Exhibit Facebook: The Discoverability and Admissibility of Social Media Evidence

Emma W. Sholl*

---

* © 2013 Emma W. Sholl. Managing Editor, Volume 16, *Tulane Journal of Technology and Intellectual Property*. J.D. candidate 2014, Tulane University Law School; B.A. *magna cum laude* 2011, Colgate University. The author would like to thank her mother for her positivity and encouragement and her father for being her first and favorite editor. The author would also like to thank the Volume 16 members for their hard work and dedication.

I. INTRODUCTION

Social media Web sites, such as Facebook, have decidedly changed the way we socialize and share information.[1] In the United States alone, there are more than 163 million users on Facebook, making up more than half of the entire U.S. population.[2] Facebook was established in 2004 as a social networking site for college students.[3] Although Facebook is now available to users of all ages, the majority of users are of the younger generation.[4] Through features such as status updates, wall posts, and photo albums, Facebook users share information about their personal lives with other members of the Facebook community and Internet community at large. Recently, attorneys have recognized the value in highly personal information on social media Web sites and have attempted to use this information as evidence at trial.[5] The use of social media evidence has raised the issues of whether Facebook users have a reasonable expectation of privacy in the personal information that they post online and whether this information should be discoverable and admissible in court.[6] These issues have caused a disconnect between the young Facebook users, who believe the content that they post is private and protected, and the older generation of lawmakers and judges, who believe the users do not have a reasonable expectation of privacy in

1. RICHARD SUSSKIND, THE END OF LAWYERS? RETHINKING THE NATURE OF LEGAL SERVICES 77 (2d ed. 2010).

2. *United States Facebook Statistics*, SOCIAL BAKERS, http://www.socialbakers.com/facebook-statistics/united-states (last visited Sept. 24, 2013).

3. Daniel Zeevi, *The Ultimate History of Facebook [INFOGRAPHIC]*, SOCIAL MEDIA TODAY (Feb. 21, 2013), http://socialmediatoday.com/daniel-zeevi/1251026/ultimate-history-facebook-infographic.

4. *United States Facebook Statistics*, *supra* note 2 (explaining that the largest age group of Facebook users falls between the ages of twenty-five and thirty-four, followed by users between ages eighteen and twenty-four).

5. Andrew C. Payne, Note, *Twitigation: Old Rules in a New World*, 49 WASHBURN L.J. 841, 845 (2010).

6. Lindsay M. Gladysz, *Status Update: When Social Media Enters the Courtroom*, 7 I/S: J.L. & POL'Y FOR INFO. SOC'Y 691, 692 (2012).

information because it has been shared with other users.[7] A survey of case law shows that the majority of courts tend to value discovery of information over the privacy concerns of Facebook users.[8]

First, this Comment will give a brief history of the constitutional standards for the right to privacy stemming from the Fourth Amendment of the United States Constitution right to be secure from "unreasonable searches and seizures."[9] The right to privacy will also be examined through one of the United States Supreme Court's most influential decisions on Fourth Amendment issues, *Katz v. United States*.[10] Additionally, this Comment will discuss the rules that govern the admissibility of electronic evidence, such as the Stored Communications Act (SCA), the 2006 Electronic Discovery Amendments to the Federal Rules of Civil Procedure, and Facebook's Privacy Policy.

Second, this Comment will list various methods of discovering and obtaining evidence from Facebook and analyze the advantages, disadvantages, and possible ethical concerns raised by each method. These methods include gathering information through informal discovery, such as a Google search or adding a party or witness as a friend on Facebook, or through methods of formal discovery, including subpoenas and motions to compel.

Third, this Comment will explore how social media evidence fits into traditional evidence rules. This Comment will analyze how social media evidence presents novel issues regarding what aspects of a user's Facebook site should be considered relevant, whether Facebook evidence is hearsay, and how to authenticate evidence taken from a Facebook account.

Fourth, this Comment will analyze current civil and criminal case law in which a party has sought to use information from a Facebook account in discovery or as evidence at trial. This Comment will discuss emerging trends in online communications case law and discuss the areas of law in which social media evidence is most likely to be used effectively.

Lastly, this Comment will give suggestions and tips for both Facebook users and attorneys on how to protect information online or, alternatively, how to use social media evidence to a client's advantage.

---

7. *Id.* at 716.

8. John G. Browning, *Digging for the Digital Dirt: Discovery and Use of Evidence from Social Media Sites*, 14 SMU SCI. & TECH. L. REV. 465, 491 (2011).

9. U.S. CONST. amend. IV.

10. Katz v. United States, 389 U.S. 347, 361 (1967).

II. BACKGROUND

A. The Right to Privacy

1. The Fourth Amendment and the Reasonableness Standard

The Fourth Amendment of the United States Constitution protects the right of the people to be "secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[11] At its core, the Fourth Amendment's purpose is to regulate government intrusion into the private lives of U.S. citizens.[12] Courts have struggled with determining what intrusions are reasonable, and the invention of the Internet and rise in electronic information has made this inquiry increasingly difficult.[13] In *United States v. Knights*, Justice Rehnquist promulgated the Fourth Amendment balancing test for reasonableness:

> The touchstone of the Fourth Amendment is reasonableness, and the reasonableness of a search is determined "by assessing, on the one hand, the degree to which it intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests."[14]

In the context of social media, the courts must balance the need for relevant electronic evidence that is essential to the promotion of legitimate governmental interests with the user's privacy interests in that information.[15]

2. *Katz v. United States* and the Distinction Between Private and Public Communications

In *Katz*, a highly influential case in Fourth Amendment jurisprudence, the Supreme Court of the United States held that the Fourth Amendment protects "people, not places."[16] In the majority opinion, Justice Stewart stated that the Fourth Amendment does not protect what a person "knowingly exposes to the public" but does protect what a person "seeks to preserve as private."[17] Justice Harlan's opinion in the concurrence set forth a two-pronged test for reasonableness of

---

11. U.S. CONST. amend. IV.
12. Gladysz, *supra* note 6, at 694.
13. *Id.*
14. United States v. Knights, 534 U.S. 112, 118-19 (2001) (quoting Wyoming v. Houghton, 526 U.S. 295, 300 (1999)).
15. Gladysz, *supra* note 6, at 694.
16. Katz v. United States, 389 U.S. 347, 351 (1967).
17. *Id.*

privacy expectations that the Court still uses today.[18] According to Justice Harlan, in order for information to be protected under the Fourth Amendment, the person first must have exhibited an "actual (subjective) expectation of privacy" and second, the expectation must be "one that society is prepared to recognize as 'reasonable.'"[19] Therefore, the *Katz* test contains both a subjective and an objective analysis.[20] The range of privacy controls on Facebook makes it very difficult for courts to categorize information as public or private and complicates the inquiry into what a reasonable expectation of privacy is in online information.[21]

3. Reasonable Expectation of Privacy in Public, Private, and Quasi-Private Online Communications

The *Katz* Court held that when an individual voluntarily exposes information to the public, that individual no longer has a reasonable expectation of privacy in that information.[22] In order to make Justice Stewart's distinction between what a person "knowingly exposes to the public" and what a person "seeks to preserve as private" to social media evidence, the court must first classify online communications as public or private.[23]

There are three levels of privacy in information: public communications, private communications, and quasi-private communications.[24] Public communications are communications that are not protected by the Fourth Amendment because they are openly shared.[25] In terms of social media, public communications include any information that is available to the general public.[26] On Facebook, public communications would include profiles or parts of profiles that are viewable to any Facebook user or anyone on the Internet.[27] In *Smith v. Maryland*, the Supreme Court held that there is no expectation of privacy in information provided voluntarily to others.[28] Accordingly, when Facebook users have not taken any steps to protect their profiles and the profiles are available to anyone on the Internet, the data would presumably not be a private

18. Gladysz, *supra* note 6, at 710.
19. *Katz*, 389 U.S. at 361 (Harlan, J., concurring).
20. *Id.*
21. Gladysz, *supra* note 6, at 711.
22. *Katz*, 389 U.S. at 361 (Harlan, J., concurring).
23. *Id.* at 351.
24. Gladysz, *supra* note 6, at 713-15.
25. *Id.*
26. *Id.*
27. *Id.* at 714.
28. Smith v. Maryland, 442 U.S. 735, 743-44 (1967).

communication and would not be protected under the Fourth Amendment.[29]

Private communications are communications that are only accessible by a limited group of people.[30] The Fourth Amendment affords the highest level of protection to private communications.[31] On Facebook, private communications could include communications between a small number of people through the use of Facebook messaging or Facebook chatting.[32] Because these communications are not intentionally divulged to the public and are similar to other electronic communications such as e-mail, phone calls, or other instant messaging services, courts are likely to consider these types of Facebook communications private and thus provide Fourth Amendment protections.[33]

Quasi-private communications are the most difficult to classify.[34] On Facebook, quasi-private communications are communications that are not accessible to the general Facebook community, but are accessible to the user's friends or networks.[35] These communications include information that the Facebook user chooses to share under the privacy controls "friends," "friends of friends," and other user-created networks.[36] Whether the Fourth Amendment provides protection for quasi-private communications on social media Web sites is an open question because courts and users may differ in their views of whether the user has a reasonable expectation of privacy in this information.[37] Average Facebook users may believe that because they have not allowed the general public to view the information, the communication is private.[38] However, courts and lawmakers usually hold that quasi-private communications are public because even though the information is not available to the general public, it is still available to a potentially large number of people.[39]

Determining whether a communication is private, public, or quasi-private is part of the analysis in the first prong of Justice Harlan's

---

29. Gladysz, *supra* note 6, at 714.
30. *Id.*
31. *Id.*
32. *Id.*
33. *Id.* at 714-15.
34. *Id.* at 715.
35. *Id.*
36. *Id.* at 717.
37. *Id.* at 716.
38. *Id.*
39. Evan E. North, Note, *Facebook Isn't Your Space Anymore: Discovery of Social Networking Websites*, 58 U. KAN. L. REV. 1279, 1296 (2010).

reasonableness test: whether the person had a subjective expectation of privacy.[40] The problem with this subjective prong is that there is a generational disconnect between the subjective expectations of privacy of the average Facebook user and of lawmakers.[41] Average Facebook users, who tend to be young, believe that the information they post on their Facebook profile is private.[42] The older generation of lawmakers and judges, whose voices are heard the loudest, believe the information is public.[43]

To determine the second, objective prong of the reasonableness test, it is useful to look at Facebook's Privacy Policy.[44] The Privacy Policy states: "Whenever you add things to your timeline you can select a specific audience, or even customize your audience."[45] Facebook provides three options for sharing information: "Public," "Friends," or "Customize."[46] Selecting the public option means that "[a]nyone, including people off of Facebook, will be able to see or access" your Facebook profile.[47] The Facebook privacy controls allow users to post information that may be seen by everyone, friends, friends of friends, networks, or only the user.[48] Thus the terms of Facebook's Privacy Policy show that users can control who can see their information.[49] Therefore, the existence of Facebook's Privacy Policy and the presence of certain protections, such as privacy controls and the password-protected login, demonstrate that there is an objective expectation of privacy in some communications posted on Facebook if the user takes measures to protect the information and limit its availability through the use of privacy controls.[50]

B. Relevant Rules and Policies

The judicial branch has not been the only branch of the U.S. government to contend with how to treat electronic evidence in the law.[51]

---

40. Gladysz, *supra* note 6, at 710.
41. *Id.* at 716.
42. *Id.* at 720.
43. *Id.*
44. Bradley R. Johnson, *Untagging Ourselves: Facebook and the Law in the Virtual Panopticon*, 13 T.M. COOLEY J. PRAC. & CLINICAL L. 185, 196 (2011).
45. *Facebook Full Data Use Policy*, FACEBOOK (Dec. 11, 2012), https://www.facebook.com/full_data_use_policy.
46. *Id.*
47. *Id.*
48. Johnson, *supra* note 44, at 196.
49. *Id.* at 197.
50. *Id.*
51. Gladysz, *supra* note 6, at 696.

Congress has also made amendments to the law in order to guide courts on questions concerning electronic communications.[52] Additionally, Facebook has its own policies regarding the disclosure of electronic information.[53]

1. The Stored Communications Act and Facebook's Privacy Policy

In 1986, Congress enacted the Stored Communications Act (SCA).[54] The SCA prohibits social media Web sites from disclosing personal information to nongovernment entities without the user's consent.[55] Therefore, the SCA prohibits Facebook from "disclosing the contents of a user's Facebook account to any non-governmental entity even pursuant to a valid subpoena or court order."[56] Congress's goals for the SCA were to prohibit Internet Service Providers (ISPs) from voluntarily releasing user information, while still giving the government, including law enforcement officials, the ability to access the information through a regulated process.[57] There are a number of exceptions to the SCA, including the ability of ISPs to release the information if the user has given lawful consent.[58] Under that exception, the SCA only requires the lawful consent of one party.[59]

The SCA applies to electronic information that is received and stored.[60] The date of transmission determines what process the U.S. government must go through in order to access the information.[61] If 180 days or fewer have passed from the transmission of the information, the government must have a warrant.[62] If more than 180 days have passed, the government needs a subpoena or court order showing probable cause.[63]

In addition to the SCA, electronic communications on Facebook are also governed by Facebook's Privacy Policy.[64] Facebook's Privacy Policy states: "We may access, preserve, and share your information in response to a legal request (like a search warrant, court order or

52. *Id.*
53. *Facebook Full Data Use Policy*, *supra* note 45.
54. Stored Communications Act, 18 U.S.C. §§ 2701-2712 (2012).
55. *Id.* § 2701.
56. Browning, *supra* note 8, at 473.
57. Gladysz, *supra* note 6, at 699.
58. *Id.* at 701.
59. *Id.*
60. *Id.* at 700.
61. *Id.*
62. *Id.*
63. *Id.*
64. *Facebook Full Data Use Policy*, *supra* note 45.

subpoena) if we have a good faith belief that the law requires us to do so."[65] Yet Facebook's Privacy Policy gives no indication of what it considers to be a "good faith belief."[66]

2. The 2006 Electronic Discovery Amendments to the Federal Rules of Civil Procedure

In 2006, the Federal Rules of Civil Procedure were amended to incorporate electronic communications.[67] Before the amendments, courts treated electronic information like traditional documents and generally admitted any relevant electronic evidence.[68] However, as technology advanced, Congress and courts realized that "digital is different."[69] Congress amended Rule 34 by including "electronically stored information" as a type of document that may be requested.[70] "Electronic stored information" is defined broadly and includes electronic communications stored in "any medium" in order to include future technological advances in electronic information.[71] The Advisory Committee also changed Rule 26 to add limitations on the disclosure of electronically stored information.[72] Now, under Rule 26: (1) parties must, pursuant to a request or court order, disclose information if there is no undue burden or cost and (2) even if there is undue burden or cost, the court may still order discovery if it finds good cause.[73] These amendments reflect a legislative preference for disclosure of electronic information.[74]

III. DISCOVERY: INFORMAL AND FORMAL METHODS FOR OBTAINING SOCIAL MEDIA EVIDENCE

Like other evidence, the discovery of electronic information is governed by the Federal Rules of Civil Procedure.[75] Rule 26 states that parties may discover all relevant information as long as it is not privileged from discovery.[76] Also, relevant information does not need to be admissible at trial if the discovery request appears "reasonably

65. *Id.*
66. *Id.*
67. Payne, *supra* note 5, at 856.
68. *Id.* at 851.
69. *Id.*
70. FED. R. CIV. P. 34.
71. FED. R. CIV. P. 34 (advisory committee's note).
72. FED. R. CIV. P. 26.
73. Gladysz, *supra* note 6, at 696.
74. *Id.*
75. FED. R. CIV. P. 26.
76. FED. R. CIV. P. 26.

calculated to lead to the discovery of admissible evidence."[77] The SCA, Facebook's Privacy Policy, and the E-Discovery Amendments to the Federal Rules of Civil Procedure all limit how government and nongovernment parties may access information on Facebook.[78] Different methods of discovery, including informal and formal methods, will determine what electronic information attorneys will be able to gather in a given case.[79]

A. Informal Methods of Discovery

Informal methods of discovery include conducting a search on a general search engine, such as Google, or conducting a search within the actual social networking Web site.[80] Studies have shown that many Facebook users leave sections of their profiles public, either on purpose or because they do not understand the privacy controls.[81] One study found that nearly half of all Facebook users gave incorrect answers about who they thought had access to their Facebook profile.[82] Additionally, there is some information on Facebook that is always publicly available, such as the user's name, profile picture, cover photo, networks, gender, and username.[83] Therefore, because information that is knowingly exposed to the public is not protected under the Fourth Amendment, an informal search can be a worthwhile option for gathering basic information in discovery.[84]

Another informal method for gaining access to information, "friending" a party or witness, may raise ethical dilemmas for attorneys.[85] Rule 4.2 of the Model Rules of Professional Conduct states that a lawyer may not communicate, or cause another person to communicate, with an opposing party without the consent of the opposing party's attorney.[86] Whether an attorney or agent of an attorney may "friend" an adverse

77. FED. R. CIV. P. 26.
78. Gladys, *supra* note 6, at 696-702.
79. *See* Browning, *supra* note 8, at 471.
80. *Id.*
81. *See* Alessandro Acquisti & Ralph Gross, Imagined Communities: Awareness, Information Sharing, and Privacy on Facebook (2006) (unpublished paper), http://www.heinz.cmu.edu/~acquisti/papers/acquisti-gross-facebook-privacy-PET-final.pdf.
82. *Id.*
83. *Facebook Full Data Use Policy*, *supra* note 45.
84. Katz v. United States, 389 U.S. 347, 351 (1967); Browning, *supra* note 8, at 471.
85. Browning, *supra* note 8, at 475.
86. MODEL RULES OF PROF'L CONDUCT R. 4.2 (2010).

party or witness remains unsettled by rule changes or ethics opinions.[87] Rule 4.1 does state, however, that a lawyer may not knowingly "make a false statement of material fact or law to a third person."[88] In 2009, a Philadelphia attorney sought the advice of the Philadelphia Bar Association as to whether he could, without revealing his affiliation with third party, have a third party "friend" a witness in order to access information to use against the witness.[89] The Professional Guidance Committee held that he could not because failing to disclose the attorney's affiliation with the third party concealed a material fact and violated Rule 4.1.[90] A year later, the New York City Bar Association debated the same issue and also held that such informal discovery was not allowed because of Rule 8.4's ban on conduct involving dishonesty, deception, fraud, or misrepresentation.[91] Therefore, although informal methods such as "friending" a witness or party to gain access to information may provide the attorney with a lot of information, the attorney must be very cautious not to violate any ethics rules.[92]

B. Formal Methods of Discovery

If a Facebook user's account is privacy-restricted, it is necessary to use formal methods of discovery.[93]

1. Issuing a Subpoena to Facebook

Many attorneys assume that the best way to obtain electronic communications from Facebook is to get the information directly from the source by issuing a subpoena directly to the social networking Web site.[94] However, because of the SCA and Facebook's Privacy Policy, social networking Web sites such as Facebook have been "notoriously resistant to such efforts" and the subpoena requests are usually futile.[95] Several courts have quashed subpoenas to ISPs that requested the release

87. Peter S. Kozinets & Aaron J. Lockwood, *Discovery in the Age of Facebook*, ARIZ. ATT'Y, July-Aug. 2011, at 42, *available at* http://www.azattorneymag-digital.com/azattorneymag/20110708#pg45?pg=45#pg45.
88. MODEL RULES OF PROF'L CONDUCT R. 4.1 (2010).
89. Browning, *supra* note 8, at 476.
90. *Id.*
91. *Id.* at 476-77.
92. *Id.* at 476.
93. *Id.* at 471.
94. *Id.* at 472.
95. *Id.*

of user information.[96] Additionally, Facebook encourages parties to resolve discovery issues without involving Facebook.[97] For these reasons, an attorney is unlikely to gain electronic information through a subpoena to Facebook.[98]

2. Discovery Request to the Facebook User

The most effective method of obtaining social media evidence is through party discovery.[99] A court order to a party is most effective because the party usually has access to the desired information: "Almost without exception, the information sought by parties to civil litigation is in the possession of, and readily accessible to, a party to the litigation."[100] A court order to the party can include a discovery request to the party himself, or a request that the party sign a consent form and give authorization permitting the opposing party to obtain electronic information directly from the social media Web site, such as Facebook.[101] Rule 34 of the Federal Rules of Civil Procedure states that when a discovery request is directed to a sender, recipient, or person who controls the information, the communication is subject to discovery.[102] The courts may also seek information from a nonparty if the nonparty is the person who controls the communication.[103]

The discovery request to the user must be specific and well-tailored.[104] Instead of making a broad request for all available Facebook content, attorneys will be more successful if they tighten the discovery request and ask for all profiles, postings, messages, and photographs relating to particular claims in the case.[105] Courts have held that broad "fishing expeditions" into social media Web sites are not allowed; therefore, it is advisable to make the discovery requests to a user as narrow as possible.[106]

Likewise, when asking the opposing party to sign a written consent under the SCA for Facebook to release the user's information, the

---

96. *See, e.g.*, *In re* Subpoena Duces Tecum to AOL, LLC, 550 F. Supp. 2d 606 (E.D. Va. 2008); Hone v. Presidente U.S.A., Inc., No 5-08-MC-80071-JF, 2008 U.S. Dist. LEXIS 55722 (N.D. Cal. July 21, 2008).

97. Browning, *supra* note 8, at 473.

98. *Id.*

99. *Id.*

100. *Id.*

101. *Id.*

102. FED. R. CIV. P. 34(a)(1); Gladysz, *supra* note 6, at 701.

103. Gladysz, *supra* note 6, at 701.

104. Browning, *supra* note 8, at 473.

105. *Id.*

106. Kozinets & Lockwood, *supra* note 87, at 44.

consent form should be well-tailored, bear the notarized signature of the person giving consent, and give a detailed description of what is being sought.[107]

3. A Motion To Compel

In the event that a party refuses to sign the written consent form to release their information from Facebook, an attorney must file a motion to compel.[108] The motion to compel seeks a court order forcing the party to give consent.[109] The party's counsel may object to the motion to compel on privacy grounds.[110] However, case authority reveals that these objections are usually overruled, and a party will be compelled to produce electronic information from their social media profile.[111]

IV. ADMISSIBILITY: EVIDENTIARY ISSUES IN ADMITTING SOCIAL MEDIA EVIDENCE IN COURT

Once an attorney has obtained social media information, the next step is to get the evidence admitted in court.[112] The party offering the evidence must show that the electronic evidence is (1) relevant, (2) not subject to being excluded under the hearsay rules, and (3) authentic.[113]

A. Relevance

Rule 402 of the Federal Rules of Evidence simply states that relevant evidence is admissible and irrelevant evidence is inadmissible.[114] Evidence is relevant if "(a) it has any tendency to make a fact more or less probable than it would be without the evidence; and (b) the fact is of consequence in determining the action."[115] However, evidence may still be excluded, even if it is relevant.[116] Rule 403 provides a balancing test for the admission of relevant evidence that allows the court to exclude relevant evidence if "its probative value is substantially outweighed by a danger of one or more of the following: unfair prejudice, confusing the

107. Browning, *supra* note 8, at 475.
108. *Id.*
109. *Id.*
110. *Id.*
111. *See, e.g.*, Romano v. Steelcase Inc., 907 N.Y.S.2d 650, 654 (Sup. Ct. 2010); Flagg v. City of Detroit, 252 F.R.D. 346, 347 (E.D. Mich. 2008); O'Grady v. Superior Court of Santa Clara Cnty., 44 Cal. Rptr. 3d 72, 88 (App. Ct. 2006).
112. Browning, *supra* note 8, at 478.
113. *Id.*
114. FED. R. EVID. 402.
115. FED. R. EVID. 401.
116. FED. R. EVID. 403.

issues, misleading the jury, undue delay, wasting time, or needlessly presenting cumulative evidence."[117]

The relevancy of Facebook and other social media evidence will be largely dependent on the facts of the case.[118] However, when a party establishes the relevance of electronic information from Facebook, and the evidence does not meet an exception to admissibility, the opposing party has a high bar to meet in order to show that the court must exclude the evidence.[119]

There are a number of instances in which Facebook can provide relevant information in both criminal and civil cases.[120] In criminal cases, Facebook can provide evidence of a defendant's whereabouts at the time of the crime or knowledge of the crime, written information proving a witness was intimidated, evidence of cyberstalking or bullying, or information to refute allegations of remorse.[121] In civil cases, information from Facebook can provide evidence in many tort cases, for example, providing photographic evidence that can either bolster or rebut claims in a personal injury suit.[122] Social media evidence is also increasingly relevant in family law and can be used to show physical or sexual abuse, drunken or drug-related behavior, and infidelity.[123]

B. Hearsay

Statements made on social media Web sites, such as Facebook, are by definition out-of-court statements and will raise traditional hearsay concerns.[124] However, hearsay usually does not prevent attorneys from admitting social media evidence.[125]

The most useful hearsay exemption when it comes to social media evidence is Rule 801(d)(2): Statements by the Parties Themselves Offered by Party Opponents.[126] This Rule means that anything a party says or does (excluding criminal defendants who were not read their

---

117. FED. R. EVID. 403.

118. Browning, *supra* note 8, at 478.

119. Kathryn R. Brown, *The Risks of Taking Facebook at Face Value: Why the Psychology of Social Networking Should Influence the Evidentiary Relevance of Facebook Photographs*, 14 VAND. J. ENT. & TECH. L. 357, 379 (2012).

120. Aviva Orenstein, *Friends, Gangbangers, Custody Disputants, Lend Me Your Passwords*, 31 MISS. C. L. REV. 185, 192-93 (2012).

121. *Id.*

122. *Id.* at 193.

123. *Id.* at 194.

124. *Id.*

125. *Id.* at 221.

126. FED. R. EVID. 801(d)(2).

Miranda Rights) is exempted from the hearsay rule.[127] On Facebook, any relevant information a party posts on their profile will be admissible if offered by the party opponent.[128] This hearsay exemption is the most useful because it encapsulates the majority of the evidence parties will try to introduce at trial.[129]

C. Authentication

Authentication of social media evidence has proved a much more confusing issue than hearsay for courts.[130] This confusion may stem from the fact that in order to determine how to authenticate evidence, the court must have a solid grasp on how online technology works.[131] Hence, in light of the constant technological advancements of the Internet, courts have been hesitant to stipulate a test for authenticating electronic data.[132]

In order to authenticate social media evidence, Federal Rule of Evidence 901 requires that the party presenting the evidence show that it is genuine.[133] It is then up to the fact finder, such as a jury, to determine the authenticity.[134] Thus, the authentication question is a two-step process.[135] The first step involves the gatekeeping role of the judge, who determines whether the jury could find the evidence authentic.[136] Second, the information goes to the jury, who decides whether it is authentic.[137]

Authentication issues usually arise in four situations: (1) where there is a lack of proper foundation, (2) where a party alleges that the social media Web site is a fake, (3) where the party alleges that the genuine profile has been hacked, or (4) where it is alleged that a third-party appropriated the site of the party.[138]

In order to prove that electronic information is authentic, attorneys can offer direct proof, circumstantial evidence, or both.[139] Direct proof includes the admission of the author of the electronic information or a

---

127. FED. R. EVID. 801(d)(2); *see* Miranda v. Arizona, 384 U.S. 436 (1966).
128. Orenstein, *supra* note 120, at 196.
129. *Id.*
130. *Id.* at 220-21.
131. *Id.*
132. *See* Steven Goode, *The Admissibility of Electronic Evidence*, 29 REV. LITIG. 1, 6-7 (2009).
133. FED. R. EVID. 901.
134. Browning, *supra* note 8, at 478.
135. Orenstein, *supra* note 120, at 202-03.
136. *Id.*
137. *Id.*
138. *Id.* at 207.
139. Browning, *supra* note 8, at 479.

stipulation of the parties.[140] Circumstantial evidence includes evidence of the similarities between the social media Web site at issue and material that has already been authenticated.[141] Attorneys can also use individualized information, such as photographs, background information, information about hobbies and interests, and circumstantial evidence to link the online profile to the user.[142] The distinctive characteristics of social media profiles give courts assurance that the alleged author is actually the one responsible for the content on the profile.[143]

The most effective way to authenticate evidence from a party or witness's profile is to illustrate connections between the individual and the evidence being offered.[144] While some courts have held that circumstantial evidence is insufficient to authenticate data, most courts are satisfied with circumstantial evidence and have noted that the evidence threshold is "quite low."[145]

V. EMERGING TRENDS IN SOCIAL MEDIA CASE LAW

The use of social media evidence in court has increased drastically in recent years.[146] In 2011, federal judges granted more than double the search warrants granting access to individuals' Facebook profiles than they did in 2010.[147] While this trend suggests that social media evidence may soon be used in all aspects of law, there are several areas of law that encounter social media evidence the most.[148]

A. Civil Cases

In civil cases, the question of admitting evidence from social media Web sites usually arises in personal injury cases and family law cases.[149]

---

140. *Id.* at 479-80.
141. *Id.* at 480.
142. *Id.* at 480-81.
143. *Id.* at 481.
144. *Id.* at 483.
145. *See* State v. Bell, 882 N.E.2d 502, 512 (Ct. C.P. Clermont Cnty. 2008); People v. Fielding, No. C062022, 2010 WL 2473344, at *4-5 (Cal. Ct. App. June 18, 2010); Commonwealth v. Williams, 926 N.E.2d 1162, 1172-73 (Mass. 2010).
146. Gladysz, *supra* note 6, at 702.
147. Jeff J. Rogers, *A New Law-Enforcement Tool: Facebook Searches*, THOMPSON REUTERS (July 12, 2011, 11:58 AM), http://www.reuters.com/article/2011/07/12/us-facebook-idUSTRE76B49420110712.
148. Gladysz, *supra* note 6, at 702.
149. *Id.* at 702-07.

1. Personal Injury

In personal injury cases, Facebook evidence is used to prove that plaintiffs are not as seriously injured as they claim to be.[150] This evidence can include photographs or status updates of the plaintiffs that suggest they are leading a happy, energetic life.[151]

In *Romano v. Steelcase Inc.*, the Suffolk Country Supreme Court in New York admitted evidence from the plaintiff's Facebook page intended to disprove claims that the plaintiff's injuries resulted in a loss of enjoyment in life.[152] The plaintiff claimed that her injuries confined her to her house and bed, but her Facebook profile showed photographs of her leading an active life.[153] The defendant in the case issued discovery requests to the plaintiff seeking full access to the plaintiff's Facebook accounts.[154] The plaintiff did not comply with the discovery request.[155] After reviewing the public portions of the plaintiff's Facebook account, the court reasoned that there was a high likelihood that the private portions of her Facebook account would be relevant and lead to the discovery of admissible evidence.[156] The court also found that the plaintiff did not have a privacy right in this information because a user of social media does not have a reasonable expectation of privacy in information shared with others through Facebook.[157] Significantly, the court reasoned that the very nature and purpose of social networking Web sites is to share information, and thus an expectation of privacy in that information is unreasonable.[158] The court wrote: "[W]hen Plaintiff created her Facebook and MySpace accounts, she consented to the fact that her personal information would be shared with others, notwithstanding her privacy settings. Indeed, that is the very nature and purpose of these social networking sites else they would cease to exist."[159] The court in *Romano* reasoned that the defendant's need for access to information outweighed the plaintiff's privacy concerns.[160]

Similarly, in *McMillen v. Hummingbird Speedway, Inc.*, a district court of common pleas in Pennsylvania granted a motion to compel the

150. *Id.*
151. *Id.* at 703.
152. Romano v. Steelcase, Inc., 907 N.Y.S.2d 650, 654 (Sup. Ct. 2010).
153. *Id.*
154. *Id.* at 653.
155. *Id.*
156. *Id.* at 655.
157. *Id.* at 654-55.
158. *Id.* at 657.
159. *Id.*
160. *Id.*

plaintiff to produce his Facebook username and password.[161] In this case, the plaintiff claimed he suffered from permanent impairment of his physical health and an inability to enjoy pleasures in life.[162] However, public portions of his Facebook profile revealed that he had gone on a fishing trip and attended the Daytona 500.[163] Like in *Romano*, the court in *McMillen* held that Facebook users do not have a reasonable expectation of privacy in the content they post on their Facebook profiles: "[W]hile it is conceivable that a person could use them as forums to divulge and seek advice on personal and private matters, it would be unrealistic to expect that such disclosures would be considered confidential."[164] Both the courts in *Romano* and *McMillen* favored disclosure of evidence over disallowance.[165]

2. Other Torts

In harassment cases, a party will attempt to use social media evidence to gain insight into the plaintiff's emotions, feelings, or mental state at the time surrounding the harassment.[166] In cases dealing with sexual harassment, some courts have insisted on narrowly tailored discovery requests due to the sensitive nature of the claim.[167]

In *Mackelprang v. Fidelity National Title Agency of Nevada, Inc.*, a district court in Nevada denied the defendant's motion to compel all private messages from the plaintiff's MySpace account, holding that the defendant was engaged in a "fishing expedition."[168] In this case, the plaintiff claimed sexual harassment and emotional distress during employment.[169] The defendant wanted access to the plaintiff's MySpace account in order to show that the plaintiff was a willing participant and used her MySpace account to facilitate sexual encounters.[170] The court reasoned that asking for all private messages "cast too wide a net" and could potentially result in irrelevant information about the plaintiff's

161. McMillen v. Hummingbird Speedway, Inc., No. 113-2010 CD, 2010 WL 4403285, at *12 (Ct. Com. Pl. Jefferson Cnty. Sept. 9, 2010).

162. *Id.* at *1.

163. *Id.*

164. *Id.* at *3.

165. *See Romano*, 907 N.Y.S.2d at 654; *McMillen*, 2010 WL 4403258.

166. *See generally* Mackelprang v. Fid. Nat'l Title Agency of Nev., Inc., 2:06-CV-00788-JCM, 2007 WL 119149 (D. Nev. Jan. 9, 2007); EEOC v. Simply Storage Mgmt., LLC, 270 F.R.D. 430, 433 (S.D. Ind. 2010).

167. *Mackelprang*, 2007 WL 119149, at *4.

168. *Id.* at *2, *6.

169. *Id.* at *1.

170. *Id.* at *3.

sexual history with nonparties.[171] The court then directed the defendant to narrow his discovery request to include only requests for production of messages that related to her sexual harassment or emotional distress claims.[172]

In *EEOC v. Simply Storage Management, LLC*, the United States District Court for the Southern District of Indiana did not share as much concern for sexual harassment claimants' privacy as the court in *Mackelprang* did.[173] In this case, the plaintiffs brought a sexual harassment claim and the defendant sought to produce photographs from the plaintiffs' Facebook pages to prove that the plaintiffs did not suffer from severe emotional distress.[174] The court found that "any profiles, postings, or messages" related to "any emotion, feeling, or mental state" around the time of the harassment claim were relevant and should be produced.[175] The court wrote, "It is reasonable to expect severe emotional or mental injury to manifest itself in some social networking site content, and an examination of that content might reveal whether onset occurred, when, and the degree of distress."[176] The court also reasoned that the need for discovery outweighed privacy concerns and argued that because the plaintiffs had already shared the information with their Facebook friends, they did not have a reasonable expectation of privacy.[177]

In *Bass v. Miss Porter's School*, the plaintiff sued her former prep school, alleging, inter alia, that the school had failed to protect her from bullying and harassment.[178] The school requested production of the plaintiff's Facebook page in order to seek information about the teasing and taunting.[179] The plaintiff only gave the defendant 100 pages out of the available 750 pages of information on her Facebook profile.[180] The United States District Court for the District of Connecticut reasoned that the determination of what evidence is relevant should not be left up to the plaintiff and ordered the plaintiff to disclose the rest of the pages.[181] The court wrote:

---

171. *Id.* at *7.
172. *Id.*
173. EEOC v. Simply Storage Mgmt. LLC, 270 F.R.D. 430, 434 (S.D. Ind. 2010).
174. *Id.* at 430.
175. *Id.* at 436.
176. *Id.* at 435.
177. *Id.* at 437.
178. Bass *ex rel.* Bass v. Miss Porter's Sch., 738 F. Supp. 2d 307, 323 (D. Conn. 2010).
179. Jonathan E. DeMay, *The Implications of the Social Media Revolution on Discovery in U.S. Litigation*, 40-SUM BRIEF 55, 58 (2011).
180. *Id.*
181. Bass *ex rel.* Bass v. Miss Porter's Sch., 3:08 CV 1807 (JBA), 2009 WL 3724968, at *1 (D. Conn. Oct. 27, 2009).

> Facebook usage depicts a snapshot of the user's relationships and state of mind at the time of the content's posting. Therefore, relevance of the content of Plaintiff's Facebook usage as to both liability and damages in this case is more in the eye of the beholder than subject to strict legal demarcations, and production should not be limited to Plaintiff's own determination of what may be "reasonably calculated to lead to the discovery of admissible evidence."[182]

The *Mackelprang*, *EEOC*, and *Bass* decisions show that courts acknowledge that a social networking Web site, such as Facebook, can be a valuable place to find information relating to a claimant's feelings and emotions when mental state is at issue in the case, but still struggle with where to draw the line between a "fishing expedition" and a request for relevant information.[183]

3. Family Law

In family law cases, such as custody or divorce, social media evidence is often used to show the party's "character or fault in the matter."[184] In divorce, evidence from a Facebook account can show that the party has engaged in an extramarital affair.[185] In custody cases, Facebook evidence can show that a party is an unfit parent and living with that party is not in the best interests of the child.[186] It is important to note that individuals who are "friends" of a party are allowed to bring the information to court.[187] Thus, admissibility of Facebook evidence is a problem in family law because it is common for estranged spouses to "unfriend" each other.[188] Family courts tend to admit electronic evidence from Facebook and favor disclosure over disallowance.[189]

---

182. *Id.*

183. *See* Mackelprang v. Fid. Nat'l Title Agency of Nev., Inc., 2:06-cv-00788-JCM, 2007 WL 119149 (D. Nev. Jan. 9, 2007); EEOC v. Simply Storage Mgmt., LLC, 270 F.R.D. 430 (S.D. Ind. 2010); *Bass*, 2009 WL 3724968.

184. Gladysz, *supra* note 6, at 704.

185. *Id.* at 705.

186. *Id.*; *see* Dexter, II v. Dexter, No. 2006-p-0051, 2007 WL 1532084, at *7 (Ohio Ct. App. 2007) (holding that the trial court did not abuse its discretion when it decided to grant custody to the father based on evidence gathered from the mother's MySpace page, on which the mother had written about her sado-masochism, bisexuality, and paganism, which the trial court reasoned would have an adverse effect on her child).

187. Gladysz, *supra* note 6, at 705.

188. *Id.*

189. *Id.*

B. Criminal Cases

In criminal law, a party can use social media evidence to show the defendant's character and lifestyle.[190] Sometimes, a criminal has been foolish enough to brag about a crime on Facebook, and the prosecution will attempt to use that information as direct evidence of a crime.[191] The prosecution can also use evidence from Facebook to show a lack of remorse.[192] During sentencing, courts will look at remorse as an indication of the defendant's character, blameworthiness, and capacity to be a law-abiding citizen, and courts may give harsher sentences when the defendant appears unrepentant.[193]

In 2009, the Department of Justice made a presentation called "Obtaining and Using Evidence from Social Networking Sites" to educate prosecutors on how to use social networking sites to establish motives, learn about relationships, provide location information, prove or disprove alibis, and establish the occurrence of a crime.[194] Prosecutors often use Facebook photographs as evidence of gang activity.[195] Defense counsel can use evidence from Facebook to find exculpatory evidence or material to impeach a witness.[196]

In December 2010, Rodney Knight Jr. broke into the home of Marc Fisher and stole a jacket, cash, and a laptop belonging to Fisher's son.[197] Knight then used the laptop to post a picture of himself wearing the jacket and holding the cash on Fisher's son's Facebook profile.[198] The Assistant United States Attorney tracked the IP address associated with the photograph and Knight was arrested within a month.[199]

In October 2006, Joshua Lipton was arrested for driving under the influence after he crashed into two other cars and severely injured a

---

190. Daniel Findlay, *Tag! Now You're Really "It:" What Photographs on Social Networking Sites Mean for the Fourth Amendment*, 10 N.C.J. L. & TECH. 171, 171 (2008).

191. Gladysz, *supra* note 6, at 706.

192. Brown, *supra* note 119, at 373.

193. *Id.* at 373-74.

194. John Lynch & Jenny Ellickson, *Obtaining and Using Evidence from Social Networking Sites: Facebook, MySpace, LinkedIn, and More*, ELEC. FRONTIER FOUND., https://www.eff.org/files/filenode/social_network/20100303__crim_socialnetworking.pdf (last visited Mar. 26, 2013).

195. Edward M. Marsico, Jr., *Social Networking Websites: Are Myspace and Facebook the Fingerprints of the Twenty-First Century?*, 19 WIDENER L. REV. 967, 970 (2010).

196. Thomas C. Frongillo & Daniel K. Gelb, *It's Time To Level the Playing Field: The Defense's Use of Evidence from Social Networking Sites*, 34 CHAMPION 14 (2010).

197. Gabe Acevedo, *World's Dumbest Criminal Would Like To Add You as a "Friend,"* ABOVE THE LAW (Mar. 11, 2011, 2:04 PM), http://abovethelaw.com/2011/03/worlds-dumbest-criminal-would-like-to-add-you-as-a-friend/.

198. *Id.*

199. *Id.*

woman.[200] Two weeks after the accident, Lipton went to a Halloween party dressed in a prison jumpsuit.[201] A picture of him in the jumpsuit was posted on Facebook.[202] At the sentencing hearing, the prosecution showed the photograph to the judge with the caption "Remorseful?"[203] The judge said that he could not ignore the photo while determining Lipton's sentence, stating, "I did feel that [the photograph] gave me some indication of how that young man was feeling a short time after a near-fatal accident, that he thought it was appropriate to joke and mock about the possibility of going to prison."[204]

The Joshua Lipton case shows how posting a photograph on a social networking Web site can have dire consequences when it comes to criminal sentencing.[205] Because of the highly prejudicial impact that these photographs can have in a criminal case, some legal scholars have argued that this evidence should be excluded under FRE 403 because it is unfairly prejudicial.[206]

VI. PRACTICE TIPS FOR USING SOCIAL MEDIA EVIDENCE

Using social media evidence in court is a relatively new tactic, and there are many questions that have been left unanswered by the courts. However, there are several actions that attorneys can take either to use social media evidence to clients' advantage, or alternatively, to protect a client's online information.

Attorneys seeking to use social media evidence against an opposing party can take several steps to discover that evidence. Before taking any action, it is important to be cognizant of the possible ethical issues in attempting to access information from an opposing party.[207] Attorneys should not, for example, try to access a social networking profile under false pretenses.[208]

First, attorneys should not overlook an informal method of discovery, such as a Google search, that can lead to the discovery of basic information.[209] A court is "more likely to find the social media relevant

200. Andrea Panciera, *Facebook Photo Plays Role in DUI Accident Sentencing*, PROVIDENCE J. (May 27, 2008, 6:55 PM), http://news.providencejournal.com/breaking-news/2008/05/facebook-photo.html.

201. *Id.*

202. *Id.*

203. *Id.*

204. Brown, *supra* note 119, at 374-75.

205. *Id.*

206. *Id.* at 393.

207. *See* Browning, *supra* note 8, at 475.

208. DeMay, *supra* note 179, at 62.

209. Browning, *supra* note 8, at 471.

and properly discoverable if publicly accessible portions of the party's social media accounts are inconsistent with its allegations in the complaint or in its discovery responses or testimony."[210] Therefore, the information gained through an informal discovery search can be helpful later on in a formal discovery request.[211]

Second, it is not advisable to try to obtain evidence by serving a subpoena to Facebook, because it is unlikely to be successful.[212] Instead, attorneys should make a discovery request directly to the Facebook user.[213] This request should be narrowly tailored and only ask for information relevant to the claim in the case.[214]

Third, in order to seek admission of the evidence in court, attorneys must authenticate it.[215] To authenticate a Facebook page, attorneys should keep a record of how they accessed the page.[216] Attorneys should also establish ownership of the page by having the user stipulate to ownership or showing circumstantial evidence that links the party to the page in question.[217]

Attorneys who want to protect their client's social media information should first question the client about whether they have a social network profile and have posted any harmful information on it.[218] Attorneys should then review this information and warn the client that it may be used in the course of litigation.[219] Attorneys should also advise clients to discontinue their use of the social network during litigation and urge clients not to post anything related to the case on Facebook.[220] Attorneys may be tempted to have clients delete any existing, harmful information that the clients have posted, but doing so may be considered obstruction of justice.[221]

VII. CONCLUSION

Social media Web sites, such as Facebook, allow and encourage users to share personal information with the click of a button.[222] Yet, as

210. DeMay, supra note 179, at 63.
211. *Id.*
212. *Id.* at 62.
213. *Id.*
214. *Id.*
215. FED. R. EVID. 901.
216. Orenstein, *supra* note 120, at 222.
217. *Id.* at 223.
218. Frongillo & Gelb, *supra* note 196, at 14.
219. *Id.*
220. *Id.*
221. *Id.*
222. North, *supra* note 39, at 1296.

one judge noted, because "Facebook is not used as a means by which account holders carry on monologues with themselves," this information is available to other Facebook users or the Internet community as a whole.[223] The availability of personal information can provide an abundance of evidence for attorneys and law enforcement officials to use in discovery or in court.[224] However, whether this information should be protected under the Fourth Amendment is still up for debate as the U.S. legal system struggles to keep up with advances in Internet technology.[225] Facebook users of the younger generation believe that they have a reasonable expectation of privacy in their information, while lawmakers of the older generation believe that this information is public.[226] The trend in social media evidence cases is to favor the discoverability of information over the privacy concerns of the users: "[I]f a litigant feels that information was good enough to share with his or her Facebook 'friends' and later asserts claims to which that information may be relevant, then the information is good enough to produce to the other side in discovery."[227] Because of the increasing use of social media evidence in court and the detrimental effects that such evidence can have on a client's case, it is essential that attorneys are knowledgeable about how to discover, admit, and protect social media evidence.[228]

223. EEOC v. Simply Storage Mgmt., LLC, 270 F.R.D. 430, 437 (S.D. Ind. 2010).
224. Payne, *supra* note 5, at 845.
225. Gladysz, *supra* note 6, at 719.
226. *Id.*
227. Browning, *supra* note 8, at 494.
228. *Id.*