin, *Pretexting, Legal Ethics and Social Networking Sites*, LLRX.COM (Oct. 5, 2009), http://www.llrx.com/features/pretexting.htm (last visited Sept. 12, 2010) (summarizing current case law and literature on pretexting).

40. *See generally* DANIEL J. SOLOVE, THE FUTURE OF REPUTATION: GOSSIP, RUMOR, AND PRIVACY ON THE INTERNET (2007), *available at* http://docs.law.gwu.edu/facweb /dsolove/Future-of-Reputation/text.htm.

41. *See, e.g.*, Jeffrey Rosen, *The Web Means the End of Forgetting*, N.Y. TIMES, July 25, 2010 (Magazine), at MM30, *available at* http://www.nytimes.com /2010/07/25/magazine/25privacy-t2.html ("All around the world, political leaders, scholars and citizens are searching for responses to the challenge of preserving control of our identities in a digital world that never forgets. Are the most promising solutions going to be technological? Legislative? Judicial? Ethical? A result of shifting social norms and cultural expectations? Or some mix of the above?"); Mark Zuckerberg, *From Facebook, Answering Privacy Concerns With New Settings*, WASH. POST, May 24, 2010, at A19, *available at* http://www.washingtonpost.com/wpdyn/content/article/2010 /05/23/AR2010052303828.html ("We have heard the feedback. There needs to be a simpler way to control your information. In the coming weeks, we will add privacy controls that are much simpler to use. We will also give you an easy way to turn off all third-party services."); Cecilia Kang, *Senate Online Privacy Hearing to Draw FTC, FCC Chairs, Google, Apple and Facebook*, WASH. POST BLOG (July 23, 2010, 11:40 AM), http://voices.washingtonpost.com/posttech/2010/07/the_senate_commerce_co mmittees.html (last visited Sept. 12, 2010) ("Analysts said greater focus from Congress on online privacy has led Web sites and online ad networks to move toward self-regulation to fend off legislation. This self-regulation is aimed at greater disclosure on Web sites that consumers are being tracked, and an easy mechanism for opting out.").

42. *See generally* SOCIAL NETWORKING PRIVACY, http://epic.org/privacy/socialnet/ (last visited Sept. 12, 2010) (collection of

Social media are analogous to open mikes. However, the unguarded remarks of millions who publish their thoughts, criticisms, and gossip on personal profiles are made under an assumed veil of privacy. The public privacy of social networking has not yet been clearly assigned a specific level of First, Fourth, or Fifth Amendment protections,[43] nor has it been given a place among the privileges in the Rules of Evidence.[44] The security of information posted on third-party host sites is defined by those sites, their terms of agreements, their privacy settings, and most importantly the discretion of visitors who can read, copy, and republish without limit. When e-mail gaffes gained prominence, a rule of thumb emerged cautioning users not put anything into an e-mail that they would not want to see printed on the front page of the *New York Times*.[45] No such

litigation and public debate about the problems and violations of consumer expectations in online privacy).

43. *See* Susan W. Brenner, *The Privacy Privilege: Law Enforcement, Technology and the Constitution*, 7 U. FLA. J. TECH. L. & POL'Y 123, 191-92 (2002), *available at* http://grove.ufl.edu/~techlaw/vol7/issue2/brenner.pdf ("The First Amendment protects the privacy of the identity and associates of an individual; the Fourth Amendment protects the privacy of the activities of an individual; and the Fifth Amendment protects the privacy of the thoughts of an individual. The degree to which they protect these different privacy interests has evolved significantly since Justices Brandeis and Warren wrote in 1890. This evolution is directly attributable to the increased sophistication and proliferation of technology. This evolution is also responsible for the shift from the *Olmstead* holding to the *Katz* holding. When the decision was made by [the] *Olmstead* Court, wiretaps were in their infancy and were therefore an exceedingly uncommon event. By the time the decision was made by the *Katz* Court, surveillance technology had become very sophisticated, due in large part to advances made during World War II, and the ability of the government to spy on the activities of people had become a matter of public concern. In changing the focus of the privacy protections of the Fourth Amendment from places to people, the *Katz* Court sought to create a more dynamic standard, one that could be used to address the increasing invasiveness made possible by technology.").

44. *Id.* at 137 ("By the time the Twenty-First Century dawned, cyberspace had become an important new venue for mankind's activities, licit and illicit. The rise and proliferation of cybercrime raised new problems for law enforcement, both with the enforcement of existing substantive laws against conduct vectored through cyberspace and also in the gathering of evidence without violating the existing privacy standards.").

45. *See E-Mail Etiquette*, JOB-HUNT.ORG, http://www.job-hunt.org/onlinejobsearchguide/article_e-mail_etiquette.shtml (last visited Sept. 20, 2010) ("Golden rule of e-mail - Don't put anything in an e-mail that

common wisdom has arisen to chasten people from putting up pictures and videos showing questionable judgment or criminal behavior. In George Orwell's *1984*, it was Big Brother that carried the burden and expense of mass surveillance, but in Web 2.0 surveillance starts from the ground up.[46] The divide between consumer privacy expectations in social networking and the legal recognition of these interests might be informed by the ongoing challenges to e-mail privacy.

Electronic mail is not the equivalent of traditional mail or even a landline phone call. One author has likened e-mails to a postcard[47] and pointed out that the privacy expectations in this format are declining. In his review of recent New York decisions, he suggested that the perception of e-mail privacy hinged on the degree of protections that the sender was willing to take:

> Courts ask, for instance, does a sender leave his or her e-mail account "open" on a computer for others to see or access? Courts also look to whether the e-mail is sent or received via a corporate system or through a personal account; whether the computer used for such communication is owned by an employer or an individual; and whether, when the communication was transmitted, the computer at issue was located in a company's office or at a home?[48]

---

you wouldn't be comfortable having your Mother or your boss - or the person you may be writing about - read on the front page of The New York Times or The Wall Street Journal.").

46. *See* Ken Strutin, *Social Networking Evidence in a Self-Surveillance Society*, N.Y. L.J., Mar. 10, 2009, at 5 (describes the evolution of mass self-surveillance and lifelogging prompted by social media technology and services and the legal implications).

47. *See* Mark A. Berman, *Expectations of Privacy in E-Mail Communications*, N.Y. L.J., July 6, 2010 ("E-mails should more properly be viewed as a 'postcard' or a conversation over a speakerphone, both open and available to a passerby to hear or see, than like a private 'confidential,' 'sealed' letter.").

48. *Id.*

In addition to personal user habits, other factors include the existence of passwords, encryption, or security measures taken by the employer or individual. The prevalence of shared access to accounts by couples, employees, or in other situations where consent to use the e-mail or a waiver of permission to view exists is an increasingly significant detail.[49]

E-mail, like social media, is hosted or transits through a third party's site. The expectation of privacy under the Fourth Amendment when e-mail contents are gleaned from an Internet Service Provider is being hotly debated. In *Warshak v. United States*,[50] the government was investigating Steven Warshak for wire fraud and money laundering. They obtained two ex parte orders under the Stored Communications Act (18 U.S.C. § 2703) ("SCA") to search plaintiff e-mails, including those stored on the Yahoo service. After nearly a year, the government notified Warshak about the orders. As a result, Warshak sought an injunction barring the government from any more ex parte e-mail searches or for using those e-mails for any purpose without a search warrant. The District Court for the Southern District of Ohio granted Warshak's motion for a preliminary injunction in part, stating:

> The United States is accordingly [enjoined], pending final judgment on the merits of Plaintiffs' claims, from seizing, pursuant to court order under 18 U.S.C. § 2703(d), the contents of any personal e-mail account maintained by an Internet Service Provider in the name of any resident of the Southern District of Ohio without providing the relevant account holder or subscriber prior notice and an opportunity to be heard on any complaint, motion, or other

49. *See, e.g.*, Boudakian v. Boudakian, 240 N.Y. L.J. 123 (Sup. Ct. Dec. 2, 2008) (finding the defendant did not have expectation of privacy in e-mail account accessible through family computer).

50. 2006 U.S. Dist. LEXIS 50076 (S.D. Ohio July 21, 2006).

pleading seeking issuance of such an order.[51]

In granting relief, the judge made an important observation about the nature of privacy in electronically communicated media:

> While the Court is prepared to reconsider its views upon the presentation of further evidence on these points, it is not persuaded—as an initial matter—that an individual surrenders his reasonable expectation of privacy in his personal e-mails once he allows those e-mails (or electronic copies thereof) to be stored on a subscriber account maintained on the server of a commercial ISP. As such, the Court finds that Warshak has shown a substantial likelihood of success on the merits of his Fourth Amendment claim.[52]

However, on appeal, the Sixth Circuit did not believe that the constitutionality of the SCA's delayed notification provision[53] and the question of whether e-mail passing through the hands of third party hosts engendered a reasonable expectation of privacy were ripe for resolution and vacated the injunction:

---

51. *Id.* at *33.

52. *Id.* at *19 (footnotes omitted).

53. 18 U.S.C. § 2703(a) (2006) ("A governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction. A governmental entity may require the disclosure by a provider of electronic communications services of the contents of a wire or electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days by the means available under subsection (b) of this section.").

> Our reluctance to hypothesize how the government might conduct a conjectural search of Warshak's e-mails, then resolve the constitutionality of that search as well as any others the government might conduct under the statute, is reinforced by another reality: The Stored Communications Act has been in existence since 1986 and to our knowledge has not been the subject of any successful Fourth Amendment challenges, in any context, whether to § 2703(d) or to any other provision. If it "is often true" that reviewing "legislation in advance of its immediate adverse effect in the context of a concrete case involves too remote and abstract an inquiry for the proper exercise of the judicial function," the same is assuredly true when we have no precedent to guide us. Discretion, indeed, is the better part of valor.[54]

While e-mail is akin to a phone call or private correspondence, social networking has an entirely different set of rules. Privacy in social media seems to be a fluctuating concept depending on the circumstances.[55] The presence of that information on a third-party site, a form of personal cloud computing,[56] is an important factor. Social media is different

---

54. Warshak v. United States, 532 F.3d 521, 531 (6th Cir. 2008) (internal citations omitted).

55. *See, e.g.*, Yath v. Fairview Clinics, N. P., 767 N.W.2d 34, 44-45 (Minn. Ct. App. 2009) ("The MySpace.com webpage that triggers Yath's claim [invasion of privacy--publication of private facts] was such a site. Access to it was not protected, as some web pages are, by a password or some other restrictive safeguard. It was a window that Yath's enemies propped open for at least 24 hours allowing any internet-connected voyeur access to private details of her life. The claim therefore survives the 'publicity' challenge." However, "[b]ecause Yath failed to produce any evidence on an essential element of her claim—specifically, that any of the defendants surviving on appeal were involved in creating or sustaining the disparaging MySpace.com webpage—her invasion-of-privacy claim fails.").

56. *See* Shane Schick, *Head in the Clouds? Welcome to the Future*, GLOBE & MAIL (Toronto), May 29, 2007, *available at* http://www.theglobeandmail.com/blogs /article799712.ece ("Cloud computing

from traditional mail, electronic mail, telephone calls, and telefacsimiles. Those familiar forms of communication transit through third party sites that incidentally and temporarily store information, contrasted with social networking services that are designed to store information as if they were a personal computer. Furthermore, social media is distinct from other mediums of communication because of its unique information sharing capabilities and the risks of unrestrained republication of personal data. In answering the questions of whether something offsite was realistically meant to be private, the terms of service, user expectations, webware, and current practices must all be examined.

There appears to be conflict in the approaches to social media privacy. People want to be popular and connected, while at the same time reserve their right to selectively fence off their activities.[57] In other words, they want to have their cake

---

is essentially a large-scale distributed computing system that taps into the vast resources of the Internet. Individual PCs access the 'cloud' of data rather than their own data centre and rent products or services such as extra storage space or applications from companies like Amazon.com or Google.").

57. *See* James Grimmelmann, *Privacy as Product Safety*, 19 WIDENER L.J. 793, 800 (2010) ("The point is not that these 'Digital Natives' prize privacy above all else or that they experience privacy in the same way previous generations did or that the social content of privacy is stable. The privacy they care about is social and relational, perhaps less concerned with databases and governmental surveillance than their parents' and grandparents' privacy. They are constantly trading their privacy off against other social opportunities and making pragmatic judgment calls about what to reveal and what to keep hidden. However, they do care about privacy, and they act accordingly.") (footnotes omitted). *See generally* MARY MADDEN & AARON SMITH, REPUTATION MANAGEMENT AND SOCIAL MEDIA 2-3 (2010), *available at* http://pewinternet.org/~/media//Files/Reports/2010/PIP_Reputation_Management_with_topline.pdf ("The increased prevalence of self-monitoring and observation of others creates a dynamic environment where people promote themselves or shroud themselves depending on their intended audience and circumstances. There are good reasons to be more vigilant. Online reputation matters; 44% of online adults have searched for information about someone whose services or advice they seek in a professional capacity. People are now more likely to work for an employer that has policies about how they present themselves online, and co-workers and business competitors now keep closer tabs on one another. Those who are dating are more likely to research their potential mates online. And even neighbors have become more curious about finding information about one another online. Yet, even those who are careful

and eat it too. Without specific remedies, they are left to regulate themselves, which can lead to posting false information online, a behavior that ethics committees, prosecutors, and service providers try to prohibit. However, this identity masking is sometimes the result of people trying to protect their reputations.

Compromising photos, ill-considered rants, or "what was I thinking moments" recorded and posted impulsively might end up in a human resources file[58] or before a university admissions committee. College-bound students have begun creating profiles with aliases to avoid being linked to a youthful indiscretion that they would not want a college recruiter to see.[59] And one scholar has pointed out how much further the masking goes:

> [A]s soon as you scratch beneath the surface of Facebook social practices, carefully modulated

about their own disclosures have to stay on top of the identifying material that others may have posted about them on social networking profiles, photo- and video-sharing sites, Twitter and blogs.").

58. *See, e.g.*, Emma Barnett, *Facebook Users Concerned About Privacy, Says Survey*, TELEGRAPH, April 26, 2010, *available at* http://www.telegraph.co.uk/technology/facebook/7635125/Facebook-users-concerned-about-privacy-says-survey.html ("F-Secure, an internet security firm which polled 450 Facebook users, found that 73 per cent were not 'friends' with their boss on the site. The survey also found that 77 per cent said that they use the site's privacy tools to safeguard their private information. The poll discovered that Facebook users have become increasingly aware of the need to ensure their personal information and status updates remain private with 35 per cent of pollsters admitting posting something on the site they later regretted.").

59. *See, e.g.*, Sarah Maslin Nir, *An Online Alias Keeps Colleges Off Their Trail*, N.Y. TIMES, Apr. 25, 2010, at ST8, *available at* http://www.nytimes.com/2010/04/25/ fashion/25Noticed.html ("Michael Goldman, who graduated last year from the Frisch School in Paramus, N.J., estimated that nearly half his friends changed their Facebook names in the last two years of high school. 'At this point it's not done as much for the sake for being functional,' Mr. Goldman said. 'Now it's gotten just more to be trendy.' Once they are accepted, most revert to their actual names. Kwame Kruw Ocran, a senior at Brooklyn Technical High School, thinks hiding behind a pseudonym isn't safe enough. He held a cleanse week last summer, where via Facebook he encouraged more than 1,000 of his fellow students to remove anything incriminating from their online profiles before applying to colleges.").

> privacy management is everywhere, Danah Boyd has documented how teens on Facebook, MySpace, and other social media use fake profiles, fake names, fake ages, and a cloud of other minor lies to keep their profiles safe from prying (usually parental) eyes while also connecting with their peers. Meanwhile, college students coming back from a night of partying have learned that the first thing they need to do is check Facebook and untag their names from any photos of them doing keg stands, lest their athletic coaches or campus police catch them drinking.[60]

In addition, false profiling or concealment can complicate the prosecution and adjudication of criminal cases. For example, threatening, harassing, and fake messages or contacts can be conducted through a phony profile. And this creates a serious concern in domestic violence cases, where the free range of Facebook and MySpace can allow any unauthenticated person to pose as anyone and make contact with a victim.[61]

---

60. Grimmelmann, *supra* note 57, at 799-800 (footnotes omitted).

61. *See* Laurie L. Baughman, *Friend Request or Foe? Confirming the Misuse of Internet and Social Networking Sites by Domestic Violence Perpetrators*, 19 WIDENER L.J. 933, 944 (2010) ("Because social networking sites allow individuals to freely post photos, comments, and other personal information, a new wealth of information is placed at the fingertips of abusers. Even if the victim does not post personal content on the Internet and does not have a page of his or her own, an abuser may be able to track down the previously unknown location of a victim if a family member, child, or friend posts a picture or other personal information about the victim and/or the victim's children online. Privacy settings allow users to limit the availability of their information to certain friends or family members, rather than the general public. However, a simple search of a social networking site allows an abuser to access information about a victim without approved access to the victim's profile or page. Additionally, social networking sites run on the honor system. The sites do not check into whether a user who creates a profile is in fact a real person, so the creation of a fake profile is as easy as the creation of a real profile. A fake profile may allow an abuser to access the site of a victim or victim's family member, when an authentic profile would act as a red flag.") (footnotes omitted).

These behaviors illustrate that social media participants have a different impression of privacy than they would expect in a sealed envelope, a phone call, or the contents of their own hard drive. They want privacy but on their own terms.[62] Social and private are usually antithetical ideas, particularly online. And if the membership of a social media service treats identity deception as an accepted and necessary practice, or as ungovernable, then pretexting by lawyers[63] and investigators might fall within the mores of that online society.

III. Discovery

The propriety of entering the fenced off portions of cyberspace in pursuit of litigation ends has kicked up a storm of reactions. Federal and state legislatures are scrambling to enact or amend laws to adjust to this new media, filling gaps in criminal behavior, e.g., cyberbullying,[64] and addressing the

---

62. Grimmelmann, *supra* note 57, at 800 ("The point is not that these 'Digital Natives' prize privacy above all else or that they experience privacy in the same way previous generations did or that the social content of privacy is stable. The privacy they care about is social and relational, perhaps less concerned with databases and governmental surveillance than their parents' and grandparents' privacy. They are constantly trading their privacy off against other social opportunities and making pragmatic judgment calls about what to reveal and what to keep hidden. However, they do care about privacy, and they act accordingly.").

63. Considering the unknown degree of deception, puffing, and exaggeration that users engage in, information quality also becomes an important, separate issue. But the first step is gaining access to the witness, whose evidence can be evaluated later in the crucible of the courtroom. *See* Seth P. Berman et al., *Web 2.0: What's Evidence Between 'Friends'?*, BOSTON B.J., Jan/Feb 2009, at 5, *available at* http://www.strozfriedberg.com/files/Publication/dc2b8838-3e1c-43c8-871d03875d982c2e/Presentation/PublicationAtta chment/0165df77-27cf-4d92-8438-15a274986a9c/bbj_janfeb_09%20First%20Principles .pdf.

64. *See* Kristopher Accardi, *Is Violating an Internet Service Provider's Terms of Service an Example of Computer Fraud and Abuse?: An Analytical Look at the Computer Fraud and Abuse Act, Lori Drew's Conviction and Cyberbullying*, 37 W. ST. U. L. REV. 67, 68-70 (2009) (describes the distinctions among the new types of offenses aimed at abusive behavior conducted through electronic media, i.e., cyberbullying, cyberstalking, and cyberharassment).

basics of procedure, e.g., service of process.[65] The equation of social networking sites with recognized forms of communication has opened the door to legal process and might support the legitimacy of other actions, such as pretrial discovery by private parties.

Facebook and MySpace have become social replay for hundreds of millions of people, where the data of their lives can be viewed and reviewed at will. And one of the core features of these sites is communication. The legal system places a premium on modes of communication, which opens up a host of applications in criminal and civil practice, from search warrants to starting a civil action. For instance, service of process, the act of providing an opposing party with notice of an action, has evolved constitutionally with technology changes. At the heart of effective service are methods "reasonably calculated" to reach the parties in interest.[66] From manually handing a notice and complaint to a person in the forum state to nail, mail, and file to telex, fax, text messaging, e-mail, and even television,[67] courts have recognized these modes as acceptable under due process and statutory standards—neither of which ever contemplated electronic service of process.[68] The underlying rationale behind the due process evolution of forms of service has been the unavailability of traditional formats, and widespread use and acceptance of new communication

---

65. *See generally* Andriana L. Shultz, *Superpoked and Served: Service of Process Via Social Networking Sites*, 43 U. RICH. L. REV. 1497 (2009) (discusses the evolution of service of process founded on due process and statutory procedures and leading to the recognition of Facebook and other media as court approved methods).

66. *See* Mullane v. Cent. Hanover Bank & Trust Co., 339 U.S. 306, 314 (1950) ("An elementary and fundamental requirement of due process in any proceeding which is to be accorded finality is notice reasonably calculated, under all the circumstances, to apprise interested parties of the pendency of the action and afford them an opportunity to present their objections.").

67. *See, e.g.*, Smith v. Islamic Emirate of Afg., Nos. 01 CIV 10132(HB), 01 CIV 10144(HB), 2001 WL 1658211, at *3 (S.D.N.Y. Dec. 26, 2001) ("Service by Smith and Doe on Bin Laden will be by publication for six (6) weeks in all of the following media outlets: (1) Afghani newspapers Hewad, Anis, Kabul News, and the Kabul Times; (2) Pakistani newspaper Wahat, the paper in which Bin Laden has published his Fatwahs; and (3) *broadcasters Al Jazeera, Turkish CNN, BBC World, ARN, and ADF*.") (emphasis added).

68. Shultz, *supra* note 65, at 1503-07.

technologies. In the right cases, unprecedented applications of new media might be sanctioned as a new approach "reasonably calculated" to serve process, and opens the door to applying them in other legal procedures.[69]

The most prominent example of social networking as communication conduit is the newly recognized use of Facebook for service of process. At the forefront, Australia's courts have approved contact through a person's profile as sufficient to satisfy the standards for serving notice, complaints and orders. In each case, social networking was the only, and as it turned out best, option available.

In the first reported case of its kind, an Australian court endorsed Facebook communication as a means of satisfying the notice requirements for a default judgment.[70] A master of the Supreme Court of the Australian Capital Territory reached beyond the furthest ends of civil procedure to recognize this new form of substituted service. "Master Harper ordered that the defendants in the case could be validly served by the plaintiff sending a message by computer to the Facebook pages of both defendants informing them of the entry of and the terms of the judgment."[71]

Two years later, another Australian litigant was granted relief through Facebook. A Sydney woman tried to obtain a paternity test from an elusive man, called Mr. Howard, whom

---

69. *Id.* at 1523 ("Courts that have upheld as constitutional service of process through new communication technologies generally have begun by noting the widespread societal embrace of the technology in other facets of life. In theory, this should have virtually no bearing on whether service is upheld in a given case because due process analyses in this context are, by nature, fact specific. In other words, the fact that the technology is widely employed in the community at large does not entail that it is reasonably calculated to provide the particular defendant notice. What is good for the goose is not always good for the gander. Nonetheless, even assuming that widespread use plays a role in the court's decision, Facebook could reasonably be taken as widespread enough to gain approval.") (Footnotes omitted).

70. Nick Abrahams, *Australian Court Serves Documents via Facebook*, SYDNEY MORNING HERALD, Dec. 12, 2008, *available at* http://www.smh.com.au/news/technology/web/court-serves-documents-via-facebook/2008/12/12/1228585107578.html.

71. *Id.*

she claimed was the father.[72] Her letters went unanswered, efforts to contact him through his parents and girlfriend failed, and the process server was unsuccessful. Although his physical address was in flux, his Facebook profile was stable and routinely used. The woman's solicitor informed Federal Magistrate Brown that a "private message" could be sent to the man's online account. Satisfied with the efficacy of this form of service, the court granted an order to serve the documents via Facebook.[73]

After receiving the documents, Mr. Howard promptly closed his Facebook and MySpace profiles. Nonetheless, the court imposed an order of paternity and child support on Mr. Howard, since he had been properly served. In the light of this second decision affirming legal process through social networking, Dr. Tim Butcher, a senior lecturer at the Royal Melbourne Institute of Technology, observed: "People are finding new ways to use social media every day," he said. "It's only natural that courts, businesses, government agencies will use these tools to track us down. You have the world at your fingertips—but the flip side is that people can find us as well."[74]

The e-service precedent begins to marshal support for other direct legal applications of Facebook, MySpace, and Twitter on the same grounds as other communication media. In these cases, the courts have approved private litigants accessing an opposing party's social networking profile to ascertain identity and the stability of the site for accepting communications. And it makes sense that a network like Facebook, with 500 million profiles, is viewed as a reliable channel for communication; indeed it is the reason the

---

72. Kim Arlington, *Court Uses Facebook to Serve Paternity Test Order*, SYDNEY MORNING HERALD, June 4, 2010, *available at* http://www.smh.com.au/technology/technology-news/court-uses-facebook-to-serve-paternity-test-order-20100603-x7dc.html.

73. *Id.* ("In a recently published judgment, delivered in Adelaide, Mr. Brown said he was satisfied Mr. Howard had been properly served with the documents and inferred Mr. Howard wanted no involvement as 'the parentage test can have only one outcome because he is [the child's] father.'").

74. *Id.*

company is in business.[75]

However, there has been no mention of the mechanism by which this information had been obtained. Did the plaintiffs already have accounts and use their privileges as members to unearth the data or did they do it surreptitiously, using a fake profile or a legitimate one that masked their purpose? Mr. Howard did not hesitate to take down his profiles after being served, indicating that he would not have willingly accepted a "Friend" request from a woman or her representative seeking a paternity test. So it is unclear what actions the lawyers, investigators, or plaintiffs undertook to complete service.

It is significant that the parties being reached could not be contacted through traditional means. Social media became the sole and best choice in these circumstances. Similarly, information impeaching a witness or providing leads to exculpatory evidence might only be found in unique places like Facebook or MySpace. Someone's online profile might be the only place that an inconsistent statement or contradictory version of testimony can be found, or even a confession pointing to someone else's guilt. For this reason alone, the "uniqueness" of the evidence source, social media investigation warrants legal and ethical sanction.[76]

Confirming the identification of the profile's owner, confronting privacy limitations and terms of service restrictions, and analyzing ethical rules about using deception or providing false statements are all issues to be considered in

---

75. "Facebook's mission is to give people the power to share and make the world more open and connected." FACEBOOK.COM, http://www.facebook.com/facebook?ref=pf/r.php?locale=en_US#!/facebook?v=info&ref=pf%2Fr.php%3Flocale%3Den_US (last visited Sept. 26, 2010).

76. Schultz, *supra* note 65, at 1528 ("The Australian case permitting service of a default judgment via Facebook foreshadows future attempts to employ social networking sites to effectuate legal ends. As this comment illustrates, attempted service of process through Facebook may very well be permissible under Rule 4(f)(3) for serving foreign defendants, and such service does not appear to constitute a per se due process violation, no matter how narrow the circumstances permitting such service might be. Necessity, the mother of invention, has frequently been the catalyst for adapting the law to implement new technologies, and if a situation arises in which a message sent via Facebook is the only available means to serve an elusive defendant abroad, the law might, in due time, adapt accordingly.") (footnote omitted).

online investigations. At the same time, courts and legislators ought to recognize the unqualified necessity of using social media as a foundation for discovery and case preparation. The principal concern in most cases is the destruction of ephemeral evidence.

IV. Spoliation: Preservation of Evidence

To address spoliation, one approach would be to seek an ex parte discovery order from the trial court, like a protective order, requiring that the party's or witness' profile be frozen and downloaded.[77] The order might be addressed to either the person who posted the profile or the network provider that hosts it. The profile's contents should be reviewed in camera to confirm identifying information, a preliminary issue linking the profile to the actual person, and then examined for content, e.g., exculpatory evidence, impeachment, or other relevant information.[78] This preservation step will be crucial to safeguarding important and unique evidence.

In *People v. Hardaway*,[79] a Michigan defendant appealed his conviction for third-degree criminal sexual conduct claiming ineffectiveness of counsel, among other issues. The crux of the appeal was his attorney's failure to preserve the contents of the victim's social networking profile and use it for impeachment at

---

77. *See* Lloyd S. van Oosternrijk, Comment, *Paper or Plastic?: Electronic Discovery and Spoliation in the Digital Age*, 42 HOUS. L. REV. 1163, 1183 (2005) ("Only a few state courts have addressed the unique role of electronic discovery in today's trials, but cost-shifting in electronic discovery cases has come into vogue in the federal arena. Generally speaking, the current Rule 26(c) allows a responding party to seek a protective order shifting the cost of discovery when the cost would create an undue burden.") (footnotes omitted).

78. *See, e.g.*, Leanne Italie, *Divorce Lawyers: Facebook Tops in Online Evidence*, SAN JOSE MERCURY NEWS, July 2, 2010, *available at* http://www.mercurynews.com /business/ci_15429107 ("Oversharing on social networks has led to an overabundance of evidence in divorce cases. The American Academy of Matrimonial Lawyers says 81 percent of its members have used or faced evidence plucked from Facebook, MySpace, Twitter and other social networking sites, including YouTube and LinkedIn, over the past five years.").

79. No. 284980, 2009 Mich. App. LEXIS 1912, at *1 (Ct. App. Sept. 17, 2009).

the bench trial:

> According to defendant, the web page would have established that the victim had a "pattern of lying" because the victim, on her MySpace page, claimed that she was 18 years old and married. Defendant also argues that counsel was ineffective for failing to inquire into the disappearance of the victim's MySpace page. Defendant claims that had counsel done so, counsel "may have been able" to establish a *Brady* violation.[80]

By the trial date, the victim's online profile had disappeared, like Mr. Howard's. Nonetheless, the evidence came in through another route, and defendant's ineffective assistance of counsel claim was denied.[81] Still, the question remains: what are an attorney's obligations under the Constitution and the Rules of Professional Conduct in this situation?

If the privacy issue and terms of service hurdles were removed, then the duties of counsel and the court might be made clear. In *Torres v. Lexington Insurance Co.*,[82] plaintiff claimed that she had been sexually assaulted during a massage she received at one of the defendants' hotel. Her complaint stated that "she suffered and continues to suffer intense mental anguish, feelings of shame, humiliation, depression, unworthiness, weeping and has been forced to undergo psychological treatment and therapy."[83] Attorneys for the

---

80. *Id.* at *2-3 (footnote omitted).

81. *Id.* at *2-3 ("However, the trier of fact knew what defendant argues the victim's MySpace page would have established—that the victim lied about her age and marital status. On cross-examination, the victim admitted that she lied on her MySpace page about her age and marital status. Accordingly, there is no reasonable probability that if counsel had investigated the disappearance of the victim's MySpace page or presented the web page as evidence at trial, the result of defendant's trial would have been different.").

82. 237 F.R.D. 533 (P.R. 2006).

83. *Id.* at 534.

defendants had learned independently, not through procedural discovery channels, that the plaintiff had several web pages "depicting an active social life, and an aspiring singing and modeling career."[84] Plaintiff and her counsel were unaware that these pages had been uncovered by the other side. The defendants downloaded and printed out most of their contents, and then notified plaintiff's counsel that "eliminating or altering the websites could be considered spoliation or evidence tampering."[85] Two days later, the web pages were gone without explanation. Defense counsel moved to dismiss the lawsuit or eliminate or reduce the damages. In response, the court ordered sanctions:

> In this case, Mrs. Torres did not make it known to defendants that she had an aspiring modeling or singing career. In fact, she attempted to depict the life of a recluse with no or little social interaction. Instead, Mrs. Torres led an active social life and announced this information to the world by posting it on very public internet sites. Then, immediately upon defendants' discovery of evidence, which could be used to contradict or impeach her allegations, Mrs. Torres removed the information from the internet. This is the type of unconscionable scheme the court seeks to deter.[86]

To remedy the spoliation problem the judge made several decisions. He declined to dismiss the complaint or limit a finding on damages, but precluded plaintiff from introducing any evidence of mental anguish. Furthermore, he concluded that the defendants' actions in preserving the pages' contents by downloading and printing them out did not factor into the

---

84. *Id.* at 533-34. *See generally* Oregon State Bar Legal Ethics Comm., Formal Op. 2005-164 (2005).

85. *Id.* at 534.

86. *Id.*

analysis.[87] The court separated the action of evidence spoliation from the mechanics of investigating and uncovering the web content. This lends support to the idea that a court would be empowered to issue a sanctionable preservation order. In addition, it leaves for separate consideration the means for opposing counsel to discover the existence of an online profile. The public or private nature of the site would be the only fly in the ointment.

The defense might make additional applications based on a due process right to present a defense[88] to seek any data that might lead to additional evidence,[89] such as a Friends list or references to *Brady* or *Jencks*[90] material. While no published decision has yet concluded that a social networking profile contained *Brady* or *Jencks'* material or impeaching evidence, there is anecdotal evidence that it can.

In New York City, a man was arrested for carrying a loaded weapon.[91] The case rested on the credibility of the arresting officer. His online reputation became a central part of the defense when evidence from his Facebook page was used for impeachment. The defendant asserted that he had been

---

87. *Id.*

88. *See* Washington v. Texas, 388 U.S. 14, 19 (1967) ("The right to offer the testimony of witnesses, and to compel their attendance, if necessary, is in plain terms the right to present a defense, the right to present the defendant's version of the facts as well as the prosecution's to the jury so it may decide where the truth lies. Just as an accused has the right to confront the prosecution's witnesses for the purpose of challenging their testimony, he has the right to present his own witnesses to establish a defense. This right is a fundamental element of due process of law.").

89. This tocsin about preservation applies with equal force to the client's page. *See, e.g.*, Damiano Beltrami, *I'm Innocent. Just Check My Status on Facebook*, N.Y. TIMES, Nov. 12, 2009, at A27 ("[Rodney Bradford's] defense lawyer, Robert Reuland, told a Brooklyn assistant district attorney, Lindsay Gerdes, about the Facebook entry, which was made at the time of the robbery. The district attorney subpoenaed Facebook to verify that the words had been typed from a computer at an apartment at 71 West 118th Street in Manhattan, the home of Mr. Bradford's father. When that was confirmed, the charges were dropped.").

90. *See generally* John T. Bandler, *The New York Rosario Rule Applied to Computerized Documents: The Rigid and Impractical Duplicative Equivalent Doctrine Requires Modification*, 22 PACE L. REV. 407 (2002).

91. *See, e.g.*, Jim Dwier, *The Officer Who Posted Too Much on MySpace*, N.Y. TIMES, Mar. 11, 2009, at A24.

stopped and assaulted by the officer and his partner (leaving him with three broken ribs); the officers then planted the gun to cover up their conduct. However, the jurors learned that the officer had set his Facebook page to "devious mood," and that he had listed his status as watching the movie *Training Day* to "brush up on proper police procedure." Ultimately, the defendant was acquitted of the gun charge, but convicted for resisting arrest.

Defense counsel were led to the officer's profile from an Internet search[92] that revealed statements he had made about video clips showing suspects being arrested, and in which he talked about "tuning up arrestees" before putting on the cuffs.[93] The online statements supported the defense's theory that the officer intended to cover-up his use of excessive force. However, there is no way to know exactly how the jurors processed this information because they acquitted on the principal felony charge but still convicted on resisting arrest.

Nonetheless, any impeachment evidence has the potential of raising reasonable doubt. The question for the defense is how to find it and for the jury how to weigh it. Social media as evidence is inextricably tied to its discoverability, and will bring up questions of authenticity, weight, and credibility.[94]

---

92. *See generally* CAROLE LEVITT & MARK ROSCH, FIND INFO LIKE A PRO, VOLUME 1: MINING THE INTERNET'S PUBLICLY AVAILABLE RESOURCES FOR INVESTIGATIVE RESEARCH (2010); Tamara Thompson, *Due Diligence with Social Networks: Benefits of This New Information Arena*, 195 N.J. L.J. 302, Feb. 2, 2009.

93. Injudicious statements and misuse of social media has sounded a warning bell in the law enforcement community, prompting a call for workplace standards. *See* Terrence P. Dwyer, *Pitfalls for Police Officers on Facebook*, POLICEONE.COM (Aug. 11, 2010), http://www.policeone.com/off-duty/articles/2304799-Pitfalls-for-police-officers-on-social-networking-sites/ ("Police administrators are well advised to adopt a social networking policy if they have not already started to do so. Police officers are advised to keep content unobjectionable at the least, but would be better off staying clear of online postings and video rants. The democratization of media use has created a 'big brother' of monstrous proportions and can quickly become a trap for the careless officer.").

94. *See generally* Kamika Dunlap, *Facebook Alibi: Social Media as Defense Evidence*, FINDLAW BLOTTER (Nov. 12, 2009, 2:00 PM), http://blogs.findlaw.com/blotter/2009/11/facebook-alibi-social-media-as-defense-eviden ce.html ("Authenticating your Facebook, Twitter, MySpace, or

The prosecutor in the New York City case argued that the *Training Day* comments were protected speech, criticism of a movie, and irrelevant to the circumstances of the arrest. Still, the judge allowed the evidence in. Privacy, freedom of expression, and weight of the evidence are all factors that must be addressed in every instance where this type of self-published evidence will be used. Context is as important as content in the world of social media evidence.

V. Spoliation: Preserving Defense Evidence

Before counsel has had an opportunity to review a client's social media profile, the government might already be aware of it and reveal its intent to use the contents through the normal course of discovery.[95] In other words, law enforcement or the prosecution may have built their indictment on the material found on MySpace or Facebook during an investigation or before bringing formal charges.[96]

In a computer-based crime, such as illicit pornography, a defendant's computer would be seized.[97] It might also happen

---

whatever social networking account you have will be key.").

95. United States v. Drummond, No. 1:09-cr-00159, 2010 U.S. Dist. LEXIS 29981 (M.D. Pa. Mar. 29, 2010) (pictures from defendant's MySpace page, where he had large amounts of cash and held a gun, were made known through the regular channels of discovery).

96. *See* Randy L. Dryer, *Advising Your Clients (and You!) in the New World of Social Media: What Every Lawyer Should Know About Twitter, Facebook, YouTube, & Wikis*, 23 UTAH B.J. 16, 19 (2010), *available at* http://www.utahbar.org/barjournal /pdf/May_June_2010.pdf ("Social media clearly expands the universe of potentially discoverable materials and impacts data retention/destruction policies. Just as requests for e-mails were the discovery rage of the last decade, requests for information on social media platforms will soon become standard. Unlike the early internet days where digital information was primarily e-mails, information now posted on social media sites includes audio, photographs, and video. Virtually everyone has a cell phone, and virtually every cell phone has both still photograph and video capabilities. And in 2010 we are seeing more and more ways for people to access their social media sites (and upload content) through their mobile phones. These new technologies are dramatically changing the discovery landscape.").

97. *See generally Electronic Evidence and Search & Seizure Legal Resources*, COMPUTER CRIME & INTELL. PROP. SEC., U.S. DEP'T OF JUST. http://www.justice.gov/criminal/cybercrime/searching.html (last visited Oct.

in prosecutions involving social media. However, what should be done with the material on the third party provider's site? Can defense counsel advise his client to take down the incriminating photographs? Can the prosecutor prevent it? And can the court intervene?

Several recent cases seem to cast doubt on the wisdom of advising a client about the disposition of online profiles or other social media. There are risks that such advice might constitute evidence tampering or obstructing governmental administration, which could lead to criminal conviction and disbarment. In *Matter of Coren*,[98] a New York attorney pleaded guilty to federal felonies that included "mail fraud, wire fraud, money laundering, conspiracy to commit money laundering and obstruction of justice (tampering with physical evidence)."[99] He had allegedly participated in a conspiracy with a client to defraud the federal government regarding the administration of funds for wage contracts.[100] The Disciplinary Committee for the New York First Judicial Department sought an order for disbarment based on the federal felony conviction. Ultimately, the attorney lost his legal challenge to downgrade the proceeding from automatic disbarment to a serious crime matter. The issue hinged on the similarity between New York and federal laws on tampering and obstruction of justice. The Appellate Division concluded that there was an "essential similarity" between the two and upheld the disbarment.[101] Noteworthy was the plea allocution:

> [R]egarding the count in the indictment charging obstruction of justice, I admit that on February 3, 2006, I advised Nomi Beig [his client] in response to a question he posed to me that he should

---

1, 2010).

98. 76 A.D.3d 285, 285 (App. Div. 1st Dep't 2010).

99. *Id.* at 286.

100. *Id.*

101. *Id.* at 287 ("Respondent's conviction for obstruction of justice in violation of 18 U.S.C. § 1512(c) is a proper predicate for disbarment because there is 'essential similarity' between that federal statute and the New York felony of tampering with physical evidence (Penal Law § 215.40[2]).").

> destroy a computer flash drive containing documents that I advised him to remove from his office when I heard that his company was under investigation. I knew that by doing so Nomi would be destroying documents that could have been used in a Government investigation.[102]

Although he did not erase the computer records himself, the attorney was charged with actual tampering, as opposed to attempted tampering that would have reduced the charge to a misdemeanor under New York law. His plea to this count of the federal indictment was sufficient to support automatic disbarment.

In another obstruction case, a Connecticut attorney, Philip D. Russell, was indicted for allegedly taking steps to destroy the contents of his client's laptop computer, which contained evidence of illicit pornography.[103] The computer belonged to the choirmaster of a church, and a fellow employee discovered the pornographic images while using it for work. A day later, officials of the church "sealed and wrapped" the laptop, anticipating its use as evidence.

The choirmaster met with Russell the following day; the lawyer took possession of the computer and destroyed the hard drive. Unknown to either of them, an FBI investigation was already underway against the choirmaster. The Department of Justice charged the attorney with obstruction of justice and violation of the Sarbanes-Oxley Act (anti-shredding prohibition).[104] Russell moved to dismiss the charges both because the federal investigation was unknown to him at the time and because the Sarbanes-Oxley Act was not intended to apply to pornographic contraband. In other words, the government did not "allege any nexus between his obstructive conduct and any federal proceeding or investigation that was

---

102. *Id.* at 288 (alterations in original); *see also* United States v. Coren, No. 07-CR-265 (ENV), 2009 U.S. Dist. LEXIS 73913, at *27 (E.D.N.Y. Aug. 20, 2009).

103. Evan T. Barr, *'Russell': Prosecuting Defense Counsel for Obstruction*, N.Y. L.J., Nov. 21, 2007 at 4.

104. United States v. Russell, 639 F. Supp. 2d 226, 230 (D. Conn. 2007).

reasonably foreseeable to him."[105] The district court judge denied Russell's motion, finding that the "indictment contains sufficient factual particularity showing a relationship in time, causation, and logic between Russell's destruction of Tate's Computer and a grand jury proceeding or a FBI investigation to put him on notice of the charges against him."[106] Russell's Sarbanes interpretation was also rejected.[107] Ultimately, he was sentenced to six-months of home confinement, a substantial fine and community service.[108]

These two cases highlight the risks of counseling or aiding a client in the destruction or removal of computer-based evidence. On the flip side, what if the prosecutor advises the complainant, law enforcement, experts, or a fact witness to purge their multimedia online profiles, forestalling defense investigators? [109]

Another important facet of this problem is when the police and prosecutors have audited the social media information of their own witnesses, whether in individual cases or routinely through department policies.[110] In such instances, the contents of those sites might become *Brady* or *Jencks* material, or fall under the scope of other provisions of the discovery statutes. Under those circumstances, a court might issue a protective order preventing its deletion or compelling disclosure.[111]

---

105. *Id.* at 232.

106. *Id.* at 236.

107. *Id.* at 237 ("Nothing in the legislative history supports a conclusion that the drafters intended to narrowly circumscribe its application to the destruction of business records and documents.").

108. *See* John Christoffersen, *Lawyer Who Destroyed Evidence in Porn Case Spared Prison Time*, ASSOCIATED PRESS, Dec. 18, 2007, *available at* http://www.law.com /jsp/article.jsp?id=1197980085647.

109. *See generally* Gregory G. Sarno, *Interference by Prosecution with Defense Counsel's Pretrial Interrogation of Witnesses*, 90 A.L.R.3d 1231 (1979).

110. *See, e.g.*, Rocco Parascandola & Laura Rivera, *NYPD Rookies Warned About MySpace, Facebook Pages*, NEWSDAY, May 6, 2008.

111. *See, e.g.*, Dryer, *supra* note 96, at 19 ("Posts on social media are within the scope of 'electronically stored information' as that term is used in Rule 34 of the Federal Rules of Civil Procedure. Litigation hold letters likely trigger an obligation to preserve such posts if they are reasonably related to the litigation. This means that just like companies had to revise their document retention and destruction policies and their internal protocols for

Other pitfalls include the risks of independent research or communication online by judges, jurors, or other parties and witnesses in a case, which might taint or prompt the deletion of such evidence.[112] A social media snapshot of the state's witnesses might be required to protect the defendant's constitutional and statutory discovery rights at a time when guidance on obtaining that information independently is unclear.

VI. Undercover Investigation (Pretexting)

The key to understanding how a lawyer should operate in the social networking context is the recognition that new approaches are necessary. All the rules that the legal profession relies on to instruct lawyer behavior were forged before the emergence of twenty-first century technology. The rule book for this young century has not been written yet, but the foundations are there. The application of those principles is informed by post-Internet thinking and current online realities.[113]

Failure to adequately investigate a crime or witnesses, whether in the real or virtual worlds, can violate the right to counsel and due process.[114] Surreptitious online investigation

---

handling litigation hold requests when e-mail became a pervasive way of communicating, so too will these policies require updating to address the nuances of social media.").

112. *See generally Pitfalls*, *supra* note 13, at 5 (discusses ethical problems that can occur when judges and lawyers contact each other through social networking, and the dangers of independent factual investigations through the same method).

113. *See generally* ABA, *Agenda for Ethics 20/20 Project Examines Impact of Technology, Disappearing Borders*, 25 LAW. MAN. PROF. CONDUCT 694 (2009), http://www.abanet.org/ethics2020/impact.pdf (Social networking is among the issues to be addressed by the ABA Commission on Ethics 20/20 during its three year tenure).

114. *See, e.g.*, Thomas v. Kuhlman, 255 F. Supp. 2d 99, 107 (E.D.N.Y. 2003) ("Counsel 'has a duty to make reasonable investigations or to make a reasonable decision that makes particular investigations unnecessary.'"). Where the nature of the crime scene is material to the defense, counsel may be deemed ineffective for having failed to investigate it properly. *See, e.g.*, Williams v. Washington, 59 F.3d 673, 680-81 (7th Cir. 1995) (ineffective assistance in part for failure to investigate crime scene where doing so would

in some cases might be the best or only method for uncovering crucial information, which might otherwise be deleted or compromised. The lawyer who fails to pursue it might risk accusations of malpractice and ineffectiveness of counsel. It is a difficult needle to thread.

With the rapid pace of technological development, lawyers have had to confront unprecedented issues on how to conduct discovery, litigation, and professional relations in the face of metadata, data mining,[115] and now social networking. This adds a new wrinkle to the initial client intake. Besides asking for contact information and employment history, an attorney may be obligated to inquire into a client's online presence. Whether the lawyer should do it independently without the client's knowledge raises ethical issues. Of course, asking the client directly begs the question of what to do with the answer.

Accessing Facebook or MySpace is not the same as a Google search about a client that would only bring up data available to anyone. The former sites have public and private areas. A visitor can search the public segment without constraint, but to go further and see a client's profile, membership (registration and agreement to terms of service) is required. Without a client's consent, the lawyer may be overstepping the network's terms of service and pushing the limits of the Rules of Professional Conduct. Mechanically, a visit to an online profile might only involve observation and recording.[116] On the other hand, Friending is a form of contact.

---

have revealed evidence that, "given the layout of the home and the relatively crowded conditions, the alleged assault could not have taken place as claimed."); People v. Donovan, 184 A.D.2d 654, 655 (N.Y. App. Div. 1992) (ineffective assistance where counsel failed "to dispatch an investigator to the scene [of defendant's arrest] . . . until after the trial had commenced," leaving him "unprepared to effectively argue [the issue] before the court").

115. *See, e.g.*, Armen Keteyian, *Digital Photocopiers Loaded with Secrets*, CBSNEWS.COM (Apr. 15, 2010), http://www.cbsnews.com/stories/2010/04/19/eveningnews/main6412439.shtml?tag=mncol;lst;1 (hard drives of common office equipment, often discarded, may contain valuable data). *See generally* Andrew M. Perlman, *Legal Ethics of Metadata Mining*, 43 AKRON L. REV. 785 (2010).

116. *But see, e.g.*, Ethics Comm. of the Colo. Bar Ass'n, Formal Op. 60 (1982), http://www.cobar.org/index.cfm/ID/386/subID/1781/CETH/Ethics-Opinion-60:-Duty-with-Respect-to-Client%27s-Incriminating-Physical-

And in the case of a witness or complainant, the act might cross the line against communicating with a represented party or influencing a witness.

The ethical analysis begins with familiar technology, the telephone. ABA Formal Opinion 337, issued in 1974, declared "with certain exceptions spelled out in this opinion, no lawyer should record any conversation whether by tapes or other electronic device, without the consent or prior knowledge of all parties to the conversation."[117] The common situations identified by the Committee included recording conversations involving clients or witnesses. They relied principally on Canon 9 of the Code of Professional Responsibility requiring lawyers to avoid the appearance of impropriety and DR 1-102(A)(4) prohibiting "dishonesty, fraud, deceit, or misrepresentation" to reach that conclusion.[118] A law enforcement exception was acknowledged but not fully explored:

> There may be extraordinary circumstances in which the Attorney General of the United States or the principal prosecuting attorney of a state or local government or law enforcement attorneys or officers acting under the direction of the Attorney General or such principal prosecuting attorneys might ethically make and use secret recordings if acting within strict statutory limitations conforming to constitutional requirements. This opinion does not address such exceptions which would necessarily require examination on a case by case basis. It should be stressed, however, that the mere fact that secret recordation in a particular instance is not illegal will not necessarily render the conduct of a public law

---

Evidence,-07/24/82/ ("When a lawyer observes incriminating evidence as a result of his representation of the client and does not alter or disturb the evidence, he must not disclose these observations to authorities.").

117. ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 337 (1974).

118. *Id.*

> enforcement officer in making such a recording ethical.[119]

In 2001, the American Bar Association Standing Committee on Ethics and Professional Responsibility reexamined its position on the propriety of a lawyer recording a phone conversation without the other party's knowledge and came to the opposite conclusion from Opinion 337, withdrawing that precedent.[120] The first reason for this change in position was the issuance of the Model Rules of Professional Conduct. The new Rules omitted Canon 9's "appearance of impropriety" admonition, removing a major pillar justifying their earlier analysis. The fraud and deceit section survived in Model Rule 8.4(c). However, in the intervening quarter century practice and perspective on this issue had changed:

> First, the belief that nonconsensual taping of conversations is inherently deceitful, embraced by this Committee in 1974, is not universally accepted today. The overwhelming majority of states permit recording by consent of only one party to the conversation. Surreptitious recording of conversations is a widespread practice by law enforcement, private investigators and journalists, and the courts universally accept evidence acquired by such techniques. Devices for the recording of telephone conversations on one's own phone readily are available and widely are used. Thus, even though recording of a conversation without disclosure may to many people "offend a sense of honor and fair play," it is questionable whether anyone today justifiably relies on an expectation that a conversation is not being recorded by the other party, absent a special relationship with or

---

119. *Id.*

120. ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 01-422 (2001).

> conduct by that party inducing a belief that the conversation will not be recorded.[121]

Although the Committee did not directly address the pretexting question,[122] it affirmed the "widespread practice" of surreptitious recording that changed a party's or witness' expectations. Phone-tapping technology was ubiquitous and law enforcement and prosecutors as well as private investigators made use of it. These same factors militate in favor of accessing a party's social media employing common technology. The difference is in the nature of the communication, not the recording. Thus far, the ABA opinion opens the door a crack for contact through the latest communication/recording medium, social networking.

The second point it made was that the recording involved a "legitimate and even necessary activity" that would be at risk from the danger of an attorney tipping her hand too soon. This concept was born of the numerous exceptions to Opinion 337's proscription found in state bar committee opinions. Of special note were opinions from Tennessee and Kentucky[123] that recognized the need for "recordings by criminal defense lawyers, reasoning that the commonly accepted 'law enforcement exception' otherwise would give prosecutors an unfair advantage."[124] It also embraced the constitutional necessity of leveling the playing field. Some of the other exceptions they listed are also used as justifications for pretexting,[125] e.g., protecting against witness or client perjury,

---

121. *Id.* (footnotes omitted).

122. *Id.* ("We conclude that the mere act of secretly but lawfully recording a conversation inherently is not deceitful, and leave for another day the separate question of when investigative practices involving misrepresentations of identity and purpose nonetheless may be ethical.").

123. *See* Bd. of Prof'l Responsibility of the Sup. Ct. of Tenn., Formal Ethics Op. 86-F-14(a) (1986), http://www.tbpr.org/Attorneys/EthicsOpinions/Pdfs/86-F-14%28a%29.pdf; Ky. Bar Ass'n, Ethics Op. KBA E-279 (1984), http://www.kybar.org/documents/ethics_opinions/kba_e-279.pdf.

124. Formal Op. 01-422, at 8.

125. *See* N.Y.C. County Lawyer's Ass'n, Formal Op. 737 (2007), http://www.nycla.org/siteFiles/Publications/Publications519_0.pdf.

uncovering housing discrimination and trademark infringement, and generally for prosecution and criminal defense investigations.[126]

Another important facet of the ABA's analysis was the determination to avoid per se rules and decide each case on its merits. It did not see the logic in creating a categorical bar swallowed by exceptions and instead advised interdicting nonconsensual recordings if accompanied by other misconduct.[127]

Lastly, the third criticism of Opinion 337, which led to its reversal, was a change in philosophy. The Mode Code's instruction for attorneys to "avoid even the appearance of impropriety" had been omitted from the Model Rules. The rights of third parties were protected under a direct approach embodied in Rule 4.4(a) "[i]n representing a client, a lawyer shall not use means that have no substantial purpose other than to embarrass, delay, or burden a third person, or use methods of obtaining evidence that violate the legal rights of such a person."[128]

As applied to nonconsensual phone recordings, Rule 4.4 looked to the purpose behind the action. An intent to "embarrass" or "burden" a witness, for example, would violate the Rule. But the Committee did not differentiate taping a phone conversation from other forms of evidence gathering since they were not unlawful. The same rationale applied to situations where the attorney misrepresented that a conversation was not being recorded. Again, it was not the acting of recording the phone call that troubled its conscience, but the accompanying false statement to a third person in violation of Rule 4.1.[129]

An attorney or investigator hiding their purpose behind Friending a witness' or a complainant's Facebook or MySpace page might run afoul of this kind of prohibition. Friending in itself is a lawful, ethical mode of contact. Being secretive about

---

126. Formal Op. 01-422, at 8.
127. *Id.*
128. MODEL RULES OF PROF'L CONDUCT R. 4.4(a) (2009).
129. Formal Op. 01-422, at 5 n.28.

the purpose or misleading the recipient of the request might border on a false representation. And it again raises the third party's privacy rights in their profile from surreptitious solicitations, whether in state law or the terms of service.

The federal and state laws governing Internet conduct are a patchwork that is continually being tested in the courts. As Opinion 01-422 pointed out in the case of one-sided phone recordings, a lawyer must be familiar with the laws of the jurisdictions involved since Rule 4.4 specifically prohibits violating the rights of a third party under state law in conducting discovery or investigation.[130] Similarly, an attorney undertaking discovery through social media must be versed in the federal and state laws on computer fraud, cyberbullying, and harassment that might ensnare her. Like telephonic communication, Internet communication naturally crosses state boundaries, imposing a burden on the lawyer to know the rules and laws for the jurisdictions involved—although it cannot be assumed that such communications are always interstate.[131]

The Committee was divided over the advisability of recording clients without consent and in general considered it inadvisable. So they recommended advising him or her at the start that conversations might be recorded. Per force, this sheds light on the advisability of an attorney viewing a client's MySpace or Facebook page to download or otherwise review its contents. To do so without the client's knowledge or consent, via pretexting, might violate a lawyer's duty of loyalty and risk damaging the ability to preserve the confidentiality of attorney-

---

130. *Id.* at 6.

131. *See* United States v. Schaefer, 501 F.3d 1197, 1201 (10th Cir. 2007) ("We recognize in many, if not most, situations the use of the Internet will involve the movement of communications or materials between states. But this fact does not suspend the need for evidence of this interstate movement. The government offered insufficient proof of interstate movement in this case.") (footnotes omitted). *See generally* Colin Fieman, *Defending Internet Pornography Cases by Challenging Interstate Jurisdictional Elements Under* U.S. v. Schaefer, CHAMPION MAG., Jan. 2009, at 32, *available at* http://www.nacdl.org/public.nsf/01c1e7698280d20385256d0b00789923/13752bbd3072166a85257560007eb864?OpenDocument (discussing the importance of distinguishing intrastate from interstate transmissions of illicit pornography as an element of the government's case).

client communications. Moreover, contacting a client through her online profile or Twitter, etc., whether directly or undercover, increases the chances of inadvertent disclosure and destroying privilege. Can a client and attorney communicate by Friending each other through social media and still expect their conversations to be privileged?

In an earlier opinion,[132] the ABA Standing Committee on Ethics and Professional Responsibility addressed the sanctity of e-mail communications, confidentiality, and inadvertent disclosure. It concluded:

> A lawyer may transmit information relating to the representation of a client by unencrypted e-mail sent over the Internet without violating the Model Rules of Professional Conduct (1998) because the mode of transmission affords a reasonable expectation of privacy from a technological and legal standpoint. The same privacy accorded U.S. and commercial mail, land-line telephonic transmissions, and facsimiles applies to Internet e-mail. A lawyer should consult with the client and follow her instructions, however, as to the mode of transmitting highly sensitive information relating to the client's representation.[133]

The Committee's reasoning relied heavily on an analysis of the privacy features of the technology being used. Under Rule 1.6, "(a) A lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent, the disclosure is impliedly authorized in order to carry out the representation or the disclosure is permitted by paragraph (b)."[134] And the attorney must take reasonable measures in selecting a mode of private communication. The

---

132. ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 99-413 (1999), http://www.abanet.org/cpr/pubs/fo99-413.html.

133. *Id.*

134. MODEL RULES OF PROF'L CONDUCT R. 1.6 (2009).

Committee cited the trustworthiness of overland mail, for example, and the privacy expectations in telephonic communications. As to other technology, some caution was indicated, such as facsimile transmission that included a greater than normal risk of misdirection, interception, or mishandling. Another area of grave concern was the cell phone.

Cordless and cellular phones broadcasting over public air waves were susceptible to interception by many commonly available models of radios and similar devices. And as voice communication, they were not digitally encoded like e-mail.

> The risks of interception and disclosure may be lessened by the recent introduction of digital cellular phones, whose transmissions are considered more difficult to intercept than their analog counterparts. New communications technology, however, does not always advance privacy concerns. The use of airplane telephones, for example, exposes users to the interception risks of cellular telephones as well as a heightened risk of disclosure due to eavesdropping on the airplane itself.[135]

Finally, they resolved that the safeguards and nature of Internet-based e-mail provided a reasonable assurance of privacy.

> The fact that ISP administrators or hackers are capable of intercepting Internet e-mail—albeit with great difficulty and in violation of federal law—should not render the expectation of privacy in this medium any the less reasonable, just as the risk of illegal telephone taps does not erode the reasonable expectation of privacy in a telephone call.[136]

---

135. Formal Op. 99-413, at n.19.
136. *Id.*

Social media embrace the most dubious characteristics of e-mail and cellular transmissions. Their semi-public nature, networking among unvetted friends, evolving privacy terms and settings, and the endless possibility of republication and the impossible task of keeping a secret among hundreds of one's closest confidants online, makes this form of communication unreasonable to preserve confidential exchanges of information with clients. And since this form of public media has not attained the sanctity of the telephone booth,[137] it throws doubt on privacy claims that might be asserted by targets of undercover defense investigation.

Again, Opinion 01-422 suggested two areas where secret recording of a client's phone conversation would not be problematic: (1) "where the lawyer has no reason to believe the client might object"; (2) "where exceptional circumstances exist."[138] The second exception could be triggered in cases where the lawyer thinks the client might commit a crime "likely" to result in "imminent death or substantial bodily harm."[139] This would also open the door to an ethical quandary surrounding those instances where a lawyer has learned from the client's profile that she has admitted responsibility for a crime attributed to an innocent third party, who was being wrongfully prosecuted for it.[140] These cases typically begin where the client has confessed to her attorney that she

---

137. *See* Katz v. United States, 389 U.S. 347, 353 (1967) ("The Government's activities in electronically listening to and recording the petitioner's words violated the privacy upon which he justifiably relied while using the telephone booth and thus constituted a 'search and seizure' within the meaning of the Fourth Amendment. The fact that the electronic device employed to achieve that end did not happen to penetrate the wall of the booth can have no constitutional significance.").

138. ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 01-422, at 7 (2001).

139. MODEL RULES OF PROF'L CONDUCT R. 1.6(b)(1) (2009) ("A lawyer may reveal information relating to the representation of a client to the extent the lawyer reasonably believes necessary: (1) to prevent reasonably certain death or substantial bodily harm").

140. *See generally* Colin Miller, *Ordeal By Innocence: Why There Should Be a Wrongful Incarceration-Execution Exception to Attorney-Client Confidentiality*, 102 NW. U. L. REV. COLLOQUY 391 (2008); Ken Strutin, *Wrongful Conviction and Attorney-Client Confidentiality*, LLRX.COM (Jan. 9, 2010), http://www.llrx.com/features/wrongfulconvictionconfidentiality.htm.

committed the crime that someone is being charged with in the course of confidential meetings. However, if a lawyer directly or discretely examined a client's social media and unearthed this information without the client's knowledge, another layer of conflict is created.

ABA Opinion 01-422 lays the groundwork for a nonconsensual contact through social media for "legitimate" and "necessary" activities associated with the right to present a defense. And it illustrates some of the potential pitfalls awaiting incautious counsel gathering evidence undercover. On the other hand there are compelling constitutional imperatives that demand an attorney investigate social media in order to prepare and present a defense.[141] The foundations for these requirements can be found in the measurement of effective assistance of counsel and the use of technology.

In *Gill v. State*,[142] a Missouri man had been convicted of first-degree murder and sentenced to death. A key issue on his appeal was the failure of his attorney to review the contents of the victim's computer. During the penalty phase of the trial, the prosecution introduced evidence of the victim's good character. Before trial and in the course of discovery, a report had been found in defendant's car detailing the contents of the victim's computer,[143] including lists of file names, folders, and instant messages. Neither defense counsel interviewed the detective who prepared the report or flagged any issues other than inquiring of the prosecutor if there was any incriminating or exculpatory information.[144]

---

141. *See* Ken Strutin, *Hiding in Plain Sight: Evidence on Social Networking Sites*, N.Y. L.J., Nov. 10, 2009, at 5 [hereinafter *Hiding in Plain Sight*].

142. 300 S.W.3d 225 (Mo. 2009).

143. *Id.* at 228 n.2 ("The victim's computer was relevant to the investigation and prosecution of the crime because, after the murder, Gill and his co-defendant, Justin Brown, used the computer to transfer $55,000 from one of the victim's accounts to an ATM-accessible account so that they could access the money.").

144. *Id.* at 228 ("The prosecutor assured defense counsel that there was nothing on the computer that he planned to use in the case or that implicated another potential defendant. Relying on the prosecutor's assertions, defense counsel decided to focus their attention away from the computer's contents.").

At a post-penalty hearing, the detective who prepared the report testified that "he knew there was pornography on the computer within a few days of creating the report. Before Gill's trial, he looked at the transcript of the instant message conversation about the 17-year-old daughter."[145] This revelation was not discovered until the attorney for Gill's co-defendant, Brown, spoke with the Lieutenant before his trial and requested a copy of the hard drive for independent analysis. The analyst testified at Gill's hearing that there were instant messages and other files containing illicit sexual content on the victim's computer. Due to this discovery, the prosecution did not introduce the same good character evidence in the co-defendant's penalty phase, thus making the information irrelevant. Brown was eventually sentenced to life in prison.[146]

On appeal of Gill's case, the court first dispensed with the *Brady* violation claim. The defense had a copy of the report that would have led to uncovering this information. The defense's failure to recognize it did not render the information undisclosed.[147] More importantly, defendant's second claim was that defense counsel should have identified the pornography evidence on the victim's computer and used it in the penalty phase to preclude the prosecution from introducing the good character evidence or to rebut it. On this point, the appellate court agreed:

> By failing to discover those files on the victim's computer, Gill's counsel's performance was deficient. A reasonably competent attorney would have carefully reviewed the report provided by the State and recognized file names like "a_slutty18girl_w38c" and "sweet_tasting_slute" as evidence of sexually explicit material on the computer. A reasonably competent attorney would have conducted

145. *Id.* at 229.
146. *Id.* at 230-31.
147. *Id.* at 231.

> further investigation as to the contents of the computer and discovered the child pornography images, bestiality content, and sexually explicit instant message conversations about the 17-year-old daughter. Then, a reasonably competent attorney would have rebutted the State's character evidence at the penalty phase.[148]

Additionally, the court held that Gill's attorneys should have interviewed the police investigator who prepared the report. The investigator was on the state's witness list and was the first to examine the victim's computer. Based on the leads in the report, a discussion with the Lieutenant would have unearthed all the details of the pornography on the victim's machine that would have proved invaluable at the sentencing phase of the trial.

The essence of the *Gill* decision was that valuable and necessary information about a victim was available from her computer, and that information had been made known to defense counsel, who did not act on it. This scenario has much in common with social media investigations. First, if a complainant or prosecution witness has posted exculpatory, impeaching, or self-incriminating information online, and the government knows about it, then it ought to be disclosed. And the defense should have the opportunity to view it independently. Facebook or MySpace are fundamentally another hard drive, a remote site where people store information similar to their home computer—actually it is duplicative in many instances since the content originates from a personal data device, which presumably stores a copy. Since the right to counsel compels a defendant's lawyer to pursue witness computer records revealed through discovery, specific motions grounded on *Brady* and *Jencks* and statutory disclosure rights should be considered for potential social networking evidence.

Social media has become the new "mass observer," and in

148. *Id.* at 233.

terms of discovery, a ready recorder of spontaneous events.[149] The defense attorney for a former Illinois police officer, accused of shooting another man in a Pontoon Beach bar parking lot and charged with aggravated battery with a firearm, filed a motion asking to subpoena Facebook for the identity of witnesses at the scene.[150] "The motion seeks disclosure from Facebook of 23 individual user profiles and the actions of a Facebook group called 'Jeff Bladdick is a bulletproof badass' going back to the day before the Nov. 9, 2008 incident."[151] The attorney learned about the Facebook group from an anonymous source. In support of his motion, counsel marshaled familiar arguments: "[H]is client's constitutional rights fall within exceptions of the 2000 Electronic Communications Privacy Act and said that law enforcement regularly accesses the same records for its own investigations."[152] This evidence was essential to mounting a self-defense argument.[153] Facebook responded by pointing to the Electronic Communications Privacy Act, which prevented it from complying. In addition, the company claimed it would be technologically overwhelming to locate twenty-three profiles out of three-hundred and fifty million.[154] The motion, which appears to have been the first of its kind, was ultimately denied and the case ended in a plea bargain.[155] In other words, social media discovery by the

149. *See generally* Beth C. Boggs & Misty L. Edwards, *Does What Happens on Facebook Stay on Facebook? Discovery, Admissibility, Ethics, and Social Media*, 98 ILL. B.J. 366 (2010), *available at* http://www6.lexisnexis.com/publisher/EndUser?Action =UserDisplayFullDocument&orgId=574&topicId=138430011&docId=l:12188 65935&isRss=true.

150. *See* Joe Harris, *Indicted Cop Challenges Facebook's Privacy Rights*, COURTHOUSE NEWS SERV., Feb. 18, 2010, *available at* http://www.courthousenews.com /2010/02/18/24801.htm.

151. *Id.*

152. *Id.*

153. *Id.* ("Watkins [defendant's attorney] claims that Pour acted in self-defense after he was attacked by two people in a Pontoon Beach bar parking lot. Watkins says Pour pulled the gun from the back of his waistband during the attack and fired, and mistakenly hit Bladdick [victim].").

154. *Id.*

155. *See* Terry Hillig, *Former St. Louis Officer Pleads Guilty in Shooting Prosecutor Offers Lesser Charge in Altercation Outside Sports Bar in Pontoon Beach in 2008*, St. Louis Post-Dispatch, Aug. 31, 2010 ("Watkins [defendant's

defense is unguided by statute or ethical code. However, the firmest grounds for making such discovery requests are the right to counsel, compulsory process, and due process, and reciprocal rights of investigation on par with the government.

When direct discovery offers no revelations and the government does not possess social media information from witnesses, it is defense counsel's duty to investigate. In light of the massive participation in social media, it would be difficult to argue that a reasonable lawyer could ignore a resource of such magnitude.[156] So the question becomes what are the risks associated with investigating prosecution witnesses in the semi-secluded online world of Facebook and MySpace?

The dilemma occurs when an attorney, in order to effectively represent her client, tries to uncover impeaching evidence on a witness computer using deception. In *Office of Lawyer Regulation v. Hurley*,[157] a man charged with sexually assaulting a child and possession and exhibition of illicit pornography hired Hurley to represent him. A key issue for the defense was the accusation that the defendant had forced a fifteen year-old child, S.B., to view pornography.[158] However, "Hurley believed that S.B. had an independent interest in, and the ability to access, the materials . . . ."[159] To uncover evidence that S.B. had been lying, Hurley devised an investigation plan that would allow him to examine the contents of S.B.'s

---

attorney] sought at one point in Pour's criminal case to subpoena records of 22 people from the Facebook social networking website. They included police officers who investigated the shooting, as well as other potential witnesses, Watkins said. Attorneys for Facebook argued that federal law prevented Facebook from disclosing the material, and Associate Judge James Hackett agreed in a ruling in July. He said disclosure was barred by the Electronic Communications Privacy Act.")

156. *See, e.g.*, Kang, *supra* note 1 ("Facebook is expected to say this week that it has reached 500 million users, making it the biggest information network on the Internet in a meteoric rise that has connected the world into an online statehood of status updates, fan pages and picture exchanges.").

157. 2008 Wisc. LEXIS 1181 (Feb. 5, 2008).

158. *Id.*

159. Office of Lawyer Regulation v. Hurley, No. 2007AP478-D (Wis. Feb. 11, 2009), *available at* http://www.jenner.com/files/tbl_s69NewsDocumentOrder/FileUpload500/6211/Office%20of%20Lawyer%20Regulation%20v.%20Hurley.pdf.

computer. If S.B. had been alerted to this plan, there was a grave risk of spoliation. Unlike *Gill*, there was some question about the detective's interest in preserving this evidence, so no direct formal discovery request was feasible.[160]

Hurley hired a private investigator and, after exploring the options together, they devised an undercover operation. The investigator sent a letter to S.B. advising him that he had been selected to participate in a computer usage survey and, in exchange for surrendering his computer for ninety days, he would get a free laptop. Hurley provided guidelines for the investigator that included making sure the mother was present during his interactions with S.B. and the child would be allowed to remove any contents from the computer he desired before turning it over. The exchange was made according to plan and the computer turned over to a forensic expert who found illicit pornographic images.

In 2007, the Wisconsin Office of Lawyer Regulation (OLR) filed a complaint[161] against Hurley for employing "dishonesty, fraud, deceit or misrepresentation" in violation of the state's Supreme Court Rules. The referee's report stated that the OLR did not meet its burden of proof. Testimony presented at the disciplinary hearing established that "there was a widespread belief in the Wisconsin bar that the type of conduct engaged in by Attorney Hurley was and is acceptable."[162] Even the prosecutor behind the grievance affirmed that deceit was a recognized practice in its undercover operations involving nonlawyer investigators. The OLR director agreed that this type of investigation practice was recognized for prosecutors, but not private attorneys, although no authority had been cited to support the differentiation.

Approving the referee's conclusion that Hurley did not intend to break any rules or realize that his conduct might have done so, the Supreme Court of Wisconsin quoted this telling paragraph from the referee's report:

---

160. *Id.*

161. Based on allegations made by the district attorney's office involved in the criminal case. *Id.* at 3.

162. *Id.* at 2.

> Mr. Hurley was faced with a very difficult decision, with concurrent and conflicting obligations: should he zealously defend his client, fulfill his constitutional obligation to provide effective assistance of counsel, and risk breaking a vague ethical rule that, according to the record, had never been enforced in this way? Or should he knowingly fail to represent [the defendant] in the manner to which he was entitled and hand him persuasive grounds for appeal, an ethics complaint, and a malpractice claim? *The Sixth Amendment seems to have broken the tie for Mr. Hurley*. A man's liberty was at stake. Mr. Hurley had to choose, and he chose reasonably, in light of his obligations and the vagueness of the [supreme court rules].[163]

Gill and *Hurley* both speak to the fundamental importance of right to counsel, which encompasses conducting a thorough investigation. The contents of personal and home computing devices have been extended firmly into the realm of third party hosts, with their own rules of conduct. Inevitably, attorneys will have to enter this virtual world to fulfill their constitutional and ethical obligations, which brings us to the paucity of authority that has treated this issue.

In 2005, the Oregon State Bar issued an opinion[164] establishing guidelines for lawyers whose investigations took them into the public lanes of the Information Highway. Essentially, they distinguished visits to a public page of an opponent's website and crossing the threshold by making contact through that website. The scenario involved a civil case in which the defendant had an Internet page accessible to anyone, which the plaintiff's lawyer wanted to view. Oregon

---

163. *Id.* (alteration in original) (emphasis added) (citing *Hurley*, 2008 Wisc. LEXIS 1181) (Referee's Report and Recommendation).

164. Oregon State Bar Legal Ethics Comm., Formal Op. 2005-164 (2005), http://www.osbar.org/_docs/ethics/2005-164.pdf.

RPC 4.2 cautioned against contacting a represented party, and has been interpreted to apply to any mode of communication. However, the purpose of the rule, to assure that represented persons had the benefit of counsel when speaking with opposing counsel, was not implicated by seeing the contents of a site open to anyone. Any public matter published by an adverse party, regardless of format, was fair game.

Moreover, the Legal Ethics Committee divorced the notion of communication from viewing online: "A lawyer who reads information posted for general public consumption simply is not communicating with the represented owner of the Web site."[165] In the footnote to this line, they make a very cogent and significant observation: "For purposes of this opinion, a Web site can be 'public' even if an access fee or a subscription fee is charged."[166] Access that implies registration brings it within the ambit of social media sites. Of course, the terms of service may vary, but the Oregon State Bar believed that joining a site or registering alone was not problematic, it would be the next step of communication that tips the balance. Notably, it avoided directly addressing the pretexting question in this same footnote.

The concern over engaging an opponent through her web page was a possible violation of the attorney-client privilege. If a lawyer knew that the person she was communicating with online was represented, such contact would violate the Rule.[167] But if the person was some low-level employee who might only be a fact witness, then the communication would not raise any eyebrows.[168] And if the attorney contacted someone via the

---

165. *Id.*

166. *Id.*

167. This would also apply to situations where clients undertake to speak with a represented party under the direction of or with the involvement of counsel. *See, e.g.*, Trumbull Cnty. Bar Ass'n v. Makridis, 77 Ohio St. 3d 73 (1996) (attorney representing client in civil suit reprimanded for overseeing a phone call by his client to opposing party to discuss client's testimony, then taking the phone and speaking to the other represented party directly).

168. Formal Op. 2005-164, at 3 ("Lawyer *A* could not use Internet communications to invade the adverse party's lawyer client privilege. If, on the other hand, Lawyer *A* does not invade the adverse party's privilege and

website that she did not know was represented, but actually was, there would still be no problem.[169]

So the complications would arise when a lawyer leaves the public side of the web and joins a social media site for the purposes of making contact with a witness. Getting in does not seem to be a problem, according to the Oregon opinion, any more than it would be for any Internet site that charged a fee or required registration. Significantly, complainants and witnesses in criminal prosecutions are largely unrepresented, so a defense attorney might likely be in the position of someone who did not "know" whether individuals in a case had counsel, dispensing with Rule 4.2 concerns. The heart of the problem is the one specifically not addressed by the Oregon Bar, pretexting.

Philadelphia Bar Association Professional Guidance Committee Opinion 2009-02, published in March 2009, is the first known authority to directly address undercover investigations in social media.[170] It involved a civil case and the deposition of an unrepresented eighteen-year-old witness who was giving evidence favorable to the opposition. During questioning she admitted having Facebook and MySpace

---

communicates only with a nonmanagerial employee who is merely a fact witness, no violation would exist.").

169. *Id.*

170. Later opinions on social networking and discovery have followed the Philadelphia approach. *See* N.Y.S. Bar Ass'n Comm. on Prof'l Ethics, Op. 843 (2010), *available at* http://www.nysba.org/AM/Template.cfm?Section=Ethics_Opinions &TEMPLATE=/CM/ContentDisplay.cfm&CONTENTID=43208 ("A lawyer who represents a client in a pending litigation, and who has access to the Facebook or MySpace network used by another party in litigation, may access and review the public social network pages of that party to search for potential impeachment material. As long as the lawyer does not 'friend' the other party or direct a third person to do so, accessing the social network pages of the party will not violate Rule 8.4 (prohibiting deceptive or misleading conduct), Rule 4.1 (prohibiting false statements of fact or law), or Rule 5.3(b)(1) (imposing responsibility on lawyers for unethical conduct by nonlawyers acting at their direction)."); Ass'n of the Bar of the City of N.Y. Comm. on Prof'l & Judicial Ethics, Formal Op. 2010-2 (2010), *available at* http://www.abcny.org/Ethics/eth2010.htm ("[A] lawyer may not use deception to access information from a social networking webpage. Rather, a lawyer should rely on the informal and formal discovery procedures sanctioned by the ethical rules and case law to obtain relevant evidence.").

accounts. The Committee observed that these personal pages limited access to certain individuals according to the account holder's preference. The deposing lawyer had reason to think that her pages might contain impeaching material. He did not directly or openly ask the witness' permission to access the pages but tried unsuccessfully to get to those pages without her consent. From what he did see, the lawyer concluded that she had a liberal policy of letting people have access to her profile. His proposed investigation plan was as follows:

> The inquirer proposes to ask a third person, someone whose name the witness will not recognize, to go to the Facebook and MySpace websites, contact the witness and seek to "friend" her, to obtain access to the information on the pages. The third person would state only truthful information, for example, his or her true name, but would not reveal that he or she is affiliated with the lawyer or the true purpose for which he or she is seeking access, namely, to provide the information posted on the pages to a lawyer for possible use antagonistic to the witness. If the witness allows access, the third person would then provide the information posted on the pages to the inquirer who would evaluate it for possible use in the litigation.[171]

This is a classic pretexting operation, and one which has been approved in cases involving civil rights, law enforcement, and intellectual property infringement.[172] On the surface, none

171. Phila. Bar Ass'n, Formal Op. 2009-02 (2009), http://www.philadelphiabar.org/WebObjects/PBAReadOnly.woa/Contents/WebServerResources/CMSResources/Opinion_2009-2.pdf.

172. *See, e.g.*, N.Y.C. County Lawyer's Ass'n, Formal Op. 737 (2007), http://www.nycla.org/siteFiles/Publications/Publications519_0.pdf ("In New York, while it is generally unethical for a non-government lawyer to knowingly utilize and/or supervise an investigator who will employ dissemblance in an investigation, we conclude that it is ethically permissible in a small number of exceptional circumstances where the dissemblance by investigators is limited to identity and purpose and involves otherwise lawful

of the recognized exceptions applied to this civil action, so the Philadelphia Committee's Opinion focused principally on Pennsylvania Rules of Professional Conduct Rule 8.4(c) concerning "dishonesty, fraud, deceit or misrepresentation." They believed that the proposed surreptitious investigation would violate this rule:

> It omits a highly material fact, namely, that the third party who asks to be allowed access to the witness's pages is doing so only because he or she is intent on obtaining information and sharing it with a lawyer for use in a lawsuit to impeach the testimony of the witness. The omission would purposefully conceal that fact from the witness for the purpose of inducing the witness to allow access, when she may not do so if she knew the third person was associated with the inquirer and the true purpose of the access was to obtain information for the purpose of impeaching her testimony.[173]

---

activity undertaken solely for the purpose of gathering evidence. Even in these cases, a lawyer supervising investigators who dissemble would be acting unethically unless (i) either (a) the investigation is of a violation of civil rights or intellectual property rights and the lawyer believes in good faith that such violation is taking place or will take place imminently or (b) the dissemblance is expressly authorized by law; and (ii) the evidence sought is not reasonably and readily available through other lawful means; and (iii) the lawyer's conduct and the investigator's conduct that the lawyer is supervising do not otherwise violate the New York Lawyer's Code of Professional Responsibility (the 'Code') or applicable law; and (iv) the dissemblance does not unlawfully or unethically violate the rights of third parties. These conditions are narrow. Attorneys must be cautious in applying them to different situations. In most cases, the ethical bounds of permissible conduct will be limited to situations involving the virtual necessity of non-attorney investigator(s) posing as an ordinary consumer(s) engaged in an otherwise lawful transaction in order to obtain basic information not otherwise available. This opinion does not address the separate question of direction of investigations by government lawyers supervising law enforcement personnel where additional considerations, statutory duties and precedents may be relevant. This opinion also does not address whether a lawyer is ever permitted to make dissembling statements directly himself or herself."). *See generally Hiding in Plain Sight*, *supra* note 141, at 5.

173. Formal Op. 2009-02, at 3.

Concealment of identity and purpose was impermissible in this context. And the witness's risky policy of accepting "Friends" with little information did not validate the lawyer's, or investigator's, approach. The privacy policy of the witness did not factor into the analysis of whether the deceit was permissible under the Code. In other words, there was no way to sanitize the conduct of any person who might have access the witness' page at the direction of the attorney, regardless of the information they provided.[174] The Committee distinguished this situation from a day in the life video that might record an unsuspecting plaintiff out in "public" to impeach her claims, because information on social networking sites was intended to be kept private.[175]

The Committee went on to consider the limitations of deception in legal investigation, criminal and civil, and exceptions to further societal good, such as uncovering unlawful and discriminatory behavior.[176] Without addressing the blanket prohibition of covert investigation recognized by some states or the exceptions endorsed in others, the Committee found that in this scenario it was unethical.[177]

This opinion was rendered in a bubble, and peremptorily

---

174. *Id.* at 4 ("The Committee believes that in addition to violating Rule 8.4(c), the proposed conduct constitutes the making of a false statement of material fact to the witness and therefore violates Rule 4.1 as well.").

175. *Id.* at 3.

176. *Id.* at 4-6.

177. The Committee also declined to answer the question about the admissibility of social media evidence obtained through pretexting. This is another important problem that has to be resolved in tandem with the ethics and legitimacy of the investigative technique; otherwise the evidence may be precluded or suppressed. *See* Berman et al., *supra* note 63, at 5 (analyzes issues associated with introducing evidence from second generation web sources such as social networking). *See generally* Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534 (D. Md. 2007) (discusses basic tenets of admitting electronic or digital evidence analyzing the difficulties in establishing relevancy, authenticity, overcoming hearsay, best evidence, and prejudice versus probity arguments); Paul W. Grimm et al., *Back to the Future:* Lorraine v. Markel American Insurance Co. *and New Findings on the Admissibility of Electronically Stored Information*, 42 AKRON L. REV. 357, 367 (2009) (update on the evidentiary foundation requirements for electronic evidence first discussed in the *Lorraine* decision, including: e-mail, web sites, text messages, and computer generated evidence).

closed off a huge and vital area of discovery. The trouble lies in the concepts of privacy and purpose, and the thin veil that can deflect legitimate and necessary covert investigations. As one scholar has observed, it was unfair to exempt government law enforcement, civil rights and intellectual property from the bar on undercover work without a critical rationale behind these choices.[178] Moreover, he suggested a "neutral" test that might be applied more fairly:

> [T]he search should be for neutral principles that reasonably balance the benefits and risks of such technology. These neutral principles should focus less on whether the lawyer/investigator is operating anonymously or with a pseudonym. Rather, they should concentrate more on the *intrusiveness of the technique* and the *risk that confidential or privileged information may be improperly revealed* in the process.[179]

A reasonable guideline for criminal cases is the "societal good" criterion, i.e., the fair administration of justice. The goal would be to prevent or address current problems in the system that result in wrongful convictions. These should be addressed at the earliest stages of a case to preserve the presumption of innocence and due process of law.

Conclusion

Today, hundreds of millions of people are sharing information, communicating, and archiving the details of their lives online. Through canyons of Internet bandwidth, an increasingly complex forum of overlapping voices are being created, preserved and transmitted worldwide. Thirty years

178. *See* Steven C. Bennett, *Ethics of "Pretexting" in a Cyber World*, 41 MCGEORGE L. REV. 271, 279 (2010) ("Ethics authorities should not arbitrarily limit the benefits of such information or favor certain categories of lawyers over others.").

179. *Id.* (emphasis added).

ago, the Supreme Court recognized that most people were getting their information about court proceedings from electronic and print media.[180] Now, our society is in the midst of a personal data revolution in which new enclaves of data and individual metrics are being created on a monumental scale.[181] Social networking will surpass diaries, photo albums, and paper correspondence; it will supersede e-mail and telephonic communication; it will even trump television, radio, and newspapers as the principal source of news and personal information.[182]

Facebook, Twitter, YouTube, and the other social media gained prominence rapidly. Their power is still unmeasured and the rules for their uses unclear. In a sense, social networking is the Promethean fire of the Information Age. Without guidance, it spells mischief for the lawyers who must use it to represent their clients. The question has changed from how to find information about witnesses and parties online, to how to find information within ethical and legal boundaries that will be in existence when the case comes to trial.[183]

---

180. *See* Richmond Newspapers, Inc. v. Virginia, 448 U.S. 555, 572 (1980) ("With the press, cinema, and electronic media now supplying the representations or reality of the real life drama once available only in the courtroom, attendance at court is no longer a widespread pastime.").

181. *See* Richard Macmanus, *The Coming Data Explosion*, N.Y. TIMES, May 31, 2010, *available at* http://www.nytimes.com/external/readwriteweb/2010/05/31/31readwriteweb-the-coming-data-explosion-13154.html ("One of the key aspects of the emerging Internet of Things—where real-world objects are connected to the Internet—is the massive amount of new data on the Web that will result. As more and more 'things' in the world are connected to the Internet, it follows that more data will be uploaded to and downloaded from the cloud. And this is in addition to the burgeoning amount of user-generated content—which has increased 15-fold over the past few years, according to a presentation that Google VP Marissa Mayer made last August at Xerox PARC. Mayer said during her presentation that this 'data explosion is bigger than Moore's law.'").

182. *See, e.g.*, Wayne, *supra* note 16. *See generally Internet Gains on Television as Public's Main News Source*, PEW RES. CENTER (Jan. 4, 2011), http://people-press.org/report/689/.

183. *See generally* Mark A. Berman, *The Ethics of Social Networking Discovery*, N.Y. L.J., Nov. 2, 2010, at 5 ("Just like conducting Westlaw or Lexis due diligence on an individual, social networking sites need to be reviewed as part of discovery protocol when seeking to obtain relevant

The big problem is that the standards of privacy and criminal behavior are being defined in large part by the terms of service and technology options set by social networking providers. The Drew Lori case taught us that a breach of contract, such as a terms of service contract, was unlikely to sustain a violation of federal criminal law.[184] Privatizing criminal law or definitions of privacy are problematic and unconstitutional. It would be an abdication of the legislative function to permit private Internet-based services to define online privacy or criminalize behavior vaguely described in browser- and clip-wrap contracts. The legislatures have to update the definitions of criminal laws related to electronic media in the discovery and penal statutes. Moreover, the courts must be adept and up to date on the latest technology innovations that might influence the interpretation of legal and ethical rules for attorney conduct in this virtual environment as in other developing areas.[185]

Social networking is a convergence technology, combining communication media and information storage in unprecedented ways. A new unified approach is necessary to administer the application of criminal law, evidentiary rules, and ethical constraints in this context. As courts and counsel

---

information concerning a person or entity."); Thomas G. Frongillo & Daniel K. Gelb, *It's Time to Level the Playing Field—The Defense's Use of Evidence from Social Networking Sites*, CHAMPION, Aug. 2010, at 14 ("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.").

184. *See* United States v. Drew, 259 F.R.D. 449, 452 (C.D. Cal. 2009).

185. *See, e.g.*, *Committee on the Development of the Third Edition of the Reference Manual on Scientific Evidence*, COMM. ON SCI., TECH. & L., http://sites.nationalacademies.org/PGA/stl/development_manual/index.htm (last visited Oct. 10, 2010) ("At the request of the Federal Judicial Center (FJC), and in collaboration with the FJC, [the Committee on Science, Technology, and Law] will develop the third edition of the Reference Manual on Scientific Evidence. The Reference Manual assists judges in managing cases involving complex scientific and technical evidence by describing the basic tenets of key scientific fields from which legal evidence is typically derived and providing examples of cases in which that evidence has been used. The development of the third edition will follow the basic structure of the current edition, but will include, in addition to updating, new topics and annotated case citations.").

wend their way through the thickets, a fundamental constitutional analysis will serve as the best guidepost. The right to present a defense and reciprocal discovery are well established and supported by Supreme Court precedent. Until the nuances of cyber criminal investigations are worked out, judges should maintain the balance of rights by leveling the playing field between prosecutors and defense. If the government is permitted access to Facebook or Twitter, if the prosecution can introduce YouTube videos and iPhone messages, then due process demands the same rights for the defense. For law enforcement, social media are among the first avenues to be investigated undercover, and there are no logical reasons why the defense should have to exhaust all other options before following the same path. In this area, the delete button and risk of spoliation of digital media make early entry into a witness social profile an unacknowledged imperative for the defense as much as for the prosecution.

We have entered a new part of the Information Age, the Social Media Era.[186] It is the time of quantum computing and the specter of nearly a billion personal profiles online. Countries around the world are evolving into societies that permit unbounded sharing and displaying of personal multimedia experiences. To paraphrase Andy Warhol, everyone wants their 15 gigabytes of fame. And all fame has its price. The cost of this freedom is a qualified privacy, a cloverleaf intersection weaving electronic human activities with the law, and the unveiling of new avenues of investigation. The best "path forward" for discovery in social space is to recognize that it is unprecedented and construct rules that remain faithful to the constitutional and ethical principles that have served society in the physical world. Due process and the fair

186. Online communities are really no different than the unregulated ancient Roman bathhouses, where people came together to talk, relax and entertain themselves, while baring all. And bandwidth, like currents of water, is the well that draws people together. *See* JAMES SALZMAN, THIRST: A SHORT HISTORY OF DRINKING WATER (2005), *available at* http://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=2043&context =faculty_scholarship ("The main reason for construction of the aqueducts was not hygienic but social. Bath houses were an integral part of Roman society and they required large volumes of water.").

administration of justice dictate that there ought to be an equal right of access and use of virtual evidence regardless of changes in the mechanics of human communication and interaction.