ARTICLE

Pamela A. Bresnahan & Lucian T. Pera

The Impact of Technological Developments on the Rules of Attorney Ethics Regarding Attorney–Client Privilege, Confidentiality, and Social Media

Abstract. This article focuses on the development of the law of ethics and technology. Emphasis is placed on how technological developments have affected the rules and means by which lawyers practice law and certain ethical pitfalls that have developed hand-in-hand with technological advancements. Topics examined include: (1) the ways by which electronic communication has increased the potential for the attorney–client privilege to be waived and the resulting impact on the present-day practice of law; (2) the effect of social media on lawyers' ethical obligations, including counseling clients regarding the client's use of social media and the lawyer's own use of social media; and (3) the impact of cloud computing on a lawyer's obligation to protect client confidences. The authors examine the development of these technological effects on the practice of law through an examination of the evolution of the American Bar Association, its Model Rules of Professional Conduct, and state ethics opinions and representative case law.

Authors. Pamela A. Bresnahan is a Partner and head of the litigation practice group in the Washington D.C. office of Vorys, Sater, Seymour and Pease LLP. Lucian T. Pera is a Partner in the Memphis, Tennessee office of Adams and Reese LLP. The authors would like to thank Adam J. Singer, an associate in the Washington D.C. office of Vorys, Sater, Seymour and Pease LLP, for his assistance in preparing this Article.

ARTICLE CONTENTS

I. INTRODUCTION

Technological advancements continue to revolutionize the way modern communication takes place and the way in which people access and utilize information. Such advancements impact almost all industries. The practice of law is no exception. Lawyers and law firms now communicate with each other and with clients by electronic means, utilize mobile devices, maintain electronic files, and even store client information "in the cloud." While new technologies provide lawyers and law firms with faster and more efficient means to practice law, they present new challenges for lawyers and law firms to comply with their ethical obligations. In many instances, the ethical rules that govern lawyers were developed prior to the implementation of new technologies that have since become commonplace in other areas of life. Indeed, the American Bar Association (ABA) formed the "Commission on Ethics 20/20"[1] in 2009, which recognizes that "[t]echnological advances and

1. *See ABA Commission on Ethics 20/20*, A.B.A, http://www.americanbar.org/groups/professional_responsibility/aba_commission_on_ethics_20_20/about_us.html (last visited Dec. 19, 2016) ("The ABA Commission on Ethics 20/20 was created by then ABA President Carolyn B. Lamm

globalization have changed our profession in ways not yet reflected in our ethics codes and regulatory structure."[2]

This Article examines how certain technological developments have affected ethics in the practice of law. Part I discusses on the impact of technology on the concept of attorney–client privilege and the resulting ethical implications. Part II focuses on ethical issues that arise with the use of social media, including the use of social media by clients and by lawyers. Part III focuses on the obligations of lawyers to protect client confidences when using new technology, with an emphasis on the use of cloud computing.[3]

II. TECHNOLOGY AND THE ATTORNEY–CLIENT PRIVILEGE

While technological developments have provided lawyers and their clients with an increased ability to communicate with each other, those developments also allow for increased opportunities for third parties to gain access to communications between a lawyer and a client. Consequently, communication by electronic means carries with it the greater potential for the attorney–client privilege not to attach to communications between a lawyer and a client in the first place or for the privilege to be waived. This Section examines the means by which the attorney–client privilege can fail to attach or be waived by the use of modern technology and the resulting implication on a lawyer's ethical obligations.

The attorney–client privilege protects communications between an attorney and client "for the purpose of obtaining or providing legal assistance for the client."[4] Confidential communications are those that are "not intended to be disclosed to third persons other than in the course of rendering legal services to the client or transmitting the communications by reasonably necessary means."[5]

---

to perform a thorough review of the ABA Model Rules of Professional Conduct and the U.S. system of lawyer regulation in the context of advances in technology and global legal practice developments.").

2. Michael E. Lackey Jr. & Joseph P. Minta, *Lawyers and Social Media: The Legal Ethics of Tweeting, Facebooking and Blogging*, 28 TOURO L. REV. 149, 154 (2012) (quoting Press Release, ABA, ABA President Carolyn B. Lamm Creates Ethics Comm'n to Address Tech. and Global Practice Challenges Facing U.S. Lawyers (Aug. 4, 2009)).

3. Unless noted otherwise, references herein to the "Rules of Professional Conduct" or a particular rule of professional conduct refer to the current American Bar Association Model Rules of Professional Conduct.

4. *In re* Lindsey, 148 F.3d 1100, 1123 (D.C. Cir. 1998) (per curiam).

5. Fed. Election Comm'n v. Christian Coal., 178 F.R.D. 61, 66 (E.D. Va. 1998), *aff'd in part, modified in part*, 178 F.R.D. 456 (E.D. Va. 1998); *see also* United States v. (Under Seal), 748 F.2d 871, 874 n.6 (4th Cir. 1984) (stating the Supreme Court Standard 503(a)(4) is "[a confidential] communication . . . not intended to be disclosed to third persons other than those to whom disclosure

The work–product doctrine, the "inseparable twin" to the attorney–client privilege, protects a lawyer's "mental impressions, opinions, and/or legal theories concerning litigation."[6] In *United States v. Nobles*,[7] the Supreme Court of the United States recognized that the work–product doctrine protects not only materials prepared by an attorney, but also those prepared by agents for an attorney.[8] This recognition was grounded in the fact that "attorneys often must rely on the assistance of investigators and other agents in the compilation of materials in preparation for trial."[9] Although the work–product doctrine is a separate concept from the attorney–client privilege, the same principles recognized by the *Nobles* Court also apply to the attorney–client privilege.[10]

With the advent of modern technology and the use of new technologies in the practice of law, lawyers are now employing agents for new and previously unforeseen purposes, such as storing client files "in the cloud." Recognizing the new purposes for which technology providers are being utilized, the ABA amended the Model Rules of Professional Conduct in 2012 "to reflect the changing role of technology in legal practice and specifically recognized the need for reliance on such technology providers in supplying legal services."[11] For example, Comment 3 to Model Rule 5.3, which generally governs a lawyer's responsibility to oversee non-lawyer assistants of all kinds, now includes the following language:

> A lawyer may use nonlawyers outside the firm to assist the lawyer in rendering legal services to the client. Examples include the retention of an investigative or paraprofessional service, hiring a document management company to create and maintain a database for complex litigation, sending client documents to a third party for printing or scanning, and using an Internet-

---

is in furtherance of the rendition of professional legal services to the client or those reasonably necessary for the transmission of the communication").

6. NXIVM Corp. v. O'Hara, 241 F.R.D. 109, 126 (N.D.N.Y. 2007).

7. United States v. Nobles, 422 U.S. 225 (1975).

8. *Id.* at 238 ("It is therefore necessary that the [work-product] doctrine protect material prepared by agents for the attorney as well as those prepared by the attorney himself.").

9. *Id.*

10. Fed. Election Comm'n, 178 F.R.D. at 66 (listing the requirements for a document to be protected under attorney–client privilege).

11. Troutman Sanders LLP, *Breaking the Seal: Does Using Third Party eDiscovery Vendors Raise Privilege and Work Product Issues?*, INFO. INTERSECTION (July 17, 2014), http://www.informationintersection.com/2014/07/breaking-the-seal-does-using-third-party-ediscovery-vendors-raise-privilege-and-work-product-issues/.

based service to store client information.[12]

However, the way in which technology providers are now being used to assist lawyers and law firms necessitates an examination of the concept of attorney–client privilege and confidentiality in the digital age. Consistent with *Nobles*, the attorney–client privilege will extend to protect otherwise privileged communications where a lawyer or a law firm shares those communications with a vendor deemed necessary to facilitate the representation.[13] Thus, a law firm generally will not be deemed to have waived information protected by the attorney–client privilege by "contracting with an independent contractor . . . to provide a necessary service that the law firm feels it needs in order to effectively represent its clients."[14]

While a law firm's legitimate use of technology providers to assist in its practice may not jeopardize the attorney–client privilege, a client's decision to use certain technology, in connection with that client's communications with counsel, might be more precarious.[15] For example, under certain circumstances, a client or potential client's communications with a lawyer or potential lawyer by e-mail may not be protected by the attorney–client privilege.[16] Generally, e-mail communications between an attorney and client or potential client will be protected by attorney–client privilege, so long as the communication was for the purpose of securing legal assistance or advice.[17] However, that may not be the case where the client utilizes an e-mail account or computer belonging to their employer.

In *Holmes v. Petrovich Development Corp.*,[18] an employee's (Ms. Holmes) e-mail communications with counsel were found to not be protected by the attorney–client privilege. The employee, who filed suit against her employer for sexual harassment, retaliation, wrongful termination, violation of her

12. MODEL RULES OF PROF'L CONDUCT r. 5.3 cmt. 3 (AM. BAR ASS'N 2016).

13. *Id.* ("When retaining or directing a nonlawyer outside the firm, a lawyer should communicate directions appropriate under the circumstances to give reasonable assurance that the nonlawyer's conduct is compatible with the professional obligations of the lawyer.").

14. Compulit v. Banctec, Inc., 177 F.R.D. 410, 412 (W.D. Mich. 1997).

15. *See* Holmes v. Petrovich Dev. Co., 191 Cal. App. 4th 1047, 1047 (Cal. Ct. App. 2011) (holding an employee's e-mail communications with her attorney using her employer's computer are not protected by attorney–client privilege).

16. *Id.*

17. *See* Wultz v. Bank of China, 979 F. Supp. 2d 479, 487 (S.D.N.Y. 2013) ("'In order to prevail on an assertion of the attorney–client privilege the party invoking the privilege' must show [they sought the communication with the lawyer] . . . 'for the purpose of securing primarily either (i) an opinion on law or (ii) legal services or (iii) assistance in some legal proceeding . . . .'" (quoting Colton v. United States, 306 F.2d 633, 637 (2d Cir. 1962))).

18. Holmes v. Petrovich Dev.Co., 191 Cal. App. 4th 1047 (Cal. Ct. App. 2011).

right to privacy, and intentional infliction of emotional distress, had used the employer's company computer to e-mail an attorney regarding her potential claims.[19] The court determined that the communications between Ms. Holmes and her attorney were not privileged because they were not confidential communications.[20] Under the circumstances, the communications were not transmitted in a manner protected from disclosure to third persons other than those necessary to further the interest of the client.[21] Although privileged communications do not lose their privileged character by virtue of the fact that they were sent by e-mail, the court concluded that such communications are not privileged where:

> (1) . . . the electronic means used belongs to the defendant; (2) the defendant has advised the plaintiff that communications using electronic means are not private, may be monitored, and may be used only for business purposes; and (3) the plaintiff is aware of and agrees to these conditions.[22]

Because Ms. Holmes used the company computer, knowing that this use violated company computer policy and that they could be discovered due to company monitoring of e-mail use, Ms. Holmes' e-mails were "akin to consulting her lawyer in her employer's conference room, in a loud voice, with the door open, so that any reasonable person would expect that their discussion of her complaints about her employer would be overheard by him."[23]

Further, Ms. Holmes' subjective belief that her e-mail communications with her attorney were private did not alter the result. Ms. Holmes believed the communications were "private because she utilized a private password to use the company computer and she deleted the e-mails after they were sent."[24] However, the company's e-mail policy made that belief objectively unreasonable.[25]Ms. Holmes was "warned that the company would monitor e-mail to ensure employees were complying with office policy not to use company computers for personal matters, and she was told that she had no expectation of privacy in any messages she sent via the company computer."[26] Additionally, Ms. Holmes' belief that the company did not,

19. *Id.* at 1056.
20. *Id.* at 1068.
21. *Id.*
22. *Id.*
23. *Id.* at 1069.
24. *Id.* at 1069.
25. *Id.*
26. *Id.*

in reality, monitor e-mail in accordance with the written policy did not alter the analysis. The court stated that "[a]bsent a company communication to employees explicitly contradicting the company's warning to them that company computers are monitored to make sure employees are not using them to send personal e-mail, it is immaterial that the 'operational reality' is the company does not actually do so."[27] Such an "operational reality" scenario was seen as an unreasonable belief on the part of the employee, analogous to one believing that he or she is able to exceed a speed limit with impunity merely because a particular roadway is seldom patrolled.[28]

In a slightly different fact pattern, Marina Stengart (Ms. Stengart) filed an employment discrimination lawsuit against her employer, Loving Care Agency, Inc. (Loving Care).[29] In anticipation of discovery, Loving Care hired a computer forensic expert to recover files stored on the company-issued laptop Ms. Stengart used while employed at Loving Care.[30] Among the files stored on that laptop were e-mails Ms. Stengart had exchanged with her attorney.[31] Although Ms. Stengart sent and received those e-mails by her personal, password-protected, web-based e-mail account, and did not use her company e-mail account, the company-issued laptop had automatically saved the e-mails to its hard drive.[32] While she did not intend for copies of the e-mails to be saved, default settings on the Internet browser, unbeknownst to her, automatically saved copies of her browsing sessions while she used her personal e-mail account.[33] In contrast with *Holmes*, the Supreme Court of New Jersey ultimately determined that the e-mails between Ms. Stengart and her attorney were protected by the attorney–client privilege and that the privilege had not been waived.[34]

Loving Care's employee handbook noted that the company "reserves and will exercise the right to review, audit, intercept, access, and disclose all matters on the company's media systems and services at any time, with or without notice."[35] Loving Care contended that the language of the policy precluded its employees from having an expectation of privacy in their use of Loving Care's computers.[36] The court, however, noted that it was not

27. *Id.* at 1071.
28. *Id.*
29. Stengart v. Loving Care Agency, Inc., 990 A.2d 650, 655 (N.J. 2010).
30. *Id.*
31. *Id.*
32. *Id.* at 655–56.
33. *Id.*
34. *Id.* at 655.
35. *Id.* at 657.
36. *Id.* at 658.

clear whether the policy covered an employee's use of personal, password-protected, web-based e-mail because the policy did not address personal e-mail accounts.[37] Therefore, employees did "not have express notice that messages sent or received on a personal, web-based e-mail account [were] subject to monitoring if company equipment [was] used to access the account."[38] The policy also did not provide notice that such e-mails would be stored on the company computer's hard drive.[39] The court ultimately determined that Ms. Stengart had a reasonable expectation of privacy in the e-mails exchanged with her attorney.[40] First, Ms. Stengart had a subjective expectation of privacy, because she took steps to protect the privacy of the e-mails by using a personal, password-protected e-mail account and did not save her account password on the company computer.[41] Her expectation of privacy was found to be objectively reasonable because Loving Care's policy did not address the use of private, web-based e-mails and did not inform employees that Loving Care could retrieve these e-mails.[42] Thus, the e-mails were protected by the attorney–client privilege.[43]

The takeaway from *Holmes* and *Stengart* is that the language of an employer's policy is instrumental in determining whether the attorney–client privilege will attach to communications between an employee and an attorney when such communications are sent or received using the employer's equipment. The language of the policy will likely determine whether the employee's subjective expectation of privacy is objectively reasonable. In *Stengart*, the court concluded that the language of the policy did not give Ms. Stengart "cause to anticipate that Loving Care would be peering over her shoulder as she opened e-mails from her lawyer on her personal, password-protected Yahoo account."[44] Therefore, the court implied that had the policy provided Ms. Stengart with notice that Loving Care would "peer over her shoulder," her expectation of privacy might not have been objectively reasonable.[45] Thus, under circumstances where company policy provides clear notice regarding e-mail usage, such as the notice provided in *Holmes*, it is crucial that employees not use company e-

37. *Id.* at 659.
38. *Id.*
39. *Id.*
40. *Id.* at 663.
41. *Id.*
42. *Id.*
43. *Id.* at 664.
44. *Id.*
45. *Id.*

mail to communicate with their attorneys.[46]

Lawyers rarely know, however, the content of the employer policies that might govern a client's use of an employer-issued computer, smartphone, or tablet computer, or even the current state of the law on the interpretation of those policies in jurisdictions whose law might apply.[47] Of course, it follows that lawyers representing clients who regularly use technology belonging to others must consider advising their clients about the risks involved, and more importantly, should seriously consider having a conversation with clients about how and with what technology they will communicate about any confidential or sensitive matters.[48] Some lawyers—especially perhaps older lawyers—may find it strange that a lawyer today should think about and actually discuss with a client at the outset of representation what technology they will use to communicate, but having such a conversation is becoming more important with each new change in the technologies clients and lawyers use.[49]

Ethics opinions also point lawyers in this direction.[50] ABA Model Rule of Professional Conduct 1.1 requires an attorney to provide competent representation to a client and ABA Model Rule 1.6 requires an attorney to protect the confidentiality of information relating to the representation of a client.[51] Because the attorney–client privilege might not attach to electronic communications sent or received using an employer's computer, the ABA Standing Committee on Ethics and Professional Responsibility has concluded that ABA Model Rules 1.1 and 1.6 require an attorney to warn a

46. Holmes v. Petrovich Dev. Co., 191 Cal. App. 4th 1047, 1068 (Cal. Ct. App. 2011) (clarifying the use of e-mail to communicate with an attorney falls under the attorney–client privilege unless "the electronic means used belongs to the defendant[,] the defendant has advised the plaintiff that communications using electronic means are not private . . . [and] the plaintiff is aware of and agrees to these conditions").

47. Jonathan Levy, Note, *Employee E-Mails and the Concept of Earning the Privilege*, J. L. & POL'Y FOR INFO. SOC'Y 245, 247 (2013) ("Courts addressing the applicability of the attorney–client privilege to employees who communicate with their attorneys via e-mail on an employer's computer have come up with a variety of conclusions.").

48. *See* Holmes, 191 Cal. App. 4th at 1056 (recounting a situation where an attorney advised against the use of client's work computer for attorney–client communications from the beginning of the consultation and proposed a conversation over the phone instead).

49. *See* Steven Masur, *Confidentiality in a High-Tech World,* GP SOLO (July/Aug. 2007), http://www.americanbar.org/content/newsletter/publications/gp_solo_magazine_home/gp_solo_magazine_index/confidentiality.html (noting the potential risk of inadvertent disclosure of a client's confidential information "[i]n our era of virtual offices, shared office spaces, and the continuing tide of ever-evolving technologies").

50. ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 11-459 (2011) (discussing the attorney's duty to protect the confidentiality of e-mail communication with clients).

51. MODEL RULES OF PROF'L CONDUCT r. 1.1, 1.6 (AM. BAR ASS'N 2016).

client regarding the client's use of e-mail in appropriate circumstances.[52] The Committee stated that:

> A lawyer sending or receiving substantive communications with a client via e-mail or other electronic means ordinarily must warn the client about the risk of sending or receiving electronic communications using a computer or other device, or e-mail account, where there is a significant risk that a third party may gain access. In the context of representing an employee, this obligation arises, at the very least, when the lawyer knows or reasonably should know that the client is likely to send or receive substantive client-lawyer communications via e-mail or other electronic means, using a business device or system under circumstances where there is a significant risk that the communications will be read by the employer or another third party.[53]

Regardless of whether such communications are legally protected by attorney–client privilege in the relevant jurisdiction, the Committee determined that:

> [A] lawyer should . . . advise [an] employee-client "about the importance of communicating with the lawyer in a manner that protects the confidentiality of email communications, just as a lawyer should avoid speaking face-to-face with a client about sensitive matters if the conversation might be overheard and should warn the client against discussing their communications with others."[54]

The warning becomes necessary because of the risk that such communications will be reviewed by others or found to be admissible in judicial proceedings.[55] Consistent with workplace realities today, the Committee observed that, unless a lawyer has reason to believe otherwise, a lawyer "ordinarily should assume that an employer's internal policy allows for access to the employee's e-mails sent to or from a workplace device or system."[56]

Although the employee-client is the predominant scenario, it is not the only circumstance under which a lawyer's ethical obligations may require a lawyer to warn a client about the use of electronic communications. Any time there is a risk that a client might send or receive attorney–client communications from a device or account to which a third party may gain

52. ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 11-459 (2011).
53. *Id.*
54. *Id.*
55. *Id.*
56. *Id.*

access, such an ethical obligation will arise. Consider, for example, the client engaged in divorce proceedings who shares a home computer or iPad with other family members or the client in a business dispute with a partner who might use the business' e-mail system for e-mail communications. The Committee concluded that:

> Whenever a lawyer communicates with a client by e-mail, the lawyer must first consider whether, given the client's situation, there is a significant risk that third parties will have access to the communications. If so, the lawyer must take reasonable care to protect the confidentiality of the communications by giving appropriately tailored advice to the client.[57]

III. THE IMPACT OF SOCIAL MEDIA ON LAWYER'S ETHICAL OBLIGATIONS

Multiple rules of professional conduct are implicated by the use of social media. A lawyer's ethical obligations may be affected as a result of a client's use of social media or the lawyer's own use of social media. Consequently, multiple state bar associations have begun to issue guidance on the ways in which lawyers' ethical obligations apply to the use of social media.

A. *A Client's Use of Social Media*

A client's use of social media may affect the attorney–client privilege in a different way than the client's use of employer e-mail. In contrast to the potential for the attorney–client privilege not to attach in the latter instance (where a client uses an employer's computer or e-mail system to send or receive electronic communications with an attorney), a client's use of social media or other forms of online communication create the potential for the attorney–client privilege to be waived with respect to communications in which the privilege has previously attached.[58] Use of social media may also provide ammunition to a party's opponent, because of a client's misunderstanding about the level of confidentiality of the client's online communications and their legal ramifications.[59]

In *Lenz v. Universal Music Corp.*,[60] comments posted by the plaintiff on a

57. *Id.*

58. *See* Lenz v. Universal Music Corp., No. 5:07-cv-03783 JF (PVT), 2010 WL 4789099, at *5 (N.D. Cal. Nov. 16, 2010) ("A party may not attempt to explain an apparent admission [posted on a social media outlet] as a misinterpretation of a conversation with counsel, and then deny the opposing party on the basis of privilege access to the very conversations at issue.") *enforcing* No. C-0703783 JF (PVT), 2010 WL 4286329 (N.D. Cal. Oct. 22, 2010).

59. *See id.* ("When a client reveals to a third party that something is 'what my lawyer thinks,' she cannot avoid discovery on the basis that the communication was confidential.").

60. Lenz v. Universal Music Corp., No. 5:07-CV-03783 JF (PVT), 2010 WL 4789099 (N.D. Cal.

blog regarding certain communications with her counsel constituted waiver of the attorney–client privilege as to those communications.[61] There, Stephanie Lenz (Ms. Lenz) sued Universal Music Corporation (Universal) after the website YouTube complied with a takedown notice sent to it by Universal.[62] The takedown notice alleged that a home video, uploaded to YouTube by Ms. Lenz, infringed on Universal's copyright in the Prince song *Let's Go Crazy*.[63] Thereafter, Ms. Lenz sued Universal, alleging that Universal knowingly misrepresented that her video infringed upon Universal's copyright.[64] In response to Ms. Lenz making comments on her blog, in e-mails, and in electronic "chats" with friends, as well as statements to reporters, Universal moved to compel discovery relating to the conversations that Ms. Lenz discussed.[65] One of Ms. Lenz's communications to a friend stated that Ms. Lenz's counsel was "very, very interested in the case" and "is pretty well salivating over getting their teeth into [Universal]."[66] Ms. Lenz also wrote to her mother that her counsel planned a "publicity blitz and/or lawsuit against Universal."[67] Universal contended that Ms. Lenz's communications with third parties revealed that her motivations for filing the lawsuit were to give her attorneys an opportunity to "get [] their teeth into [Universal]," and not to vindicate her First Amendment rights.[68] Ms. Lenz countered that the comments only revealed information regarding her attorneys' motives for representing her pro bono, not her own motivations for filing suit.[69] The magistrate judge disagreed with Ms. Lenz and found that her communications related to the substance of her conversations with counsel.[70] The magistrate, therefore, determined the attorney–client privilege had been waived and ordered further discovery regarding Ms. Lenz's communications, a determination that the district court affirmed.[71]

Nov. 17, 2010), *enforcing* No. C 07-03783 JF (PVT), 2010 WL 4286329 (N.D. Cal. Oct. 22, 2010).

61. *Id.* at *1.

62. *Id.*

63. *Id.*

64. *Id.*

65. *Id.*

66. *Id.* at *2.

67. *Id.*

68. *Id.*

69. *Id.* at *3.

70. *See id.* at *2 (citing Judge Trumbell's decision that Universal is owed further discovery concerning those attorney–client conversations since Lenz's communication to third parties revealed the actual substance of attorney–client discourse).

71. *See id.* (upholding the court's order granting defendant's motion to compel production of privileged testimony).

In *McMillen v. Hummingbird Speedway, Inc.*,[72] Bill R. McMillen, Sr. (Mr. McMillen) filed suit to recover damages for injuries sustained during a cool down lap at a stock car race.[73] Defendant, Hummingbird Speedway, Inc. (Hummingbird) asked Mr. McMillen, in an interrogatory, whether he belonged to any social networking websites, and if so, to provide his user name and password to such websites.[74] Mr. McMillen responded by stating that he belonged to Facebook and MySpace but that he would not provide his login credentials.[75] Hummingbird and the other defendants filed a motion to compel after their review of the public portions of Mr. McMillen's Facebook page revealed Mr. McMillen had made comments about a fishing trip and his attendance at the Daytona 500 race.[76] Defendants contended such comments on the publicly-accessible portion of Mr. McMillen's Facebook page provided cause to believe that the non-publicly accessible portions of Mr. McMillen's social media accounts might contain additional evidence relevant to Mr. McMillen's claim for damages.[77] Mr. McMillen argued that communications shared with one's private friends on social media are confidential and should be protected from disclosure.[78] The court determined while each website at issue provided a certain level of privacy by allowing users the opportunity to choose which posts are public and which are shared only with identified persons, "their terms and privacy policies should dispel any notion that information one chooses to share, even if only with one friend, will not be disclosed to anybody else."[79] Users are put on notice that their communications may be disseminated by those users with whom a post is shared.[80] Additionally, the operators of social networking websites have access to each post.[81] Thus, "[w]ithout more, the complete access afforded to the Facebook and MySpace operators defeats McMillen's proposition that his communications are confidential [and t]he law does not even protect otherwise privileged communications made in the

72. McMillen v. Hummingbird Speedway, Inc., No. 113-2010 CD, 2010 WL 4403285 (Pa. Com. Pl. Sept. 9, 2010).

73. *Id.* at *1.

74. *Id.*

75. *Id.*

76. *Id.*

77. *Id.* at *1–2.

78. *Id.* at *2.

79. *Id.* at *3–4.

80. *Id.* at *4. *See generally Data Policy*, FACEBOOK, https://www.facebook.com/about/privacy/ (last visited Dec. 19, 2016).

81. McMillen v. Hummingbird Speedway, Inc., No. 113-2010 CD, 2010 WL 4403285, at *4–5 (Pa. Com. Pl. Sept. 9, 2010).

presence of third parties."[82] Therefore, the court concluded that Facebook and MySpace users have consented to their posts being reviewed by a third party, the site operators, which is "wholly incommensurate with a claim of confidentiality."[83] Because the public portions of Mr. McMillen's social media revealed content suggesting that Mr. McMillen may have exaggerated his injuries, it was reasonable to assume that the private portions might contain additional information relevant to the defendants' defense.[84] Accordingly, the court ordered Mr. McMillen to provide to defense counsel his user names and passwords, and told him to not take any steps to delete or alter information on his Facebook and MySpace accounts.[85]

Not surprisingly, the risks that social media might present to a client's case, such as what occurred in *McMillen*, has caused state bar associations to examine attorneys' ethical obligations regarding a client's use of social media. The Pennsylvania Bar Association has concluded that competent representation, pursuant to the Pennsylvania version of Rule 1.1 of the ABA Model Rules of Professional Conduct generally requires a lawyer to "advise clients about the content of their social media accounts, including privacy issues, as well as their clients' obligation to preserve information that may be relevant to their legal disputes."[86] Further, it is reasonable to expect that opposing counsel will monitor a client's use of social media and, therefore, it may be appropriate to track one's own client in order to stay informed of potential developments in a case.[87]

With respect to the advice a lawyer may provide to a client regarding the client's use of social media, bar associations that have examined the topic have generally concluded that a lawyer may advise a client to change social media privacy settings and may also advise a client regarding what content should be made private or be removed from the client's social media pages.[88] The Florida Bar Association has even concluded a lawyer may

82. *Id.* at *5.

83. *Id.*

84. *Id.* at *6.

85. *Id.* at *8.

86. *See* Pa. Bar Ass'n Legal Ethics & Prof'l Responsibility Comm., Formal Op. 2014-300 (2014) (indicating a lawyer's duty includes advising clients about the content of their social media activity as it relates to privacy and preservation thereof, especially with regard to legal disputes); *see also* MODEL RULES OF PROF'L CONDUCT r. 1.1 (AM. BAR ASS'N 2016) (discussing a lawyer's duty to provide competent advice to clients).

87. Pa. Bar Ass'n Legal Ethics & Prof'l Responsibility Comm., Formal Op. 2014-300 (2014).

88. *See id.* (confirming a lawyer may ethically advise a client to modify privacy settings on social media platforms, and remove content provided there is no violation of statutes, rules, or common law relating to evidence preservation); *see also* Fla. Bar Ass'n Prof'l Ethics Comm., Op. 14-1 (2015) (protecting lawyers' abilities within the law to advise clients to maximize privacy settings on their social

advise a client to remove content from the client's social media that is relevant to a foreseeable judicial proceeding.[89] However, a lawyer may only provide such advice if the information or data to be removed is preserved.[90] When it is permissible for a lawyer to counsel a client to remove certain information from social media, the Philadelphia Bar Association has warned that the lawyer must also "take appropriate action to preserve the information in the event it should prove to be relevant and discoverable."[91]

Additionally, ethics opinions have determined that "[a] [lawyer] may not advise a client to post false or misleading [content]."[92] Also, a lawyer may not offer evidence of social media content in a judicial proceeding that the lawyer knows is false.[93] Doing so violates Rule 4.1 of the Model Rules of Professional Conduct, which prohibits a lawyer from "mak[ing] false statement[s] of material fact or law."[94]

B. *A Lawyer's Use of Social Media*

The pervasiveness of social media in recent years has sparked ethics opinions to address not only the advice lawyers should provide to clients regarding social media use, but also the permissible ways in which attorneys may use social media in their own practices. Social media websites have been described as having become "indispensable tools used by legal professionals and those with whom they communicate."[95] The rapid growth of social media has even prompted the Commercial and Federal

media platforms and to remove content where a duty to preserve evidence under law does not exist); *accord* N.Y. Cnty. Lawyer Ass'n Prof'l Ethics Comm., Op. 745 (2013) (clarifying an attorney's competent duty to advise clients concerning social media privacy settings, and permitting lawyers to advise clients against posting certain content on public and/or private pages and whether content may be removed, provided that there is no violation of rules or substantive law regarding evidence preservation).

89. *See* Fla. Bar Ass'n Prof'l Ethics Comm., Op. 14-1 (2015).

90. *Id.* ("The [Florida Bar] is of the opinion that if the inquirer does so, the social media information or data must be preserved if the information or data is known by the inquirer or reasonably should be known by the inquirer to be relevant to the reasonably foreseeable proceeding.").

91. Phila. Bar Ass'n Prof'l Guidance Comm., Op. 2014-5 (2014).

92. *See* Pa. Bar Ass'n Legal Ethics & Prof'l Responsibility Comm., Formal Op. 2014-300 (2014) ("[A]n attorney may not advise a client to post false or misleading information on a social networking website; nor may an attorney offer evidence from a social networking website that the attorney knows is false.").

93. *Id.*

94. *Id.* (enforcing Rule 4.1 of the Model Rules of Professional Conduct); *accord* MODEL RULES OF PROF'L CONDUCT r. 4.1(a) (AM. B. ASS'N 2016) (proscribing lawyers from knowingly falsifying information to third persons).

95. James M. Wicks et al., *Social Media Ethics Guidelines*, COM. & FED. LITIG. SEC., N.Y. ST. B. ASS'N 1 (Updated June, 9 2015), http://www.nysba.org/Sections/Commercial_Federal_Litigation/Com_Fed_PDFs/Social_Media_Ethics_Guidelines.html.

Litigation Section of the New York State Bar Association to recommend a useful set of guidelines regarding the ethical implications of a lawyer's use of social media.[96]

As part of its mandate to update the ABA Model Rules in light of technological changes, the ABA Commission on Ethics 20/20 focused on rules relating to attorney advertising, a topic commonly implicated by a lawyer's use of social media.[97] As a result, the Commission recommended certain changes to the comments of Rule 7.2 of the Model Rule of Professional Conduct, which were adopted by the ABA.[98] Specifically, the Commission proposed adding "'the Internet, and other forms of electronic communication'" to the list of 'powerful media'" found in the comments to Rule 7.2.[99] Comment 3 to ABA Model Rule 7.2 now reads as follows:

> Questions of effectiveness and taste in advertising are matters of speculation and subjective judgment. Some jurisdictions have had extensive prohibitions against television and other forms of advertising, against advertising going beyond specified facts about a lawyer, or against "undignified" advertising. Television, the Internet, and other forms of electronic communication are now among the most powerful media for getting information to the public, particularly persons of low and moderate income; prohibiting television, Internet, and other forms of electronic advertising, therefore, would impede the flow of information about legal services to many sectors of the public. Limiting the information that may be advertised has a similar effect and assumes that the bar can accurately forecast the kind of information that the public would regard as relevant. But see Rule 7.3(a) for the prohibition against a solicitation through a real-time electronic exchange initiated by the lawyer.[100]

Although perhaps a minor clarification, the inclusion of the phrase "the Internet, and other forms of communication" in Comment 3 has been noted by ethics opinions which have concluded that attorneys may advertise using social media, in compliance with Rule 7.2.[101] For instance, the West Virginia Bar Disciplinary Board concluded that social media advertising was

---

96. *Id.*

97. *See* Lackey, Jr. & Minta, *supra* note 2, at 160 (discussing how social media innovations caused the ABA Commission on Ethics 20/20 to conduct an in-depth study of attorney advertising under the ABA Model Rules).

98. *See id.* (referencing comment three on Rule 7.2 of the ABA Model Rules of Professional Conduct).

99. *Id.* at 161 (quoting MODEL RULES OF PROF'L CONDUCT r. 7.2 cmt. 3 (AM. BAR ASS'N 2013)).

100. MODEL RULES OF PROF'L CONDUCT r. 7.2 cmt. 3 (AM. BAR ASS'N 2016).

101 *Id.*

permissible, pursuant to West Virginia Rule of Professional Conduct 7.2, because social media advertising "constitutes advertising via the Internet and/or electronic communication."[102] In support of its conclusion, the West Virginia Lawyer Disciplinary Board stated:

> Indeed, Comment [3] to Rule 7.2 pointedly notes that "[t]elevision, the Internet, and other forms of electronic communication are now among the most powerful media for getting information to the public, particularly persons of low and moderate income; prohibiting television, Internet, and other forms of electronic advertising, therefore, would impede the flow of information about legal services to many sectors of the public."[103]

Therefore, attorneys may generally use social media as a platform to advertise their services, but must, of course, do so in compliance with the rules regarding attorney advertising.[104] For instance, a lawyer "shall not advertise areas of practice under headings in social media platforms that include the terms 'specialist,' unless the lawyer is certified by the appropriate accrediting body in the particular area."[105] The New York City Bar recently adopted a five-element test to determine whether a lawyer's LinkedIn profile or other social media content constituted attorney advertising.[106] The Bar concluded that a LinkedIn profile constitutes attorney advertising if the following criteria are met: (1) the LinkedIn content is a communication made by or on behalf of the lawyer; (2) the primary purpose of the content is to attract new clients to retain the lawyer for pecuniary gain; (3) the content relates to the legal services offered by the lawyer; (4) the content is intended to be viewed by potential new clients; and (5) the content does not fall within any recognized exception to the definition of attorney advertising.[107]

Social media has become a popular and effective way for lawyers to market their services. However, the nature of social media typically allows not only the lawyer/account holder, but also third parties, to post information on the lawyer's social media presence. For example, certain social media websites allow users to submit reviews, recommendations or

---

102. W. Va. Law. Disciplinary Bd., Op. 2015-02 (2015).

103. *Id.* (quoting MODEL RULES OF PROF'L CONDUCT r. 7.2 cmt. 3 (AM. BAR ASS'N 2016).

104. W. Va. Law. Disciplinary Bd., Op. 2015-02 (2015).

105. Wicks et al., *supra* note 95, at 7.

106. *See* N.Y. City B. Prof'l Ethics Comm., Formal Op. 2015-7 (2015) ("An attorney's individual LinkedIn profile or other content constitutes attorney advertising only if it meets all five of the following criteria . . . .").

107. *Id.*

endorsements of a lawyer's services.[108] The ability of third parties to post content to a lawyer's social media page could lead to violations of the lawyer's ethical duties if the lawyer is not vigilant in monitoring what others post on the lawyer's behalf. For example, Rule 8.4(c) prohibits a lawyer from "[engaging] in conduct involving dishonesty, fraud, deceit or misrepresentation."[109] Accordingly, content posted by lawyers on their social media pages must be true, accurate, and non-misleading. Ethics opinions have concluded that lawyers also have an obligation to ensure that content posted to their social media pages by others meets this high standard set for lawyers. For example, the Pennsylvania Bar Association determined that a lawyer should: "(1) monitor his or her social [media] websites, (2) . . . verify the accuracy of any information posted, and (3) . . . remove or correct any inaccurate endorsements."[110]

While social media provides a marketing platform to feature endorsements or recommendations of a lawyer's services, it may also provide a platform for unsatisfied clients to post content that could harm a lawyer's reputation or practice. Lawyers who come across a negative review, while monitoring their social media presence, may feel inclined to respond to protect their practice from the damage such a review might cause. However, responding in-kind could cause attorneys to reveal confidential information, in violation of Rule 1.6.[111] In fact, lawyers have been disciplined for doing so.

For example, a proposed mild form of discipline for one lawyer was rejected as too lenient by the Supreme Court of Georgia, where the lawyer had posted personal and confidential information about a former client in response to a negative review.[112] In her petition for voluntary discipline, Ms. Skinner admitted to "[violating] Rule 1.6 of the Georgia Rules of Professional Conduct" and requested the mildest form of punishment available in Georgia for doing so.[113] The court rejected Ms. Skinner's request.[114] Following rejection of Ms. Skinner's petition, a special master

108. *See* Pa. Bar Ass'n Legal Ethics & Prof'l Responsibility Comm., Formal Op. 2014-300 (2014) (noting certain social networking cites permit clients to review, recommend, or endorse attorneys).

109. MODEL RULES OF PROF'L CONDUCT r. 8.4(c) (Am. B. Ass'n 1983).

110. Pa. Bar Ass'n Legal Ethics & Prof'l Responsibility Comm., Formal Op. 2014-300 (2014).

111. *See* MODEL RULES OF PROF'L CONDUCT r. 1.6 (Am. Bar Ass'n 2016) (stating attorneys cannot reveal a client's information except in specific circumstances).

112. *See In re* Skinner, 740 S.E.2d 171, 171–73 (Ga. 2013) (per curiam) (rejecting the mildest form of discipline for an attorney that posted personal and confidential information about a former client even though the post was in self defense).

113. *Id.* at 172–73.

114.*Id.* at 173.

conducted an evidentiary hearing and concluded that Ms. Skinner had violated Rule 1.6 among other rules.[115] After a client whom Ms. Skinner was representing in an uncontested divorce discharged Ms. Skinner and hired new counsel, the client posted negative reviews of Ms. Skinner on three consumer Internet pages.[116] Ms. Skinner subsequently posted a response to the client's reviews, which "contained personal and confidential information about her former client that Skinner had obtained in the course of her representation of the client."[117] "In particular, Skinner identified the client by name, identified the employer of the client, stated how much the client had paid Skinner, identified the county in which the divorce had been filed, and stated that the client had a boyfriend."[118] After noting there were significant mitigating circumstances involving personal problems experienced by Ms. Skinner during her representation of the client and at the time she posted the confidential information, the Supreme Court of Georgia ordered Ms. Skinner to receive a public reprimand and to consult with the state's law practice management services.[119]

The Hearing Board of the Illinois Attorney Registration and Disciplinary Commission similarly reprimanded an attorney who responded inappropriately to a negative online client review.[120] Ms. Tsamis had represented a client in securing unemployment benefits from the client's former employer.[121] The client terminated Ms. Tsamis' representation after the Illinois Department of Employment Security denied the client's claim for unemployment benefits and, thereafter, posted a negative review of Ms. Tsamis on the legal referral website AVVO.[122] Although AVVO removed the client's post, the client subsequently posted a second negative review to which Ms. Tsamis replied.[123] Ms. Tsamis' response "contained information relating to her representation of [the client] and exceeded what was necessary to respond to [the client's] accusations."[124]

Bar associations have weighed in on the applicability of Rule 1.6's self-defense exception to a lawyer's response to online client reviews. Although

115. *In re* Skinner, 758 S.E.2d 788, 788 (Ga. 2014).

116. *Id.* at 789.

117. *Id.*

118. *Id.*

119. *Id.* at 790.

120. *See* Tsamis, Comm. File No. 2013PR00095 (Ill. 2013), https://www.iardc.org/rd_database/rulesdecisions.html. (reprimanding an attorney for inappropriately revealing information online about a former client).

121. *Id.* at ¶ 4.

122. *Id.* at ¶ 7–8.

123. *Id.* at ¶ 9–10.

124. *Id.* at ¶ 10.

Rule 1.6 allows a lawyer to reveal information otherwise prohibited "to establish a claim or defense on behalf of the lawyer in a controversy between the lawyer and the client . . . or to respond to allegations in any a proceeding concerning the lawyer's representation,"[125] the Pennsylvania Bar Association concluded that "a negative online client review is not a circumstance that invokes the self-defense exception."[126] The Bar Association of San Francisco similarly concluded that the self-defense exception is inapplicable in the context of responding to a negative review. That opinion concluded with:

> Attorney is not barred from responding generally to an online review by a former client where the former client's matter has concluded. Although the residual duty of loyalty owed to the former client does not prohibit a response, Attorney's on-going duty of confidentiality prohibits Attorney from disclosing any confidential information about the prior representation absent the former client's informed consent or a waiver of confidentiality. California's statutory self-defense exception, as interpreted by California case law, has been limited in application to claims by a client (against or about an attorney), or by an attorney against a client, in the context of a formal or imminent legal proceeding. Even in those circumstances where disclosure of otherwise confidential information is permitted, the disclosure must be narrowly tailored to the issues raised by the former client. If the matter previously handled for the former client has not concluded, it may be inappropriate under the circumstances for Attorney to provide any substantive response in the online forum, even one that does not disclose confidential information.[127]

The Social Media Ethics Guidelines of the Commercial and Federal Litigation Section of the New York State Bar Association issued the following guideline:

> Where a lawyer learns that a client has posted a review of her services on a website or on social media, if the lawyer chooses to respond to the client's online review, the lawyer shall not reveal confidential information relating to the representation of the client. This prohibition applies, even if the lawyer is attempting to respond to unflattering comments posted by the client.[128]

To aid lawyers in responding to an unflattering post, the Pennsylvania Bar Association has proposed a suggested response that a lawyer may ethically

125. MODEL RULES OF PROF'L CONDUCT r. 1.6 (AM. BAR ASS'N 2016).
126. Pa. Bar Ass'n Legal Ethics & Prof'l Responsibility Comm., Formal Op. 2014-300 (2014).
127. The B. Ass'n of S.F. Legal Ethics Comm., Op. 2014-1 (2014).
128. Wicks et al., *supra* note 95, at 23.

post in response to a negative review. That response is as follows:

> A lawyer's duty to keep client confidences has few exceptions and in an abundance of caution I do not feel at liberty to respond in a point-by-point fashion in this forum. Suffice it to say that I do not believe that the post presents a fair and accurate picture of the events.[129]

Another rule implicated by a lawyer's use of social media is Rule of Professional Conduct 4.2, which prohibits a lawyer from communicating with a party represented by counsel, unless the lawyer has been granted permission by that party's counsel.[130] Ethics opinions analyzing the prior consent provision of state analogs of Rule 4.2 have interpreted that provision strictly. For example, the New York City Bar and North Carolina State Bar have each concluded that Rule 4.2 prohibits a lawyer from sending a "reply all" e-mail in response to an e-mail sent by opposing counsel, where opposing counsel copied his or her client on the original e-mail, unless opposing counsel has provided express or implied consent to do so.[131]

In the context of social media, the sending of a "friend request" has been interpreted to constitute a communication in violation of Rule 4.2, where a represented party's counsel has not consented to the request.[132] However, accessing the public portion of a represented party's social media website has generally been found to be permissible.[133] Accessing the public portion of a party's social media website, which is that portion that is available to anyone who is a member of that particular social media network, is analogous to "obtaining information that is available in publicly accessible online or print media, or through a subscription research service such as Nexis or Factiva, and that is plainly permitted."[134] Where a lawyer attempts to access the private portions of a party's social media, an ethical boundary

---

129. Pa. Bar Ass'n Legal Ethics & Prof'l Responsibility Comm., Formal Op. 2014-200 (2014).

130 *See* MODEL RULES OF PROF'L CONDUCT r. 4.2 (AM. BAR ASS'N 2016) ("In representing a client, a lawyer shall not communicate about the subject of the representation with a person the lawyer knows to be represented by another lawyer in the matter, unless the lawyer has the consent of the other lawyer or is authorized to do so by law or a court order."). .

131. *See* N.C. State Bar, Formal Op. 7 (2013) (interpreting Rule 4.2 to prohibit an attorney from responding to opposing counsel's e-mail via "reply all" if opposing counsel has copied his client on the e-mail and has not consented to his client being contacted); *see also* The Ass'n of the B. of the City of N.Y. Comm. on Prof'l and Judicial Ethics, Formal Op. 2009-1 (2009) (concluding absent consent, an attorney cannot respond to opposing counsel's e-mail using "reply all" if opposing counsel's client was copied on the original e-mail).

132. *See, e.g.*, Pa. Bar Ass'n Legal Ethics & Prof'l Responsibility Comm.., Formal Op. 2014-300 (2014) ("[T]his Committee also finds that 'friending' a represented party violates Rule 4.2.").

133. *Id.*; *see also* N.Y. State Bar Ass'n, Comm. on Prof'l Ethics, Op. 843 (2010).

134. N.Y. State Bar Ass'n, Comm. on Prof'l Ethics, Op. 843 (2010).

may be crossed, because accessing the private portion entails sending a request, i.e. a communication, to the party, which is, of course, prohibited if that party is represented.[135]

On the other hand, where a party is unrepresented, sending a "friend request" does not implicate Rule 4.2. However, lawyers must remain mindful of their obligations in dealing with unrepresented parties, when sending a "friend request" to a person not represented by counsel. Rule 4.3 requires that "a lawyer . . . not state or imply that the lawyer is disinterested," when dealing with an unrepresented party on behalf of a client, and to "make reasonable efforts to correct the misunderstanding" the unrepresented person may have regarding the lawyer's role.[136] While communicating with an unrepresented party through social media is not prohibited by the ban on lawyer contact with represented parties, the Pennsylvania Bar Association concluded that an "attorney must use his or her own name and state the purpose for contacting the individual" to comply with the attorney's ethical obligations in dealing with an unrepresented party.[137] Further, the lawyer must expressly state the purpose of the request, because failing to do so would be implying that the lawyer is disinterested, according to the opinion, in violation of Rule 4.3.[138]

While a number of bar associations have reached the conclusion that a lawyer must state the purpose for a request to access the private portions of an unrepresented party's social media pages, as the Pennsylvania Bar Association did, not all bar associations have reached this conclusion. The Oregon State Bar determined that a request for access to the private portion of an unrepresented party's social media page "does not in and of itself make a representation about the [l]awyer's role."[139] Therefore, according to the Oregon State Bar, the failure of the lawyer to state the purpose for a request to access private social media pages of an unrepresented party does not imply that the lawyer is disinterested. "On the contrary, it suggests that [the] [l]awyer is interested in the person's social networking information, although

---

135. *See* Pa. Bar Ass'n Legal Ethics & Prof'l Responsibility Comm., Formal Op. 2014-300 (2014) ("[A] request to access the represented party's private page is a prohibited communication under Rule 4.2.").

136. *See* MODEL RULES OF PROF'L CONDUCT r. 4.3 (AM. BAR ASS'N 2016) ("In dealing on behalf of a client with a person who is not represented by counsel, a lawyer shall not state or imply that the lawyer is disinterested. When the lawyer knows or reasonably should know that the unrepresented person misunderstands the lawyer's role in the matter, the lawyer shall make reasonable efforts to correct the misunderstanding.").

137. Pa. Bar Ass'n Legal Ethics & Prof'l Responsibility Comm., Formal Op. 2014-300 (2014).

138. *Id.*

139. Or. State Bar Legal Ethics. Comm., Formal Op. 2013-189 (2013).

for an unidentified purpose."[140] Further, because the social media account holder has control over which persons are granted access to information protected by privacy settings, "the holder's failure to inquire further about the identity or purpose of unknown access requestors is not the equivalent of misunderstanding Lawyer's role in the matter."[141] Thus, according to the Oregon State Bar, a lawyer is not required to state the purpose of a request to access the private portions of an unrepresented party's social media pages. However, if the party asks for additional information or the "[l]awyer has some other reason to believe that the person misunderstands [the lawyer's] role, [then the] [l]awyer must provide the additional information or withdraw the request."[142] Accordingly, there is a split of authority regarding an attorney's ethical obligations when contacting an unrepresented party, in an attempt to gain access to that party's private social media pages.

In contrast with the standards for contacting a represented or unrepresented party, ethics opinions have stated it is never permissible for a lawyer to send a request to gain access to the private portions of a juror's or potential juror's social media pages.[143] Model Rule of Professional Conduct 3.5 states a lawyer shall not "seek to influence a judge, juror, prospective juror or other official by means prohibited by law" or "communicate ex parte with such a person during the proceeding unless authorized to do so by law or court order."[144] The ABA has concluded that a lawyer's review of the public portions of a juror or potential juror's social media presence does not constitute a violation of Model Rule 3.5.[145] However, a request to view private portions of a juror or prospective juror's social media pages is considered "a communication to a juror asking the juror for information that the juror has not made public."[146] "This would be the type of ex parte communication prohibited by Model Rule 3.5(b)."[147] Therefore, although a lawyer may, under certain circumstances, request access to a represented or unrepresented party's

140. *Id.*

141. *Id.*

142. *Id.*

143. ABA Comm'n On Ethics & Prof'l Responsibility, Formal Op. 466 (2014) ("[A] lawyer may passively review a juror's public presence on the Internet, but may not communicate with a juror. Requesting access to a private area on a juror's [social media page] is communication within this framework.").

144. MODEL RULES OF PROF'L CONDUCT r. 3.5(a)–(b) (AM. B. ASS'N 2016).

145. ABA Comm'n on Ethics & Prof'l Responsibility, Formal Op. 466 (2014).

146. *Id.*

147. *Id.*

private social media presence, a lawyer "may not . . . request . . . access [to] the private portions of . . . a juror's social networking website."[148]

C. *Online Communications with Prospective Clients*

The ABA Commission on Ethics 20/20 also proposed—and the ABA adopted—revisions to Rule 1.18 (duties to a prospective client) to clarify the applicability of that rule to online communications.[149] One of the Commission's recommendations was to define a "prospective client" as one who has "a reasonable expectation that the lawyer is willing to consider forming a client–lawyer relationship."[150] The Commission believed this proposed definition of a "prospective client" made the applicable standard "more capable of application to electronic communications."[151] Although Rule 1.18 does not currently define a prospective client in those terms,[152] Comment 2 to Rule 1.18 now includes the following example:

> [A] consultation does not occur if a person provides information to a lawyer in response to advertising that merely describes the lawyer's education, experience, areas of practice, and contact information, or provides legal information of general interest. Such a person communicates information unilaterally to a lawyer, without any reasonable expectation that the lawyer is willing to discuss the possibility of forming a client-lawyer relationship, and is thus not a "prospective client."[153]

Thus, the Commission's recommendation regarding language that more accurately applies to electronic communications provides guidance on the applicability of Rule 1.18 to social media and other electronic communications. Indeed, in the age of social media, lawyers should be aware that participation in online discussions "may trigger duties owed to prospective clients, including a risk of disqualification from representation of an adverse party, fiduciary obligations, and malpractice liability (as well as

148. *See* Pa. Bar Ass'n Legal Ethics & Prof'l Responsibility Comm., Formal Op. 2014-300 (2014) (stating an attorney may access the public information of a juror's social networking site, but a request or attempt to access the private portions of the site would be a violation of Rule 3.5(b)).

149. Lackey, Jr. & Minta, *supra* note 2, at 154 (citing Press Release, A.B.A., ABA President Carolyn B. Lamm Creates Ethics Commission to Address Technology and Global Practice Challenges Facing U.S. Lawyers (Aug. 4, 2009)).

150. *Id.*

151. *Id.*

152. *See* MODEL RULES OF PROF'L CONDUCT r. 1.18 (AM. B. ASS'N 2016) ("A person who consults with a lawyer about the possibility of forming a client-lawyer relationship with respect to a matter is a prospective client.").

153. *Id.* r. 1.18 cmt. 2.

the possible unauthorized practice of law where an attorney provides legal advice in a jurisdiction in which he or she is not licensed)."[154]

IV. CLIENT CONFIDENCES IN THE AGE OF THE CLOUD

One of the most significant technological advancements that implicates a lawyer's obligation to protect client confidences is the use of cloud computing. Cloud computing is described as a "sophisticated form of remote electronic data storage on the internet."[155] "Unlike traditional methods that maintain data on a computer or server at a law office or other place of business, data stored 'in the cloud' is kept on large servers located elsewhere and maintained by a vendor."[156] Use of cloud computing can provide lawyers with increased access to client data and provide clients with increased access to their files over the Internet.[157] Its use may also protect against loss of data, where information is duplicated across multiple servers and regular backups are performed.[158]

Not all services commonly or even fairly described as "cloud computing" raise the same kind of risks for lawyers, because the phrase mostly describes access by way of the Internet to a remote server on which data and applications may be stored, without regard to who owns or controls the servers and the links to it. No matter who owns the technology, however, the lawyer or law firm that stores client confidential information on it has an obligation to take reasonable steps to protect its confidentiality.[159] Still, where the lawyer or law firm "buys" the service of cloud storage of confidential data on technology that the lawyer does not directly own or control, as is the case in many "cloud" services, the risks are different, and the lawyer's obligations are different.[160] The main risk affecting a lawyer's duty to protect client confidences in this context arises from the fact that the information the lawyer is obligated to protect is not under the direct

154. Merri A. Baldwin, *Ethical and Liability Risks Posed by Lawyers' Use of Social Media*, A.B.A. (July 28, 2011), http://apps.americanbar.org/litigation/committees/professional/articles/summer2011-liability-social-media.html.

155. Ala. State Bar Disciplinary Comm'n., Op. 2010-02 (2010) (quoting Richard Acello, *Get Your Head in the Cloud*, A.B.A. J., Apr. 2010, at 28, 28–29).

156. *Id.* (quoting Richard Acello, *Get Your Head in the Cloud*, A.B.A. J., Apr. 2010, at 28, 28).

157. *Id.*

158. *See* Meghan C. Lewallen, Note, *Cloud Computing: A Laywer's Ethical Duty to Act with Reasonable Care When Storing Client Confidences "In the Cloud,"* 60 CLEV. ST. L. REV. 1133, 1139 (2013) (discussing the benefits of cloud computing and how regular back-up and duplication of information across several servers protect users from loss of data in the instance of hardware failure).

159. *See id.* at 1135 (arguing an attorney or law firm is required "to act with reasonable care when storing client confidences in the cloud").

160. *Id.* at 1141–43 (discussing risks of third party cloud services).

control of the lawyer, but, instead, is stored on a vendor's server.[161] The nature of cloud computing also means that an unauthorized third-party has the potential to gain access to the vendor's server and, thus, confidential client information.[162] The risk that information subject to a lawyer's Rule 1.6 obligation to protect will be accessed by unauthorized third-parties is present not only in the context of cloud computing, but also by a lawyer's use of laptops, smartphones, tablets, and other modern technology that a lawyer may utilize in their practice.

The reality of hacking and the risk it presents in the practice of law has led to the addition of a new subpart (c) to Rule 1.6, which now provides that "[a] lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client."[163] Additionally, the Comment to Rule 1.6 now provides guidance regarding reasonableness in the context of steps taken to prevent unauthorized access to client information. Revised Comment [18] reads:

> Paragraph (c) requires a lawyer to act competently to safeguard information relating to the representation of a client against unauthorized access by third parties and against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer's supervision. See Rules 1.1, 5.1 and 5.3. The unauthorized access to, or the inadvertent or unauthorized disclosure of, information relating to the representation of a client does not constitute a violation of paragraph (c) if the lawyer has made reasonable efforts to prevent the access or disclosure. Factors to be considered in determining the reasonableness of the lawyer's efforts include, but are not limited to, the sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed, the cost of employing additional safeguards, the difficulty of implementing the safeguards, and the extent to which the safeguards adversely affect the lawyer's ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use). A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to forgo security measures

161. *See* Ala. State Bar Disciplinary Comm'n., Op. 2010-02 (2010) (discussing an attorney's ethical responsibilities concerning the retention, ownership, production, storage, and destruction of client files).

162. *Id.*

163. Peter Geraghty, Lucian T. Pera & Alfred J. Saikali, *Lawyer's Obligations to Provide Data Security Arising from Ethics Rules and Other Law Specifically Governing Lawyers*, *in* THE ABA CYBERSECURITY HANDBOOK 62, 63 (Jill D. Rhodes & Vincent I. Polley eds., 2013) (quoting MODEL RULES OF PROF'L CONDUCT r. 1.6(c) (AM. B. ASS'N 1983)).

> that would otherwise be required by this Rule. Whether a lawyer may be required to take additional steps to safeguard a client's information in order to comply with other law, such as state and federal laws that govern data privacy or that impose notification requirements upon the loss of, or unauthorized access to, electronic information, is beyond the scope of these Rules. For a lawyer's duties when sharing information with nonlawyers outside the lawyer's own firm, see Rule 5.3, Comments [3]-[4].[164]

Revised Comment 19 now reads:

> When transmitting a communication that includes information relating to the representation of a client, the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients. This duty, however, does not require that the lawyer use special security measures if the method of communication affords a reasonable expectation of privacy. Special circumstances, however, may warrant special precautions. Factors to be considered in determining the reasonableness of the lawyer's expectation of confidentiality include the sensitivity of the information and the extent to which the privacy of the communication is protected by law or by a confidentiality agreement. A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to the use of means of communication that would otherwise be prohibited by this Rule. Whether a lawyer may be required to take additional steps in order to comply with other law, such as state and federal laws that govern data privacy, is beyond the scope of these Rules.[165]

Although cloud computing presents the risk that confidential client information will be accessed by third-parties, ethics opinions that have examined the issue have not deemed the risk severe enough to warrant a prohibition of cloud computing in the practice of law. In fact, the use of cloud computing has generally been approved, subject to appropriate precautions being put in place.[166] In 2006, the Nevada State Bar concluded that an attorney "may use an outside agency to store confidential client information in electronic forms, and on hardware located outside the attorney's direct supervision and control, so long as the attorney observes the usual obligations applicable to such arrangements for third party storage

---

164. MODEL RULES OF PROF'L CONDUCT r. 1.6, cmt. 18 (AM. B. ASS'N 2016).

165. *See id.* r. 1.6, cmt. 19.

166. *See Cloud Ethics Opinions Around the U.S.*, A.B.A., http://www.americanbar.org/groups/departments_offices/legal_technology_resources/resources/charts_fyis/cloud-ethics-chart.html (last visited Dec. 19, 2016) [hereinafter *Cloud Ethics Opinions Around the U.S.*] , for an extensive list of ethics opinions addressing the use of cloud computing.

services."[167] In 2010, the Alabama Disciplinary Commission agreed, stating that "a lawyer may use 'cloud computing' or third-party providers to store client data provided that the attorney exercises reasonable care in doing so."[168] That duty of reasonable care requires a lawyer "to become knowledgeable about how the provider will handle the storage and security of the data being stored and to reasonably ensure that the provider will abide by a confidentiality agreement in handling the data."[169] "Additionally, because technology is constantly evolving, the lawyer will have a continuing duty to stay abreast of appropriate security safeguards that should be employed by the lawyer and the third-party provider."[170]

The Arizona State Bar has similarly concluded that a lawyer "should periodically review security measures in place to ensure that they still reasonably protect the security and confidentiality of the clients' documents and information."[171] The Arizona opinion also provided examples of steps a lawyer should take to comply with the duty of reasonable care, which included the use of "firewalls, password protection schemes, encryption, anti-virus measures, etc."[172] However, the duty of reasonable care "does not require a guarantee that the system will be invulnerable to unauthorized access."[173] Nonetheless, the Arizona Bar quoted with approval a New Jersey ethics opinion, which stated that a lawyer "is required to exercise sound professional judgment on the steps necessary to secure client confidences against foreseeable attempts at unauthorized access."[174] The duty of reasonable care espoused by these and other state ethics opinions has been described as follows:

> In short, a lawyer cannot take the "ostrich" approach of hiding his head in the sand and hoping that his office or firm will not suffer a data breach that compromises client information. Lawyers must implement administrative, technical, and physical safeguards to meet their obligation to make reasonable efforts to protect client information.[175]

State bars have further weighed in on what techniques are appropriate to implement to protect against data breaches and inadvertent disclosures of

167. Nev. State Bar Comm. on Ethics and Prof'l Responsibility, Formal Op. No. 33 (2006).
168. Ala. State Bar Disciplinary Comm'n, Op. 2010-02 (2010)
169. *Id.*
170. *Id.*
171. Ariz. State Bar Comm. on Prof'l Conduct, Op. 09-04 (2009).
172. *Id.*
173. *Id.*
174. *Id.* (quoting N.J. B. Ethics Op. 701 (2006)).
175. Geraghty, Pera & Saikali, *supra* note 163, at 64.

client information. For example, the Virginia State Bar concluded that the proper level of care requires that a lawyer "examine the third party provider's use of technology and terms of service in order to know whether it adequately safeguards client information, and if the lawyer is not able to make this assessment on her own, she will have to consult with someone qualified to make that determination."[176] The Maine Board of Bar Overseers went further and provided a list of internal policies and procedures that a lawyer should implement to satisfy their obligations under the Maine Rules of Professional Conduct and a separate list of safeguards that should be adopted to deal with a third-party cloud vendor.[177] The internal policies and procedures suggested by the Maine Board are as follows:

1. backing up data to allow the firm to restore data that has been lost, corrupted, or accidentally deleted;
2. installing a firewall to limit access to the firm's network;
3. limiting information that is provided to others to what is required, needed, or requested;
4. avoiding inadvertent disclosure of information;
5. verifying the identity of individuals to whom the attorney provides confidential information;
6. refusing to disclose confidential information to unauthorized individuals (including family members and friends) without client permission;
7. protecting electronic records containing confidential data, including backups, by encrypting the confidential data;
8. implementing electronic audit trail procedures to monitor who is accessing the data;
9. creating plans to address security breaches, including the identification of persons to be notified about any known or suspected security breach involving confidential data; and
10. educating and training employees of the firm who use cloud computing to abide by all end-user security measures, including, but not limited to, the creation of strong passwords and the regular replacement of passwords.[178]

The Maine Board also concluded that a lawyer should ensure the vendor of cloud computing services or hardware:

176. Va. State Bar, Op. 1872 (2013).

177. *See* Me. Bd. of Overseers of the Bar, Op. No. 207 (2013) (addressing how changes in technology over time affect the way the ethical constraints on counsel are satisfied).

178. *Id.*

1. explicitly agrees that it has no ownership or security interest in the data;
2. has an enforceable obligation to preserve security;
3. will notify the lawyer if requested to produce data to a third party, and provide the lawyer with the ability to respond to the request before the provider produces the requested information;
4. has technology built to withstand a reasonably foreseeable attempt to infiltrate data, including penetration testing;
5. provides the firm with the right to audit the provider's security procedures and to obtain copies of any security audits performed;
6. will host the firm's data only within a specified geographic area. If the date is hosted outside of the United States, the law firm must determine that the hosting jurisdiction has privacy laws, data security laws, and protections against unlawful search and seizure that are as rigorous as those of the United States and Maine;
7. provides the ability for the law firm, on demand, to get data from the vendor's or third-party data hosting company's servers for the firm's own use or for in-house backup.[179]

The Massachusetts Bar Association has also weighed in on cloud computing. Following its review of reasonable measures that should be taken to protect confidential client information, the Massachusetts Bar reminded lawyers that, regardless of their choice to use cloud computing services, they remain "bound to follow an express instruction from [a] client that [their] confidential information not be stored or transmitted by . . . the Internet, and . . . should refrain from storing or transmitting particularly sensitive client information by means of the Internet without first seeking and obtaining the client's express consent . . . ."[180]

Prior to storing client information in the cloud, lawyers would be wise to consult the ABA's compilation of ethics opinions regarding the use of cloud computing to locate that jurisdiction's opinion regarding the appropriate steps to implement when using cloud computing.[181]

V. CONCLUSION

The introduction of new technology to the practice of law, such as social media and cloud computing, often provides lawyers with an increased opportunity to market their services and manage their practices more efficiently. However, these technology developments may present new

179. *Id.*

180. Mass. Bar Ass'n Comm. on Prof'l Ethics, Op. 12-03 (2012).

181. See *Cloud Ethics Opinions Around the U.S.*, *supra* note 166, for a chart comparing ethics opinions regarding cloud computing across different jurisdictions.

ways for lawyers to run afoul of their ethical obligations. Moreover, the applicable ethics rules are often outpaced by the technological advancements. Thus, it is important for lawyers to be mindful of their existing ethical obligations in the context of new scenarios that may be presented by their use of new technologies.