APPLYING MODEL RULE 4.2 TO WEB 2.0: THE PROBLEM OF SOCIAL NETWORKING SITES

YVETTE OSTOLAZA AND RICARDO PELLAFONE*

Cite as 11 J. HIGH TECH. L. 56 (2010)

I. Introduction

Model Rule of Professional Conduct 4.2 ("Rule 4.2") is the current version of the profession's "no-contact" rule.[1] It generally prohibits an attorney from communicating about the subject matter of a representation with a person that the attorney knows to be represented by another attorney in the matter.[2] Although its application has historically been rather straightforward, recent developments in online communication have complicated matters.[3] In particular, the surge in popularity of dynamic, user-driven websites that employ complex privacy mechanisms—websites such as Facebook.com ("Facebook") and MySpace.com ("MySpace")—presents a new challenge to courts and ethics committees seeking to interpret Rule 4.2: with millions of individuals now maintaining profiles on these, or similar, websites, how far can an attorney go in an effort to obtain

* Ms. Ostolaza is the co-head of the Complex Commercial Litigation Practice Group of Weil, Gotshal & Manges LLP; Mr. Pellafone is an associate in that group. The authors thank Matthias Kleinsasser for his assistance in researching this article.

1. *See* Geoffrey C. Hazard, Jr. & Dana Remus Irwin, *Toward A Revised 4.2 No-Contact Rule*, 60 HASTINGS L.J. 797, 797-800 (2009) (discussing the history of the "no-contact" rule and its current incarnation as Rule 4.2).

2. *See* MODEL RULES OF PROF'L CONDUCT R. 4.2 (2007) (detailing the restriction on attorney communication with a represented party).

3. *See infra* notes 9-10 (discussing the evolution of websites into more dynamic forms).

 ISSN 1536-7983.

information about a represented party from one of these sites?[4]

In the past, authorities that have attempted to apply Rule 4.2 to websites (and recently, public pages on social networking sites) have done so by holding that they are the equivalent of a book or magazine article, reasoning that this online conduct should be judged by the same rule as its offline counterpart.[5] And initially, this approach made sense; the first wave of online content generation and communication was largely static and inherently public in nature,[6] such that the creation of a personal website was at least roughly analogous to the offline publication of materials.[7]

4. *See* MODEL RULES OF PROF'L CONDUCT R. 4.2 cmt. 5 (2007) (using an investigative agent as an example of legal communication that must nevertheless comply with Rule 4.2). Rule 4.2 applies equally to an investigator acting at the direction of an attorney, but we exclusively use "attorney" throughout this Article for two reasons. *See id.* This is important for brevity and because the type of investigative work discussed in Part III can be done by an attorney for no cost, within minutes, from any computer with an Internet connection. *See infra* note 70 (using Google cache as an example of the ease in finding a user's MySpace profile). As a result, we predict it will be more likely for attorneys will simply attempt these online investigations themselves. *See infra* note 69 (detailing an attorney's use of MySpace in investigating insurance fraud).

5. *See, e.g.*, Oregon State Bar Ass'n Bd. of Governors, Formal Op. 2005-164, 452-53 (2005) [hereinafter 2005 Oregon Op.] (stating that electronic and nonelectronic forms of contact are indistinguishable); Oregon State Bar Ass'n Bd. of Governors, Formal Op. 2001-164, 1-2 (2001) (withdrawn 2004) [hereinafter 2001 Oregon Op.] (noting the similarity between viewing information on a passive website and reading a newspaper). The 2005 Oregon Opinion states that "[f]or purposes of this opinion, there is no reason to distinguish between electronic or nonelectronic forms of contact. Both are permitted or both are prohibited. Accessing an adversary's public website is no different from reading a magazine article or purchasing a book written by that adversary." 2005 Oregon Op., at 453. The 2001 Oregon Opinion states that "[v]iewing (or even downloading) information posted on a passive site is the equivalent of reading a newspaper, magazine, or other document available for public consumption. Following links to other websites is the equivalent of turning pages or locating other issues of the publication." 2001 Oregon Op., at 2. *See also* N.Y. State Bar Assoc. Comm. on Prof. Ethics, Op. 843 (2010). In determining whether an attorney could view a represented litigant's public profiles (as defined herein) on Facebook and MySpace, the New York Bar Association Committee on Professional Ethics reasoned that this was permissible because it was "similar to obtaining information that is available in publicly accessible online or print media."

6. *See* Jonathan Strickland, *Is There a Web 1.0?*, HOWSTUFFWORKS, Aug. 30,

But things have changed.[8] The paradigm for Internet usage today is no longer dominated by static, proprietary websites.[9] Instead, the second wave of web design—often referred to by the marketing term "Web 2.0"[10]—is marked by collaborative content generation on user-friendly platforms.[11] Users do not have to know any coding language, understand FTP, or even invest the time to learn the interface of a simple web design tool; they simply have to input text into boxes, and their web presence is established.[12]

In many cases, this takes the form of creating a profile on a social networking site such as Facebook.[13] The way that Facebook and other social networking sites have lowered the barriers to online publication dramatically impacts their ability to be compared to an offline publication; the way a user with minimal computer skills can quickly publish content on a social networking site bears little relation to the process of generating a static website during the "Web 1.0" era—let alone the process of publishing an offline book or article.[14]

2010, *archived at* http://www.webcitation.org/5sNHIgwde (identifying first-wave web design as "static" and not "interactive").

7. *See infra* note 12 (outlining the limited nature of early social networking sites).

8. *See infra* notes 9-10 (comparing the differences between "Web 1.0" and "Web 2.0").

9. See *DAVID WEINBERGER, EVERYTHING IS MISCELLANEOUS THE POWER OF THE NEW DIGITAL DISORDER (2007) (indicating the evolving nature of social networking sites and the Internet in general).*

10. *See id.* (introducing the concept of "Web 2.0"); *see also* Tim O'Reilly, *What is Web 2.0*, O'REILLY MEDIA, Sept. 30, 2005, *archived at* http://www.webcitation.org/5sNbSbKvX (discussing Web 2.0 as a concept). Although O'Reilly Media is credited with coining the term, sources vary on the exact identity of its progenitor. *See id.; compare* Dylan Tweney, *Tim O'Reilly: Web 2.0 Is About Controlling Data*, WIRED, Apr. 13, 2007, *archived at* http://www.webcitation.org/5uO4JVSRa (quoting "It's not too late to get on the 'web 2.0' bandwagon, [sic] says publishing magnate Tim O'Reilly, who coined the term."), *with* Strickland, *supra* note 6 (crediting "Dale Dougherty of O'Reilly Media" with coining the term "Web. 2.0").

11. *See* O'Reilly, *supra* note 10 (discussing the beneficial changes of the Web 2.0 platform).

12. *See* Danah M. Boyd & Nicole B. Ellison, *Social Network Sites: Definition, History, and Scholarship,* 13 J. OF COMPUTER-MEDIATED COMM. 1 (2007), *archived at* http://www.webcitation.org/5subDikzL (reviewing the ease of creating a social networking profile for Web 2.0 users).

13. *See* Boyd & Ellison, *supra* note 12 (explaining how a web presence is established). Facebook is the second-most popular website on the Internet in

More importantly, these social networking sites offer complex privacy structures that users can choose to implement to protect their content from prying eyes.[15] Rather than making a profile public or only available to a pre-selected few, social networking sites also allow users to create more nuanced privacy settings that grant or deny access to other users based on the settings they have in their own profiles.[16] For example, a user can create a privacy setting that only allows access to other users who have verified that they work at a certain company by registering a company e-mail address with the social networking site.[17] There are no such books or magazines that employ this kind of privacy structure; these sites create scenarios that simply do not exist in the offline world.[18]

Thus, as the nature of online communication continues to grow increasingly complex—and by doing so, moves even further away from resembling offline publishing—a different analysis is necessary in order to promote a consistent, predictable approach to the application of Rule 4.2.[19] In this Article, we argue that the observation exception to Rule 4.2 supplies that analysis.[20] To that end, Part I of this Article describes and defines social networking sites, what kind of profiles they contain, and how

terms of traffic; at the end of 2010, over 37% percent of the world's Internet users visited Facebook daily, on average. *See Facebook.com,* ALEXA.COM, January 4, 2011, *archived at* http://www.webcitation.org/5vZCOhD8c (providing Internet traffic statistics for Facebook.com).

14. *See* Boyd & Ellison, *supra* note 12 (describing the ease of creating a web presence in the Web 2.0 era).

15. *See* Boyd & Ellison, *supra* note 12 (detailing social networking site privacy settings).

16. *See Help Center: Privacy*, FACEBOOK.COM, January 4, 2011, *archived at* http://www.webcitation.org/5vZCx7dy0(outlining Facebook's privacy options).

17. *See id.* (listing Facebook's privacy setting menu choices).

18. *See* Boyd & Ellison, *supra* note 12 (discussing how the "backbone" of social networking sites allows a user to control the content of their profiles). *See also Help Center: Privacy*, *supra* note 16 (setting out the varying options of control users can exercise over their profile content).

19. *See* Boyd & Ellison, *supra* note 12 (referencing online communication's rapid growth and its trend away from traditional offline publishing).

20. *See infra* Part II.A-B (providing the definition of the "observation exception").

they can be used in litigation.[21] Part II discusses Rule 4.2 and how it has been applied to websites (including public social networking profiles) in the past, arguing that this approach does not adequately account for the unique situations presented by recent trends in online content, and that the observation exception to Rule 4.2 provides the appropriate analytical framework.[22] Part III applies the observation exception to social networking profiles, concluding that "public" and some "network" profiles fall under the exception, while other "network" profiles and all "private" profiles do not.[23] Part IV concludes.

II. Social Networking Sites: Defined, Profiles Types, and Usage

This Part introduces the concept of a social networking site and provides a definition of the term. It then categorizes social networking profiles into three categories based on the type and degree of privacy controls that a user has chosen to employ. Finally, this Part describes the potential uses that social networking sites have in litigation.

A. Social Networking Sites: Defined

For purposes of this Article, we define a "social networking site" as a web-based service that allows individuals to (1) construct a public, semi-public, or private profile within a bounded system ("social networking profile"), (2) articulate a list of other users with whom they share a connection, either prior to the creation of the profile or by virtue of the social networking site, and (3) view and traverse their list of connections and those made by others within the system.[24] Users log on to social

21. *See infra* Part I (defining social networking sites and potential litigation uses).
22. *See infra* Part II (discussing Rule 4.2 and application of the observation exception).
23. *See infra* Part III (describing what types of social networking profiles fall under the observation exception).
24. *See* Boyd & Ellison, *supra* note 12 (defining social network sites). Boyd & Ellison note:
[W]e define social network sites as web-based services that allow individuals to (1) construct a public or semi-public profile within a bounded system, (2)

networking sites to articulate, make public, and expand their existing, offline social and professional networks.[25] Depending on the social networking site, users can create profiles with background information, post photos, provide short updates about what they are doing at that time, link their profile to others, join groups or networks, and view and track the profiles of other users.[26] These features can also be used for business and marketing purposes.[27] Social networking sites are generally free,[28] although some sites charge for certain features.[29]
It would be difficult to overstate the popularity of social networking sites, particularly considering their relative youth.[30] These sites are part of the "Web 2.0" concept, a marketing phrase coined after the crash of the dot-com bubble in 2001 that predicted the future of Internet business as driven by dynamic,

articulate a list of other users with whom they share a connection, and (3) view and traverse their list of connections and those made by others within the system.
Id.
We have expanded Boyd and Ellison's definition of "social network site" to target the concerns implicated by Rule 4.2, as well as features present in certain sites that provide their litigation use—in particular, proactive business networking. *Id.* Accordingly, we use "social networking site" instead of "social network site" to reflect that particular function and avoid confusion. *Id.*

25. *See* Boyd & Ellison, *supra* note 12 (reviewing various ways in which users may use social networking sites).

26. *See* Boyd & Ellison, *supra* note 12 (describing range of options users have when posting information on their social networking sites).

27. *See* Boyd & Ellison, *supra* note 12 (indicating that the use of social networking sites is not limited to individuals). Boyd and Ellison's definition of a "social network site" excludes explicit networking. *See id.* As previously stated, we have adapted their definition for this Article to include this feature. *See also supra* text accompanying note 24 (expanding the definition of "social networking site"). For a discussion of social networking sites' popularity in the legal world as a means of networking, see Brian Malcolm, *Trends: This Just In . . . Lawyers Like Web 2.0*, YOUNG LAWYERS BLOG, July 22, 2009, *archived at* http://www.webcitation.org/5sOxe5VXS (discussing the popularity of social networking sites with attorneys).

28. *See, e.g.*, *Welcome to Facebook!,* FACEBOOK.COM, Oct. 12, 2010, *archived at* http://www.webcitation.org/5tQbzMQHp (offering users to "[s]ign Up . . . It's free and always will be."); *MySpace*, MYSPACE.COM, Aug. 31, 2010, *archived at* http://www.webcitation.org/5uS19mD2b (stating "All Your Faves For Free… Free Music... Free Games… Free TV").

29. *See Compare Account Types*, LINKEDIN.COM, Aug. 31, 2010, *archived at* http://www.webcitation.org/5sOzOsoMd (describing LinkedIn's different account types and premium features).

30. *See* Boyd & Ellison, *supra* note 12 (discussing the growing popularity of social networking sites between 1997 and 2007).

platform-based, user-driven and collaborative content—as opposed to the static, controlled, and pre-packaged nature of pre-crash web content.[31] Indeed, neither Facebook nor MySpace existed seven years ago.[32] Today, they are the second[33] and forty-seventh[34] most-popular websites on the Internet, with Facebook alone claiming over 500 million active users.[35] Similarly, LinkedIn.com ("LinkedIn"), the most popular social networking site focused on business networking, was launched in May 2003;[36] it currently has over ninety million registered users,[37] and is the twenty-second most popular website on the Internet.[38]

B. Types of Social Networking Profiles

Because of their dynamic nature and variety of uses, social networking profiles can be categorized in a variety of ways. For

31. *See* O'Reilly, *supra* note 10 (defining "Web 2.0" and showing myriad ways in which "Web 2.0" is versatile); *see also* Malcolm, *supra* note 27 (arguing that Web 2.0 was particularly important during the 2008-2009 recession).

32. *See Facebook Factsheet,* FACEBOOK.COM, Oct. 12, 2010, *archived at* http://www.webcitation.org/5tQbvXagy (noting that Facebook.com was founded in 2004); *see also* Richard Siklos, *News Corp. to Acquire Owner of MySpace.com*, N.Y. TIMES, July 18, 2005, *archived at* http://www.webcitation.org/5sQEulVJi (stating that MySpace.com was launched in 2003).

33. *See* ALEXA.COM, *supra* note 13 (finding that Facebook.com is the second-most popular social networking site).

34. *See Myspace.com*, ALEXA.COM, January 4, 2011, *archived at* http://www.webcitation.org/5vZD6MgbL (providing MySpace.com's popularity ranking).

35. *Press Room*, (December 30, 2010), *archived at* http://www.webcitation.org/5vZDYQKtM (providing the estimated number of Facebook users). Note that this figure represents the number of "active" accounts; the question of how many individuals actually use a given social networking site is debatable. *See id. See also* Barbarian, *Debunking the MySpace Myth of 100 Million Users*, FOREVERGEEK (Sept. 27, 2006), *archived at* http://www.webcitation.org/5sQGFK6dU (disagreeing with claims that MySpace has 100 million users).

36. *Company History*, LINKEDIN.COM, Sept. 1, 2010, *archived at* http://www.webcitation.org/5sQGw5IWw (showing that LinkedIn.com was launched in 2003).

37. *See About Us,* LINKEDIN.COM, *archived at* http://www.webcitation.org/5vZDzVXyD (providing estimated number of LinkedIn.com users).

38. *See LinkedIn.com Site Info*, ALEXA.COM, Dec. 30, 2010, *archived at* http://www.webcitation.org/5vZE9ei1p (showing LinkedIn.com's popularity ranking).

example, certain social networking sites now delineate between personal profiles and those maintained for a business;[39] others offer special profiles for certain professions.[40] Here, the relevant factor is the amount and kind of privacy measures a user has chosen to apply to their profile.[41] Although social networking sites vary in how they allow users to protect their profiles from prying eyes—and privacy policies and measures tend to change rapidly, both in granting users more protection and taking it away—user profiles can be categorized into one of three types based on the privacy controls that have been applied to their accessibility.[42]

39. *Compare Welcome to Facebook!*, FACEBOOK.COM, Oct. 12 2010, *archived at* http://www.webcitation.org/5tQbzMQHp (offering option to sign up as a business instead of as an individual), *with Create a Page*, FACEBOOK.COM, Oct. 12, 2010, *archived at* http://www.webcitation.org/5tQbp6U5H (showing the sign-up page for businesses).

40. *See Signup for MySpace*, MYSPACE.COM, January 4, 2011, *archived at* http://www.webcitation.org/5vZEGDu8j signup (showing different options for musicians, comedians, and filmmakers, as well as the standard form for creating personal profiles).

41. *See Help Center: Privacy*, *supra* note 16 (showing Facebook's options for privacy settings). The privacy controls a represented party chooses to implement dictates how intrusive an attorney must be in order to view their profile; loosely-controlled profiles can be viewed by anyone, while tight controls mean that the profile's owner has to give explicit permission to any person wishing to view their profile. *See id.* It is this continuum of interaction between the attorney and the represented party that is implicated by Rule 4.2; thus, it is appropriate to categorize social networking profiles on this basis. *See* MODEL RULES OF PROF'L CONDUCT R. 4.2 cmt. 4 (2007) (providing examples of permitted communications).

42. *See* Dan Farber, *Facebook Beacon update: No activities published without users proactively consenting*, ZDNET: BETWEEN THE LINES, Nov. 29, 2007, *archived at* http://www.webcitation.org/5sQMkdh8A (describing Facebook's Beacon update and its potential problems). Facebook's launch of its Beacon feature in 2007 probably presents the most notorious example of a social networking site changing privacy policies to make user profiles more public. *Id.* This feature allowed users to share their habits on participating websites with their Facebook friends. *Id.* For example, if a user allowed reviews they posted to Yelp.com ("Yelp!") to be shared with Facebook, their Facebook friends would receive an automatic notification any time they posted a new review to Yelp!, so long as the user was logged into Facebook when posting the review. *Id.* This feature represented a potential advertising goldmine for Facebook, but it launched as an "opt-out" service, with all users automatically enrolled, resulting in their activity on numerous websites being broadcast on Facebook. *Id.* Facing withering criticism from privacy advocates and users, Facebook changed the service to "opt-in" within a month. *Id.; see also* Brad Stone, *Facebook Executive Discusses Beacon Brouhaha*, N.Y. TIMES BLOG (Nov. 29, 2007), *archived at* http://www.webcitation.org/5sQOBDmXo (discussing the features of Facebook's Beacon update); Louise Story and Brad Stone, *Facebook*

1. Public Profiles

The first category is the public profile.[43] We define a public profile as a social networking profile that has no privacy controls applied to it, and which can be accessed by any member of the public.[44] Some social networking sites require individuals to register with the site before they can view a public profile, while others allow any Internet user to view the profiles directly.[45] They can be easily found by searching the relevant social networking site, and they are generally indexed in full by search engines.[46] This is the default setting for some sites upon sign-up.[47] And although it is generally easy for a user to adopt

Retreats on Online Tracking, N.Y. TIMES, Nov. 30, 2007, *archived at* http://www.webcitation.org/5sQP0H6nC (explaining the decision to alter the website tracking feature, Beacon). Alternatively, MySpace has repeatedly had its privacy features compromised by relatively simple work-arounds that even individuals with minimal computer skills can exploit. *See How Private Are Private MySpace Profiles?*, MYSPACEMASTER BLOG (June 16, 2008), *archived at* http://www.webcitation.org/5sQPPhlrg (addressing the profile privacy options on MySpace).

43. *See Help Center: Privacy: Privacy Settings and Fundamentals*, January 4, 2011, *archived at* http://www.webcitation.org/5vZERZaQi (detailing options that allow a user to make their profile open to the public).

44. *See id.* (offering options to allow a user to control how others view his or her profile).

45. *See, e.g., Profile of Tom Anderson*, MYSPACE.COM, Sept. 1, 2010, *archived at* http://www.webcitation.org/5sQRoahZ2 (showing that profile of one of MySpace's founders, Tom Anderson, is accessible without logging in).

46. *See Profile of Tom Anderson,* MYSPACE.COM, *supra* note 45 (noting that Anderson's profile is easily located within an Internet search); Pete Cashmore, *Facebook Profiles Will Appear in Google Results Next Month*, MASHABLE.COM, Sept. 5, 2007, *archived at* http://www.webcitation.org/5sQfqjlkq (describing how Google began indexing public profiles); *Facebook's Privacy Policy*, FACEBOOK.COM, January 4, 2011, *archived at* http://www.webcitation.org/5vZEhav7z (describing how Facebook's default privacy setting for certain information is public); *Search: Public search listings on Internet search,* FACEBOOK.COM, Oct. 12, 2010, *archived at* http://www.webcitation.org/5tQgVqy8e (default setting for Facebook users over eighteen years of age allows search engine indexing). Facebook does not provide privacy settings for a user's name and profile picture, which are always public. *See Facebook's Privacy Policy, supra* note 46 (noting lack of privacy settings for certain information).

47. *See* Boyd & Ellison, *supra* note 12 (discussing default privacy settings of several social networking sites); *see also* Annika Mengisen, *Besmirching Ourselves Online: A Q&A With the Author of* The Future of Reputation, N.Y. TIMES, Apr. 29, 2008, *archived at* http://www.webcitation.org/5vLVSl6lF (observing that several social networking sites have public access as default setting). In interviewing the author of *The Future of Reputation*, Mengisen writes:

more stringent privacy settings, many do not–Facebook estimated in 2009 that 80% of its users did not enact any privacy controls.[48]

2. Private Profiles

At the opposite end of the spectrum is the private profile. We define a "private profile" as a social networking profile that can only be viewed by another user who has been individually granted access by the profile's owner.[49] That is, anyone who wishes to view a private profile must first contact the profile's owner for permission.[50] This is typically done via a "friend request," which is an automated message that a user can send to another user to request access to their profile, typically allowing the recipient to view the sender's profile in return; in some cases, the recipient will be granted automatic access to the sender's profile for a limited amount of time without having to approve the friend request in order to help them determine if they should

Q: You say the design choices of websites and their default settings have an enormous impact on privacy. Can you suggest a way a current website might be changed to improve privacy along these lines?
A: Many social network websites are set up with a default setting that makes information fully available to the public. This is the easiest setting, and many people just go with the default.
. . . .
If sites were structured to set the defaults toward making disclosure more restricted, it would help matters quite a bit—and make people think before exposing information to the entire world.
Id.

48. *See* Brad Stone, *Is Facebook Growing Up Too Fast?*, N.Y. TIMES, Mar. 28, 2009, at BU1, *archived at* http://www.webcitation.org/5sT4982uy (noting that a mere twenty percent of Facebook users take advantage of the offered privacy settings). Additionally, many social networking sites have found that promoting their privacy features turns off potential users, resulting in these sites downplaying those features. *See* Karl Flinders, *Privacy Rankings: LinkedIn and Bebo high, Facebook and MySpace average, Badoo low*, COMPUTERWEEKLY.COM, July 21, 2009, *archived at* http://www.webcitation.org/5sT590M9Z (noting that because open discussion of privacy disaffects users, websites do not produce "explicit or accessible" privacy guidelines).

49. *See Privacy: Who Can See My Profile and Content?*, FACEBOOK.COM, Oct. 12, 2010, *archived at* http://www.webcitation.org/5tQayRf4I (noting that "[w]ith the most private option, 'Only Friends,' only users who are your confirmed friends will be able to see your profile.").

50. *See id*. (explaining that only a confirmed friend can see a private profile).

accept the request.[51] Private profiles may or may not come up in search results from the social networking site's internal search engine, and may or may not be indexed by Internet search engines at large.[52] But if they can be reached via search, only a limited search result will be viewable; the actual profile will be blocked from view unless the would-be viewer requests permission from the profile owner.[53]

3. Network Profiles

The final category is the network profile, which strikes a balance between the previous two extremes. As defined here, a network profile is a social networking profile that is viewable to anyone who satisfies pre-determined criteria for access, as set by the profile user, but which does not require any additional permission.[54] For example, a Facebook user has a network profile if they allow access to anyone who belongs to the same educational, work, or (until 2009) regional network as the user.[55] We further classify these network profiles into "open network" and "closed network" profiles depending on the kind of network used. [56]

51. *See* Help Center: Privacy: What Can People See If I Message Them or Add Them As a Friend?, Facebook.com, January 4, 2011, *archived at* http://www.webcitation.org/5vZF8xoJc. (noting that people added as friends will only have access to limited information before friendship is confirmed).

52. *See* Press Release, European Comm'n, European Comm'n Calls on Soc. Networking Cos. to Improve Child Safety Policies (Feb. 9, 2010), *archived at* http://www.webcitation.org/5sRxpsJvM (addressing the visibility of minors' user profiles and companies committed to increasing privacy options to shield content); Nancy R. Linder, *Refine Your Use of Linkedin*, 198 N.J. L.J. 611 (2009) (noting that Linkedin private profiles are not indexed in external search engines); Ryan Singel, *Facebook Private Profiles Not As Private As You Think They Are—UPDATED With Facebook Changes*, THREAT LEVEL BLOG (June 27, 2007), *archived at* http://www.webcitation.org/5sS14s0NR (explaining that despite a user choosing a private setting, some profile information may be visible through search engines).

53. *See* Singel, *supra* note 52 (clarifying that Facebook makes "names and non-revealing information" from private profiles publicly available without having access to a user's profile).

54. *See* Boyd & Ellison, *supra* note 12 (defining network profile).

55. *See* Boyd & Ellison, *supra* note 12 (explaining the function of selecting a particular network for membership).

56. *See My Account*, FACEBOOK.COM, Oct. 12, 2010 http://www.facebook.com/editaccount.php?networks (follow the "Facebook" URL; then log into personal account to view the "Add Networks" page) (until

a. Open Network Profiles

First, there is the open network profile; this type of network profile belongs to at least one network that any member of the public can join. The most significant example of an open network is the geographic network offered by Facebook from 2006 to 2009,[57] When active, any person could join any geographic network on Facebook, and there was no requirement (or even suggestion) that a user should actually live in, or have any connection to, the underlying geographic area.[58] As a result, any member of the public could view a person's Facebook profile that was viewable to those in the same network as the target profile, so long as they associated their profile with the same geographic network as the targeted user.[59] Thus, the open network profile is a social networking profile that allows others to view it based on a predetermined criterion that any member of the public may satisfy.

Accordingly, open network profiles are only slightly more difficult to access than public profiles. In a typical case, a person who wishes to view an open network profile would find the profile via an Internet search, or by using the social networking site's search engine–using that search result to determine which networks the profile is associated with.[60] To view that profile, a

2009, typing the name of a region or city allowed the user to join the network; typing in the name of an educational institution or company prompts the user to supply an e-mail address issued by that entity). Not all networks were publicly accessible. *Id.* For example, educational or work networks typically required the user to have an e-mail address issued by the institution or company, but geographic networks were open to any user. .

57. *See* Ben Parr, *LOST: Regional Networks Removed from Facebook*, Mashable.com (Sept. 1, 2009), *archived at* http://www.webcitation.org/5vZFK40zx (explaining history and removal of regional networks from Facebook).

58. *See How to Join a Regional Network on Facebook*, eHow.com, last accessed January 4, 2011 (providing steps demonstrating the ease of joining an "open" network when Facebook's regional networks were functional).

59. *See id.* (explaining that a user can access another user's profile within the same network if privacy settings permit).

60. *See What Is a Public Search Listing?*, FACEBOOK.COM, Oct. 12, 2010, *archived at* http://www.webcitation.org/5tQb2qbPy (specifying that profile information is available by conducting a public search). For example, limited information from Facebook profiles are indexed by search engines by default, which means that any member of the public can find out if a profile exists by

person will need to register and create a profile of their own, and then associate it with the same networks as the targeted user.[61] In many cases, this only represents another step in the registration process beyond what would be necessary to view a public profile.[62] Thus, although the profile is not immediately accessible, it can be made accessible using an easy workaround; the entire process of crafting a new profile and associating it with the target user's open networks only takes a few minutes.[63]

b. Closed Network Profiles

By contrast, a "closed network" profile belongs to networks that are closed to the general public, requiring that a user who wishes to join them affirm a statement that they belong to the network.[64] Most often, the user's affirmation takes the form of a showing that they have an e-mail address issued by the organization represented by the network.[65] For example, a

running a simple Internet search, even if they cannot access the full profile. *Id.* Once a user has logged in to Facebook, searching for a person's name using Facebook's internal search engine will create a list of all users with that name–and the networks associated with each user's profile. *See Can People That Find Me in Search Click on My Profile?*, FACEBOOK.COM, Oct. 12, 2010, *archived at* http://www.webcitation.org/5tQb7yECR (explaining that when a person is found using Facebook's internal search engine, network information is still accessible).

61. *See Controlling How You Share,* FACEBOOK.COM, Oct. 12, 2010, *archived at* http://www.webcitation.org/5tQbBq4iv.

Networks are visible to everyone so you can see who else is part of your network (and will have access to your information) before choosing "Friends and Networks" for any of your privacy settings. Other information in this section, including hometown and interests, is visible by default to help friends and other people you have things in common with connect with you.

Id.

62. *See Facebook's Privacy Policy*, *supra* note 46. This page shows that "[o]nce you register you can provide other information about yourself by connecting with, for example, your current city, hometown, family, relationships, networks, activities, interests, and places. You can also provide personal information about yourself, such as your political and religious views." *Id.*

63. *See Welcome to Facebook!*, *supra* note 28 (exhibiting the sign-up process for a Facebook profile); *see also Find Your Friends*, FACEBOOK.COM, Oct. 12, 2010, *archived at* http://www.webcitation.org/5tQbXtQnM (then-current page outlining how to search for profiles through chosen networks).

64. *See My Account*, *supra* note 56 (observing that Facebook requires an institute-supplied e-mail address to join a closed network).

65. *See My Account*, *supra* note 56.

closed network is one that is only open to Microsoft employees and requires anyone who wants to join the network to register an e-mail address issued by Microsoft.[66]

C. Litigation Value of Social Networking Sites

As more people catalog the details of their lives on social networking sites, the sites have found an increasing number of less "friendly" uses. Probation officers leverage these sites in tracking their charges.[67] Human resources departments check to see if potential hires have profiles on social networking sites– and, if so, review the content.[68]

Lawyers have also used these sites to assist them in litigation. For example, this usage has typically manifested itself in insurance fraud and disability investigations conducted by defense attorneys.[69] Because claims of insurance fraud and disability are easily undermined by photographic evidence,

66. *See My Account*, *supra* note 56 (providing that in order to join the Microsoft network, a user must have a Microsoft e-mail address).

67. *See* Press Release, United States Att'y's Office, N. Dist. of Iowa, MySpace Gun Pictures Lead to Federal Conviction (July 6, 2009), *archived at* http://www.webcitation.org/5sTKdZ28V (detailing federal criminal conviction based on pictures found on MySpace by probation officer). A man's probation officer found pictures of him on MySpace posing with guns; a probation search of the man's residence found a semiautomatic rifle, which resulted in a charge of being a felon in possession of a firearm and ammunition. *Id*.

68. *See* Alan Finder, *For Some, Online Persona Undermines a Résumé*, N.Y. TIMES, June 11, 2006, *archived at* http://www.webcitation.org/5sTLJ1zB7 (giving examples of businesses researching employment candidates online); *see also* Donald Carrington Davis, Note, *MySpace Isn't Your Space: Expanding the Fair Credit Reporting Act to Ensure Accountability and Fairness in Employer Searches of Online Social Networking Services*, 16 KAN. J.L. & PUB. POL'Y 237, 237 (2007) (arguing that the Fair Credit Reporting Act should be expanded to prohibit this sort of conduct).

69. *See* N.Y. STATE INS. DEP'T, INSURANCE FRAUDS INFORMATION: ARRESTS FOR FEBRUARY 2007 (2007), *archived at* http://www.webcitation.org/5sTMzhswt (detailing New York insurance fraud arrests in February 2007). A couple was arrested in connection with filing fraudulent auto insurance claim after investigators found "photos of the accident posted on MySpace.com before the claim was made with the caption: 'This is what happens when you drink and drive.'" *Id*.; *see also* Brian Goldfinger, *How Facebook Can Impact Your Personal Injury/Disability Claim in Ontario*, KNOL.GOOGLE.COM (Feb. 27, 2009), *archived at* http://www.webcitation.org/5sTNiB5sg (cautioning claimants that insurance companies are now investigating Facebook and MySpace pages).

litigators have successfully used photographs posted on social networking profiles to disprove these claims.[70]

As more individuals create profiles on social networking sites, their potential uses in litigation increase as well.[71] For example, a securities litigator attempting to prove a contract was signed in New York for choice-of-law purposes could track the movements of a party who obsessively catalogs her travels by reviewing archived "status updates" she has posted to her Facebook profile.[72] Likewise, a claim that a party violated a restrictive employment covenant can be investigated by reviewing the date at which the party claims to have joined a competitor on their LinkedIn profile.[73] And when marital strife spills onto a couple's social networking profiles, they become of interest to divorce and family attorneys.[74]

Leveraging multiple social networking sites in tandem offers even further uses.[75] In the case of a corporate party, an attorney can gain an understanding of organizational structure,

70. *See* Benjamin Rolf, Brenda Gierke & Erik Salveson, *The Usefulness of Social Networking Websites to a Resourceful Defense Team*, 3 STRICTLY SPEAKING 1, 1-3 (2008), *archived at* http://www.webcitation.org/5sZDASu8k (describing specific instance of using photos posted on a user's MySpace page to defeat disability claim). As to privacy, note that the authors' statement that "former versions [of MySpace pages] are not accessible" is untrue in many circumstances—depending on a user's privacy settings and how long they have maintained their profile, cached versions may be available via search indexers. *Id.* at 2; *see also Tom (Tom Anderson)*, MYSPACE.COM, Sept. 28, 2010, *archived at* http://www.webcitation.org/5t5F21xVh (showing Google cache of MySpace founder's profile page to demonstrate ease of accessing someone's MySpace page).

71. *See* Rolf et al., *supra* note 70 (noting the usefulness of social networking websites to defense teams).

72. *See* Virginia Heffernan, *Being There*, N.Y. TIMES, Feb. 10, 2009, *archived at* http://www.webcitation.org/5sZFB93M1 (discussing "status updates" and their uses). The author notes the ease of tracking the whereabouts of an individual by monitoring their status updates. *Id*.

73. *See Profiles—Overview*, LINKEDIN.COM, Sept. 7, 2010, *archived at* http://www.webcitation.org/5sZG3kT3X (showing that one of the key features of a LinkedIn profile is a listing of the user's previous job positions).

74. Belinda Luscombe, *Facebook and Divorce*, TIME MAG., June 22, 2009, at 93, *archived at* http://www.webcitation.org/5sZGk0FJd (demonstrating the availability of evidence on social networking websites for divorce lawyers).

75. *See id*. (illustrating how lawyers monitor multiple social networking sites for possible evidence).

function, and personnel by mining information from social networking sites.[76] On Facebook, the attorney can type the target corporation's name into its search function and obtain a list of every profile that matches the query.[77] Many of these profiles will be inaccessible, but they will have a list of names, including those of current or former employees.[78] To the extent that the profiles are accessible, the attorney may also find titles and job descriptions for current or former employees.[79]

Next, the attorney can take this list of names to LinkedIn. Because LinkedIn focuses explicitly on business networking, users focus their profiles on their professional lives more than on the socially-oriented Facebook or MySpace.[80] The attorney can plug in both the corporation's name and the list of names obtained from Facebook, using the links between the resulting profiles and others, as well as any "recommendations" they contain, to craft a rough organizational chart and identify potential document custodians or key individuals for subpoena.[81]

76. Ethan J. Wall, *Social Networking Sites Look Like Plunder to Attorneys*, L. TECH. NEWS (Feb. 20, 2009), *archived at* http://www.webcitation.org/5sZJ7zWLO (discussing the potential usefulness of social networking sites to attorneys).

77. *See Can People That Find Me in Search Click on My Profile?*, FACEBOOK.COM, http://www.facebook.com/help/?faq=14813 (last visited July 24, 2009) (providing instructions for user profiles and content). After log-in, a search query appears on the interface screen that users can use to search profiles, groups, and pages on the site; after retrieving results, users can narrow the results to responsive profiles by selecting the "Profiles" tab. *See id.*

78. *See* Singel, *supra* note 52 (stating that "names and non-revealing info" are accessible through a search). False positives will often appear if the targeted company sells consumers goods, with the search results yielding profiles that simply reference the company's products. *Id.* In that case, it would be advisable to search for the company's name plus a common job title. *Id.* For example, the search strings "(company name) manager marketing" and "(company name) IT director" would provide more useful results than simply searching for the company's name alone. *Id.*

79. *See Help Center: Privacy: What Can People See if I Message Them or Add Them As a Friend?*, *supra* note 51 (stating that work information may be viewable in some circumstances).

80. *Compare Profiles—Overview*, LINKEDIN.COM, *supra* note 73 (describing LinkedIn as a professional networking site), *with Welcome to Facebook!*, *supra* note 28 (noting that Facebook's goal is to "help you connect and share with the people in your life.").

81. *See* Keith Casey, *LinkedIn Intelligence–Part II*, CASEYSOFTWARE.COM (Oct. 19, 2007), *archived at* http://www.webcitation.org/5sZabYrKP (describing how to analyze patterns of recommendations for competitive intelligence

Thus, by understanding how individuals use these sites and what information they contain, an attorney can obtain insider information about a corporate party using publicly-available sources.[82]

Ultimately, the potential attorney use of social networking sites is limited by only two factors: first, the discretion of the sites' users (which is often lacking),[83] and second, the constraints of the ethical rules governing attorneys.[84] Indeed, as social networking sites evolve and become more complex, the amount and types of information that users will post on them will likewise grow.[85] Attorneys who wish to have done their due diligence on an adversary are well-advised to check for their presence on these sites; these sites are a treasure trove of potentially useful and easily-obtainable information, provided that attorneys navigate them within the limitations of the ethical rules.[86] We now turn to a discussion of one such limiting rule.

purposes); *see also* Singel, *supra* note 52 (providing the type of information available through a search).

82. *See* Casey, *supra* note 81 (reiterating the variety of ways in which patrolling social networking page content can be useful to attorneys).

83. *See, e.g.*, Christopher Null, *How to Avoid Facebook and Twitter Disasters*, PC WORLD (June 24, 2009), *archived at* http://www.webcitation.org/5vLWD37L8 (indicating that potential employers may check social networking profiles); Helen A.S. Popkin, *Getting the skinny on Twitter's "Cisco Fatty,"* MSNBC.COM, Mar. 27, 2009, *archived at* http://www.webcitation.org/5sZbqYyxT (detailing the "Cisco Fatty" story); Helen A.S. Popkin, *Twitter Gets You Fired in 140 Characters or Less*, MSNBC.COM, Mar. 23, 2009, *archived at* http://www.webcitation.org/5sZbewgaU (telling the story of "Cisco Fatty" and relating it to stories of social networking disasters). The "Cisco Fatty" story told of a job candidate who posted an update to her Twitter account stating, "Cisco just offered me a job! Now I have to weigh the utility of a fatty paycheck against the daily commute to San Jose and hating the work," only to receive a response from a Cisco insider stating, "Who is the hiring manager. [sic] I'm sure they would love to know that you will hate the work. We here at Cisco are versed in the web." *Id.*

84. *See* Peter Brown, *Discovery and Spoliation: Internet and Electronic Media Issues*, 80 PLI/NY 391 (2000) (highlighting the ethical concerns attorneys must be aware of when conducting background searches on social networking sites).

85. *See* Boyd & Ellison, *supra* note 12 (discussing the rapidly evolving use of social networking sites).

86. *See* Brown, *supra* note 84 (discussing why attorneys should use Internet sources to do background research on opponents and ethical concerns implicated by such work).

III. RULE 4.2 AND THE OBSERVATION EXCEPTION

Having established the definition, types, and use of social networking sites and profiles in litigation, we now turn to Rule 4.2 itself. This part briefly addresses the history and purpose of Rule 4.2, then turns to a discussion of the authorities that have applied Rule 4.2 to websites and public social networking profiles. After discussing the approach used by those authorities, this part argues that this approach is problematic when extended beyond fully-public websites and profiles and argues for the application of the observation exception to Rule 4.2 instead. This part concludes with a discussion of the observation exception and its purpose.

A. Rule 4.2: Purpose and General Application to Websites

Rule 4.2 prevents an attorney from communicating about the subject-matter of a representation with a person that the attorney knows to be represented by another attorney in the matter, unless the attorney has consent from that person's counsel or is otherwise authorized to do so by law or a court order.[87] It is the modern implementation of a "no-contact rule" based in the original 1908 ABA Canons of Professional Ethics,[88] present in its current prophylactic form since 1970.[89] Some version of Rule 4.2 is in force in all U.S. jurisdictions.[90]

87. *See* MODEL RULES OF PROF'L CONDUCT R. 4.2 (2007).

88. *See* Hazard & Irwin, *supra* note 1, at 799 (describing how and why Rule 4.2 was created). The authors state:

[Rule 4.2's] roots can be found in Canon 9 of the 1908 Canons of Professional Ethics, which advised that "[a] lawyer should not in any way communicate upon the subject of controversy with a party represented by counsel; much less should he undertake to negotiate or compromise the matter with him, but should deal only with his counsel."

Id.

89. *See* Hazard & Irwin, *supra* note 1 (quoting, "[a]fter the promulgation of the ABA Model Code of Professional Responsibility in 1970, this early formulation of the rule was expanded into the current prophylaxis of 'no contact.'").

90. *See* RESTATEMENT (THIRD) OF THE LAW GOVERNING LAWYERS § 99 cmt. b (2000) (noting that all American jurisdictions follow the no-contact rule).

Historically, Rule 4.2 and its predecessor provisions were born out of paternalism; the no-contact rule was implemented to protect the legal interests of unsophisticated laypersons, particularly when those individuals were dealing with an attorney.[91] In its current incarnation, Rule 4.2 has the stated purpose of protecting represented persons from three types of conduct: overreaching by other attorneys in the matter, interference from those attorneys in the person's own attorney-client relationship, and the un-counseled disclosure of information related to the representation.[92]

Only one authority has addressed how Rule 4.2 affects an attorney's ability to view a social networking site and find information disclosed by represented parties, and that authority only addressed public profiles – referring to them as public websites and not reaching those using more restrictive privacy settings.[93] Moreover, there is a startling lack of analysis on how Rule 4.2 applies to websites generally;[94] the Oregon State Bar Association Board of Governors ("Oregon State Bar") is the only

91. Hazard & Irwin, *supra* note 1, at 799-800 (quoting, "[i]nitially, ethics committees and courts treated DR 7-104(A)(1) with a more or less uncritical deference. They viewed the no-contact rule as providing necessary protection to lay persons who often lack the knowledge, training, and skills to protect their own interests, particularly when dealing with a lawyer representing an adversary.").

92. *See* MODEL RULES OF PROF'L CONDUCT R. 4.2. cmt. 1 (2007), stating that:
This Rule contributes to the proper functioning of the legal system by protecting a person who has chosen to be represented by a lawyer in a matter against possible overreaching by other lawyers who are participating in the matter, interference by those lawyers with the client-lawyer relationship and the un-counselled disclosure of information relating to the representation.
Id.

93. *See* N.Y. State Bar Assoc. Comm. on Prof. Ethics. *supra* note 5.

94. Most of the authorities and commentators addressing Rule 4.2 have done so in the context of chat rooms and bulletin boards. *See, e.g.*, Phila. Bar Ass'n Prof'l Guidance Comm., *supra* note 93 (discussing impact of Rule 4.2 on bulletin boards and chat rooms); Brown, *supra* note 84, at 396 (2000) (discussing impact of Rule 4.2 on chat rooms); O'Reilly, *supra* note 10, at 1 (noting the differences between Web 1.0 and Web 2.0). Historically, websites were generally static pages that were roughly analogous to a book or magazine article. *Id.* So, the comparatively innovative nature of chat rooms and bulletin boards on the first wave of Internet usage correctly drew the bulk of ethical scrutiny at that time; websites were fairly limited in scope and their creation was limited to the technologically proficient, and it is only in the last few years that the average Internet user has been able to quickly and easily establish a web presence. *Id.*

authority that has addressed how Rule 4.2 applies to websites: once in 2001,[95] and again in 2005.[96] Both opinions conduct the analysis under the principle that online communication is translatable to the offline world, and so conduct prohibited offline would be prohibited online.[97] Thus, a party who posts information on the Internet is considered to be the same as a party who publishes an article or book.[98] And so long as an attorney does not communicate with the website's owner with the expectation of a personalized response, the website is considered to be the equivalent of a book or magazine article, and the attorney may view it without violating Rule 4.2.[99] This is the case even if the website requires registration and a password (so long as any person can obtain these),[100] charges an access fee or subscription,[101] or runs an e-store that the attorney orders

95. *See* 2001 Oregon Op., *supra* note 5 (discussing how Oregon's ethical code applied to websites in 2001).

96. *See* 2005 Oregon Op., *supra* note 5 (addressing how attorneys should act when visiting public websites and conducting Internet communications).

97. *See* 2005 Oregon Op., *supra* note 5 (quoting, "[f]or purposes of this opinion, there is no reason to distinguish between electronic or nonelectronic forms of contact. Both are permitted or both are prohibited."); 2001 Oregon Op., *supra* note 5, at 1-2 (stating that viewing a website is the "equivalent" of reading a newspaper or magazine, and analogizing between prohibited conduct in person and online).

98. *See* 2005 Oregon Op., *supra* note 5, at 453 (quoting, "[a]ccessing an adversary's public Website is no different from reading a magazine article or purchasing a book written by that adversary."); 2001 Oregon Op., *supra* note 5, at 2 (quoting, "[v]iewing (or even downloading) information posted on a passive site is the equivalent of reading a newspaper, magazine, or other document available for public consumption.").

99. *See* 2001 Oregon Op., *supra* note 5, at 2 (reasoning that a lawyer may communicate with a party's website in certain circumstances). Such communication is allowed so long as the response is essentially formulaic, as in the case of ordering a product from a website; but when the lawyer "sends a message with the expectation of receiving a personal response," they are communicating with the website within the meaning of the rule. *Id.*

100. *See* 2001 Oregon Op., *supra* note 5 at 21 n.1 (describing how even a password protected website can be available to the public). "Some Websites require registration and, occasionally, a password for access. If anyone can register and have access, then the site is available to the public." *Id.*

101. *Compare* 2001 Oregon Op., *supra* note 5 at 2 n.1 ("For purposes of this opinion, [subscription-only websites] would not be sites accessible to the public."), *with* 2005 Oregon Op., *supra* note 5, at 453 n.1 ("For purposes of this opinion, a Website can be 'public' even if an access fee or a subscription fee is charged."). The Oregon State Bar initially held the contrary position, but appears to have reversed itself. *See supra*.

products from.[102] The overarching distinction drawn by the Oregon State Bar is not between types of publication or websites, but whether the online communication takes the character of a phone or face-to-face conversation.[103] The sole authority on the application of Rule 4.2 to a social networking profile, because it addresses only public profiles, uses the same line of reasoning by analogy to conclude that a public social networking profile is the rough equivalent of any other publicly-available website or print media source and therefore may be viewed without running afoul of Rule 4.2.[104]

Although this sort of reasoning by analogy is persuasive in the context of the relatively static websites and public profiles that these opinions appear to contemplate, it fails as a general principle when extended beyond that context—and even there, it is flawed.[105] An individual can post content on the web for free, making it instantly accessible to anyone who wishes to view it; there are no barriers to enter the world of online publishing apart from accessing the Internet.[106] By contrast, even if the same individual has the means to self-publish a book or article—bypassing the numerous barriers to entry present in traditional paths to publishing—there are still issues of cost, lead time, and limited reach that do not exist in the online world.[107]

102. *See* 2001 Oregon Op., *supra* note 5, at 2 (discussing the use of an e-store for business investigations). The Oregon State Bar analogizes the use of an e-store to the business investigation context of the observation exception to Rule 4.2, without identifying it as such. *Id.* The Bar focuses its analysis on whether the party being contacted would be represented by the business' attorney. *Id.*

103. *See* 2001 Oregon Op., *supra* note 5, at 2 (emphasizing the character of the communication as the distinguishing factor in the analysis).

104. *See* N.Y. State Bar Assoc. Comm. on Prof. Ethics. *supra* note 5.

105. *See* Boyd & Ellison, *supra* note 12 (discussing the ease and relative quickness by which information can be added and removed from social networking sites).

106. *See Welcome to Facebook!*, *supra* note 28 ("Sign Up . . . It's free and always will be."). In particular, the majority of social networking sites are free to use, and users can set up a profile—"publishing" it to millions—within minutes. *Id.*; *see MySpace*, *supra* note 28 ("Sign Up Free"). Internet users can also create a blog or micro-blog within minutes, and those services are likewise largely free to use. *See Blogger: Create Your Free Blog*, BLOGGER.COM, Sept. 08, 2010, *archived at* http://www.webcitation.org/5sb5RPHQ4 ("Create a blog. It's free.").

107. *See* David Carnoy, *Self-Publishing a Book: 25 Things You Need To Know*,

Offline publishing forces a period of self-reflection and editing before making the published material publicly-available, which simply does not exist in the online world, particularly today.[108] It is these barriers and delay, inherent in the production of offline book or magazine publishing and absent in the world of Internet content generation, that help support Rule 4.2's policy goal of preventing the un-counseled disclosure of information.[109] It is far more likely that an attorney will be able to review and address any concerns about their client's proposed publication if the content requires significant funds and time to generate—particularly when compared with a situation where the client can instantly self-publish for no incremental cost.[110] This fact will be even more pronounced in cases where a client will not recognize their online publications as "publications," let alone the equivalent of a book or magazine article—specifically, cases where a client maintains a social networking profile.[111] These concerns are not addressed by the Oregon State Bar's opinions, although they arguably did not matter in the questions presented; the opinions generally seem to contemplate a corporation's website, which in most cases will have had significant internal vetting by a company's marketing or public relations professionals.[112] And both opinions were issued before social networking sites began to reach the saturation levels they

CNET REVIEWS - FULLY EQUIPPED BLOG, July 27, 2010, *archived at* http://www.webcitation.org/5sb6Rzmbw (discussing the costs and hurdles inherent in self-publishing).

108. *See id.* (explaining the editing differences between online and offline publishers).

109. *See* MODEL RULES OF PROF'L CONDUCT R. 4.2. cmt. 1 (2007) (stating that the rule is aimed at protecting people from overreaching by another party's counsel).

110. *Compare Welcome to Facebook!*, *supra* note 28 (allowing users instant and free publication), *and MySpace*, *supra* note 28 (offering free access, profile accessibility, and instant sharing of music), *with* 2001 Oregon Op., *supra* note 5, at 2 n.1 (describing sites that are not accessible to the public, requiring subscription, and limiting access to certain users).

111. *See* Dr. Rhonda Savage, *Facebook: Fired Up or Just Fired? The Good, the Bad and the Ugly of Social Media in the Workplace*, OKLA. STATE BAR ASS'N, June 2010, *archived at* http://www.webcitation.org/5sbJMtX0W (citing a study showing eight percent of employees were dismissed for behavior on sites like Facebook).

112. *See* 2005 Oregon Op., *supra* note 5, at 453-54 (discussing websites in greater depth). The analysis seems to contemplate organizational or corporate sites by focusing its reasoning on business investigations. *Id.*

are at today—Facebook, the most popular social networking site, limited its membership to students until 2006.[113] But as more individuals self-publish material on the Internet, thornier issues arise that reveal the problem with such an analysis, and particularly with addressing all websites as equivalent for the purposes of Rule 4.2.[114] Although these issues have not yet been forced to a head, because the sole opinion addressing social networking sites under Rule 4.2 only considers public profiles,[115] as the online world grows increasingly complex, courts will find themselves without a basis for sorting through these ethical issues if the only guidance they can find is a suggestion to treat a website like a book.[116]

Thus, a better approach is needed. We suggest that the "observation exception" to Rule 4.2 is the best way for courts and ethics committees to analyze online modes of communication, particularly websites.[117] This exception reaches the same result as the existing opinions, relies on premises that do not undercut the policy goals of Rule 4.2, and has the additional benefit of being easily extended to more complex situations.[118] We will now turn to a discussion of this exception.

113. *See* Boyd and Ellison, *supra* note 12 (describing the early history of social networking sites such as Facebook).

114. *See* Dennis P. Duffy, The University of Texas School of Law 16th Annual Labor and Employment Law Conference: Selected Ethics and Professionalism Issues in Labor and Employment Law Cases (May 2009), at 67, *archived at* http://www.webcitation.org/5sccrsMZj (discussing Oregon opinions, and noting that "these issues apply equally to the 'personal' website of a plaintiff."). Although the Oregon opinions do not explicitly endorse this position, the language is more than broad enough to include it. *Id.*

115. *See generally* N.Y. State Bar Assoc. Comm. on Prof. Ethics. *supra* note 5.

116. *See* 2001 Oregon Op., *supra* note 5, at 2-3 (suggesting guidelines for website treatment pursuant to Rule 4.2); 2005 Oregon Op., *supra* note 5, at 453 (treating websites as newspapers or like publications under Rule 4.2).

117. *See* MODEL RULES OF PROF'L CONDUCT ANN. R. 4.2 Ann. *Observing (2007) (listing "observing" as one of the circumstances that do not violate the Anticontact Rule).

118. *See* 2001 Oregon Op., *supra* note 5, at 2-3 (applying Rule 4.2 to websites by treating websites like magazines or similar publications); 2005 Oregon Op., *supra* note 5, at 453 (outlining appropriate treatment of websites under Rule 4.2).

B. The Observation Exception

The "observation exception" is a well-recognized exception to Rule 4.2 that allows an attorney to observe a represented party's conduct if the attorney is acting as a member of the general public in their interactions with the represented party.[119] In its classic incarnation, this takes the form of an attorney sitting in his car on a public street, videotaping the public conduct of a personal injury plaintiff to see if the claimed injury really exists.[120] In this scenario, there is no contact between the attorney and the represented party at all; the attorney simply monitors the party's public conduct.[121] And because any other member of the public could have made the same observation, the attorney is not intruding into any expectation of privacy by observing the targeted person.[122]

This exception has also allowed limited contact with a represented party in the context of business investigations.[123] In

119. *See* MODEL RULES OF PROF'L CONDUCT ANN. R. 4.2 annot. *Observing (2007) (listing "observing" as one of the circumstances that do not violate the Anticontact Rule).

120. *See id.* (outlining proper actions that would qualify as observing); State *ex rel.* State Farm Fire & Cas. Co. v. Madden, 451 S.E.2d 721, 730 (W. Va. 1994) (finding no violation of the state counterpart to Rule 4.2 in a specific circumstance). An investigator acting at the behest of a defense attorney sat in a car parked on the public street near a personal injury plaintiff's place of employment. *Id.* The investigator's observation of the plaintiff's activities, undertaken "in full view of the general public," did not violate the rule. *Id.; see also* Pa. Bar Ass'n Comm. on Legal Ethics and Prof'l Responsibility Op. 2009-02, at 3 (describing "videotaping the public conduct of a plaintiff in a personal injury case" as "common" and "ethical").

121. *See State Farm*, 451 S.E.2d at 730 (explaining the lack of contact between the attorney and the personal injury plaintiff).

122. *See id.* (noting that even in the criminal context, a person is not entitled to Fourth Amendment protection within his own home). The *State Farm* court reasoned that when "[a person] conducts his activities in a manner that can be seen by the unaided viewing of a person lawfully standing outside," he "had no reasonable expectation of privacy." *Id. See also* Johnson v. Corp. Special Servs., Inc., 602 So. 2d 385, 388 (Ala. 1992) (refusing to find invasion of privacy where investigator parked car outside home of workman's compensation claimant and observed claimant in his front yard). The *Johnson* court held that because the claimant's activities "could have been observed by any passerby," the investigator's intrusion into his privacy was not wrongful and thus not actionable. *Id.*

123. *See* Gidatex v. Campaniello Imps., Ltd., 82 F. Supp. 2d 119, 126 (S.D.N.Y. 1999) (finding no violation of ethical rules when "investigators merely

this context, an attorney may enter a business and interact with its employees and salespersons in order to discover information relevant to the attorney's case.[124] The nature of the attorney's interactions with the business and its employees determines whether they are permitted by Rule 4.2; when the attorney acts as any other member of the public, limiting their interactions to the type of relatively formulaic conversations other consumers would have, there is no violation.[125] However, when the attorney asks specific questions targeted to gather information about the represented matter–questions that a member of the general public would not ask–the attorney violates Rule 4.2.[126]

recorded [a] normal business routine").

124. *See id.* (noting that attorneys who hired private investigators to perform interviews were not violating ethical rules); Hill v. Shell Oil Co., 209 F. Supp. 2d 876, 879-80 (N.D. Ill. 2002) (discussing the appropriateness of employing outside individuals to enter a business and test the quality of customer service within); *see also* Apple Corp. v. Int'l Collectors Soc'y, 15 F. Supp. 2d 456, 474-75 (D.N.J. 1998) (implying that ordering stamps via telephone is analogous to entering a business and interacting with its employees).

125. *See Hill*, 209 F. Supp. 2d at 880. The *Hill* court stated:

Lawyers (and investigators) cannot trick protected employees into doing things or saying things they otherwise would not do or say. They cannot normally interview protected employees or ask them to fill out questionnaires. They probably can employ persons to play the role of customers seeking services on the same basis as the general public.

Id.; *Apple Corp.*, 15 F. Supp. 2d. at 474-75. The *Apple Corp.* court stated:

RPC 4.2 cannot apply where lawyers and/or their investigators, seeking to learn about current corporate misconduct, act as members of the general public to engage in ordinary business transactions with low-level employees of a represented corporation. To apply the rule to the investigation which took place here would serve merely to immunize corporations from liability for unlawful activity, while not effectuating any of the purposes behind the rule.

15 F. Supp. 2d at 474-75.

126. *See* Midwest Motor Sports, Inc. v. Arctic Cat Sales, Inc., 144 F. Supp. 2d 1147, 1157-58 (D.S.D. 2001) (holding that an attorney may not circumvent Rule 4.2 by hiring an investigator to obtain information from a represented party), *aff'd*, 347 F.3d 693 (8th Cir. 2003). *Midwest Motor Sports, Inc.* is unique among cases with similar facts in finding that Rule 4.2 had been violated. *Compare Midwest Motor Sports, Inc.*, 144 F. Supp. 2d at 1157-58 (holding that Rule 4.2 is violated in any situation where an attorney hires an investigator to obtain any information from a represented party), *with Gidatex*, 82 F. Supp. 2d at 126 (holding that Rule 4.2 is not violated when an attorney hires an investigator to obtain normal business information from a represented party). In light of *Midwest Motor Sports, Inc.* and *Gidatex*, subsequent courts have held that whether Rule 4.2 has been violated is highly dependent on the facts of the case. *Hill*, 209 F. Supp. 2d at 880 ("Although *Midwest Motor Sports* is considerably more restrictive than *Gidatex*, we think there is a discernible continuum in the cases from clearly impermissible to clearly permissible

Some commentators have suggested that this conclusion is, or should be, driven by the underlying conduct that the attorney is investigating.[127] Specifically, racially discriminatory practices and violations of intellectual property rights have been offered by commentators as types of wrongful conduct that support this conclusion.[128] The cases, however, do not make this distinction, and rightfully so: considering the underlying conduct being investigated–instead of focusing solely on the attorney's conduct–would introduce an unnecessary element of uncertainty into the analysis, in turn inviting more aggressive tactics by attorneys when they believe that they can characterize the investigated conduct as particularly insidious.[129] The fact that the attorney was acting as any other member of the public was enough.[130]

conduct."). *See also Apple Corp.*, 15 F. Supp. 2d at 474-75 (noting that Rule 4.2 is not an absolute bar to obtaining information about the represented matter by direct questioning); Phillip Barengolts, *Ethical Issues Arising From the Investigation of Activities of Intellectual Property Infringers Represented by Counsel*, 1 NW. J. TECH. & INTELL. PROP. 3, 23-25 (2003) (arguing that *Midwest Motor Sports, Inc*. can be reconciled with *Gidatex*). In *Apple Corp.*, the court ruled that the attorney may still obtain information by direct questioning as long as the questions are of the sort the average member of the public would ask. *See* 15 F. Supp. 2d at 474-75. In such cases, the investigated wrongdoing manifests itself in the business relationship with the public. *Id.*

127. *See* Barengolts, *supra* note 126, at 41 ("There is no sound basis for a rule of law that affords less information to litigants than to the typical consumer."). *See also* Julian J. Moore, *Home Sweet Home: Examining the (Mis)application of the Anti-Contact Rule to Housing Discrimination Testers*, 25 J. LEGAL PROF. 75, 88-90 (2001) (discussing how public policy favors the use of discrimination testers even though they may act in a deceptive manner).

128. *See* Moore, *supra* note 127, at 91 (arguing that there is no violation of Rule 4.2 when attorneys or investigators "act as members of the general public to engage in ordinary business transactions . . ."); Barengolts, *supra* note 127, at 40-44 (detailing how violations of intellectual property rights also fall under the scope of Rule 4.2).

129. *See Midwest Motor Sports, Inc*., 144 F. Supp. 2d at 1157-58 (sanctioning an attorney for sending a private investigator into a store to solicit information from the sales staff); *Gidatex*, 82 F. Supp. 2d at 125-26 (refusing to sanction an attorney due to the nature of the solicited information); *Apple Corp.*, 15 F. Supp. 2d at 474 (finding that Rule 4.2 was not violated because the individual's identity was not the nature of the claim).

130. *See* Barengolts, *supra* note 126, at 43 (discussing the lesson from *Midwest Motor Sports*). The court stated that, "if an investigator is sent to an infringer's place of business, he should understand that his sole purpose is to behave as an ordinary consumer and not actively attempt to seek admissions." *Id.*

The observation exception, then, provides a simple test for governing the online conduct of attorneys: is the attorney acting as any other member of the public, either by passively observing a party's public conduct or, if the party is a business, is the attorney interacting with them in the same formulaic, limited manner that any other consumer would?[131] If so, the attorney's conduct is acceptable; it is not the type of conduct that Rule 4.2 seeks to proscribe.[132] Note that this test does not disrupt the existing authorities; it comports with the existing opinions from the Oregon and New York State Bars, which address websites and profiles open to the general public.[133] And even more valuable is the test's prospective application: because it approaches online conduct on its own merits, it will provide more consistent results than reasoning by analogy, which will be increasingly jarring as

131. *See* 2005 Oregon Op., *supra* note 5, at 453-54 (discussing the possibility of extending the limited contact permitted in business investigation cases when the interaction is of a personal nature). For example, a person may post an automated poll on their personal blog, and an attorney would be able to take the poll under the observation exception. *See Gidatex*, 82 F. Supp. 2d at 122 (holding that access to information may be obtained when the conduct is part of a normal business routine). When information is made accessible to the public, and when attorneys do not communicate directly with the represented party, the information is ethically obtained under the observation exception. *Id.* Apart from this sort of automated, mechanized communication, however, the circumscribed conduct of those cases should not be extended to contact with individual parties, even when the conduct appears to be formulaic. *See* MODEL RULES OF PROF'L CONDUCT R. 4.2 (2007).

132. *See Gidatex*, 82 F. Supp. 2d at 126 (implying that obtaining information which is available to the general public does not violate rule 4.2).

133. *See* N.Y. State Bar Assoc. Comm. on Prof. Ethics. *supra* note 5; 2005 Oregon Op., *supra* note 5, at 453 (stating that accessing information posted on a public website does not constitute communication with the represented party); 2001 Oregon Op., *supra* note 5, at 2 ("A lawyer who reads information posted for general consumption is not communicating with the represented owner of the Website."). Both Oregon opinions contemplate that the represented party is operating a static website open to any member of the public. *See* 2005 Oregon Op., *supra* note 5, at 453; 2001 Oregon Op., *supra* note 5, at 2. An attorney may view this sort of public conduct under the observation exception. *See* 2005 Oregon Op., *supra* note 5. Moreover, the Oregon opinions can be read as independently applying the observation exception to a book or article as well, such that the analogy between those offline publications and the static websites at issue is merely illustrative, rather than operative. *See id.;* 2001 Oregon Op., *supra* note 5. By doing so, we preserve the existing opinions and scholarship while transforming its import into a more usable format for more complicated cases, such as those we describe in Part III. *See infra* Part III.

online conduct continues to evolve.[134] We next provide one such example of this application.

IV. THE OBSERVATION EXCEPTION AND SOCIAL NETWORKING SITES

We now turn to an analysis of Rule 4.2's application to attorney use of social networking sites. First, we address public profiles, which we conclude to be permissible under the observation exception. Next, we address network profiles, which should be permissible in some circumstances (*e.g.,* open network profiles) and likely barred in others (*e.g.,* closed network profiles). Finally, we discuss private profiles, which we conclude are barred by Rule 4.2.

A. Public Profiles Are Permissible Under the Observation Exception to Rule 4.2

Public profiles are, by definition, acceptable for viewing under the observation exception to Rule 4.2 because they can be passively viewed by anyone, requiring no contact with the represented party by any viewer.[135] Because these profiles can be viewed by any member of the public, the observation exception permits an attorney to follow suit.[136] Thus, these profiles represent the simplest and most straightforward application of the observation exception.[137]

Public profiles also represent an instance where the Oregon State Bar's analysis is applicable; as the New York State Bar Association's Committee on Professional Ethics recently recognized, these profiles are indistinguishable from the kind of

134. *See Gidatex*, 82 F. Supp. 2d at 124 (providing an explanation of the observation exception test).
135. *See* State *ex rel.* State Farm Fire & Cas. Co. v. Madden, 451 S.E.2d 721, 730 (W. Va. 1994) (holding the observation exception is applicable to conduct undertaken in full view of the public, and no privacy concerns are implicated in such circumstances).
136. *See id.* (reasoning that exclusion of testimony regarding activities viewable by the public serves no legitimate deterrent purpose).
137. *See id*. (indicating that accessing information obtainable by the general public is not a violation of Rule 4.2).

publicly-available website analyzed by those opinions, and in both cases the analogy to offline publication is workable.[138] Of course, the same limitations discussed in Part II(A) apply; maintaining a social networking profile is not the same thing as publishing a book or a magazine article, and the translation of that offline conduct into the world of online publishing still undercuts one of Rule 4.2's policy goals.[139] The analogy will at least reach the correct result here, if by unsatisfying means.

B. The Observation Exception Permits an Attorney to View Open Network Profiles

Next, we turn to the network profile scenario. In this context, the observation exception yields different results for the two sub-types of network profiles.

First, open network profiles fall under the observation exception.[140] Although these profiles are less public in theory than a true public profile,[141] they are equivalent in practice: just as any member of the public can view a public profile by (at most) registering for the social networking site, any person can likewise associate their profile with the targeted user's open network in order to gain access;[142] the open network profile's owner is making their content available to anyone who wishes to

138. *See* 2005 Oregon Op., *supra* note 5, at 453 (showing that public website content is available in much the same way as offline public material). *See also* N.Y. State Bar Assoc. Comm. on Prof. Ethics. *supra* note 5 (referring to public profiles as the equivalent of a publicly-accessible website or online media source).

139. *See* Hazard & Irwin, *supra* note 1, at 799 (implying that online communications make lay persons more susceptible to disclosing information to opposing counsel). The implication is that online communication does not inherently provide a user with a period of self-reflection before disclosing information. *Id.*

140. *See State Farm*, 451 S.E.2d at 730 (holding that when conduct is undertaken in full view of the public, no privacy matters are implicated, and the observation exception controls); 2005 Oregon Op., *supra* note 5, at 453 (stating that an attorney may access information made available for public consumption without running afoul of Rule 4.2).

141. *See* Boyd & Ellison, *supra* note 12 (acknowledging that open network profiles are less public because they are only open to people within a certain network).

142. *See* Boyd & Ellison, *supra* note 12 (noting that joining someone's social network is a way to gain access to the targeted user's information).

view it, and the profile's owner does not need to be contacted.[143] Thus, an attorney should be able to view a open network profile under the observation exception without running afoul of Rule 4.2.[144]

Closed network profiles present more complicated issues.[145] In most cases, the question is moot; if the attorney does not have access to the requisite credentials, the attorney lacks the means to join the closed network.[146] This leaves two circumstances in which this question is relevant: first, cases where the attorney does not have access to the requisite credentials but is able to acquire them, and second, cases where the attorney already legitimately has the credentials required to join the network.[147]

When an attorney does not have access to the requisite credentials, but has the ability to acquire them, analysis under the observation exception turns on exactly how the attorney can acquire the credentials.[148] For example, if the attorney can access the Microsoft network by borrowing the log-in of a friend who works at Microsoft, that sort of conduct is barred under the

143. *See* Boyd & Ellison, *supra* note 12 (showing that a profile owner does not need to be contacted in order to have their content viewable by anyone in the network); *see also My Account*, *supra* note 56 (demonstrating that users can make profiles viewable by network members).

144. *See* 2005 Oregon Op., *supra* note 5 (implying that an attorney may access an open network profile without violating Rule 4.2). Moreover, the act of registering for access to a website has already been described by the Oregon State Bar–the only authority considering this issue–as acceptable under Rule 4.2, so long as any member of the public can likewise register for access. *See* 2001 Oregon Op., *supra* note 5, at 2.

145. *See My Account*, *supra* note 56 (closed network profiles).

146. *See My Account*, *supra* note 56.

147. *See My Account*, *supra* note 56 (inferring what an attorney must do to gain access to a closed network).

148. *See* Boyd & Ellison, *supra* note 12 (indicating that existing case law and commentary does not suggest when third parties, including attorneys, may have access to closed network profiles); *see also* Matthew J. Hodge, Note, *The Fourth Amendment and Privacy Issues on the "New" Internet: Facebook.com and MySpace.com*, 31 S. ILL. U. L.J. 95, 120 (2006) (explaining that the administrators of MySpace.com "will not disclose personal information to any third party unless that disclosure is necessary: (1) to conform to legal requirements . . .").

observation exception–that is not something any member of the public could do.[149]

By contrast, if any member of the public could access the closed network profile because the credentials were publicly available, the observation exception would allow this conduct.[150] This situation, however, may only be hypothetical; since an organization typically represented by a closed network does not issue e-mail addresses to any random member of the public, circumstances where this would be the case would likely involve some element of a user's log-in information being compromised or some other, similarly dubious situation.[151] Thus, even though the observation exception would logically govern that use, it would only play out in situations that would push the limits of the observation exception.[152]

Similar concerns are raised when an attorney already has legitimate access to the requisite credentials that they need to access the closed profile.[153] When an attorney wishes to view the

149. *See* Shannon Awsumb, *Social Networking Sites: The Next E-Discovery Frontier*, 66 BENCH & B. MINN., 22, 24 (2009) (indicating that such practices are deceptive in nature). "While attorneys can—and should—engage in efforts to informally locate publicly available social networking information, they should be mindful of the ethical limitations." *Id.*

150. *See* Awsumb, *supra* note 149, at 24 (discussing ethical ways to obtain information through social networking sites).

151. *See* Boyd & Ellison, *supra* note 12 (stating that accessing closed corporate networks requires user to have an appropriate ".com" address given through that corporation); *see also* Hodge, *supra* note 148, at 119-20 (noting that private information on social networking sites is only given out by the administers of the site as required by law).

152. *See Hill*, 209 F. Supp. 2d at 880 (discussing the limitations to the observation exception). Authorities have not addressed the *degree* to which an attorney may interact with parties under a claim that they are acting as a member of the general public, although the *Hill* court recognized the existence of a continuum of conduct ranging from *Gidatex* (acceptable) to *Midwest Motor Sports, Inc.* (unacceptable). *Id.* ("[t]here is a discernable continuum in the cases from clearly impermissible to clearly permissible conduct."). This scenario would likely be on the *Midwest Motor Sports, Inc.* end of the scale. *See* Midwest Motor Sports, Inc. v. Arctic Cat Sales, Inc., 347 F.3d 693, 699-700 (2003); *see also Hill*, 209 F. Supp. 2d at 880 (discussing *Midwest Motor Sports Inc.* lying on the impermissible side of continuum).

153. *See* Awsumb, *supra* note 149, at 24 (analogizing legitimate access to profile to videotaping in a permitted area to show that despite being permitted, ethical considerations exist).

closed network profile of a party whose profile is available to members of a university network, and the attorney still has an e-mail address from their own time at that university, the temptation to join the network to view the party's profile will be strong.[154] But the observation exception bars this conduct as well: the university's network is not open to the public, and, therefore the attorney is barred from viewing the profile.[155] The relevant question is not whether the attorney has authorized access to the profile, but whether the public has such access.[156] Thus, the observation exception bars even legitimate access to closed network profiles.[157]

Again, this analysis avoids the problem of attempting to analogize this conduct to a real-world situation. If the above example is analogous to the attorney attending an alumni function that the represented party also attends, is the attorney's conduct the equivalent of listening to a speech that the represented party makes, or of eavesdropping on the represented party's conversations? Persuasive arguments could be made for either analogy, and this helps to illustrate how that sort of analysis does not provide for predictable or consistent results.

The observation exception offers a more consistent and rational approach to this problem. The question becomes simple: can any member of the public join a given closed network?[158]

154. *See My Account*, *supra* note 56 (addressing requirement of having an educational institute issued e-mail address to join same network).

155. *See Hill*, 209 F. Supp. 2d at 880 (asserting that the observation exception requires a distinction between information available and not available to the general public).

156. *See id*. (noting that attorneys may employ persons to seek information that is available to the general public).

157. *See id*. (implying that attorneys may not employ persons to provide information that is available to that person but not available to the general public). If a situation does arise where the institution or organization implicated in a given closed network is distributing e-mails to the general public, we suggest that an attorney seek out a court order or advisory opinion before attempting to access the represented party's profile; if such conduct is deemed ethical, it seems to us it would be a rare case. *See* ANN. MODEL RULES OF PROF'L CONDUCT R. 4.2 cmt. 6 (2007) (advising attorney to seek court order if uncertain about legality of communication with represented party).

158. *See Hill*, 209 F. Supp. 2d at 880 (discussing the importance of the

The answer is in almost every case no[159]–this is not truly public conduct.[160] An attorney may not view a closed network profile, even when they can legitimately access it.[161] Thus, the observation exception permits attorneys to view open network profiles and may ban them, for all practical purposes, from viewing closed network profiles.[162]

C. Private Profiles are Barred Under Rule 4.2

Finally, we turn to the private profile. By definition, access to a private profile requires prior approval from the profile's owner, and therefore the general public does not have access to a given private profile.[163] Nor does the attorney's request for access fall under the exceptions for limited contact articulated in the business investigations cases; although any member of the public may request access to the profile, that request (and response) is not what the attorney wishes to observe, and the profile itself is not publicly-available.[164] Moreover, while the attorney's request for access may be formulaic and rote, the response is personalized and discretionary; this is not the sort of interaction protected by the business investigation cases.[165] As a result, efforts to view private profiles fall outside of the

distinction of publicly accessible information).

159. *See* Boyd & Ellison, *supra* note 12 (stating that access to certain sites will be limited by site and user privacy settings).

160. *See Hill*, 209 F. Supp. 2d at 880 (discussing that material not accessible to the general public does not qualify under the observation exception).

161. *See id*. (noting "a discernible continuum in cases from clearly impermissible to clearly permissible conduct").

162. *See id*. (finding such "interactions do not rise to the level of communication protected by rule 4.2").

163. *See Privacy: Who Can See My Profile and Content?*, *supra* note 49 (restricting private profile access to approved users).

164. *Cf.* Gidatex, Ltd., 82 F. Supp. 2d 119, 126 (S.D.N.Y. 1999) (finding no violation of ethical rules when "investigators merely recorded [a] normal business routine"); Hill, 209 F. Supp. 2d 876, 879-80 (N.D. Ill. 2002) (discussing the appropriateness of employing outside individuals to enter a business and test the quality of customer service within); *Apple Corp.*, 15 F. Supp. 2d at 474-75 (implying that ordering stamps via telephone is analogous to entering a business and interacting with its employees and thus an ethical way to investigate a party).

165. *See* 2001 Oregon Op., *supra* note 5 at 2 (reasoning that a lawyer may communicate with a party's website so long as the response is essentially formulaic).

protection of the observation exception and are properly barred under Rule 4.2.[166]

The Philadelphia Bar Association Professional Guidance Committee reached this same conclusion–albeit in the context of an unrepresented party–in an advisory opinion issued in 2009.[167] There, the Committee rejected an inquirer's suggestion that accessing a private profile was akin to the "common and ethical" situation of videotaping the public conduct of a plaintiff in a personal injury case.[168] The Committee stated that accessing a private profile was more similar to gaining access to a private residence by using deception and then videotaping conduct undertaken in the home, and thus was impermissibly deceptive.[169]

But the inquirer also proposed a twist on this analysis; he represented that he believed that the targeted witness would "allow access to anyone who asks."[170] The Committee questioned how he could have known that;[171] although there was no further analysis, the point is well-taken: assuming that such a practice would allow the attorney to view the profile, would it be possible for an attorney to make that showing?[172]

166. *See* ANN. MODEL RULES OF PROF'L CONDUCT R. 4.2 Ann. *Observing (2007) (excepting observation of information on public website from Rule 4.2 violation).

167. *See* Phila. Bar Ass'n Prof'l Guidance Comm., Op. 2009-02, 1, 3 (2009) (concluding that it would be unethical for a lawyer to attempt to access a private profile by "friending" an unrepresented witness).

168. *See id.* (refusing to find similarity between videotaping public conduct of plaintiff in personal injury case and accessing a private profile).

169. *See id.* ("[t]he fact that access to pages may readily be obtained by others who either are or are not deceiving [a] witness . . . does not mean that deception at the direction of the inquirer is ethical").

170. *Id.* at 1 (demonstrating the tendency of a particular user to accept any friendship request).

171. *See* Phila. Bar Ass'n Prof'l Guidance Comm., Op. 2009-02, 1, 1 (2009) (showing that social networking site users tend not to be overly selective when accepting friend requests).

172. *See id.* (indicating how attorneys attempt to get around the rule by having third parties "friend" witnesses).

The answer is no in any conceivable sense.[173] Apart from a public invitation from the represented party stating that they will accept any friend request—for example, a posting by the represented party on a publicly-accessible Internet forum—there is no way to know whether someone will accept all friend requests; even if an attorney could show that the party had thousands of friends, that would fail to demonstrate that the party had never rejected any requests, or that they accepted all requests as a policy.[174] And even if an attorney could point to such a public invitation by the represented party it would still not be enough; the fact that the user had at one point made such an invitation would not mean that this invitation was made in perpetuity, nor would there be any way to show that this was the case.[175] Ultimately, there is nothing inherent to a social networking profile that invites such requests in the same manner that a business' e-store or feedback form invites contact; on the contrary, the fact that the user has chosen to require approval before granting access indicates that the opposite is true.[176] The Philadelphia Bar properly rejected this argument.[177]

There is one other circumstance where it could be conceivably appropriate for an attorney to request access to a

173. *See id.* at 3 (stating that "the Committee believes that the proposed course of conduct . . . would violate [the Rule] because the planned communication by the third party with the witness is deceptive").

174. *See id.* (suggesting that there is no possible way to demonstrate that a particular user will accept any friendship request). Even if the attorney was granted access, there is no way for the attorney to show that they were granted access as a matter of rote, standardized response, instead of as a discretionary, personalized judgment by the user. *See id.* at 1. It is possible that a user may have 150,000 friends and still maintain discretionary control over who they allow access; at best, the attorney can only tell whose friend requests the user has approved—not if they have rejected anyone. *See id.*

175. *See* Phila. Bar Ass'n Prof'l Guidance Comm., Op. 2009-02, 1, 1 (2009) (concluding that a showing of one's apparent readiness to accept all friend requests does not make the practice any less deceptive); *see also* Awsumb, *supra* note 149, at 24 (noting further the deceptive nature of this practice despite one's willingness to accept friend requests).

176. *See* Hodge, *supra* note 148, at 106 (suggesting that a distinction exists between the privacy expectations inherent to different forms of online communication); *see also Facebook's Privacy Policy*, *supra* note 46 (demonstrating the ability of Facebook users to limit access to their profiles).

177. *See* Phila. Bar Ass'n Prof'l Guidance Comm., Op. 2009-02, 1, 1 (2009) (accepting the notion that a social network user can successfully limit access to their profile).

represented party's private profile: when the represented party's act of approving or disapproving access to their profile is the conduct that the attorney wishes to observe.[178] In that case, the attorney is acting as any other member of the public, and as stated, their conduct is formulaic–they are literally just filling out a form.[179] But this situation is a true hypothetical; it is almost impossible to imagine a matter where a represented party's practice of accepting or denying friend requests would be at issue. Moreover, even if that were the case, this should still be barred because it might result in the represented party granting access–which would result in the private profile becoming available to the attorney.[180] Since the actual profile would still not be available to the general public, and still not be protected by the observation exception, this would result in a violation of Rule 4.2, even if the attorney was not seeking to access the profile itself.[181] And again, although the attorney's request may be formulaic, the response is not; the profile's owner is rendering a personalized response unique to the attorney's request, not a formulaic response in the manner of a business fulfilling an order from an e-store.[182]

Thus, Rule 4.2 bars an attorney from attempting to access a represented party's private profile.[183] Any conceivable circumstance where this might be permissible is theoretical at best. Any attorney believing that they have found the exception

178. *See* Awsumb, *supra* note 149, at 25 (declaring that when information contained on a social networking profile is "placed at issue in the case," discovery may be permitted).

179. *See* 2001 Oregon Op., *supra* note 5, at 2 (reasoning that a lawyer may communicate with a party's website so long as the response is essentially formulaic); *see also* State *ex rel. State Farm*, 451 S.E.2d at 730 (equating attorney's conduct to that of general public).

180. *See* 2005 Oregon Op., *supra* note 5, at 452 (prohibiting attorney communication with a represented party).

181. *See* ANN. MODEL RULES OF PROF'L CONDUCT R. 4.2 Ann. *Observing (2007) (stating observation of information on public website not a violation of Rule 4.2).

182. *See* 2001 Oregon Op., *supra* note 5, at 2 (implying that viewing and purchasing products from a represented party's e-store is formulaic).

183. *See* MODEL RULES OF PROF'L CONDUCT R. 4.2 (2006) (prohibiting attorney communication with a represented party).

to this rule is advised to seek a court order before attempting access.[184]

IV. CONCLUSION

Internet culture and technologies tend to evolve and change at remarkably fast speeds. Whether a particular social networking site–or social networking sites in general–will continue to be the web juggernaut they have been over the past few years will remain to be seen, but in the absence of any new platform or transformative event, they are likely to continue to rise in popularity for the foreseeable future. At any rate, because attorneys and law enforcement professionals have already started to utilize these websites in litigation and law enforcement actions, it is necessary for there to be some sort of rubric by which bar committees and courts can analyze this behavior under the ethical rules. At least as to Rule 4.2, that rubric is the observation exception. The observation exception reaches the same result as the cases already decided and provides a more consistent framework for analyzing new scenarios than direct analogy to offline conduct. When applied to social networking sites, it yields the results of allowing attorneys to view public and open network profiles, and prohibiting them from viewing private and closed network profiles.

184. *See* MODEL RULES OF PROF'L CONDUCT R. 4.2 cmt. 6 (2006) (advising attorney to seek court order if uncertain about legality of communication with represented party).