Marquette Law Review

Volume 93
Issue 4 *Summer 2010*

Article 43

The Fourth Amendment and the Brave New World of Online Social Networking

Nathan Petrashek

THE FOURTH AMENDMENT AND THE BRAVE NEW WORLD OF ONLINE SOCIAL NETWORKING

I. INTRODUCTION

> New technologies create interesting challenges to long established legal concepts. Thus, just as when the telephone gained nationwide use and acceptance . . . and when cellular telephones came into widespread use, now personal computers, hooked up to large networks, are so widely used that the scope of Fourth Amendment core concepts of "privacy" as applied to them must be reexamined.[1]

During a recent visit to the University of Florida Levin College of Law, Associate Justice Clarence Thomas was asked whether he believed the Court has kept pace with rapidly shifting technological changes. According to Justice Thomas, technological change within the Court was less important than that occurring on the outside:

> [It's] changed the way we work, but it's also changed some of the issues. . . . I think you all are in for some interesting times because there used to be these zones of privacy. . . . Things were over here in the private sphere and then the public sphere was over here. Now look how [they've] merged. You put something on your Facebook, [and] it's there on somebody's hard drive forever. . . . We also see it with respect to how the government can obtain information in the criminal justice context. [The government doesn't] actually have to come onto property now, to look into your private affairs. . . . I think you all are in for the brave new world of technology in a way that we, of course, couldn't have anticipated.[2]

No phenomenon is more demonstrative of the brave new technological world than online social networking. Each day, millions of Americans log on to social networking web sites, whose astonishingly rapid user growth has turned many into multi-billion-dollar marketing machines. But wholly aside from their business impact, these web services perform important social functions by allowing users to meet or remain in touch with others, share

---

1. United States v. Maxwell, 45 M.J. 406, 410 (C.A.A.F. 1996).

2. Clarence Thomas, Associate Justice, U.S. Supreme Court, Address at the University of Florida Levin College of Law Marshall Criser Distinguished Lecture Series (Feb. 4, 2010).

ideas, start organizations, and generally contribute to a vibrant and open society.

Left unstated by Justice Thomas is his notion of how the thorny legal issues surrounding this new communicative forum should be resolved. Existing Fourth Amendment doctrine is ill-equipped to handle the convergence of the public and the private; generally, one loses all privacy expectations in what is shared with the world.[3] Though this tension between constitutional doctrine and social practice has yet to play out in the courts, it may soon do so.

With so many individuals sharing so much information, it is no surprise that social networking services have attracted the attention of both criminals and police. Social networking sites are frequent targets of sexual predators, identity thieves, and con artists.[4] As a result, police scrutiny of these web sites has increased, and law enforcement officials are more often using social networking services as criminal investigation tools.[5] This fact creates a problem of constitutional dimension: how much protection do social networking users have in their online content?

This Comment evaluates whether social networking users maintain a reasonable expectation of privacy in their online social networking activity such that police scrutiny is subject to the Fourth Amendment's warrant requirement. Part II explores the contours of a social networking web site and describes its operation. This Part considers the origins of the social networking phenomenon and examines two of the largest social networking web sites, Facebook and MySpace, in some detail. Part III explains the social benefits derived from social networking and the risks involved, including the increasing risk of police surveillance. Part IV describes the current state of Fourth Amendment search doctrine and explains why it is a poor lens through which to analyze a user's online social networking content. Part V discusses the consequences should courts refuse to protect online user content. Finally, Part VI concludes that courts should recognize, in most circumstances, users' asserted privacy expectations in their online social networking content.

II. FUNDAMENTALS OF ONLINE SOCIAL NETWORKING

Understanding whether and how the Fourth Amendment regulates police scrutiny of virtual social networking content requires some attention to the

3. *See, e.g.*, Katz v. United States, 389 U.S. 347, 351 (1967) ("What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection.").

4. Terrence Berg, *The Changing Face of Cybercrime: New Interest Threats Create Challenges to Law Enforcement*, MICH. B.J., June 2007, at 18, 18–19 (2007).

5. *Id.* at 18.

fundamental characteristics of that medium. Fourth Amendment protection often depends upon the type of information obtained, the method of its collection, and the location from which it is seized.[6] It is therefore necessary to sketch out the core attributes of an online social network—what it is, who uses it, and how it functions. These defining characteristics are all relevant when determining whether police activity constitutes a "search."

Such a comprehensive review is no easy task. Social networking web sites are novel communication tools whose dynamics are not yet well understood (or firmly established). Indeed, because their business models require them to capture and hold the attention of a fast-paced society, social networking web sites are among the most prone to anticipate "the way the world is moving."[7] Users of these rapidly changing instruments have little choice but to go along for the ride.[8] In addition, the fluid nature of the Internet guarantees that, on any given day, any number of social networking web sites might pop into creation or wink out of existence. A truly comprehensive review of the social networking phenomenon is therefore impossible.

This Part's goals are more modest. The first is to define the communication tools to which this Comment's analysis applies. Second, a brief discussion of online social networking's origins demonstrates the novelty of the medium and its potential for future growth. Finally, this Part will provide a practical look at two well-established social networking sites, MySpace and Facebook.

A. Defining an Online Social Network

No discernable consensus exists with respect to the definition of online

6. *See* Orin S. Kerr, *Four Models of Fourth Amendment Protection*, 60 STAN. L. REV. 503, 508–09, 512–13 (2007).

7. Alexei Oreskovic, Facebook Privacy Revamp Draws Fire, Reuters (Dec. 10, 2009), http://www.reuters.com/article/idUSTRE5B82F320091210 (quoting Facebook spokesman Barry Schnitt).

8. One popular social networking web site, for example, recently adopted broad changes to its privacy policy. The effect was to turn what was previously considered a private social network into a much more public forum. Jason Kincaid, The Facebook Privacy Fiasco Begins, TechCrunch (Dec. 9, 2009), http://www.techcrunch.com/2009/12/09/facebook-privacy. *But see* Riva Richmond, A Guide to Facebook's New Privacy Settings, Gadgetwise, http://gadgetwise.blogs.nytimes.com/2010/05/27/5-steps-to-reset-your-facebook-privacy-settings/?scp=2&sq=facebook%20privacy&st=cse (May 27, 2010, 16:41 EST) (describing subsequent changes to Facebook's privacy policy scaling back the types of user data considered public). Users are generally powerless to prevent these changes unless they object in truly significant numbers. *See* Brad Stone & Brian Stelter, *Facebook Backtracks on Use Terms*, N.Y. TIMES, Feb. 19, 2009, at B1 (describing Facebook's retraction of a modified user contract following objections from tens of thousands of members accompanied by bloggers and advocacy groups).

social networking.[9] At least one court has ventured into the morass and offered a starting point:

> [A] "social networking web site" . . . allows its members to create online "profiles," which are individual web pages on which members post photographs, videos, and information about their lives and interests. The idea of online social networking is that members will use their online profiles to become part of an online community of people with common interests.[10]

While the court's definition is a useful one to build upon, by itself it is insufficient. While some social networking communities previously consisted only of members with some common affiliation—attendance at a particular university or college, for example—this is increasingly uncommon. Many virtual communities include individuals with whom a user has no shared life experience or interests. Facebook's recent abandonment of a classification system grouping members according to their educational institution or geographic location reflects this reality.[11] The court's definition also provides an incomplete description of the activities of social networking users and ignores the nuanced process by which users create their virtual communities. For all its faults, the court's definition does accurately identify the principal function of online social networking: to allow members to connect to a broad virtual community via a personal profile.[12] Most social networking web sites are built, to varying degrees, around two basic elements: the "profile" and the "community."[13]

---

9. Cydney Tune & Marley Degner, *Blogging and Social Networking: Current Legal Issues*, *in* INFORMATION TECHNOLOGY LAW INSTITUTE 2008: NEW DIRECTIONS: SOCIAL NETWORKS, BLOGS, PRIVACY, MASH-UPS, VIRTUAL WORLDS & OPEN SOURCE 7–8 (2008) ("[S]ocial networking sites lack a clear definition, and courts that have tackled the task of defining them have either relied on dictionary definitions or have used general or vague definitions.").

10. Doe v. MySpace, Inc., 474 F. Supp. 2d 843, 845–46 (W.D. Tex. 2007). On appeal, the Fifth Circuit Court of Appeals provided a shorter definition, stating that "[o]nline social networking is the practice of using a Web site or other interactive computer service to expand one's business or social network." Doe v. MySpace, Inc., 528 F.3d 413, 415 (5th Cir. 2008), *aff'g* Doe v. MySpace, Inc., 474 F. Supp. 2d 843 (W.D. Tex. 2007), *cert. denied*, 129 S. Ct. 600 (2008).

11. Matthew J. Hodge, Comment, *The Fourth Amendment and Privacy Issues on the "New" Internet: Facebook.com and MySpace.com*, 31 S. ILL. U. L.J. 95, 97–98 (2006). Definitions proposed by commentators can also fall into this trap. *See, e.g.*, John S. Wilson, Comment, *MySpace, Your Space, or Our Space? New Frontiers in Electronic Evidence*, 86 OR. L. REV. 1201, 1204 (2007) (defining "social-networking sites" as "interactive web sites that connect users based on common interests and that allow subscribers to personalize individual web sites").

12. *Doe*, 474 F. Supp. 2d at 845–46.

13. Richard M. Guo, Note, *Stranger Danger and the Online Social Network*, 23 BERKELEY TECH. L.J. 617, 620 (2008); *cf.* Patricia Sanchez Abril, *A (My)Space of One's Own: On Privacy and Online Social Networks*, 6 NW. J. TECH. & INTELL. PROP. 73, 74 (2007) (noting the "self-invention within a perceived community" that online social networking facilitates).

Generally, a person is required to create a profile when registering for a social networking web site. Profile creation is accomplished by filling out a series of virtual forms eliciting a broad range of personal data. The information requested varies depending upon the particular web site, but users are commonly asked to provide their name, home address, e-mail address, age, sex, location, and birth date.[14] The web site populates the user's profile with the supplied information and allows a user to "aggregate and present her personal information, photos, web journals, favorite hyperlinks, and the like" into one web page.[15] The populated profile becomes "a multimedia collage that serves as one's digital 'face' in cyberspace using images, video, audio, and links to other profiles and websites."[16]

Profile creation allows the member to participate in the community element of social networking sites. Users establish virtual communities by linking their profiles in a process known as "friending" or "connecting."[17] One user requests to add another as a friend, and the recipient may either accept or reject the invitation.[18] If the recipient accepts, the profiles are linked and the connected members are generally able to view one another's online content without restriction.[19] The network created by the linking process allows a user to chat with friends,[20] display support for particular causes, "join

14. *See* Guo, *supra* note 13, at 619–20.

15. *Id.* at 619.

16. Abril, *supra* note 13, at 74. The fact that a user profile is entirely self-generated can lead to significant mischief and presents an interesting conundrum for law enforcement: a person observing the online profile of a user with whom the observer is unacquainted has no idea whether the profile is legitimate. In fact, the user may be entirely fictitious. *See* Snyder v. Blue Mountain Sch. Dist., No. 3:07cv585, 2008 WL 4279517, at *1 (M.D. Pa. Sept. 11, 2008) (student created false Internet profile purporting to be her school principal); *see also* Samantha L. Millier, Note, *The Facebook Frontier: Responding to the Changing Face of Privacy on the Internet*, 97 KY. L.J. 541, 542 (2009) (discussing the case of Freddi Staur, a toy frog with a Facebook account).

17. *See* Guo, *supra* note 13, at 620.

18. Social networking users may face external limitations on the types of individuals they may virtually befriend. Florida's Judicial Ethics Advisory Committee recently recommended judges refrain from friending lawyers, fearing the act would create the appearance of impropriety. John Schwartz, *For Judges on Facebook, Friendship Has Limits*, N.Y. TIMES, Dec. 11, 2009, at A25. A minority of the panel concluded that "social networking sites have become so ubiquitous that the term 'friend' on these pages does not convey the same meaning that it did in the pre-internet age." Fla. Sup. Ct. Comm. on Judicial Ethics, Advisory Op. 2009-20 (2009), http://www.jud6.org/LegalCommunity/LegalPractice/opinions/jeacopinions/2009/2009-20.html (discussing whether a judge may post messages and other information on her social networking site).

19. This is not universally the case. Some websites feature person-specific privacy settings that allow a user to restrict a particular individual's ability to access her online content. On Facebook, for example, users retain this ability even if the target of the restrictions is a virtual friend. *See* Facebook.com, Facebook's Privacy Policy § 3, http://www.facebook.com/policy.php (last visited May 8, 2010).

20. Some social networking web sites permit only private messages, while others allow users to post public messages to another's profile.

interest groups dedicated to virtually any topic," and otherwise "hang out."[21]

Social networking web sites allow users to virtually hang out by encouraging self-disclosure.[22] There exists a direct relationship between the growth of a user's profile and growth of her online community. The more information the user supplies, the greater her ability to connect with others. Web sites therefore will commonly question members about their interests, favorite groups or organizations, work history, education, relationship status, and preferences.[23] Self-disclosure also directly benefits the web site, which uses targeted marketing to generate revenue.[24]

An online social network can therefore be defined as an online service that encourages self-disclosure by requiring members to populate a profile with personal information and allows them to create a virtual community by linking their personal profile with those of other members.[25] Most of the hundred million or so web sites on the Internet will fall outside this definition, and perhaps police surveillance of those sites is less objectionable.[26] However, the number of web sites falling within this definition is sure to increase as more sites adopt similar principles in an attempt to replicate the success of social networking services.[27] The creation and rapid expansion of online social networking over the past decade makes this evident.

B. Development of Online Social Networking

Online social networking rose from the ashes of the dot-com bubble burst of 2001 that left many web-based businesses in shambles.[28] Scholars dubbed

---

21. Abril, *supra* note 13, at 74.

22. *Id.*

23. *See* Hodge, *supra* note 11, at 97; *cf.* Abril, *supra* note 13, at 74 (describing online social networks as "[a] high tech cross between a bumper sticker and a diary").

24. Kermit Pattison, How to Market Your Business with Facebook, N.Y. Times on the Web (Nov. 12, 2009), http://www.nytimes.com/2009/11/12/business/smallbusiness/12guide.html. MySpace's privacy policy offers a good example: "[B]ased on your music interests we might display an advertisement to make sure you are advised when your favorite band is coming to town." MySpace.com, Privacy Policy, http://www.myspace.com/index.cfm?fuseaction=misc.privacy (last visited May 8, 2010).

25. Personal information in this sense is broader than the definition provided in statutes prohibiting identity theft, and includes references to a person's interests and activities. *See, e.g.*, WIS. STAT. § 943.201(1)(b) (2007–2008).

26. For example, in *United States v. Gines-Perez*, 214 F. Supp. 2d 205, 225–26 (D.P.R. 2002), the district court concluded no expectation of privacy was violated when police downloaded "a commercial photograph [of the defendant], placed on [an] under-construction web page, for obvious commercial, marketing purposes."

27. Gary Rivlin, *Wallflower at the Web Party*, N.Y. TIMES, Oct. 15, 2006, § 3, at 1 ("Roughly once a week, David L. Sze, a venture capitalist at Greylock Partners, hears from entrepreneurs who say they have the next MySpace . . . .")

28. Guo, *supra* note 13, at 618.

the new web services growing out of that collapse "Web 2.0."[29] The earliest social networking web site, Friendster, was created in 2002 and offered users "a site where they could browse profiles posted by friends and the friends of friends in search of dates and playmates."[30] Friendster was a trailblazer, but also a complete disaster; as of 2006, Friendster was one of the least popular social networking websites, trailing behind a site started in 2005 by a 16-year-old high school student.[31]

Despite the lackluster success of Friendster, online social networking has flourished. The years 2003 and 2004 marked the respective births of the two most popular social networking services, MySpace and Facebook.[32] Since their debut, they have attracted hundreds of millions of users[33] and their values have skyrocketed as advertisers realized the marketing potential of this new communicative forum.[34] Less than a decade after their creation, social networking websites have truly become the "soda fountains" of the twenty-first century, where "members of a community . . . gather . . . to 'chew the fat'—discuss matters of local politics, share the latest gossip, or complain about the weather."[35]

C. Social Networking Behemoths: MySpace and Facebook

While countless web sites have attempted to cash in on the social networking phenomenon, two services merit particular attention because of their vast member base and high visibility. Each day hundreds of millions of users connect to one another using the services of Internet behemoths

29. *Id.* at 618–19. Guo articulates seven principles that allow one to identify a creature of Web 2.0 origin: (1) "Services, not packaged software, with cost-effective scalability"; (2) "Control over unique, hard-to-recreate data sources that get richer as more people use them"; (3) "Trusting users as co-developers"; (4) "Harnessing collective intelligence"; (5) "Leveraging the long tail through customer self-service"; (6) "Software above the level of a single device"; and (7) "Lightweight user interfaces, development models, AND business models." *Id.* at 619 (citing Tim O'Reilly, What Is Web 2.0? Design Patterns and Business Models for the Next Generation of Software, O'Reilly (Sept. 30, 2005), http://www.oreillynet.com/pub/a/oreilly/tim/news/2005/09/30/what-is-web-20.html). Guo concludes online social networks are creatures of Web 2.0 because they embrace the second, third, and fourth principles. *Id.*

30. Rivlin, *supra* note 27. By 2002, Google had already offered to buy out Friendster for $30 million. *Id.*

31. *Id.*

32. Wilson, *supra* note 11, at 1221–22.

33. Facebook alone has a membership roughly equal to the population of the United States. Shannon Awsumb, *Social Networking Sites: The Next E-Discovery Frontier*, BENCH & BAR OF MINNESOTA, Nov. 2009, at 22, 22, *available at* http://www2.mnbar.org/benchandbar/2009/nov09/networking.html. Its expansion has been rapid. MySpace and Facebook had a collective membership of only 175 million users as of 2008. Guo, *supra* note 13, at 620–21.

34. In January 2008, investors valued Facebook at over $15 billion. *Connections Are His Currency*, L.A. TIMES, Jan. 21, 2008, at C3.

35. Wilson, *supra* note 11, at 1219–20.

MySpace and Facebook. Not surprisingly, these web sites are among those most frequently targeted by police to detect criminal activity.[36] Differing privacy functions, user controls, and even guiding philosophies mandate the two services receive individual attention.[37]

1. MySpace

Since its creation in 2003, MySpace has quickly grown to one of the most frequently visited web sites on the Internet.[38] While its corporate history remains controversial even seven years later,[39] the web site's huge marketing audience has dramatically increased its value; MySpace cost Rupert Murdoch's News Corporation $580 million when it purchased MySpace in 2005, and it remains under News Corporation ownership today.[40] Although MySpace's growth remained steady throughout 2006 and 2007, the web site has since yielded its position as the most popular social networking site to chief rival Facebook.[41] As of January 2008, 110 million active users were regularly accessing the web site, and it was growing at an average rate of 300,000 new users per day.[42] In America, one in four citizens has a MySpace page, and MySpace is the most visited site on the Internet.[43] One commentator has compellingly characterized this growth: "If MySpace alone were a country and each of its profiles a person, it would be the [twelfth] most populous nation in the world."[44]

A MySpace profile is an amalgamation of mandatory registration information and optional non-personally identifiable information. MySpace's success can be attributed in part to the absence of restrictive membership criteria; to join, a potential MySpace member need only be at least fourteen years old and have Internet access and an e-mail account.[45] Other information

36. *See* Berg, *supra* note 4, at 18–19.

37. *See* Catherine Dwyer et al., Trust and Privacy Concern Within Social Networking Sites: A Comparison of Facebook and MySpace, Proceedings of the Thirteenth Americas Conference on Information Systems (Aug. 9–12, 2007) (comparing the web sites).

38. *See* Karen Barth Menzies, *Perils and Possibilities of Online Social Networks*, TRIAL, July 2008, at 58.

39. Wilson, *supra* note 11, at 1222–23. The company claims that two friends, Tom Anderson and Chris DeWolfe, took earlier social networking service concepts and expanded upon them, while others claim MySpace was populated by what amounted to a massive spam mail campaign. *Id.*

40. *Id.* at 1223.

41. Shira Ovide & Nick Wingfield, *MySpace Ads Up for Grabs*, WALL ST. J., July 6, 2010, at B1 (measuring popularity by number of unique visitors worldwide); Brian Stelter & Tim Arango, *Losing Popularity Contest, MySpace Tries a Makeover*, N.Y. TIMES, May 4, 2009, at B3.

42. Menzies, *supra* note 38, at 58.

43. *Id.*

44. Abril, *supra* note 13, at 74.

45. *See id.*; Guo, *supra* note 13, at 621.

collected at registration includes the user's full name and gender.[46] MySpace members may also choose to store and display non-personally identifiable information on their profiles.[47] When creating a profile, the user is asked to fill out "several information sections, known as 'blurbs.'"[48] The two standard sections are titled "About Me" and "Who I'd Like to Meet,"[49] but MySpace profiles also store a user's interests, hobbies, lifestyle choices, groups with whom they are affiliated (schools, companies), videos and pictures, private messages, bulletins, or personal statements.[50] There are limits on what users may post: MySpace's Terms of Use supply a lengthy list of prohibited profile content, including that which "furthers or promotes any criminal activity."[51] Users may change their registration or profile information at any time.[52]

MySpace permits users to connect with one another in many ways. The court in *Doe v. MySpace, Inc.* thoroughly chronicled MySpace's community element, documenting the interaction process:

> Once a profile has been created, the member can use it to extend "invitations" to existing friends who are also MySpace.com users and to communicate with those friends online by linking to their profiles, or using e-mail, instant messaging, and blogs, all of which are hosted through the MySpace.com platform.
>
> Members can also meet new people at MySpace.com through user groups focused on common interests such as film, travel, music, or politics. . . . MySpace.com members can also become online "friends" with celebrities, musicians, or politicians who have created MySpace.com profiles to publicize their work and to interface with fans and supporters.[53]

In addition, members may interact using third-party applications, like games,

46. MySpace.com, Privacy Policy, *supra* note 24. MySpace is also permitted to collect a user's telephone number, mailing address, and credit card number upon registration, but does not actively do so at this time. *Id.*

47. *Id.*

48. Guo, *supra* note 13, at 621.

49. *Id.*

50. *See generally* MySpace.com, Terms & Conditions, http://www.myspace.com/index.cfm?fuseaction=misc.terms (last visited May 8, 2010). Profile information provided in structured profile fields or questions, or information added to open-ended profile fields and questions, "may . . . be used to customize the online ads [users] encounter to those [MySpace] believe[s] are aligned with [the user's] interests." MySpace.com, Privacy Policy, *supra* note 24.

51. MySpace.com, Terms & Conditions, *supra* note 50, § 8.11.

52. MySpace.com, Privacy Policy, *supra* note 24.

53. Doe v. MySpace, Inc., 528 F.3d 413, 415–16 (5th Cir. 2008) (footnote omitted).

on the MySpace platform.[54]

MySpace users can, within limits, determine the extent to which their profile content is accessible to others.[55] MySpace profiles are public by default, with certain limited exceptions.[56] A profile, once created, is instantly viewable to any Internet user, without notice to its creator.[57] Certain information (e.g., a user's name and photograph) will always remain public, but access to other profile content may be restricted to certain groups of users.[58] Any profile content that remains public may be indexed by search engines.[59] In addition, MySpace may share profile content with companies using the service for advertising or marketing.[60] MySpace disclaims ownership rights in profile content, but reserves the right to use or reproduce content.[61]

A search function allows MySpace users to locate other users' profiles.[62] MySpace's privacy policy describes the web site's search capabilities:

> In order to locate other MySpace Members that you may already know in the physical world, MySpace allows Users to search for Members using Registration PII [personally identifiable information] (i.e., full name or email address). MySpace also allows Users to browse for certain Profile Information in order to help connect with Members (i.e., schools and/or companies where Users may have attended or worked).[63]

Each search yields up to 3,000 profile links, ordered by the searcher's choice of newest profiles, recently updated profiles, most recent log-in, or distance from a specified zip code.[64] Results can change almost instantaneously depending upon the search criteria. Once a profile shows up

---

54. MySpace.com, Privacy Policy, *supra* note 24. The policy defines third-party applications as "small bits of software, often with interactivity, that can be installed into Members' profiles or shared with other Users." *Id.*

55. A.B. v. State, 885 N.E.2d 1223, 1224 (Ind. 2008).

56. Guo, *supra* note 13, at 621–22. One exception is for teenagers: although "[p]rior to 2008, users who were fourteen or fifteen had their profiles automatically restricted to their friends," MySpace recently changed this policy and raised the age to eighteen. *Id.*

57. *See id.* at 620.

58. *A.B.*, 885 N.E.2d at 1224 (citing MySpace.com, Privacy Policy, Mar. 31, 2008).

59. MySpace.com, Privacy Policy, *supra* note 24.

60. *Id.*

61. MySpace.com, Terms & Conditions, *supra* note 50, § 6.1.

62. Megan A. Moreno et al., *Reducing At-Risk Adolescents' Display of Risk Behavior on a Social Networking Web Site*, 163 ARCH. PEDIATR. ADOLESC. MED. 35, 36 (2009).

63. MySpace.com, Privacy Policy, *supra* note 24.

64. Megan A. Moreno et al., *Display of Health Risk Behaviors on MySpace by Adolescents*, 163 ARCH. PEDIATR. ADOLESC. MED. 27, 28 (2009).

in the results list, simply clicking on it will bring up the user's profile.[65] If the user has not modified her privacy settings, all profile content will be accessible to the searcher.

2. Facebook

Facebook quietly entered the social networking scene in 2004 when Mark Zuckerberg, then an undergraduate student at Harvard, sought to electronically emulate the paper facebooks distributed to incoming students and staff.[66] The web site spread from the Harvard dorms to other Ivy League institutions, then to other universities. During the web site's early stages, only college students with an e-mail address assigned by a university could use the service.[67] As a result, Facebook experienced markedly slower user growth than MySpace.[68] These restrictions were motivated by Facebook's desire to enhance the user's "'interaction with [his] real friends, based on real relationships and the real world around them.'"[69] The success of its more popular competitor quickly convinced Facebook to abandon this philosophy; by 2006, anyone at least thirteen years old with a valid e-mail address could create a profile.[70]

Facebook allows users to build a profile in much the same way as MySpace. Facebook prompts new users to supply their name, e-mail address, sex, and birth date. Perhaps as a vestige of Facebook's restrictive roots, users are also asked to name any high schools, colleges, or universities attended. Users may build upon this foundation by supplying additional information in any of four sections that compose the profile: "Basic Information," which includes the user's current city, hometown, relationship status, and political and religious views; "Personal Information," which includes interests, activities, and favorite music, movies, and books; "Contact Information,"

65. *Id.*

66. Wilson, *supra* note 11, at 1221; Millier, *supra* note 16, at 541–42. Facebook's origin is not without controversy either. Fellow Harvard undergraduates Tyler Winklevoss, Cameron Winklevoss, and Divya Narendra filed suit against Zuckerberg, arguing that they had come up with the idea for a similar social networking web site and hired Zuckerberg to help them write code for it. ConnectU LLC v. Zuckerberg, 522 F.3d 82, 86 (1st Cir. 2008). According to their history, Zuckerberg "not only failed to carry out the assignment but also stole their idea, business plan, and rudimentary (unfinished) source code in order to launch a competing social networking website." *Id.*

67. Guo, *supra* note 13, at 622.

68. *Id.*

69. *Id.* (quoting the posting of Donna Bogatin to Digital Markets, Facebook Talks "The Real Deal" in Exclusive Interview, http://blogs.zdnet.com/micro-markets/?p=533 (Oct. 12, 2006, 08:27 CDT)). This social networking business model is known as the "confirmed friendship" model. Guo, *supra* note 13, at 622. By contrast, MySpace has been criticized for encouraging long friend lists, a model that technology entrepreneur Christopher Allen argues eschews quality for quantity. Marcia Clemmitt, *Cyber Socializing*, 16 C.Q. RESEARCHER 627, 636 (2006).

70. Guo, *supra* note 13, at 622.

which includes web sites, addresses, phone numbers, and instant messaging screen names; and "Education and Work," which is largely self-descriptive. "Status" posts allow users to update their profiles with up-to-the-minute information, offering users a virtual soapbox to their online community.[71]

Facebook's community element is perhaps more sophisticated than that of MySpace. The web site's design makes it easy for users to "compile lists of their friends, post public comments on friends' profiles, . . . send private messages to other users[,] . . . [and] create groups of people with similar interests. . . ."[72] Members may upload photographs, and both Facebook and MySpace allow users to "tag" their friends in the image. Tagging "creates a link [in] the individual's profile from the photograph, making users easily identifiable, even when the viewer of the photograph is not 'friends' with the photograph's subjects."[73] Facebook's user interface sports a search function similar to MySpace's.[74] New features are often introduced, and users have greater opportunities to showcase their preferences and activities with third-party applications built into the Facebook platform.[75]

Facebook offers users an advanced series of privacy settings to restrict others' ability to access their profile content. Users can control the visibility of nearly all the information shared through Facebook, including their interests and activities, family and relationships, education and work, and status updates and comments.[76] Nonetheless, a user's perceived ability to maintain control over her online information is largely illusory, as that information "may remain viewable elsewhere to the extent it has been shared with others"—even if the user removes the information from her profile or deletes her account.[77] Moreover, Facebook has deemed certain information—including a user's name, profile photograph, gender, geographic region, and networks—"publicly available," and as a result these categories lack a privacy setting.[78] In addition, some information cannot be deleted by the user at all.[79]

Facebook's abandonment of the "confirmed friendship" model—in which

---

71. Millier, *supra* note 16, at 542.

72. Hodge, *supra* note 11, at 97.

73. Millier, *supra* note 16, at 544.

74. *See* Hodge, *supra* note 11, at 97.

75. Users have the option to add hundreds of third-party applications designed for Facebook. *See* Facebook.com, Application Directory, http://www.facebook.com/apps/directory.php (last visited May 8, 2010). The use of third-party applications carries additional privacy risks, as their compliance with Facebook's usage terms is apparently determined entirely by the applications' developers. *See* Facebook.com, Statement of Rights and Responsibilities § 9, http://www.facebook.com/terms.php (last visited May 8, 2010).

76. Facebook.com, Facebook's Privacy Policy, *supra* note 19, § 3.

77. *Id.*

78. *Id.*

79. *Id.* Messages between users are one such category of information. *Id.*

the web site "group[ed] users into networks based on affiliation with a university, high school, region of the country, or company, and . . . allow[ed] other users within a network to view each others' profiles"[80]—has led to sweeping, but criticized,[81] changes to its privacy policy. The changes, which are designed to make user content more public, are an effort to compete with social networking up-and-comer Twitter, a web site allowing users to share 140-character messages with one another in real time from nearly anywhere on the planet. The major change is a default privacy setting for certain information:

> Information set to "everyone" is publicly available information . . . [and] may be accessed by everyone on the Internet (including people not logged into Facebook), be indexed by third party search engines . . . and may also be associated with you . . . even outside of Facebook. . . . The default privacy setting for certain types of information you post on Facebook is set to "everyone."[82]

Facebook has experienced steady user growth, adding new members at a rate of 200,000 per day.[83] These additions supplement the nearly 300 million active users who already utilize Facebook's services. With "55,000 regional, work-related, collegiate, and high school networks,"[84] Facebook is bound to remain one of the most popular social networking web sites well into the foreseeable future.

III. THE ATTRACTION OF ONLINE SOCIAL NETWORKING TO USERS AND LAW ENFORCEMENT

> As the uses of technology become more intrusive, claims of personal privacy will grow in importance. As the methods of criminal enterprises become more sophisticated, the needs of law enforcement in combatting them will also grow.[85]

The creation and rapid growth of online social networking prompts the question: What makes it so appealing? People are flocking to social networking web sites and disclosing more information than ever using these services.[86] While generally this type of information-sharing produces social

80. Hodge, *supra* note 11, at 98.

81. Oreskovic, *supra* note 7.

82. Facebook.com, Facebook's Privacy Policy, *supra* note 19, § 3.

83. Guo, *supra* note 13, at 622.

84. Wilson, *supra* note 11, at 1222.

85. United States v. McNulty (*In re Steven M. Askin*), 47 F.3d 100, 105 (4th Cir. 1995).

86. In a recent study, 100% of Facebook users revealed their real name and 94% disclosed their e-mail address. Dwyer, *supra* note 37. While these percentages were much lower for MySpace users

good, certain disclosures encourage illegal activity, and excessive disclosure attracts an undesirable criminal element. Criminal utilization of online social networking, in turn, attracts law enforcement. This mixture of excessive disclosure, criminals, and police is certain to produce frequent constitutional issues in the near future.

A. Benefits of Online Social Networking

Richard Guo has identified at least two specific benefits resulting from the use of social networking media. First, use of social networking media encourages self-expression and socialization in a way in-person interaction might not.[87] Social networking web sites contribute to this development by providing a virtual forum for peer interaction that helps users understand the contours of (and, one would hope, establish) healthy relationships.[88] Although this opportunity to enhance one's personal identity may benefit all users, the growth is most perceptible in younger social networking members.[89]

A second primary benefit of online social networking participation is the ability to stay connected with others even when separated by vast geographical distance.[90] This connectivity permits family and friends to remain close and keep informed on events in each other's lives. While a user benefits from this "surveillance" function through a better understanding of the other member's life, the monitored member might also benefit when the monitoring member recognizes antisocial behavior and intervenes.[91]

Another substantial advantage of social networking participation is the ability to meet new people virtually. This connection may occur as a result of a user's searches, or may result from the user's interaction with existing online friends or membership in an online group. Whatever the cause, many users now utilize social networking web sites to make new friends or professional connections.[92]

(66.7% and 40%, respectively), MySpace members were significantly more likely to reveal other information, such as relationship status. *Id.*

87. *See* Guo, *supra* note 13, at 624.

88. *Id.*

89. *Id.* This benefit may be particularly important, as "[v]arious sources cite MySpace user demographics to be predominantly between the ages of fourteen and thirty-four, with thirty-four being considered a high estimate due to people altering their ages to skew higher in some cases to mask their true age or to be humorous." A.B. v. State, 885 N.E.2d 1223, 1224–25 (Ind. 2008). This is not to say that online social networking is a young person's game: "As of January 2008, the fastest-growing demographic among Facebook users was people older than 24." Menzies, *supra* note 38, at 58–59.

90. Guo, *supra* note 13, at 624–25.

91. Cliff Lampe et al., A Face(book) in the Crowd: Social Searching vs. Social Browsing, Proceedings of the Twentieth Anniversary Conference on Computer Supported Cooperative Work (Nov. 4–8, 2006).

92. LinkedIn.com, for example, is a social networking web site designed to facilitate

These advantages suggest an increasing segment of the population will utilize online social networking services. As the web sites expand feature sets and improve user interaction, their appeal to otherwise resistant individuals will grow.[93] This growth, in turn, suggests even greater amounts of personal information will soon be available to other users—both those with benign and criminal intentions.

B. The Utility of Online Social Networking to Law Enforcement

Two problems are immediately visible with respect to the increasing disclosure of personal information. First, as the amount of personal information disclosed on online social networks increases, so does the probability that it will reveal users engaged in illegal or high-risk behavior. High-risk behavior can include alcohol or drug abuse, sexual conduct, and violence.[94] A recent study concluded that over half of the sampled profiles of eighteen-year-old MySpace users displayed one or more of these risk behaviors.[95] Although the most common risk behavior was alcohol use, users also frequently described sexual activities.[96] Because users can easily connect with others who have similar interests, users can display or model risk behaviors and thus make such conduct (and its disclosure) the norm.[97]

The second problem associated with increased disclosures on online social networks is the risk that a greater number of criminals will utilize these web sites for nefarious ends. U.S. Attorney Terrence Berg commendably describes this effect in his 2007 article "The Changing Face of Cybercrime":

> With millions of users packing these sites with personal information of every type, from family photos and movies to career interests to what used to pass for private gossip among close friends, these sites are gargantuan warehouses of valuable personal identity, consumer preference, personality and family issues, and online usage/habit information that could be exploited if made accessible to those with criminal ends in mind. They are a treasure trove for the Internet child

---

professional networking.

93. An older group of "digital immigrants" has somewhat cautiously migrated to the digital medium, but has not been as receptive as the younger group of "digital natives" who have been "raised in an Internet-immersed culture[and] are extremely cyber-savvy." Abril, *supra* note 13, at 76–77.

94. *See* Moreno et al., *supra* note 64, at 27–28.

95. *Id.* at 30. This result is consistent with an earlier study that concluded that "approximately 47% of 16- and 17-year-olds displayed references to risk behaviors of sexual activity and substance use on MySpace public profiles." *Id.* at 31.

96. *Id.* at 30.

97. *See id.* at 31.

predator or ID thief.[98]

The threats identified by Berg—child sexual predation and ID theft—underscore the risks inherent in the voluntary disclosure of extensive personal information to online "friends." Although more traditional Internet forums (e.g., chat rooms) are susceptible to child solicitation, this problem is especially pronounced in online social networks because they "promote sharing a vast amount of personal information divulged on a user's MySpace or Facebook page and engender a feeling of trust among 'friends' in the social network."[99] "MySpace has already been the forum for some celebrated cases of child solicitation," and social networking web sites' aggregation of information "presents a target-rich environment for those seeking to steal data, and runs the risk that viruses or worms intended either to collect data or damage systems will have devastating multiplier effects because so many users are interlinked."[100]

There is already significant evidence that authorities have begun to use online social networks to keep tabs on individuals within their jurisdiction. "[P]oint-and-click" police are increasingly turning to online communities to aid in their investigations.[101] In 2006, for example, police arrested a sixteen-year-old and charged him with juvenile possession of a handgun after officers discovered MySpace pictures of him holding the weapons.[102] Indeed, inculpatory user photographs appear to have the most utility to law enforcement officials.[103] Law enforcement organizations make it clear that they endorse the practice: "'It really does behoove police departments to really be technically proficient on computers, and that includes social networking sites as well, because that's a very popular way for youth to

98. Berg, *supra* note 4, at 19.

99. *Id.*

100. *Id.* at 19–20.

101. Wilson, *supra* note 11, at 1224. Some police are forthright about their use of online social networking sites: "'If I have a slower assignment, or [ten] minutes at the beginning of my shift, I use a series of [twenty] different searches,'" confessed one University of Wisconsin-Milwaukee police officer who uses Facebook to "root out campus crime." Erica Perez, *Getting Booked by Facebook*, MILWAUKEE J. SENTINEL, Oct. 3, 2007, at 1A.

102. Wilson, *supra* note 11, at 1225. Wilson notes that some of the heightened police concern about this case may have been justifiable since the teen was a student in the same school district as Columbine High School, where seven years earlier two students had killed thirteen people in a school shooting spree. *Id.* at 1225 n.122.

103. Authorities appear to be using social networking photographs more frequently and for a wide variety of purposes. User photographs may provide the basis for criminal charges. Wilson, *supra* note 11, at 1225 ("[T]he Attorney General of Utah filed sexual-exploitation charges against a twenty-seven-year-old man after investigators discovered a photo on his MySpace profile that featured the man and two boys with whom he had been court-ordered not to have contact."). Or the photographs may assist authorities in criminal investigations. *Id.* (noting a police detective who used profile pictures of social networking users to create a lineup).

socialize or to transmit information about parties and protests.'"[104] Some foreign police agencies, such as the United Kingdom's Greater Manchester Police, have identified Facebook as such a useful tool that they have established a permanent virtual presence on the web site.[105]

Traditional law enforcement agencies are not the only government actors that have realized the investigative value of social networking. The Secret Service has used information posted on the social web to investigate threats against the President.[106] The National Security Agency is currently funding research intended to develop its capability to "harvest" massive amounts of social networking information.[107] School administrators frequently reprimand students who have posted information "critical of professors, teachers, and principals."[108] Surveillance by school officials has become so prevalent, MySpace has issued a document entitled "The Official School Administrator's Guide to Understanding MySpace and Resolving Social Networking Issues."[109]

Thus, as both legitimate members and criminals use and abuse the social networking structure provided by web sites, law enforcement will be increasingly attracted to the user content posted on them. The use of posted information by law enforcement and other government actors has constitutional implications for the online social network phenomenon. More specifically, when a government actor views a user's profile in an effort to evaluate that user's ability to conform his conduct to the requirements of the law, has a search occurred? That is the question this Comment seeks to answer.

IV. MEASURING PRIVACY EXPECTATIONS IN ONLINE SOCIAL NETWORKING CONTENT

Taking its command literally, the Fourth Amendment does not prohibit government searches and seizures, but requires only that they be conducted

104. Perez, *supra* note 101 (quoting Lisa Sprague, president-elect of the national group, International Association of Campus Law Enforcement Administrators).

105. Rich Bowden, UK Police First to Use Facebook, Tech Herald (Apr. 21, 2008), http://www.thetechherald.com/article.php/200817/764/UK-police-first-to-use-Facebook (U.K. police launched an application on Facebook to get information from the public regarding criminal cases).

106. Hodge, *supra* note 11, at 96.

107. Clemmitt, *supra* note 69, at 629. These federal surveillance programs are particularly problematic for social networking users because they are often "classified . . . and rarely subjected to public scrutiny." Patrick Marshall, *Online Privacy*, 19 C.Q. RESEARCHER 933, 947 (2009).

108. Hodge, *supra* note 11, at 96.

109. MySpace.com, The Official School Administrator's Guide to Understanding MySpace and Resolving Social Networking Issues, http://cms.myspacecdn.com/cms/SafetySite/documents/SchoolAdministratorGuide.pdf (last visited May 8, 2010).

under reasonable circumstances.[110] Ordinarily, a search is reasonable only if police obtain a warrant prior to intruding upon the individual's privacy.[111] What constitutes a "search" under the Amendment has, however, generated much confusion and controversy as a result of the Supreme Court's meandering Fourth Amendment doctrine.[112] This places the police in the difficult position of having to readily distinguish between those situations in which a warrant is necessary and those in which it is not, with the consequence being suppression of any evidence gained if officers guess wrongly.[113]

Identifying which government intrusions constitute a search is rarely an easy task, but it becomes increasingly difficult where technological developments allow police to observe private conduct previously thought inaccessible. Although the Supreme Court has occasionally issued pronouncements under these circumstances,[114] it would be practically impossible for the Court to establish rules governing each new advance in technology.[115] Thus, it will fall upon the lower courts to deal with rapid technological shifts, but they ordinarily will do so within the mold of existing

110. The Fourth Amendment provides, in pertinent part, that: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated." U.S. CONST. amend. IV. The "seizure" portion of the Amendment is, as constitutional provisions go, fairly straightforward and not the focus of this Comment. *See* 1 WAYNE R. LAFAVE, SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT § 2.1(a) (4th ed. 2008).

111. *See, e.g.*, Katz v. United States, 389 U.S. 347, 357 (1967) ("[S]earches conducted outside the judicial process, without prior approval by judge or magistrate, are *per se* unreasonable under the Fourth Amendment—subject only to a few specifically established and well-delineated exceptions.") (footnotes omitted).

112. *See* Kerr, *supra* note 6, at 503 (noting the Supreme Court has "refused to provide a consistent explanation for what makes an expectation of privacy 'reasonable'" and describing four co-existing approaches used by the Court).

113. *Cf. id.* at 539 (noting police uncertainty where law regulating permissible investigative techniques is in flux).

114. *See* Kyllo v. United States, 533 U.S. 27, 29, 40 (2001) (holding that police use of a thermal imaging device to scan a defendant's house for elevated heat signatures indicative of marijuana growth lamps constituted a search). Further, even when the Supreme Court does speak on Fourth Amendment privacy, its "guidance tends to be very narrow." Kerr, *supra* note 6, at 538–39 (noting that *Kyllo* did not establish a rule governing either devices not in general public use or sense-enhancing devices directed at cars or people).

115. Some commentators have suggested this fact should compel deference to legislative bodies, which possess greater institutional competence to respond to rapid technological shifts. *See* Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 805, 857–82 (2004) (arguing that "considerations of doctrine, history, and function . . . teach that courts should place a thumb on the scale in favor of judicial caution when technology is in flux, and should consider allowing legislatures to provide the primary rules governing law enforcement investigations involving new technologies"). *But see* Kerr, *supra* note 6, at 533–34 (positive law may be enacted for reasons having nothing to do with the reasonableness of police investigations and may inadequately deal with rapid technological changes).

Supreme Court doctrine.[116]

A. Katz *and the "Reasonable Expectation of Privacy" Test*

Early efforts by the Court to adopt a rule distinguishing searches from non-searches focused on the significance of physical intrusions into a person's home or effects.[117] Thus, courts primarily protected a citizen's "spatial privacy" and discouraged government actors from breaking down doors and rummaging through personal belongings.[118]

This rule was generally sufficient until police began using increasingly sophisticated technology—like wiretaps—that neither involved physical trespass nor left the individual with any indication she was under surveillance. The Court's first wiretap case, *Olmstead v. United States*, required the Court to determine whether police interception of telephone conversations using wiretaps placed outside a person's residence implicated the Fourth Amendment.[119] The issue placed the Court in a quandary. Abandoning a physical intrusion requirement meant departing from the literal command of the Fourth Amendment—which prevented unreasonable searches of "persons, houses, papers, and effects"—and crafting a new, and almost assuredly more amorphous, standard. Reaffirming the physical trespass standard was probably equally unsatisfying, as it meant insulating new police practices and investigative techniques from review by the courts.[120]

The Court rejected the defendants' arguments, adhered to the concept of spacial privacy, and held police activity not involving physical intrusion did not amount to a search. Justifying the Court's position in the text of the Fourth Amendment, Chief Justice Taft, writing for the Court, drew back from prior opinions suggesting the Amendment be given a broad reading:

> Justice Bradley in the *Boyd* case, and Justice Clarke in the *Gouled* case, said that the Fifth Amendment and the Fourth Amendment were to be liberally construed to effect the purpose of the framers of the Constitution in the interest of liberty. But that [cannot] justify enlargement of the language employed beyond the possible practical meaning of houses, persons, papers, and effects, or so to apply the words search

116. Kerr, *supra* note 6, at 539, 545–49 (noting that the Supreme Court will leave most Fourth Amendment matters to be resolved by lower courts, which will reason by analogy to prior cases).

117. Thomas K. Clancy, *What Is a "Search" Within the Meaning of the Fourth Amendment?*, 70 ALB. L. REV. 1, 4–7 (2006).

118. *See* Susan W. Brenner, *The Fourth Amendment in an Era of Ubiquitous Technology*, 75 MISS. L.J. 1, 7 (2005).

119. 277 U.S. 438, 455 (1928).

120. *See* Clancy, *supra* note 117, at 1–2.

> and seizure as to forbid hearing or sight.[121]

The Amendment's language, in the eyes of the Court, required that the search "be of material things—the person, the house, his papers or his effects."[122] The Court was not persuaded that the invention and widespread use of the telephone demanded a different result.[123] The *Olmstead* rule prevailed for much of the twentieth century, during which police were generally free to use new technology to their advantage without judicial oversight.[124]

By the time the Supreme Court granted certiorari in *United States v. Katz* in 1967, the continuing vitality of *Olmstead* was in serious doubt. That same year, the Court decided *Berger v. New York*, in which the Court considered a constitutional challenge to a statute authorizing eavesdropping conducted pursuant to a warrant; in turn, the statute authorized issuance of a warrant where authorities had "reasonable ground to believe that evidence of crime may be thus obtained."[125] While the Court ultimately invalidated the statute on the grounds that the statutory warrant process lacked constitutionally required particularization,[126] the Court also determined "'conversation' was within the Fourth Amendment's protections, and that the use of electronic devices to capture it was a 'search' within the meaning of the Amendment."[127] The Court recognized this holding as in direct conflict with *Olmstead*: "Statements in [*Olmstead*] that a conversation passing over a telephone wire cannot be said to come within the Fourth Amendment's enumeration of 'persons, houses, papers, and effects' have been negated by our subsequent cases. . . ."[128]

Such was the state of the law when *Katz* came before the Court later that year. During February 1965, police watched Charles Katz place daily calls from a bank of three public telephone booths during certain times of the

---

121. *Olmstead*, 277 U.S. at 465.

122. *Id.* at 464.

123. *Id.* at 465 ("The language of the Amendment [cannot] be extended and expanded to include telephone wires reaching to the whole world from the defendant's house or office. The intervening wires are not part of his house or office any more than are the highways along which they are stretched.").

124. *See* Clancy, *supra* note 117, at 1–2; *see also* Goldman v. United States, 316 U.S. 129, 135 (1942) (holding that the use of a detectaphone by government authorities was not a violation of the Fourth Amendment). Although some states prohibited the use of wiretaps and "bugs," by and large the practice of electronic eavesdropping was largely unregulated by state law or the Fourth Amendment. *See* Berger v. New York, 388 U.S. 41, 47–49 (1967).

125. *Berger*, 388 U.S. at 54–55 (internal quotation marks omitted).

126. *Id.* at 55–56.

127. *Id.* at 51.

128. *Id.*

day.[129] Toward the end of February, police attached microphones and a recorder to the tops of two booths and disabled the third.[130] The microphones, which did not physically penetrate the interior of the booths, captured only Katz's end of the conversation, and police activated them only while Katz was inside.[131] Police recorded several incriminating statements suggesting Katz was involved in a betting operation and were permitted to introduce those statements at Katz's trial for violating a federal anti-wagering statute.[132]

The Court reversed Katz's conviction, concluding the government's conduct constituted a warrantless search requiring suppression of the evidence.[133] The Supreme Court began the *Katz* opinion by rejecting the *Olmstead* notion that the execution of a search hinged on whether the police had invaded a "constitutionally protected area."[134] The Court leveled a scathing rebuke against the attorneys for formulating the issue in such a misleading manner, famously declaring "the Fourth Amendment protects people, not places."[135] It explicitly overruled *Olmstead*, concluding "the underpinnings of *Olmstead* and *Goldman* have been so eroded by our subsequent decisions that the 'trespass' doctrine there enunciated can no longer be regarded as controlling."[136]

The majority's conclusion was compelled by its recognition of the social significance of the public telephone:

> One who occupies [the telephone booth], shuts the door behind him, and pays the toll that permits him to place a call is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world. To read the Constitution more narrowly is to ignore the vital role that the public telephone has come to play in private communication.[137]

---

129. Katz v. United States, 369 F.2d 130, 131 (9th Cir. 1966).

130. *Id.*

131. *Id.* Today, where electronic surveillance by law enforcement is increasingly common, the process of reducing the amount of irrelevant information intercepted is known as "minimization." *See* 50 U.S.C. § 1801(h) (2006).

132. *Katz*, 369 F.2d at 131–32.

133. Katz v. United States, 389 U.S. 347, 359 (1967).

134. *Id.* at 350.

135. *Id.* at 351. It was, of course, the Court itself that had formulated the issue precisely this way in *Olmstead*, and it appears the Court's criticism is, at least with respect to Katz's attorney, entirely unwarranted. *See* Peter Winn, Katz *and the Origins of the "Reasonable Expectation of Privacy" Test*, 40 MCGEORGE L. REV. 1, 9–10 (2009) (noting the petitioner's attorney, Harvey Schneider, realized the *Olmstead* trespass standard was obsolete and focused on articulating a less property-based test during oral argument).

136. *Katz*, 389 U.S. at 353.

137. *Id.* at 352.

This "celebrated but underappreciated discussion of the telephone booth"[138] demonstrates a willingness on the part of the Court to analyze the impact of its holding on the communicative practices of average citizens.[139] The Court concluded protection was warranted for private communications—even those occurring in a place accessible to the public.

Katz unquestionably expanded the coverage of the Fourth Amendment[140] in a way suggesting virtual user content on social networking web sites should be protected from warrantless police scrutiny. This is so even though, as in *Katz*, some private communications may be seen or overheard by the public. As did the public telephone, online social networking has revolutionized the way individuals communicate. This is not to suggest our conception of privacy must be redefined at the inception of each novel communicative medium. As Justice Thomas recognized, however, online social networking has fundamentally altered the balance between the public and the private in a way that cannot be constitutionally ignored.[141] To do so would "ignore the vital role" that online social networking has come to play in private communications.[142]

Yet the Court's discussion of the social role of the public telephone has not been *Katz*'s lasting legacy. The majority's analysis was subtle, yet complex, and subsequent courts have chosen to rely upon Justice Harlan's concurring opinion for the applicable standard: "My understanding of the rule that has emerged from prior decisions is that there is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'"[143] Justice Harlan's statement finds little support in the Court's opinion,[144] and "came with a heavy thumb on the scale of law enforcement," as the following sections demonstrate.[145]

---

138. Jonathan Simon, Katz *at Forty: A Sociological Jurisprudence Whose Time Has Come*, 41 U.C. DAVIS L. REV. 935, 945 (2008).

139. These consequences are discussed more thoroughly in Part V.

140. LAFAVE, *supra* note 110, § 2.1(b), at 384–85.

141. Justice Thomas, *supra* note 2.

142. *See Katz*, 389 U.S. at 352.

143. *Id.* at 361 (Harlan, J., concurring).

144. The only statement of the majority arguably supporting such an approach comes near the end of the Court's analysis, is stated in a conclusory fashion, and appears almost as an afterthought: "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." *Id.* at 353.

145. Simon, *supra* note 138, at 953. This heavy thumb has not prevented the Court from recognizing a privacy expectation in all instances. *See, e.g.*, Kyllo v. United States, 533 U.S. 27, 34 (2001) (finding that the Fourth Amendment protects one from home searches conducted using technology not in general public use).

1. The Third-Party Doctrine

Online social networking is built upon a bedrock of voluntary disclosure. To create a profile, a potential user must share some information about himself. The user's ability to interact with others relies upon these initial disclosures and that interaction encourages the user to volunteer additional information. Throughout this process, the user's information is communicated to, and stored upon, the social networking web site's servers, waiting to be accessed by an end user.[146]

Under current search doctrine, voluntary disclosure to third parties has a dramatic effect upon the reasonableness of a citizen's privacy expectations. In *Smith v. Maryland*,[147] the Supreme Court held no search occurred when officers installed a pen register on telephone company property that recorded the numbers dialed from a telephone but did not disclose the content of telephone conversations.[148] This conclusion was premised upon the Court's belief that "people in general [do not] entertain any actual expectation of privacy in the numbers they dial."[149] This was so, reasoned the Court, because telephone users had to convey the phone numbers to the telephone company to complete the calls.[150] Thus, because citizens expected the seized information to be collected by the telephone companies anyway (after all, the dialed numbers are listed on the phone bill), any privacy expectation in that information was unreasonable.[151] The simple act of disclosure to a third party can destroy one's privacy expectations in shared non-content information.

The *Smith* dissenters, perhaps viewing the majority opinion as a significant step back from *Katz*, offered a spirited defense of the defendant's privacy rights. In Justice Stewart's view, the fact that the telephone company recorded dialed numbers was irrelevant to the Fourth Amendment analysis, as it did no more than describe "the basic nature of telephone calls," all of which involve the use of telephone company property and payment for telephone service.[152]

Justice Marshall launched a broader assault on the third-party doctrine,

---

146. Rich Miller, Facebook Now Has 30,000 Servers, Data Center Knowledge (Oct. 13, 2009), http://www.datacenterknowledge.com/archives/2009/10/13/facebook-now-has-30000-servers. Facebook operates an estimated 60,000 servers that perform more than 50 million operations per second. Rich Miller, Facebook Server Count: 60,000 or More, Data Center Knowledge (June 28, 2010), http://www.datacenterknowledge.com/archives/2010/06/28/facebook-server-count-60000-or-more.

147. 442 U.S. 735 (1979).

148. *Id.* at 745–46.

149. *Id.* at 742.

150. *Id.*

151. *Id.*

152. *Id.* at 746–48 (Stewart, J., dissenting).

announcing "whether privacy expectations are legitimate within the meaning of *Katz* depends not on the risks an individual can be presumed to accept when imparting information to third parties, but on the risks he should be forced to assume in a free and open society."[153] To Justice Marshall, these risks did not include the government's interception of non-content information, for he noted (in language similar to that found in *Katz*) the "vital role telephonic communication plays in our personal and professional relationships."[154] Emphasizing the chilling effect unregulated government monitoring would have on free speech and affiliation rights, Justice Marshall concluded any scheme to intercept personal contact information should receive the scrutiny of a neutral and detached magistrate prior to collection.[155]

The Supreme Court has never determined whether and how the third-party doctrine applies to Internet communications,[156] and the dissenters' views may yet carry the day. It is difficult to draw the line required by *Smith*; if disclosure to a third party eliminates a caller's privacy expectation in non-content information, why should a caller possess a reasonable privacy expectation in the content of her conversation? In both instances, the telephone company acts as a conduit between the caller and the recipient. The distinction between content and non-content information breaks down even further on the Internet, where "[u]sers disclose both content and routing information, in exactly the same technical manner, to an enormous number of third parties."[157] This fact may be sufficient to motivate a majority of the Court to adopt the dissenters' position, particularly where social networking information is concerned, because every piece of information posted to a social networking web site like Facebook is stored on third parties' servers as well, just waiting to be retrieved.[158] Moreover, this information is not simply stored for the convenience of the web site user; instead, the web site operators collect revenue by using this information to display ads tailored to the user's particular interests. As one commentator succinctly put it, "[t]he only way that *Smith*'s reasoning based on third-party disclosure could make sense in the Internet age would be an undesirable (and likely factually inaccurate) holding that people have no expectation of any privacy in their Internet

153. *Id.* at 750 (Marshall, J., dissenting).

154. *Id.* at 751.

155. *Id.* Justice Marshall displayed incredible foresight; police scrutiny of a user's online social networking content creates substantial tension with the First Amendment's guarantee of freedom of association. *See* Katherine J. Strandburg, *Freedom of Association in a Networked World: First Amendment Regulation of Relational Surveillance*, 49 B.C. L. REV. 741, 783–86 (2008); *infra* notes 218–225 and accompanying text.

156. Robert Ditzion, Note, *Electronic Surveillance in the Internet Age: The Strange Case of Pen Registers*, 41 AM. CRIM. L. REV. 1321, 1334 (2004).

157. *Id.* at 1336.

158. *See* Miller, *supra* note 146.

communications."[159]

Courts and lawyers may struggle to fit social networking information within *Smith*'s content/non-content framework, but this framework will remain the focus of analysis in the absence of guidance from the Supreme Court. Recent cases reaffirm the continuing vitality of the content/non-content distinction fundamental to *Smith*. In a highly criticized decision, the Ninth Circuit recently extended the third-party doctrine to sanction government interception of the "to" and "from" addresses of e-mail messages, IP addresses of web sites visited, and the total volume of data used by an account.[160] This information was unprotected, according to the *Forrester* court, because users "should know that [the to/from addresses of their e-mail messages and IP addresses of the web sites they visit are] provided to and used by Internet service providers for the specific purpose of directing the routing of information."[161] Yet the court emphasized the fact that the government was accessing neither the content of the e-mails nor particular web pages on the web sites the person viewed. "At best, the government may make educated guesses about what was said in the messages or viewed on the websites based on its knowledge of the e-mail to/from addresses," but the court found this "no different from speculation about the contents of a phone conversation on the basis of the identity of the person . . . dialed."[162]

The courts' continuing commitment to distinguishing between content and non-content data means social networking information must be classified in one category or the other. In contrast to *Smith* and *Forrester*, police interception of user social networking information involves seizure of content, not mere address or routing data. When police observe a user's online pictures or messages, they are observing the type of information that typically would be transmitted in a telephone or e-mail conversation. In other words, profile content is not mere "routing" information. The Fourth Amendment generally protects individuals from warrantless government seizure of their substantive information. In *United States v. Maxwell*, for example, the U.S. Court of Appeals for the Armed Forces determined "that the transmitter of an e-mail message enjoys a reasonable expectation that police officials will not intercept the transmission without probable cause and a search warrant."[163]

Recognition of a privacy expectation in this type of information does not totally insulate the information from police scrutiny. Courts have uniformly

159. Ditzion, *supra* note 156, at 1336.

160. United States v. Forrester, 512 F.3d 500, 510 (9th Cir. 2008).

161. *Id.*

162. *Id.*

163. United States v. Maxwell, 45 M.J. 406, 418 (C.A.A.F. 1996) (analogizing an e-mail to a letter). The court went on to note that no constitutional issue is created when the recipient of that e-mail directs it to police. *Id.* at 417–19.

held no privacy expectation inheres in subscriber information submitted to Internet service providers and obtained by police through the legal process.[164] The privacy policies of both MySpace and Facebook indicate those services will make required disclosures of user information to comply with court orders or subpoenas.[165]

That online social networking content may be protected under the third-party doctrine does not completely resolve the question. What do we make of the fact that much virtual user content is publicly accessible without a warrant or compulsory legal action directed toward the third-party web site? What are the Fourth Amendment implications of a user's failure to adequately safeguard her online information—by, for example, adjusting privacy controls to a more restrictive setting? Are police free to obtain a user's registration information, which users are now generally required to make public?

2. The Public Vantage Doctrine

Stated simply, the public vantage doctrine provides that no Fourth Amendment search has occurred where a law enforcement officer perceives evidence from a lawful vantage point through the use of the officer's senses.[166] Though this observation by itself does not give the officer justification to seize the evidence immediately in the absence of some valid exception to the warrant requirement,[167] the doctrine is a powerful tool that permits police to establish probable cause supporting a warrant. The doctrine acts as a boundary limiting the reasonableness of one's privacy expectation based upon the incriminating object's degree of exposure to the public at large. The public vantage doctrine maintains a tight relationship with the *Katz* test, for even in that decision the Supreme Court noted that "[w]hat a person knowingly exposes to the public, even in his own home or office, is not a

164. *See*, *e.g.*, Guest v. Leis, 255 F.3d 325, 335–36 (6th Cir. 2001); United States v. Hambrick, 55 F. Supp. 2d 504, 507 (W.D. Va. 1999), *aff'd* 225 F.3d 656 (4th Cir. 2000); United States v. Kennedy, 81 F. Supp. 2d 1103, 1110 (D. Kan. 2000).

165. Facebook.com, Facebook's Privacy Policy, *supra* note 19 ("We may disclose information pursuant to subpoenas, court orders, or other requests (including criminal and civil matters) if we have a good faith belief that the response is required by law."); MySpace.com, Privacy Policy, *supra* note 24 ("MySpace may access or disclose [personally identifiable information], Profile Information or non-[personally identifiable information] without providing you a choice in order to . . . comply with the law or legal process.").

166. Florida v. Riley, 488 U.S. 445, 449–50 (1989) (plurality opinion).

167. 1 LAFAVE, *supra* note 110, § 2.2(a), at 399–400 (right of seizure does not flow automatically from the plain view); *see also* Texas v. Brown, 460 U.S. 730, 738 (1983) (noting the "'plain view' [doctrine] provides grounds for seizure of an item when an officer's access to an object has some prior [Fourth Amendment] justification"). Thus, unlike the public vantage doctrine, the plain view doctrine permits seizure of the item observed because it is "not . . . an independent 'exception' to the Warrant Clause, but simply . . . an extension of whatever the prior justification for an officer's 'access to an object' may be." *Brown*, 460 U.S. at 738–39.

subject of Fourth Amendment protection."[168]

The breadth of the public vantage doctrine is illustrated by decisions such as *California v. Ciraolo*[169] and *Florida v. Riley*.[170] In *Ciraolo*, the Supreme Court granted certiorari to determine whether warrantless aerial observation of a fenced-in backyard from an altitude of 1,000 feet violated the Fourth Amendment.[171] Police officers responding to an anonymous report of marijuana growth in the respondent's backyard were frustrated upon discovering two layers of fencing as high as ten feet obstructing their view.[172] As a result, two officers trained in marijuana identification secured a private plane and flew over the house.[173] They observed and photographed marijuana vegetation, obtained a search warrant, and seized seventy-three marijuana plants.[174]

The Court, applying Justice Harlan's formulation of the *Katz* test, concluded the defendant's expectation of privacy in the contents of his backyard was not reasonable because "[a]ny member of the public flying in this airspace who glanced down could have seen everything that these officers observed."[175] Though the Court declined to determine whether the defendant exhibited a subjective expectation by constructing the ten-foot fence (laughably speculating the backyard may have been visible to "a citizen or a policeman perched on the top of a truck or a two-level bus"),[176] the mere possibility of public access, however implausible, was sufficient to defeat the asserted privacy interest. Not surprisingly, the majority's discussion engendered a few jeers from the four dissenting Justices, who maintained that the Court disregarded the "qualitative difference" between police surveillance and public use of the airspace for business or pleasure.[177]

In *Riley*, the Court considered "'[w]hether surveillance of the interior of a partially covered greenhouse in a residential backyard from the vantage point of a helicopter located 400 feet above the greenhouse constitutes a "search" for which a warrant is required under the Fourth Amendment.'"[178] Florida law enforcement officials had received a tip that marijuana was being grown inside the greenhouse and circled twice above the greenhouse in a helicopter

168. Katz v. United States, 389 U.S. 347, 351 (1967).
169. 476 U.S. 207 (1986).
170. 488 U.S. 445 (1989) (plurality opinion).
171. *Ciraolo*, 476 U.S. at 209.
172. *Id.*
173. *Id.*
174. *Id.* at 209–10.
175. *Id.* at 213–14.
176. *Id.* at 211–12.
177. *Id.* at 224–25 (Powell, J., dissenting).
178. Florida v. Riley, 488 U.S. 445, 447–48 (1989).

in an attempt to observe its contents. The officials correctly identified marijuana plants within the confines of the greenhouse, but were met with a motion to suppress the evidence because the flyover allegedly violated the defendant's Fourth Amendment rights.[179]

Concluding that *Ciraolo* compelled the Court's decision, Justice White authored a plurality opinion in which four Justices concluded the defendant "could not reasonably have expected that his greenhouse was protected from public or official observation from a helicopter had it been flying within the navigable airspace for [a] fixed-wing aircraft."[180] Just as in *Ciraolo*, this holding again turned upon the degree to which the defendant had exposed the evidence observed by the officials to the public.[181] Justice White extensively cited Federal Aviation Administration (FAA) regulations to support his position, arguing there was no bar on helicopter traffic at the height at which the police helicopter was traveling.[182]

Justice O'Connor concurred in the judgment and provided the fifth vote for affirming the defendant's conviction, but took pains to make clear that in her view "[t]he fact that a helicopter could conceivably observe the curtilage at virtually any altitude or angle, without violating FAA regulations, does not in itself mean that an individual has no reasonable expectation of privacy from such observation."[183] Rather, Justice O'Connor focused on "whether the helicopter was in the public airways at an altitude at which members of the public travel with sufficient regularity that Riley's expectation of privacy from aerial observation was not 'one that society is prepared to recognize as 'reasonable.'"[184] Justice O'Connor concluded that the defendant had not met the burden to prove a search had occurred because he had introduced no evidence showing the public did not use that airspace.[185]

The public vantage doctrine is a powerful tool for the government, and at least one court has used it to preclude tort recovery for privacy invasion stemming from the publication of a social networking user's profile content.[186] In *Moreno v. Hanford Sentinel, Inc.*, the plaintiff, Cynthia Moreno, wrote a poem disparaging her hometown and published it to her MySpace page.[187] Although she removed the poem six days later, she was too late; the principal of

179. *Id.* at 448–49.

180. *Id.* at 450–51.

181. "Any member of the public could legally have been flying over Riley's property in a helicopter at the altitude of 400 feet and could have observed Riley's greenhouse." *Id.* at 451.

182. *Id.* at 451 n.3.

183. *Id.* at 454 (O'Connor, J., concurring).

184. *Id.* (quoting Katz v. United States, 389 U.S. 347, 361 (1967)).

185. *Id.* at 455 (O'Connor, J., concurring).

186. Moreno v. Hanford Sentinel, Inc., 91 Cal. Rptr. 3d 858 (Cal. Ct. App. 2009).

187. *Id.* at 861.

a local high school submitted the poem to a local newspaper, which published it and attributed it to Cynthia.[188] In her suit against the newspaper, Cynthia argued the publication was a tortious violation of her privacy rights. Although the court acknowledged "'[i]nformation disclosed to a few people may remain private[,]'"[189] it reasoned that "[b]y posting the article on myspace.com, Cynthia opened the article to the public at large."[190] "Under these circumstances," the court stated, "no reasonable person would have an expectation of privacy regarding the published material."[191]

Courts have reached similar conclusions in cases concerning public "chat rooms" or electronic bulletin boards in which users may virtually converse with one another and oftentimes share images or documents as well. "Messages sent to the public at large in the 'chat room' or e-mail that is 'forwarded' from correspondent to correspondent lose any semblance of privacy," declared the *Maxwell* court.[192] In *Guest v. Leis*, the court found no violation of the Fourth Amendment where government officers assumed undercover identities, accessed an electronic bulletin board, and downloaded sample images, because "[u]sers would logically lack a legitimate expectation of privacy in the materials intended for publication or public posting."[193]

At first blush, the public vantage doctrine appears to doom any asserted privacy expectation in public social networking content. Since authorities may be lawfully present in any space open to the public, nothing prevents police from patrolling web sites as they would a public street without first obtaining a warrant. This means a great deal of user information could be viewed by government officials, since many users never adopt more restrictive privacy settings. Even where a sophisticated user has done so, a significant amount of information remains publicly accessible—on Facebook, for example, this includes a user's name, profile photo, gender, and networks.[194]

This is not an obvious result. While a chat room or electronic bulletin board user might intend to broadcast his or her messages to the world at large, this is increasingly not true of social networking users. Privacy settings

188. *Id.*

189. *Id.* at 863 (quoting M.G. v. Time Warner, Inc., 107 Cal. Rptr. 2d 504, 511 (Cal. Ct. App. 2001)).

190. *Id.*

191. *Id.* at 862.

192. United States v. Maxwell, 45 M.J. 406, 419 (C.A.A.F. 1996). The court suggested that as the number of recipients increases, the sender's privacy expectations decrease. *Id.* This discussion may simply reflect that as the number of recipients increases, so too does the risk that one or more of the recipients will communicate with the police.

193. 255 F.3d 325, 333 (6th Cir. 2001).

194. Facebook.com, Facebook's Privacy Policy, *supra* note 19, § 3; *see also* Richmond, *supra* note 8.

remain an advanced feature of social networking web sites, and their modification requires some degree of user sophistication. Thus, many users who may not wish to share profile content with the public nonetheless do so because they lack sufficient knowledge of the web site's operation to effectively change these settings and accomplish the desired restrictions.

Recent social science data underscore the extent to which users may be unaware that their profile information is public. A January 2009 study found that 42% of sampled MySpace users between the ages of eighteen and twenty who displayed risk behaviors changed their profiles within a month of being informed their profiles were publicly viewable.[195] This finding is consistent with the observation that many Internet users simply do not possess, and do not feel that they need to obtain, an in-depth understanding of a social networking web site's operation to fully utilize it. For most users, it is sufficient that they know how to create a profile and virtually socialize. The web sites have also contributed to the diminishing need for this knowledge by developing fast and easy sign-up processes and encouraging mobile use.[196] Indeed, setting up a profile is "so easy that, quite literally, a child could do it."[197]

The intent to publish normally inferred from the use of a public electronic bulletin board or chat room cannot be inferred from the use of social networking web sites. Even those users who are aware of the web site's privacy settings and possess the technical competence necessary to achieve the desired level of privacy may wish to leave the settings in their default state. This does not necessarily demonstrate an intention to publish profile content to the world at large, but for these users more likely reflects a recognition that restrictive privacy settings are somewhat inconsistent with the purpose of online social networking in the first instance. A user must allow some degree of access to her profile if she intends to meet other members through the web site. To the extent privacy restrictions impair the members' ability to fully utilize social networking services, they defeat one of the

195. Erica Perez, *Many Teens Divulge Risk Behaviors Online, Study Says*, MILWAUKEE J. SENTINEL, Jan. 7, 2009, at 1B (citing Moreno et al., *supra* note 62). The authors of the study conceded that they could not "determine the active ingredient of the intervention with certainty[,]" but acknowledged that one mechanism through which the intervention may have affected the removal decision "is that by reading our e-mail message, adolescents may have realized how publicly available their [social networking] profiles have become." Moreno et al., *supra* note 62, at 39.

196. *See* Abril, *supra* note 13, at 74; Guo, *supra* note 13, at 620; *see also* Adam M. Gershowitz, *The iPhone Meets the Fourth Amendment*, 56 UCLA L. REV. 27, 43 (2008) (noting police seizure of a person's cell phone may expose social networking content that "might be rich sources of incriminating information").

197. Sasha Leonhardt, *The Future of "Fair and Balanced": The Fairness Doctrine, Net Neutrality, and the Internet*, 2009 DUKE L. & TECH. REV. 8, ¶ 27, http://www.law.duke.edu/journals/dltr/articles/2009dltr008.html.

principal functions of these web sites.[198]

Application of the public vantage doctrine rests, of course, upon the user's profile being publicly accessible. The doctrine has no application where a user has modified her privacy settings to restrict access to content.[199] What result should occur where a user has demonstrated a subjective intention to shield online information from prying eyes by limiting disclosure to friends?[200]

3. The Misplaced Confidences Doctrine

If a user has taken affirmative steps to limit profile access, a police observer's attempts to access most potentially incriminating information will be frustrated. Rarely has an officer's initial lack of success at gaining access to incriminating information ended the matter. In the social networking context, authorities have two ways to obtain information about a user if they find his profile restricted.

First, a police officer may create a profile and convince the targeted user to add her as a friend. The officer may create a legitimate profile in hopes that the user indiscriminately accepts friend requests, or may adopt a technique popular among chat room investigators and create an alternate persona—perhaps a fictional person who shares many of the user's publicly observable characteristics.

In the alternative, the officer may use publicly available information to seek out individuals whom the officer believes the user has befriended online.[201] Nothing prevents police from obtaining incriminating information directly from these virtual friends, who have access to the suspect's profile content by virtue of their online connection.

Both methods are permissible according to the misplaced confidences doctrine, a slight variation of the third-party doctrine that traces its roots to *Hoffa v. United States*.[202] In *Hoffa*, an informant accompanying James Hoffa throughout his trial for violations of the Taft-Hartley Act reported to federal

198. *See* Hodge, *supra* note 11, at 116 ("[U]sers sign up to connect to friends and give these friends their information."). As another commentator has noted, "voluntary disclosure of personal information and gossip about others are sources of intimacy and lead to healthy interpersonal relations." Abril, *supra* note 13, at 85.

199. This is not true if profile sections that always remain public contain the incriminating information.

200. This proposition is consistent with another commentator's conclusion about the Fourth Amendment's application to a limited online social networking profile. *See* Hodge, *supra* note 11, at 115–16.

201. Note this investigative method may not be permissible if the public vantage doctrine does not apply to social networking information. *See supra* notes 194–198 and accompanying text.

202. 385 U.S. 293 (1966).

agents conversations in which Hoffa discussed bribing members of the jury.[203] Responding to Hoffa's contention that the government's use of an informant violated the Fourth Amendment, the Court noted Hoffa merely relied upon his "misplaced confidence" that those with whom Hoffa was conversing would not reveal his wrongdoing.[204] In the Court's view, the Fourth Amendment does not protect "a wrongdoer's misplaced belief that a person to whom he voluntarily confides his wrongdoing will not reveal it."[205]

The seminal misplaced confidences case is *United States v. Miller*,[206] in which the government obtained Miller's financial information from banks, pursuant to defective subpoenas, and used it to convict him of defrauding the United States of tax revenue.[207] Miller challenged the evidence, arguing the documents were illegally seized in violation of his Fourth Amendment rights.[208] The Supreme Court upheld Miller's conviction, concluding Miller possessed no protectable privacy interest in the bank documents because, once shared with the bank, the account records were not Miller's "private papers."[209] Citing the old *Katz* law that "[w]hat a person knowingly exposes to the public . . . is not a subject of Fourth Amendment protection,"[210] the Court noted "[a]ll of the documents obtained, including financial statements and deposit slips, contain only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business."[211] From this, it reasoned:

> The depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government. This Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.[212]

This rule does not operate differently when the evidence in question is derived from electronic communications, rather than from in-person

203. *Id.* at 294–95.
204. *Id.* at 302.
205. *Id.*
206. 425 U.S. 435 (1976).
207. *Id.* at 436.
208. *Id.* at 437.
209. *Id.* at 440–41.
210. Katz v. United States, 389 U.S. 347, 351 (1967).
211. *Miller*, 425 U.S. at 442.
212. *Id.* at 443 (citations omitted).

conversations. The misplaced confidences doctrine has been applied to dispel asserted privacy expectations in e-mail[213] and chat room conversations.[214] Indeed, where disclosure to the government occurs through the recipient, the communicator's privacy expectation in the content of the communication generally will be defeated, regardless of the medium used.

While the misplaced confidences doctrine is a fairly straightforward rule, it has serious implications for a social networking user's privacy. Unlike the third-party doctrine, it permits government officials to obtain user content without legal compulsion. The only way a user may protect his content from this type of disclosure is by carefully selecting which friends he adds. This is, of course, easy to preach but difficult to practice. Online social networks are designed to share information among large groups, and individuals who request another's virtual friendship and are rejected may feel slighted. It is often easier for users to accept all friend requests, or all those in a particular group (say, coworkers), than to pick and choose whom to add and whom to reject. As the *Maxwell* court recognized, there is a direct relationship between the number of recipients and the risk that one or more of them will use the information (be it a photograph, video, or status update) in a way harmful to the communicator.[215]

V. THE IMPORTANCE OF PROTECTION FOR ONLINE SOCIAL NETWORKING USER CONTENT

Although application of the Court's search jurisprudence to new communicative technology presents difficult questions, there is little doubt courts will be called upon to provide answers as online social networking becomes more prevalent. As the foregoing discussion has demonstrated, the Court's current Fourth Amendment doctrines suggest a user might maintain a reasonable expectation of privacy in his online profile content unless he misplaces confidence in a virtual friend who reveals incriminating content to authorities. This is by no means a clear result, and, in this Part, I wish to highlight two practical consequences of the refusal to extend Fourth Amendment protection to online social networking content.

First, non-recognition of privacy expectations in online social networking content threatens to erode protection for a wide range of commonly disclosed information. In *Kyllo v. United States*, the Court suggested technology can indeed "shrink the realm of guaranteed privacy."[216] Although the Court held

213. Commonwealth v. Proetto, 771 A.2d 823, 831 (Pa. Super. Ct. 2001); United States v. Maxwell, 45 M.J. 406, 417 (C.A.A.F. 1996).

214. *Proetto*, 771 A.2d at 832; United States v. Charbonneau, 979 F. Supp. 1177, 1178–79 (S.D. Ohio 1997).

215. *Maxwell*, 45 M.J. at 419.

216. 533 U.S. 27, 34 (2001).

that a "search" occurred when law enforcement officers scanned the defendant's home using thermal imaging systems in an attempt to identify warmer portions that might house high-intensity lamps used for growing marijuana,[217] the fact that thermal imaging technology was not in use by the general public was critical to the Court's analysis.[218]

The Court's analysis suggests information revealed by publicly used technology is not entitled to Fourth Amendment protection. Online social networking has already become a practice widely embraced by the masses, and many individuals apparently have little reservation displaying intimate details of their lives on a Facebook profile. This includes a great deal of information many individuals in our society would deem private, including one's sexual preferences or favorite books. If the court's "general public use" analysis is to have future significance (and it is not clear it will), privacy expectations in this type of information may be unreasonable in the future. Given the staggering growth rates of social networking web sites, this prediction may not be all that far-fetched.

Unregulated police surveillance of social networking users also potentially burdens the exercise of well-established constitutional rights. "[T]he Court has recognized a right to associate for the purpose of engaging in those activities protected by the First Amendment—speech, assembly, petition for the redress of grievances, and the exercise of religion."[219] "This right is crucial in preventing the majority from imposing its views on groups that would rather express other, perhaps unpopular, ideas."[220] Further, an individual's choice to "enter into and maintain certain intimate human relationships" is a "fundamental element of personal liberty" protected against encroachment by the state.[221] Indeed, government action infringing these expressive associations must serve compelling state interests, unrelated to the suppression of ideas, that cannot be achieved through "means significantly less restrictive of associational freedoms."[222]

Police scrutiny of social networking web sites threatens to undermine these associational interests "by providing the government with means to obtain information about group membership."[223] Information collection

---

217. *Id.* at 29.

218. *Id.* at 34.

219. Roberts v. U.S. Jaycees, 468 U.S. 609, 618 (1984); *see also* Kusper v. Pontikes, 414 U.S. 51, 56–57 (1973) ("There can no longer be any doubt that freedom to associate with others for the common advancement of political beliefs and ideas is a form of 'orderly group activity' protected by the First and Fourteenth Amendments.").

220. Boy Scouts of Am. v. Dale, 530 U.S. 640, 647–48 (2000).

221. *Roberts*, 468 U.S. at 617–18.

222. *Id.* at 623.

223. *See* Strandburg, *supra* note 155, at 769.

"impairs expressive activity not directly through regulation, but indirectly through deterrence."[224] Thus, unrestrained police scrutiny of social networking web sites threatens to chill the formation of protected associations in several ways: by disclosing their existence and membership, by creating the potential for legitimate associations to be unfairly scrutinized, and by the risk that some individuals will be treated as a member of a group to which they did not wish to be associated.[225] Viewing the Fourth Amendment through this "special First Amendment lens" provides additional support for crediting an individual's asserted privacy expectation in online social networking content.[226]

VI. CONCLUSION

The brave new technological world envisioned by Justice Thomas, and the corresponding merger of the public and private spheres, creates difficult constitutional questions. As social networking services grow in popularity, they will be frequently utilized by authorities to gather information and pursue criminal investigations. While existing Fourth Amendment doctrine, built around envelopes and telephones, is difficult to apply in these circumstances, the analogy suggests police must first obtain a warrant before scrutinizing online profile content, unless acting pursuant to the misplaced confidences doctrine. In addition to preserving user associational freedoms and non-user privacy interests, this result has the added benefit of restoring significance to *Katz*'s recognition that the role of technology in facilitating communication is important.

NATHAN PETRASHEK*

224. *See id.* at 785.

225. *See id.* at 785–86.

226. *Id.* at 795.

* J.D. 2009, Marquette University Law School. Law Clerk to the Honorable Edward R. Brunner, Wisconsin Court of Appeals (2009–2011). I would like to thank my family, especially my parents, for their unwavering support.