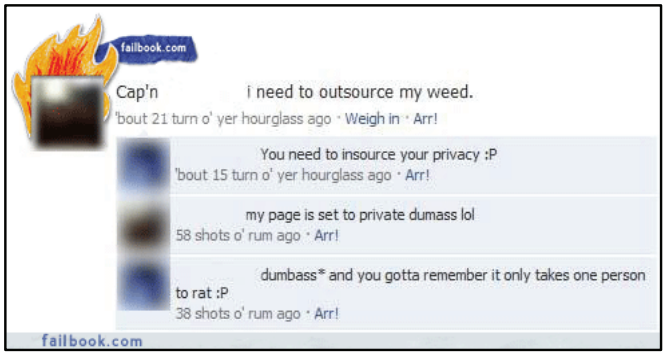
BALANCING THE SCALES OF JUSTICE: UNDERCOVER INVESTIGATIONS ON SOCIAL NETWORKING SITES

Shirin Chahal*



* J.D. candidate, 2011, University of Colorado Law School; B.S., University of Southern California, 2007. Thanks to my parents and family for their support. Also thanks to Professors Paul Ohm and William Pizzi for their inspiration and guidance, and Professor Pat Furman for his helpful comments on early drafts. Finally, thanks to Devin Looijen, Blake Reid, Meredith Simmons, and the rest of the staff of the Journal on Telecommunications and High Technology Law for their excellent editorial work.

INTRODUCTION 286
I. A BRIEF BACKGROUND ON THE RISE AND USE OF SOCIAL NETWORKING SITES 289
II. THE LAW GOVERNING ONLINE PRIVACY IN THE UNITED STATES IS LESS THAN CLEAR 291
A. The Fourth Amendment 291
B. The Electronic Communications Privacy Act 293
C. The Inherent Privacy Risks of Social Networking 298
III. CRIMINAL DISCOVERY AND LEGAL ETHICS 300
A. The Rules of Criminal Procedure 301
B. Legal Ethics 305
C. A Proposed Framework for How a Defense Attorney Can Conduct Research on a Social Networking Site 308
CONCLUSION 310

INTRODUCTION

According to media research group The Nielsen Company, social network use in February 2009 exceeded Web-based e-mail use for the first time.[1] Social networking sites ("SNSs") such as Facebook, MySpace, Twitter, and LinkedIn[2] have pioneered new kinds of services "unseen in human history, in which hundreds of millions of people are connected in an intimate way, sharing information and e-mails and photos in real time, making new contacts, and rapidly erasing 'the fine line between public and private.'"[3] Use of SNSs is unlikely to decline as the youngest generations of Internet users continue to completely integrate their personal and social lives with these sites. Additionally, as Internet use has increased, so has the legal use of information mined from SNSs.[4] Law enforcement officials and attorneys are increasingly finding information

1. NIELSEN ONLINE, THE NIELSEN CO., THE GLOBAL ONLINE MEDIA LANDSCAPE 6 (2009).

2. FACEBOOK, http://www.facebook.com (last visited Nov. 23, 2010); MYSPACE, http://www.myspace.com (last visited Nov. 23, 2010); TWITTER, http://twitter.com (last visited Nov. 23, 2010); LINKEDIN, http://www.linkedin.com (last visited Nov. 23, 2010).

3. *Facebook: The Privacy Backlash*, THE WEEK, May 20, 2010, at 18 [hereinafter *Privacy Backlash*].

4. *See, e.g.*, Nancy Hass, *In Your Facebook.com,* N.Y. TIMES, Jan. 8, 2006, at 4A30; Vesna Jaksic, *Finding Treasures for Cases on Facebook,* NAT'L L.J., Oct. 15, 2007, http://www.law.com/jsp/lawtechnologynews/PubArticleLTN.jsp?id=900005493439; Daniel L. Brown & Aimee R. Kahn, *Savvy Use of Social Networking Sites,* N.Y. L.J., Special Section (Sept. 8, 2009).

online that is highly relevant to their civil and criminal cases, and there are numerous instances where information gleaned from an SNS proved to be a key part in a legal action.[5] Despite this increased use of SNS information, the legal community has not yet reached a consensus on the legal and ethical issues involved in using these sites for investigations.

This note focuses on criminal discovery and the way both the government and the defendant can obtain access to information on social networking profiles. Both sides acknowledge that SNS research has become a critical investigative tool during discovery and trial.[6] However, defense attorneys lament the critical differences between the government and the defendant in the way SNS research can be conducted, and many have expressed concern that this disparity may gravely impact concepts of adversarial fairness and the pursuit of justice in the criminal legal system.[7]

Prosecutors, as government agents, have traditionally had more access than defense attorneys to resources that may reveal information on which to build their cases and convict defendants. This inequality has been justified under the government's duty to protect the public from the harm of criminal conduct. Today, however, defense attorneys desire access to SNS research tools because these processes may be just as likely to uncover exculpatory information that could help prove innocence as they are to uncover inculpatory information.

The government is afforded several ways to obtain private SNS

---

5. *See, e.g.,* Clark v. State, 915 N.E.2d 126, 130 (Ind. 2009) (The Indiana Supreme Court allowed evidence from the defendant's MySpace page as character evidence when his defense strategy relied upon his propensity for irresponsible behavior to obtain a jury verdict on the lesser-included offense of reckless homicide.); People v. Liceaga, 2009 Mich. App. LEXIS 160, *7-8 (Mich. Ct. App. 2009) (The prosecutor admitted photographs from defendant's MySpace page as evidence of intent and planning.); *In re K.W.,* 666 S.E.2d 490, 494 (N.C. Ct. App. 2008) (An alleged child abuse victim's MySpace page was admitted as impeachment evidence.); Eamon McNiff, *Teen Party Crashers Allegedly Cause $45,000 Worth of Damage to House,* ABC NEWS (Mar. 31, 2010), http://abcnews.go.com/TheLaw/Technology/teen-party-crashers-arrested-destroying-house/story?id=10240377 (Police found teens bragged about vandalism on a Facebook page entitled "The Homewrecker Crew."); Mary Pat Gallagher, *MySpace, Facebook Pages Called Key to Dispute Over Insurance Coverage for Eating Disorders,* LAW.COM (Feb. 1, 2008), http://www.law.com/jsp/law/LawArticleFriendly.jsp?id=900005559933; Vesna Jaksic, *Finding Treasures for Cases on Facebook,* NAT'L L.J., Oct. 15, 2007, http://www.law.com/jsp/lawtechnologynews/PubArticleLTN.jsp?id=900005493439 (The defense attorney was able to prove a man other than his client was the initial aggressor because the man's MySpace page contained a video of him beating someone up.); Jim Dwyer, *The Officer Who Posted Too Much on MySpace,* N.Y. TIMES, March 10, 2009, at A24 (A defense attorney used MySpace and Facebook evidence to question the credibility of the defendant's arresting officer.).

6. To hear some of these discussions, see podcasts: Conference on Social Networks: Friends or Foes? Confronting Online Legal and Ethical Issues in the Age of Social Networking, held by UC Berkeley School of Law (Oct. 23, 2009), *available at* http://www.law.berkeley.edu/7458.htm.

7. *Id.*

information from an individual's profile or account. First, the prosecutor can be closely involved in deceptive, undercover operations. For example, the Electronic Frontier Foundation, a San Francisco-based civil liberties group, recently obtained a Justice Department document that detailed the use of SNSs by FBI and other law enforcement agents to exchange messages with suspects, identify a target's friends or relatives, and browse private information such as postings, personal photographs and video clips.[8] Second, the Electronic Consumer Privacy Act ("ECPA") provides the prosecutor with tools to compel the production of SNS information.[9] These legal processes are similar to others used by government agents outside the virtual world (e.g., subpoenas, search warrants). However, many practitioners argue that SNSs have such great potential to store exculpatory, impeachment, and other types of evidence that this inequality of legal process as well as the lack of access to undercover data puts them at a crucial disadvantage.

Part I of this note explores how SNSs work and the kind of information that can be found on an SNS profile. Part II examines some of the privacy issues that involve SNSs, including the scope and applicability of relevant law. Part II.A surveys the privacy laws in the United States and some of the arguments on how these laws should apply to cyberspace in general and to SNSs in particular. Part II.B takes a look at the ECPA and explains how the statute compels private communications providers to turn over records and other information to the government. Part II.C argues that neither SNS providers nor the law can properly address all the privacy issues and concerns raised by the legal use of SNS information. Therefore, this section argues that the onus must be on the SNS user to assess the risk and protect his information accordingly.

Part III looks at criminal discovery and the constitutional, statutory, and ethical obligations that guide and regulate it. Part III.A examines the current procedures followed by prosecutors and defendants in bringing convictions and preparing for trial. Part III.B summarizes some of the competing ideas on how a non-government attorney can conduct SNS research within the confines of constitutional, statutory, and ethical constraints. Finally, Part III.C demonstrates how a more liberal approach to SNS investigation can be supported by current ethics rules and some of the accepted policies behind our criminal judicial system.

Overall, this paper focuses on how disparate standards in criminal

8. Richard Lardner, *Feds Going Undercover on Facebook, Twitter, Other Social Networking Sites*, ATLANTA J.-CONSTITUTION (Mar. 31, 2010, 04:36 PM), http://www.ajc.com/news/feds-going-undercover-on-423303.html.

9. Electronic Communication Privacy Act of 1986, Pub. L. 99-508, 100 Stat. 1848 (codified in scattered sections of 18 U.S.C.).

procedure, the ECPA, and the ethical rules have created a confusing landscape for the lawyer looking to conduct factual research on an SNS. These disparities should be reconciled in order to aid the criminal discovery process and the pursuit of justice. Specifically, in trying to access SNS information, certain practices that involve the use of undercover investigative techniques, particularly those conducted by an attorney's agents, should be allowed in order to rectify the disparity between prosecutors and defense attorneys. This note will show that similar practices conducted outside of cyberspace have been endorsed by the courts and can readily be applied to SNSs without breaking website terms of service or use.

I. A BRIEF BACKGROUND ON THE RISE AND USE OF SOCIAL NETWORKING SITES

Facebook, MySpace and Twitter are three of the most popular social networking sites.[10] Facebook has over 500 million users, half of whom log in at least once a day.[11] MySpace has 125 million monthly active users.[12] Twitter currently has more than 100 million users worldwide.[13] These sites offer their members the ability to connect and communicate with other members, including friends, relatives, colleagues, and the general public.[14]

Users of Facebook and MySpace create online profiles where they can post a photo of themselves, list contact information, school information, personal information, and post additional photo albums or personal blog posts.[15] Besides creating profiles and posting information, Facebook and MySpace users can also compile lists of friends that they can link to, post public comments on their profiles, and send private messages.[16] Users can also create groups of people with similar interests

10. *See Top Sites in United States*, ALEXA, http://www.alexa.com/topsites/countries/US (last visited Mar. 31, 2010).

11. *Press Room Statistics*, FACEBOOK, http://www.facebook.com/press/info.php?statistics (last visited Mar. 31, 2010).

12. *Press Room*, MYSPACE, http://www.myspace.com/pressroom?url=/fact+sheet (last visited Mar. 31, 2010).

13. *Twitter Snags over 100 Million Users, Eyes Money-Making*, ECON. TIMES, Apr. 15, 2010, http://economictimes.indiatimes.com/infotech/internet/Twitter-snags-over-100-million-users-eyes-money-making/articleshow/5808927.cms.

14. *Help Center, Find Your Friends*, FACEBOOK, http://www.facebook.com/help/?ref=pf#!/help/?guide (last visited Feb. 15, 2010) [hereinafter *Find Your Friends*].

15. *Help Center, Set Up a Profile*, FACEBOOK, http://www.facebook.com/help/?ref=pf#!/help/?guide=set_up_profile (last visited Feb. 15, 2010); *Help Center*, MYSPACE, http://faq.myspace.com/app/home (last visited Feb. 15, 2010).

16. *Find your Friends*, *supra* note 14; *Help Center, How do I find friends on MySpace?*, MYSPACE, (http://faq.myspace.com/app/answers/detail/a_id/56/kw/find%20friends/r_id/100061 (last

and announce events and invite people to these events.[17] Facebook and MySpace also have search functions, which allow users to look up other users by name or interests.[18] Until very recently, Facebook allowed its users to limit those who viewed their profiles by grouping users into networks based on affiliation with a school, region of the country or company.[19] At the end of 2009, Facebook removed this network-based privacy option and now only allows privacy settings based on "Friends," "Friends of Friends," and "Everyone."[20] In October 2010, the site created an additional feature that allows users to target their updates to specific sets of friends or "Groups," without posting the information to everyone in their network.[21] MySpace, in contrast, has no networks or inherent limitations on the viewing of profiles.

Facebook's photo sharing system is one of its most popular features. When users upload photos, they can click on a person in the photo, enter that person's name, and create a link to the "tagged" person's own profile.[22] This tagging system can be initiated by anyone on Facebook, even someone who does not know the user who originally uploaded the files.[23] Many of the activities on Facebook generate event notifications that are displayed in a general "News Feed" that is visible on all users' home pages. After the success of Facebook's photo tagging and News Feed systems, MySpace adopted similar features.

Twitter is slightly different than these two traditional SNSs. While the site allows users to maintain personal profiles and compile friend lists, the site's main component is its "microblogging" service, which

---

visited Feb. 15, 2010).

17. *Help Center, How do I create a group?*, FACEBOOK, http://www.facebook.com/help/?guide=set_up_profile#!/help/?faq=13034 (last visited Feb. 15, 2010); *Help Center, How to use the Events application*, FACEBOOK, http://www.facebook.com/help/?guide=set_up_profile#!/help/?page=828 (last visited Feb. 15, 2010); *Help Center, How do you join, add and manage MySpace groups?*, MYSPACE, http://faq.myspace.com/app/answers/detail/a_id/202/kw/groups/r_id/100061 (last visited Feb. 15, 2010); *Help Center, How do you invite your friends to a party?*, MYSPACE, http://faq.myspace.com/app/answers/detail/a_id/296/kw/myspace%20events/r_id/100061 (last visited Feb. 15, 2010).

18. *Find your Friends*, *supra* note 14.

19. Paul McDonald, *Growing Beyond Regional Networks*, THE FACEBOOK BLOG (June 2, 2009, 4:14 PM), http://blog.facebook.com/blog.php?post=91242982130.

20. *A Guide to Privacy on Facebook,* FACEBOOK, http://www.facebook.com/privacy/explanation.php?ref=pf (last visited Nov. 23, 2010).

21. David Goldman, *Facebook Unveils New Groups Tool,* CNNMONEY.COM (Oct. 7, 2010, 9:05 AM ET), http://money.cnn.com/2010/10/06/technology/facebook_event.

22. *Help Center, Photos*, FACEBOOK, http://www.facebook.com/help/?guide=set_up_profile#!/help.php?page=830 (last visited Feb. 15, 2010).

23. *Help Center, How does tagging work? How do I remove a tag?*, FACEBOOK, http://www.facebook.com/help/?guide=set_up_profile#!/help/?faq=13407 (last visited Feb. 15, 2010).

enables users to send and read user messages called "tweets."[24] Tweets are text-based posts of up to 140 characters displayed on a user's profile page.[25] Tweets are publicly visible by default, but senders can restrict message delivery to only their friend list.[26] Users may also subscribe to other author tweets; this is known as "following."[27] The site proclaims: "Whether it's breaking news, a local traffic jam, a deal at your favorite shop or a funny pick-me-up from a friend, Twitter keeps you informed with what matters most to you today."[28]

II. THE LAW GOVERNING ONLINE PRIVACY IN THE UNITED STATES IS LESS THAN CLEAR

More than forty years ago, the Supreme Court acknowledged that "[t]he law, though jealous of individual privacy, has not kept pace with recent advances in scientific knowledge."[29] Today, with the advent of the Internet, GPS tracking devices and mobile communications, this observation holds true more than ever before. In the words of privacy scholar Professor Daniel J. Solove:

> Privacy is far too vague a concept to guide adjudication and lawmaking, as abstract incantations of the importance of "privacy" do not fare well when pitted against more concretely stated countervailing interests. . . . [I]nformation privacy is significantly more vast and complex, extending to Fourth Amendment law, the constitutional right to information privacy, evidentiary privileges, dozens of federal privacy statutes, and hundreds of state statutes.[30]

This section will explore some of the current laws that govern privacy on the Internet.

A. The Fourth Amendment

Under modern privacy law, a communication medium or platform is

24. *About Tweets #New Twitter*, TWITTER, http://support.twitter.com/groups/31-twitter-basics/topics/146-new-twitter/articles/221118-about-tweets-newtwitter (last visited Sept. 25, 2010).

25. *Id.*

26. *About Private Messages (Direct Messages) #New Twitter,* TWITTER, http://support.twitter.com/groups/31-twitter-basics/topics/146-new-twitter/articles/219981-about-private-messages-direct-messages-newtwitter (last visited Sept. 25, 2010).

27. *How to Follow Others #New Twitter*, TWITTER, http://support.twitter.com/groups/31-twitter-basics/topics/146-new-twitter/articles/226649-how-to-follow-others-newtwitter (last visited Sept. 25, 2010).

28. *About*, TWITTER, http://twitter.com/about (last visited Sept. 26, 2010).

29. Berger v. New York, 388 U.S. 41, 49 (1967).

30. Daniel J. Solove, *A Taxonomy of Privacy,* 154 U. PA. L. REV. 477, 478 (2006).

not vested with Fourth Amendment[31] protection unless the user has a reasonable expectation of privacy therein. This is a twofold requirement, set out in Justice Harlan's concurrence in the seminal case *Katz v. United States,* which requires, first, that a person have an actual subjective expectation of privacy and, second, that the expectation is one that society is prepared to recognize as reasonable.[32] If both prongs are met, the government must acquire a warrant with its corresponding probable cause requirement to search the protected area or information.[33] This inquiry, which delves into the objective reasonableness of an expectation of privacy, is based on precedent from previous rulings. However, the Supreme Court has yet to tackle the issue of Fourth Amendment privacy in cyberspace. Thus, courts have had to draw analogies to previous non-cyberspace rulings.[34]

In *Smith v. Maryland,* the Supreme Court held that the defendant had no subjective expectation of privacy in a search conducted by a pen register, a device installed by telephone companies that can track the dialed phone numbers for outgoing calls.[35] The Court stated that telephone users must realize that they "convey" phone numbers to the telephone company because they see a list of their calls on their monthly bills.[36] The Court also noted that pen registers do not "acquire the *contents* of communications,"[37] paving the way for the content/non-content distinction followed today.[38] When applied to Internet communications, there is a lesser expectation of privacy in e-mail addresses, IP addresses, and URLs because these are likened to non-content telephone numbers.[39]

In *United States v. Miller*, the Supreme Court held that there was no

31. "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV.

32. 389 U.S. 347, 361 (1967) (Harlan J., concurring).

33. *Id.* at 357.

34. Ric Simmons, *From Katz to Kyllo: A Blueprint for Adapting the Fourth Amendment to Twenty-First Century Technologies*, 53 HASTINGS L.J. 1303, 1322 (2002); *see, e.g.* United States v. Maxwell, 45 M.J. 406, 417-18 (C.A.A.F. 1996) (comparing e-mails to first-class mail and phone calls and distinguishing them from the open Internet).

35. 442 U.S. 735, 742 (1979).

36. *Id.*

37. *Id.* at 741 (emphasis in original).

38. This standard distinguishes "content" information, which conveys the substance, purport, or meaning of the communications from "non-content" information, which conveys dialing or routing information. Thus, for a phone call, the phone number dialed to initiate the call is non-content information and the actual ensuing conversation, namely the words spoken, is the content information. *See id.* at 743.

39. Orin S. Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 STAN. L. REV. 1005, 1027-28 (2010).

protected Fourth Amendment interest in a person's bank records.[40] The Court supported this holding by stating that such documents "contain only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business."[41] Further, it stated, "[a person] takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government."[42] Thus, *Miller* solidified *Smith*'s dicta suggesting that records and documents handed over to third parties are stripped of their Fourth Amendment protections.

Finally, relying on *Katz,* the Supreme Court held in *California v. Ciraolo* that the mere possibility of exposure to the public eye diminishes and sometimes obviates the individual's privacy expectation.[43] However, if someone "seals" or takes precautions to protect their information, this creates a reasonable expectation of privacy.[44]

In applying the two-pronged "legitimate expectation of privacy" test to SNSs, there is clearly a range of analyses. The subjective and objective expectations of privacy are different for a default MySpace profile that can be viewed by anyone on the Web and a profile that has been set to the highest "private" settings afforded by the SNS provider.[45] However, even in the latter category, the inherent nature of an SNS profile's everyday use works against the notion of privacy expectations. By signing on to an SNS and providing personal information for friends to see, users make a choice to publicize this information to others. Furthermore, unlike postal mail or bank accounts, there is no substantial need to have a profile on an SNS to participate in society. Thus, an aggressive investigator can always argue that an SNS profile is better compared to a yearbook, directory, or bulletin board rather than a piece of mail or a closed container, and thus find that any information posted on a profile, be it photos, bulletins, or wall posts, holds no protection under the Fourth Amendment.

B. The Electronic Communications Privacy Act

After the Supreme Court provided a very narrow view of privacy

40. 425 U.S. 435, 440 (1976).

41. *Id.* at 442.

42. *Id.* at 443.

43. 476 U.S. 207, 213 (1986) ("What a person knowingly exposes to the public, even in his home or office, is not a subject of Fourth Amendment protection." (quoting *Katz,* 389 U.S. at 351)).

44. *United States v. Jacobsen*, 466 U.S. 109, 114 (1984) ("[S]ealed packages are in the general class of effects in which the public at large has a legitimate expectation of privacy . . . .").

45. *See* Matthew J. Hodge, *The Fourth Amendment and Privacy Issues on the "New" Internet: Facebook.com and MySpace.com,* 31 S. ILL. U. L. J. 95, 106-17 (2006).

rights under the Fourth Amendment in *Smith* and *Miller*, Congress enacted legislation partly superseding these decisions.[46] The Federal Wiretap Act was first enacted in 1968 to regulate telephone wiretaps and hidden microphones.[47] In 1986, Congress amended the Federal Wiretap Act to include electronic communications by enacting the Electronic Communications Privacy Act ("ECPA").[48] This set of statutory privacy laws supplements the Fourth Amendment and regulates the collection of digital evidence stored and transmitted on computer networks.

The portion of the ECPA that compels the production of stored communications and records, the Stored Communications Act ("SCA"), applies only to providers of "electronic communication services" ("ECS") and providers of "remote computing services" ("RCS"). The ECPA defines the former as "any service which provides to users thereof the ability to send or receive wire or electronic communications" and defines these provider's storage capabilities as "any temporary, intermediate storage of wire or electronic communication incidental to the electronic transmission thereof."[49] The latter category of provider is defined as "the provision to the public of computer storage or processing services by means of an electronic communications system."[50]

If these two categories seem foreign or obsolete, this is because many of the statute's definitions of electronic communications are based upon the existing technologies of 1986. The RCS category is especially indicative of the networks of yesteryear. In the past, computer processing power and storage capabilities were at a premium, and users would pay to have remote computers store extra files or process data. Today, a simple spreadsheet program can accomplish the tasks of the "remote computing service" providers of the late-'80s.[51] Further, the network service providers of today are multifunctional, providing communication services in some contexts, storage and processing in others, and important privacy-implicating services that fall into neither category.[52] However,

46. *See, e.g.* 12 U.S.C. § 3405 (2006) (requiring that financial records be relevant to a "legitimate law enforcement inquiry" and that a copy of the summons be served on the customer before government can access the records); 18 U.S.C. § 3121 (2006) (requiring a court order before use of pen registers).

47. Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. §§ 2510-2520 (2006).

48. Electronic Communication Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended in scattered sections of 18 U.S.C.).

49. 18 U.S.C. § 2510(17)(A).

50. 18 U.S.C. § 2711(2).

51. For example, the Microsoft software spreadsheet product "Excel" can accomplish such tasks.

52. *See e.g.*, Quon v. Arch Wireless Operating Co., 529 F.3d 892, 900-03 (9th Cir. 2008), *rev'd on other grounds sub nom.* City of Ontario v. Quon, 130 S. Ct. 2619 (2010) (holding that, for the purpose of archived messages, the provider of a text messaging service was an ECS, not an RCS, and therefore violated the SCA when it released transcripts of text

the statutory distinction remains significant because a remote computing service can release communications only with the consent of the subscriber, while an electronic communication service must obtain the consent of "the originator or an addressee or intended recipient of such communication."[53] Additionally, some communications mediums fall outside the scope of the SCA altogether, and they are thus afforded only traditional Fourth Amendment privacy protections.[54]

Facebook receives 10-20 law enforcement requests per day.[55] Many of these are in the form of general court-ordered subpoenas.[56] However, some of these requests are brought under ECPA because Facebook is a public network service provider.[57]

The SCA[58] is the main statutory source that aids government investigators and prosecutors in obtaining information from SNSs that is not readily available on the Web.[59] Through the SCA, government investigators can compel MySpace and Facebook to turn over logs of the times and dates that their users have logged into the network via a § 2703(d) court order.[60] A § 2703(d) court order requires only that the government show "specific and articulable facts showing that there are reasonable grounds to believe" that the logs are "relevant and material to an ongoing criminal investigation," a far lesser showing than a standard warrant's probable cause and particularity requirements under the Fourth

---

messages).

53. 18 U.S.C. § 2702(b)(3).

54. *See e.g.,* In re Jetblue Airways Corp. Privacy Litig., 379 F. Supp. 2d 299, 307-10 (E.D.N.Y. 2005) (holding that JetBlue did not violate the SCA when it disclosed data from its passenger reservation system because JetBlue was neither an ECS, in merely transmitting data to customers to offer its traditional products and services over the Internet rather than providing Internet access itself, nor an RCS, in provided neither computer processing services or computer storage to the public).

55. Mark Howtinson, Deputy Gen. Counsel, Facebook, Panel comments at UC Berkeley School of Law Conference on Social Networks: Friends or Foes? Confronting Online Legal and Ethical Issues in the Age of Social Networking: Does Overt Access to Social Networking Data Constitute Spying or Searching? (Oct. 23, 2009) http://www.law.berkeley.edu/7458.htm.

56. *Id.*

57. James Aquilina, Exec. Managing Dir. and Deputy Gen. Counsel, Stroz Friedberg, Panel comments at UC Berkeley School of Law Conference on Social Networks: Friends or Foes? Confronting Online Legal and Ethical Issues in the Age of Social Networking: Does Overt Access to Social Networking Data Constitute Spying or Searching? (Oct. 23, 2009) http://www.law.berkeley.edu/7458.htm.

58. 18 U.S.C. §§ 2701-11.

59. Conference on Social Networks: Friends or Foes? Confronting Online Legal and Ethical Issues in the Age of Social Networking, held by UC Berkeley School of Law (Oct. 23, 2009), *available at* http://www.law.berkeley.edu/7458.htm.

60. Each of these logs is called a "session ID." A session ID is a unique number that a website's server assigns a specific user for the duration of that user's visit. Session IDs allow websites to confirm that users are logged in and identify the user across multiple Web page requests. *See Session ID*, WIKIPEDIA, http://en.wikipedia.org/wiki/Session_ID (last visited Feb. 15, 2010). The process for a § 2703(d) court order is described at 18 U.S.C. § 2703(d).

Amendment. This lesser standard reflects the content/non-content distinction.

Government investigators and prosecutors can compel SNSs to turn over content through a warrant under § 2703(a).[61] Content is defined as "any information concerning the substance, purport, or meaning of that communication."[62] A § 2703(a) warrant is "issued using the procedures describe in the Federal Rules of Criminal Procedure," and thus requires (1) probable cause that evidence of a crime will be found on the SNS and must also (2) describe the place to be searched and the information sought with particularity.

There are arguments that the SCA does not apply to Facebook at all, particularly with regard to the information stored on a user's profile page. The statute applies only to communications *incidentally* in storage for transmission by an ECS, or files held solely for computer processing or storage by an RCS. Thus, certain communications on SNSs may not fit any of these categories.[63]

Facebook advertises itself as a "social utility," a description that encompasses its many functions including private user-to-user messages, photo albums, status updates, user applications and more.[64] Since the ECPA is applied on a communication-by-communication basis, each Facebook function must be analyzed separately to determine what processes may be available to compel disclosure under the statute. Facebook's chat and user-to-user messaging functions are clearly analogous to e-mail and instant messaging, and they probably fall under ECS.[65] Facebook's user-to-user wall post function is also a medium for two-way communication like chats and e-mails.[66] However, wall posts can be viewed by third parties, which arguably affect the amount of privacy that is expected in such communications. Does this affect the function's classification under the SCA? Facebook status updates are a one-way means for a user to alert all his or her friends at once.[67] This

61. 18 U.S.C. § 2703(a) ("A governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication. . . only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure. . .").

62. 18 U.S.C. § 2510(8).

63. *See, e.g., In re* JetBlue Airways Corp. Privacy Litig., 379 F. Supp. 2d 299 (E.D.N.Y. 2005) (where an airline's passenger reservation system was found to be neither an RCS nor an ECS).

64. *Factsheet*, FACEBOOK, http://www.facebook.com/press/info.php?factsheet (last visited Feb. 15, 2010).

65. *Help Center, How to use the Chat feature,* FACEBOOK, http://www.facebook.com/help/?ref=pf#!/help.php?page=824 (last visited Feb. 15, 2010).

66. *Help Center, How to use the Wall and Wall privacy*, FACEBOOK, http://www.facebook.com/help/?ref=pf#!/help/?page=820 (last visited Feb. 15, 2010).

67. *Help Center, Status*, FACEBOOK, http://www.facebook.com/help/?ref=pf#!/help/?page=706 (last visited Feb. 15, 2010).

appears to fall outside the scope of ECS, being more like a traditional website that imparts information to an audience, such as a news site like CNN.com or a blog. However, Facebook allows a user's friends to leave comments under these status updates. Thus, these status updates are similar to both a publicly-viewable chat that would not be covered under the SCA, and also private e-mail chains that would be protected by the SCA.

There is a valid argument that Facebook's photo sharing function is an RCS because users can store their photos on the website instead of on their personal hard drives. But, is the purpose of the user to use Facebook as such, or is the purpose of the user to upload photos in order to share them and publicize their own activities? For status updates, if a user regularly employs this function their profile will soon contain a long string of information about a user's activities or thoughts and feelings. This could render Facebook an RCS because it is storing these tidbits in one place, similar to a diary or journal. However, most Facebook users probably do not intend their collection of status updates and wall posts to be a diary and may rarely click through their old posts. Thus, their motive is not to use Facebook as a "computer storage or processing service." Similarly, a user does not place his personal work, relationship, hobby, and contact information on Facebook to store it there, but to share it with others on the website. Thus, while it is a form of communication, this personal information seems to fall outside the scope of ECS and RCS.

Despite these arguments, Facebook itself has generally acquiesced to any orders or warrants that appear to be valid.[68] The battle Facebook has chosen to fight is over the scope of content and non-content information. The company has also recognized that its users' expectations of privacy are not easy to define and that its exhaustive privacy policy does not protect itself from user outrage when privacy appears to have been breached.[69] In the spring of 2010, Facebook faced a user backlash after it announced its new "partner"-site information-sharing feature, prompting some to call for a "Quit Facebook Day."[70] Thus, as a legal strategy and publicity tool Facebook has adopted a policy that defines "content" extremely broadly. It also publicly rebukes any

68. Howtinson, *supra* note 55.

69. Juan Carlos Perez, *Facebook's Beacon More Intrusive than Previously Thought*, PC WORLD (Nov. 30, 2007, 4:10 PM), http://www.pcworld.com/article/140182/facebooks_beacon_more_intrusive_than_previously_thought.html.

70. *See Privacy Backlash*, *supra* note 3; *see also Why 'Quit Facebook Day' Failed: 3 Theories*, THE WEEK (June 1, 2010, 11:11 AM), http://theweek.com/article/index/203554/why-quit-facebook-day-failed-3-theories ("Quit Facebook Day," scheduled for May 31, 2010, was largely a failure.).

attempts to obtain such information through a non-warrant process.[71]

C. *The Inherent Privacy Risks of Social Networking*

Facebook and MySpace hold an incredible amount of information about their users. A fully-completed Facebook profile contains a wealth of personal information: name, gender, sexual preference, birthday, political and religious views, relationship status, educational and employment history, and more. Wall posts can contain information about the posting user ("Thanks for helping me out with my car the other day."), the receiving user ("Hungover? You were crazy last night!!"), or both. Uploaded and tagged photos document what a user looks like, places they have been, and things they do. A photo also connects those pictured together in the image and connects the people in the photo with the user who uploaded the image.[72] Further, Facebook offers many tools that allow a user to search out other profiles and potential contacts.

SNSs allow users to restrict access to their profile to only allow those who they accept as "friends" to view their profile.[73] This setting is not the default for either MySpace or Facebook; users must take an active step to turn it on.[74] There is a strong argument however, that even this step should not overcome the presumption that by posting information on a profile, users should not actually expect privacy because they are sharing information with numerous other third parties.[75] This argument implicates the limitation on privacy expectations set forth in *Miller*.[76] Even a profile set to private can be readily accessed by hundreds of individuals: the user's "friends."[77] Thus, a user should have no legal recourse if one of these "friends" shares his information in a way that is later used by an attorney during trial.

When a single entity collects and controls so much personal data, it raises a host of privacy concerns because of the potential that such data could be misused. However, most of the personal data on an SNS exists because of the initiative of users (control) and is based upon their

71. 18 U.S.C. § 2702(b)(3) (2006).

72. *See supra* discussion accompanying note 23 on tagging.

73. *See, e.g., Help Center, Privacy: Update to Privacy Settings*, FACEBOOK, http://www.facebook.com/help/?ref=pf#!/help.php?page=927 (last visited Feb. 15, 2010).

74. *See, e.g., Help, Control Privacy on MySpace Profile*, MYSPACE, http://faq.myspace.com/app/answers/detail/a_id/288/session/L3NpZC9ZS1Q1cWdZag%3D%3D (last visited Mar. 31, 2010).

75. Hodge, *supra* note 45, at 111.

76. *Miller*, 425 U.S. at 443. This idea is referred to as the "third-party doctrine." Namely, by disclosing information to a third party, an individual gives up all his privacy rights in the information revealed.

77. The average number of "friends" for a Facebook user is 130, however, some users have more than 1,000, all of which have access to the user's profile information, *see Press Room Statistics*, *supra* note 11.

consent. The idea of privacy as a form of *consent* and *control* is echoed by many privacy scholars.[78] SNSs provide a valuable, flexible and completely voluntary social tool. Users log onto SNSs because they want to share their information and access information others want to share.[79] Thus, in exchange for using this tool, SNS users should accept the inherent risks that may be involved.

The burden of protecting all the information a user posts cannot be placed on SNS providers or the government alone. One reason for this is that most SNS users do not define their privacy expectations based on constitutional or statutory legal principles, but in terms of social and societal roles. In the words of Professor James Grimmelmann of New York Law School, "users think socially, not logically."[80] Thus, the biggest privacy breaches relating to SNSs are those that involve peer-produced privacy violations, e.g. when a user's "friend" discloses private information to an unauthorized third party or posts an unflattering photograph or a photograph that depicts the user engaging in unsavory behavior.[81]

Neither SNS providers nor the government have any way to protect users against these kinds of violations. Indeed, in response to the Spring 2010 backlash, Facebook CEO Mark Zuckerberg stated that Facebook's obligation was merely to reflect "current social norms" that favored "exposure over privacy."[82] SNS users may assume that social norms against snooping and sharing will place limits on how far the information they post will spread, but they should not reasonably expect that every "friend" will respect or even be able to recognize another's privacy interests. Additionally, it is not easy to uniquely associate each piece of information with one person. For example, a photograph may be taken by one individual, but depict a set of other individuals. Here, based on social norms alone, it becomes hard to understand who should control the distribution of the photograph. Whoever has control over the information can use it in ways that others with a legitimate interest in it do not like.

Facebook has done its best to warn users of these privacy risks through its detailed and thorough privacy policy.[83] Despite this, most

78. *See, e.g.*, DANIEL SOLOVE & PAUL SCHWARTZ, PRIVACY, INFORMATION, AND TECHNOLOGY (2009).

79. *See Principles*, FACEBOOK, http://www.facebook.com/policy.php (last visited Feb. 15, 2010).

80. James Grimmelmann, *Saving Facebook,* 94 IOWA L. REV. 1137, 1206 (2009).

81. For example, someone blackmailed Miss New Jersey 2007 by sending racy pictures from a private Facebook album to pageant officials. Austin Fenner, *N.J. Miss in a Fix over Her Pics*, N.Y. POST, July 6, 2007, at 5.

82. *See* Jeffrey Rosen, *The Web Means the End of Forgetting,* N.Y. TIMES, July 21, 2010, at MM30.

83. Facebook's privacy policy, revised April 22, 2010, is 5,830 words long and disclaims

users still expect some amount of privacy on Facebook because they assume their "friends" will respect privacy bounds similar to those offline. A college student does not expect his fraternity brothers to hand over photos from last weekend's kegger to school administrators or the dean.[84] However, such risks are present in cyberspace just as much as in the real world, and the burden can only be placed on the individual to carefully asses what information he puts on his SNS profile and monitor what others do with this information.

Accordingly, the most supportive argument behind the defense attorney's use of undercover investigative techniques on SNSs is the idea that disclosure on these sites is done at the user's own risk. This notion stems from the ideas behind the third party doctrine first set forth in *Miller*. It also stems in part from the Sixth Circuit's conclusion in *Guest v. Leis*[85] that "[u]sers would logically lack a legitimate expectation of privacy in the materials intended for publication or public posting."[86] Thus, the method of undercover investigating proposed in this note has nothing to do with circumventing SNS technologies or breaking website code. Rather, the investigative techniques outlined here mirror those that take advantage of what users choose to post on their SNS profiles and the social relationships that control how this information is shared. Many of these techniques are supported by the third-party doctrine and are routinely used and approved of outside of cyberspace in the real world.[87]

III. CRIMINAL DISCOVERY AND LEGAL ETHICS

This section provides an overview of the rules and standards of both criminal discovery and legal ethics. It will show that the policy goals behind both these areas indicate that information on a social networking

---

responsibility for various privacy breaches quite explicitly:

> Although we allow you to set privacy options that limit access to your information, please be aware that no security measures are perfect or impenetrable. We cannot control the actions of other users with whom you share your information. We cannot guarantee that only authorized persons will view your information. We cannot ensure that information you share on Facebook will not become publicly available. We are not responsible for third party circumvention of any privacy settings or security measures on Facebook.

Privacy Policy, FACEBOOK, http://www.facebook.com/policy.php (last visited Mar. 31, 2010).

84. *See* Jodi S. Cohen, *Cop Snares College Pals in Own Web*, CHI. TRIB., Aug. 3, 2006, at C1 (A University of Illinois at Urbana-Champaign student was caught publicly urinating by a police officer. The student ran away but the officer was able to question another student at the scene. The officer later logged on to Facebook and recognized the fleeing student on the other student's profile. He ticketed both of them.).

85. 255 F.3d 325 (6th Cir. 2001).

86. *Id.* at 333.

87. *See infra* Part III.C for specific examples.

site should be available to the government and the defendant alike.

A. The Rules of Criminal Procedure

There has always been inequality in the access of information given to prosecutors and defense attorneys under the Federal Rules of Criminal Procedure. For example, under Rule 16, prosecutors are not required to give their opposing counsel police reports or the names of witnesses.[88] Also, when conducting their investigations, prosecutors can subpoena documents and records relevant to the case, can acquire tangible and verbal evidence from court-ordered searches and electronic eavesdropping, and can obtain forensic proof from well-staffed and experienced crime laboratories.[89] In contrast, the defendant's ability to acquire almost all of this information is severely limited.[90]

There are many reasons for this distinction, and the reasons are still highly debated. Critics of broad criminal discovery argue that such practices would facilitate perjured defense testimony and the intimidation of witnesses, and would favor the accused because the privilege against self-incrimination protects defendants from reciprocal disclosures.[91] Further, critics of broad criminal discovery point to the fact that the prosecutor carries a high burden of proof: "beyond a reasonable doubt." On the other side, advocates of broader criminal discovery argue that a trial should be a search for truth and the truth is more likely to emerge when each side is equipped with all relevant information about the case (similar arguments have largely been accepted as applied to civil discovery).[92] However, proponents argue that expanded discovery is necessary in order to offset the substantial advantages possessed by the prosecution in its investigation of crime. Advocates of broader criminal discovery also argue that there may be a fundamental conflict of interest between a prosecutor's personal motivation to advance his or her career based on successful convictions and a prosecutor's role as a quasi-judicial official seeking justice in the name of the state.[93] Allowing criminal defendants to access more information for trial could ease the tension between these dual roles.

Starting in the 1970s, prosecutors began to wield increasingly more power as crime became more complex and sophisticated (narcotics trafficking, racketeering, business fraud) and as policies emphasized the

88. FED. R. CRIM. P. 16.

89. Bennett L. Gershman, *The New Prosecutors,* 53 U. PITT. L. REV. 393, 449 (1992).

90. *Id.*

91. *See* State v. Tune, 98 A.2d 881 (N.J. 1953).

92. United States v. Proctor & Gamble Co., 356 U.S. 677, 682 (1958).

93. Stanley Z. Fisher, *In Search of the Virtuous Prosecutor: A Conceptual Framework,* 15 AM. J. CRIM. L. 197, 198-202 (1988).

"war on crime" over an individual's due process rights during investigations.[94] The prosecutor has always had a significant role in the early stages of a case, but today he or she may develop and coordinate the key strategies in a criminal investigation.[95] Also, prosecutors are afforded full discretion in bringing charges and are largely immune from judicial review under the presumption that they will act in good faith.[96] Likewise, prosecutors can obtain the cooperation of key witnesses through grants of immunity,[97] and the federal sentencing guidelines give them greater leverage to either compel plea bargaining or force cooperation.[98]

Prosecutors can apply for authorization to obtain eavesdropping and surveillance warrants and subpoena records.[99] Also, in 1994, the Department of Justice and Federal Bureau of Investigation successfully lobbied Congress to enact the Communications Assistance for Law Enforcement Act,[100] obligating Internet service providers to configure their networks to be able to quickly assist law enforcement monitoring. Additionally, a host of other legislation provides the prosecutor with new definitions of crimes and new ways to investigate them, including the Racketeer Influenced and Corrupt Organizations Act,[101] Continuing Criminal Enterprises Act[102], Criminal Forfeitures Act,[103] Money Laundering Act,[104] Comprehensive Thrift and Bank Fraud Act,[105] and of course, the ECPA. Also, the Supreme Court has narrowed the scope of the exclusionary rule, allowing more evidence to be presented at trial.[106] The ECPA does not even have an exclusionary remedy for when its provisions have been violated. Finally, prosecutors have been allowed to use deceptive, undercover techniques to acquire evidence of crime, despite ethical rules barring lawyers from engaging in "dishonesty, fraud,

94. Charles H. Whitebread, *The Burger Court's Counter-Revolution in Criminal Procedure: The Recent Criminal Decisions of the United States Supreme Court,* 24 WASHBURN L.J. 471, 471 (1985).

95. Gershman, *supra* note 89, at 395.

96. *See* Imbler v. Pachtner, 424 U.S. 409, 430 (1976); *see also* Burns v. Reed, 500 U.S. 478, 487 (1991) (both holding that a prosecutor is absolutely immune from civil liability for charging excesses).

97. Gershman, *supra* note 89, at 395.

98. *Id.* at 418-19.

99. *Id.* at 395.

100. Communications Assistance for Law Enforcement Act of 1994, Pub. L. No. 103-414, 108 Stat. 4279 (codified as amended at 47 U.S.C. §§1001-1010 (2006)).

101. 18 U.S.C. §§ 1961-68 (2009).

102. 21 U.S.C. § 848 (2008).

103. 21 U.S.C. § 853 (2009).

104. 18 U.S.C. § 1956.

105. 18 U.S.C § 1001.

106. *See* United States v. Leon, 468 U.S. 897 (1984) (Court created the "good faith" exception to the exclusionary rule); *see also* New York v. Quarles, 467 U.S. 649 (1984) (Court created "public safety" exception to the requirement that Miranda warnings be given before questioning; defendant's incriminating statements were admissible).

deceit, or misrepresentation."[107] Through this combination of broad investigative powers, narrowing of the exclusionary rule, and ability to set up elaborate undercover operations, many commentators have noted that the inherent inequality between the prosecutor and defendant has made the adversary system severely lopsided.[108]

An attorney's use of an SNS involves the control of and access to information, whether it is used as evidence itself, or whether it merely provides a lead to obtain other evidence. In contrast to a prosecutor's broad array of tools and strategies to obtain information from an SNS provided under the ECPA, the defense attorney has no statutory right to access to most of the prosecutors "data-gathering machinery."[109]

Under the Federal Rules of Criminal Procedure, the defense is entitled to any statements made by the defendant, the defendant's prior record, reports of examinations and tests, and statements made by expert witnesses.[110] Further, a prosecutor must turn over any materials that consist of exculpatory or impeaching information material to the guilt or innocence or to the punishment of a defendant.[111]

A defendant may obtain documents and other physical records through a *subpoena duces tecum.* In federal court, these are governed by Rule 17 of the Rules of Criminal Procedure.[112] Certain materials unrelated to the prosecution's criminal investigation or not otherwise subject to the discovery limitations imposed by Rule 16(a)(2) may be subpoenaed without a motion or corresponding court order.[113] Ex parte procedure is usually permissible.[114] If a court order is required, the movant must show that (a) the material sought is evidentiary and relevant; (b) the material is not otherwise procurable reasonably in advance of trial by exercise of due diligence; (c) that the party cannot properly prepare for trial without such production and inspection in advance of trial and that the failure to obtain such inspection might tend unreasonably to delay trial; (d) that the application is made in good faith and is not intended as a general "fishing expedition."

---

107. MODEL R. OF PROF'L CONDUCT R. 8.4(c) (2010); *see also* United States v. Russell, 411 U.S. 423, 432 (1973).

108. Gershman, *supra* note 89; *see also* State v. Rummer, 432 S.E. 2d 39, 70 (W. Va. 1993) (Neely, J., dissenting) ("Today, prosecutors have more power and less judicial supervision than ever before. Today's prosecutors are like the sheriffs of the old wild west: they are the law.")

109. Gershman, *supra* note 89, at 449.

110. FED. R. CRIM. P. 16(b).

111. Brady v. Maryland, 373 U.S. 83 (1963) (where the Supreme Court held that that suppression by the prosecution of evidence favorable to a defendant who has requested it violates due process).

112. FED. R. CRIM. P. 17.

113. INGA L. PARSONS, FOURTH AMENDMENT PRACTICE AND PROCEDURE 261 (2004).

114. *See, e.g.* United States v. Reyes, 162 F.R.D 468, 471 (S.D.N.Y. 1995).

A defense attorney may thus try to obtain information from an SNS by serving the site provider with a subpoena. However, the SNS provider may resist turning over the information by bringing a motion to quash, supported by arguments that constitutional or federal law prohibits divulging the requested information. Such was the case in September 2009 when Facebook pages were subpoenaed by the State of Virginia's Workers Compensation Commission in regard to a worker's compensation dispute.[115] The subpoena requested, "all documents, electronic or otherwise, related directly or indirectly, to all activities, writings, photos, comments, e-mails, and/or postings" on the Facebook account. Facebook resisted the subpoena, saying that the request must come from a California court, and that it was "overly broad" because the ECPA protected the privacy of user accounts.[116] The Commission backed off and stopped levying its $200-a-day fine before the issue was fully litigated before a court.[117]

A defense attorney armed with a subpoena may easily run into similar problems when seeking information from an SNS, particularly under Facebook's broad definition of which user data falls under "content" under the ECPA. Also, a defense attorney would not have the additional processes afforded to prosecutors under the SCA, namely the § 2703(d) court order or the § 2703(a) warrant. Finally, although prosecutors are required to turn over exculpatory evidence under *Brady,*[118] a prosecutor has neither the motive nor the time to do a defense attorney's work by coming up with various theories of defense and providing SNS information that may form the bases for these theories.

A defendant seeking to compel an SNS to turn over content information could potentially rely on cooperation from the prosecutor. Many prosecutors divulge information beyond what is required under the Rules because it will assist the defense attorney in counseling his or her client on whether to accept a plea offer or take the case to trial.[119] In this vein, a defendant may ask a prosecutor to obtain a § 2703(a) warrant or a regular warrant on his or her behalf. The prosecutor may give in to the request. However, in order to access most of the content on an SNS profile under § 2703(a), the warrant would need to establish probable cause that a user's SNS profile page has evidence *of the crime.* As discussed before, the variety of information that an SNS profile can harbor means that it can contain evidence beyond mere evidence of a

115. Declan McCullagh, *Facebook fights Virginia's demand for user data, photos*, CNET NEWS (Sept. 14, 2009, 4:34 PM PDT), http://news.cnet.com/8301-13578_3-10352587-38.html.

116. *Id.*

117. *Id.*

118. Brady v. Maryland, 373 U.S. 83, 85-87 (1963).

119. PARSONS, *supra* note 113, at 256.

crime. A comment posted on a Facebook wall or a photograph buried in a "Spring Break 2008" photo album could be the key in a defendant's case.[120]

Most importantly, even where prosecutors are required to disclose evidence, many may be entrenched in their own biased analysis of the facts and risk assessment. Evidence that may be deemed exculpatory by a defense lawyer may not be disclosed because the prosecutor has already concluded which evidence is "material" based upon her own theory of the case. Further, many prosecutors' offices carry a heavy caseload. In the context of SNS investigations, it is unreasonable to require a prosecutor to research not only his side of the case, but to use the SCA to uncover any bit of relevant information that might help a defense attorney explore a myriad of theories of defense. Consequently, a defense attorney cannot rely on the prosecutor to turn over important or relevant content information gleaned from SNSs and must be allowed to access such information through his own investigations.

B. Legal Ethics

In the realm of legal ethics, all states have adopted rules of professional conduct for lawyers similar to the standards promulgated by the American Bar Association in its Model Rules of Professional Conduct.[121] Lawyers who violate these rules are subject to sanctions before the disciplinary committee within their jurisdictions.[122] Further, most jurisdictions have adopted a version of the Model Rules 3.8 titled "Special Responsibilities of a Prosecutor."[123] However, the vast majority of reported decisions of lawyer discipline are cases involving solo practitioners or practitioners in small firms.[124] Many scholars and commentators have noted that there is an astonishing absence from appellate court decisions or reports by disciplinary committees of any cases dealing with misconduct by prosecutors.[125] This is particularly notable after the work of organizations such as the Innocence Project, which have conducted groundbreaking work in the use of post-

120. *See, e.g.*, Damiano Beltrami, *His Facebook Status Now? 'Charges Dropped'*, N.Y. TIMES (Nov. 11, 2009, 11:10 AM), http://fort-greene.blogs.nytimes.com/2009/11/11/his-facebook-status-now-charges-dropped.

121. Ellen Yaroshefsky, *Wrongful Convictions: It Is Time to Take Prosecution Discipline Seriously,* 8 UDC/DCSL L. REV. 275, 276 (2004).

122. *Id.*

123. *See* MODEL R. OF PROF'L CONDUCT R. 3.8 (2006) (This rule outlines the duty to charge only on the basis of probable cause and the obligation to disclose exculpatory evidence.).

124. *Id.*

125. *See, e.g.*, Gershman, *supra* note 89, at 449; Yaroshefsky, *supra* note 121, at 277; Fred C. Zacharias, *The Professional Discipline of Prosecutors,* 79 N.C. L. REV. 721, 745 n.84 (2001); United States v. Acosta, 111 F. Supp. 2d 1082, 1093-1094 (E.D. Wis. 2000).

conviction DNA testing to exonerate the wrongfully convicted and tied prosecutorial misconduct to many of these wrongful convictions.[126]

With no access to warrants or court orders, a defense attorney may think he can access private SNS profile information by becoming a "friend" of the profile owner. He may also want to ask a third person whose name the individual may not recognize to go to the SNS website, contact the profile owner and seek to "friend" her to obtain access to the private information. In March 2009, the Philadelphia Bar Association Professional Guidance Committee addressed these situations.[127] It was one of the first ethics committee opinions regarding SNSs. The committee took a conservative approach, stating that the aforementioned investigative techniques would violate Model Rule 8.4(c), which prohibits a lawyer from engaging in conduct that involves "dishonesty, fraud, deceit or misrepresentation."[128] The techniques were also found to violate Model Rule 4.1, which prohibits the making of false statements of material fact or law to a third person in the course of representing a client. The Committee reasoned the techniques were "deceptive" and "omit[ted] a highly material fact, namely, that the third party who asks to be allowed access to the witness's [profile] pages is doing so only because he or she is intent on obtaining information and sharing it with a lawyer . . . ."[129]

Many other courts and authors who have commented on misrepresentations by lawyers or their investigators have assumed, like the Philadelphia Bar, that the Model Rules flatly prohibit any sort of undercover activity or misleading behavior on the part of lawyers and their agents.[130] However, such a literal reading would condemn as unethical many practices universally upheld by court decisions, such as undercover investigations by police or "discrimination testers" who apply for jobs and housing.[131] These widely accepted practices use misrepresentations solely for purposes of discovering information and gathering facts.

Several policies have been set forth justifying a prosecutor's use of undercover investigations and informants, and a lawyer or his agent's use

126. Yaroshefsky, *supra* note 121, at 278.

127. The Philadelphia Bar Ass'n Prof'l Guidance Comm., Opinion 2009-02 (2009).

128. MODEL RULES OF PROF'L CONDUCT R. 8.4(c) (2010).

129. The Philadelphia Bar Ass'n, *supra* note 127, at 3.

130. *See, e.g.*, In re Paulter, 47 P.3d 1175 (Colo. 2002) (holding that no deception whatever is allowed and recognizing that many may find their position "too rigid"); *see also* In re Conduct of Gatti, 8 P.3d 966 (Or. 2000).

131. David B. Isbell & Lucantonio N. Salvi, *Ethical Responsibility of Lawyers for Deception by Undercover Investigators and Discrimination Testers: An Analysis of the Provisions Prohibiting Misrepresentation Under the Model Rules of Professional Conduct*, 8 GEO. J. LEGAL ETHICS 791, 802 (1995). Isbell is a former chair of the American Bar Association Standing Committee on Ethics and Professional Responsibility.

of discrimination testers. First, enforcement of the law is a desirable goal, and undercover investigations may provide an effective enforcement mechanism for detecting and proving illegal activity.[132] Second, undercover investigations may provide information or prove violations that may otherwise escape discovery or proof and cannot be uncovered by other means.[133] Third, undercover investigators and discrimination testers have traditionally been widely employed by both public and private attorneys.[134] Finally, the Model Rules work in part to preserve public confidence in the legal system.[135] Under all these considerations, a result-sensitive reading of the ethical obligations against misrepresentation imposed on lawyers is appropriate, interpreted by whether the lawyer is to use a misrepresentation solely to discover information and gather facts in order to uphold the law. A defense attorney trying to uncover SNS profile information within the confines of the website ("friending" a potential witness or having a third person do so) conducts a similar misrepresentation only as to identity or purpose, and it is solely conducted for evidence-gathering purposes.

The Supreme Court of Wisconsin recently recognized that, like a prosecutor, a defense attorney may be able to use his own arsenal of deceptive investigative practices. In *Office of Lawyer Regulation v. Hurley*,[136] a private defense attorney hired an investigator to find out information on a minor who was accusing his client of sexual misconduct. Through these investigations, the defense attorney was able to obtain the minor's laptop, which contained numerous pornographic images involving adults, children, and animals.[137] The prosecutor in the case filed a grievance with the state's Office of Lawyer Regulation ("OLR"), who filed a complaint against the defense attorney.[138]

The presiding judge in the matter noted that the defense attorney's type of conduct was utilized by state district attorneys who "frequently supervise a variety of undercover activities and sting operations carried out by non-lawyers who use deception to collect evidence . . . ."[139] The prosecutor and the OLR director tried to argue that this type of conduct was not acceptable for private attorneys but were unable to point to any rule, statute, ethics opinion, or Wisconsin case that drew this distinction between prosecutors and other attorneys.[140] Indeed, the ABA Model

132. *Id.* at 801.
133. *Id.* at 802.
134. *Id.* at 803.
135. *Id.* at 804.
136. No. 07AP478-D, 2008 Wisc. LEXIS 1181, at *7 (Feb. 5, 2008).
137. *Id.* at *11.
138. *Id.* at *12.
139. *Id.* at *28 (internal quotation marks omitted).
140. *Id.* at *32-33.

Rules contain no reference to a public lawyer/private lawyer dichotomy.[141] The presiding judge held that the defense attorney's duty to "zealously defend his client[and] fulfill his constitutional obligation to provide effective assistance of counsel" was stronger than the "risk of breaking a vague ethical rule that, according to the record, had never been enforced in this way."[142] The presiding judge noted that "[t]he Sixth Amendment seems to have broken the tie for Mr. Hurley."[143] The Wisconsin Supreme Court upheld the presiding judge's conclusions.[144]

If a defense attorney feels the need to access SNS information solely for the purpose of gathering facts on a case, she should not be confined to the literal reading of the Model Rules promulgated by the Philadelphia Bar. The Sixth Amendment[145] should "break the tie" and defense attorneys should be allowed to use third parties to try to gain access to SNS information. This still does not render the SNS profile owner powerless. He can still be diligent in monitoring whose "friend requests" to accept and edit his profile, comments, and photos to remove information he would rather not have online.

C. A Proposed Framework for How a Defense Attorney Can Conduct Research on a Social Networking Site

A defense attorney looking to conduct investigations on social networking websites should be aware that in addition to the ethical rules, he must comply with the website's terms of use and applicable state and federal laws.[146] When ethical or legal restrictions are unclear, the attorney must weigh the value of the information to be obtained against the potential risks or consequences of getting it. One problem facing attorneys in this balancing act is the aforementioned wealth and scope of information that can be found on an SNS. It can be hard to determine beforehand just how relevant the information might be to a lawyer's case. A dangerous attitude is that SNSs are a "treasure trove" or "Pandora's box"[147] for the discovery process. This mindset may make an attorney think that a questionable search will later prove to be justified.

---

141. Isbell & Salvi, *supra* note 131, at 807.

142. *Hurley*, 2008 Wisc. LEXIS 1181, at *37.

143. *Id.*

144. *Id.*

145. "In all criminal prosecutions, the accused shall enjoy the right . . . to have the Assistance of Counsel for his defence." U.S. CONST. amend. VI.

146. *See, e.g.*, The Stored Communications Act, 18 U.S.C. §§ 2701-2711 (2006); *MySpace Terms of Use Agreement*, MYSPACE, http://www.myspace.com/index.cfm?fuseaction=misc.terms (last visited June 25, 2009).

147. *See, e.g.*, Jaksic, *supra* note 4; Kathryn S. Vander Broek et al., *Blog Now, Pay Later – Legal Issues Concerning Social Networking Sites*, HINSHAW & CULBERTSON, LLP (Nov. 18, 2008), http://www.hinshawlaw.com/11-18-2008.

Obviously, an investigating attorney can always access publicly-available information on the Internet, viewable by anyone online without needing to join a site or log in. Many profiles on MySpace are publicly accessible and could be found through a standard search engine like Google. An attorney can also create an account on an SNS with accurate information and conduct any research with the use of that account. She can join groups, see the names of the members of those groups, and access the profiles of people that are enabled by joining the group. She may also ask individuals to be her "friend" as long as the person is not a witness disclosed by the opposing party or represented by counsel.[148] If the person is a victim or witness disclosed by the opposing party, the attorney may still ask to be a "friend" as long as she clearly identifies herself and who she represents.[149]

If the client or another third party member of an SNS provides the attorney with information obtained from an SNS, the attorney can use that information. This could disclose printouts of complete profile pages, messages, or photos. Along the same lines, an attorney may ask her client or a witness to let her observe the client/witness browsing the SNS. The attorney can direct the browsing and ask the client/witness to save or print information. If the client/witness gives explicit permission, the attorney can also use the account on her own for "passive browsing." This means the attorney can search for and look at any profiles available through the client/witness account, but cannot message, friend request, or in any way communicate with the borrowed account. This approach may be particularly useful if the client is in custody and unable to access the Internet, but this could be argued as a "gray area" since the attorney is representing herself to be someone else as far as the SNS is concerned.[150]

An attorney should avoid making any misrepresentation on her own if it could be classified as being "in the course of representing a client."[151] This language comes from Model Rule 4.1(e), but is not necessarily implicated by the mere presence of a lawyer-client relationship. To come under this rule, the lawyer must be functioning "*as a lawyer*."[152] The boundaries of this distinction are less than clear, but may allow an attorney to make minor misrepresentations if the conduct meets the dual prongs of falling out the "course of representation" and if done solely for the investigative purpose of evidence gathering. To be safe, an attorney

148. *See* MODEL R. OF PROF'L CONDUCT R. 4.3 (2010).

149. *See id.*

150. Facebook's terms of use state, "You will not provide any false information on Facebook . . . You will not share your password, let anyone else access your account." *Statement of Rights and Responsibilities*, FACEBOOK, http://www.facebook.com/terms.php?ref=pf (last visited Oct. 4, 2010).

151. MODEL R. OF PROF'L CONDUCT R. 4.1(e) (2010).

152. Isbell & Salvi, *supra* note 131, at 814.

can engage the help of a non-lawyer investigator, who would not be acting as an attorney and thus fall outside the limits of Rule 4.1(e).[153] However, if the investigator creates a fake profile to gain access to other user's information, he may violate the SNS website's terms of use, though steering clear of any legal ethics violations.[154]

CONCLUSION

SNSs have become an integral part of many of their users' lives and have proved to be an important source of information for the lawyer looking for evidence while preparing for a case. As a new generation of lawyers and police officers, comfortable with the use and role of SNSs, enters the workforce, the legal use of SNS information will become even more prevalent. Police officers and prosecutors will use the tools available under the ECPA and other statutes with more frequency, and even the best-intentioned prosecutor looking to fulfill her duty to disclose exculpatory evidence may miss or simply not recognize a highly relevant piece of information contained in the electronic records obtained. Further, the information that can be found on an SNS may provide evidence not only of a defendant's innocence, but evidence used to impeach key witnesses or even identify an alternative suspect and build an alternative theory of a case.

For these reasons, defense attorneys need to be provided with a way to gather information on SNSs that provides some balance to the inequality of access given to prosecutors through their considerable array of tools and resources. Although one solution would be to amend the SCA or the Rules of Criminal Procedure to allow defendants to compel disclosure through legal processes, a far easier solution that would require no legislative overhaul is to allow an attorney or her agents to conduct undercover investigations online.

As time goes by, the inequality of access to important online information and evidence could pose a serious threat to the pursuit of justice in our legal system. The disparate standards in criminal procedure, the use and application of the ECPA, and the disagreement between various ethics committees and scholars make the landscape a tricky one for defendants building their cases. These elements should be brought into conformance with each other, with emphasis placed on maintaining a fair balance between the information available to the prosecutor and the

153. *Id.* at 815.

154. For example, in *U.S. v. Drew*, the government unsuccessfully tried to bring criminal charges against a woman who created an entirely fictitious MySpace profile under the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, for violating MySpace's terms of use. 259 F.R.D. 449 (C.D. Cal. 2009).

defendant. The right balance during the criminal discovery process will best guide the search for truth and the pursuit of justice.