

April 2012

Social Media and eDiscovery: Emerging Issues

Adam Cohen
Ernst & Young

Follow this and additional works at: <http://digitalcommons.pace.edu/plr>



Part of the [Civil Procedure Commons](#), and the [Legal Profession Commons](#)

Recommended Citation

Adam Cohen, *Social Media and eDiscovery: Emerging Issues*, 32 Pace L. Rev. 289 (2012)

Available at: <http://digitalcommons.pace.edu/plr/vol32/iss2/2>

Social Media and eDiscovery: Emerging Issues

Adam Cohen*

Courts, as well as private sector and government policymakers, have only just begun to address the practical litigation issues raised by the proliferation of social media channels and content. This Article comments on some of those issues as they relate to electronic discovery (“eDiscovery”) and examines how they have been approached in emerging case law. It does not address proposed legislation on a domestic and international level that may impact social media’s use in litigation, nor does it purport to be in any way comprehensive in its coverage of developments and potential developments in the legal implications of social media.

The term “social media” is vague and ever-evolving. For present purposes, the term will be used to refer to Facebook, MySpace, Twitter, and services like them. In some ways, older forms of communications—even electronic mail—would fall under some definitions and uses of the term social media. As an example of the varying forms social media can take, recently internal corporate modes of communication facilitated over intranets have been referred to as social media.¹

The power of social media is indisputable. This power goes well beyond the ability to share with friends and family news about birthdays and to make unwanted connections with long-forgotten fellow students from high school. One prominent area where social media’s power has been demonstrated is in promoting political change. Recently, the oppressive Iranian regime sought to extend its stranglehold on power through a transparently rigged election.² A popular civil rights movement

* Adam Cohen is a principal at Ernst & Young in New York. He is the co-author of *Electronic Discovery: Law and Practice* (Aspen Publishers 2003) and author of the forthcoming *Social Media: Managing Legal Risk Through Corporate Policy* (Wolters Kluwer 2012). He teaches eDiscovery courses at Pace and Fordham Law Schools and lectures on eDiscovery issues nationally and internationally.

1. See, e.g., *Intranet 2.0: Social Media Adoption*, PRESCIENT DIGITAL MEDIA, <http://www.prescientdigital.com/articles/intranet-articles/intranet-2-0-social-media-adoption/> (last updated Jan. 3, 2012).

2. Robert F. Worth & Nazila Fathi, *Defiance Grows as Iran’s Leader Sets Vote*

developed and accelerated; when the government tried to prevent the global dissemination of accurate information about the dramatic movement, social media outlets provided a vehicle that circumvented the censorship.³

However interesting the examples of social media's use in attempts to effect political change in places where democratic government is absent, the legal discussion about social media has been primarily focused on privacy rights. Specifically, the outcry about social media's actual and potential ability to invade personal privacy has prompted examination of government and corporate policy and spawned a wide variety of proposed legislation.⁴ This intense interest in privacy has highlighted the tendency of the discovery process, aimed at uncovering the truth, to butt heads with individual expectations of privacy, reasonable or not.

As was the case with eDiscovery in general, the initial wave of social media eDiscovery cases was comprised of criminal cases. Online child pornography cases were largely responsible for the development of the jurisprudence of admissibility of electronic evidence, the technology of forensic collection of electronically stored information, and the opportunities and necessities of preserving, collecting, and disclosing such evidence.⁵ Electronic evidence admissibility is always premised on proper preservation and collection ensuring the authenticity of the evidence.⁶

A search for social media cases still indicates a pronounced prevalence of criminal cases. This means that the technology involved in the handling of social media for litigation purposes is likely to develop most rapidly in the context of criminal law. As witnessed by the introduction of other forms of electronic evidence in criminal cases the acceptance or non-acceptance of such technology by courts will

Review, N.Y. TIMES, June 16, 2009, at A1, available at <http://www.nytimes.com/2009/06/16/world/middleeast/16iran.html>.

3. Brad Stone & Noam Cohen, *Social Networks Spread Defiance Online*, N.Y. TIMES, June 16, 2009, at A11, available at <http://www.nytimes.com/2009/06/16/world/middleeast/16media.html>.

4. See, e.g., Deleting Online Predators Act of 2006, H.R. 5319, 109th Cong. (2006); Social Networking Privacy Act, S. B. 242, 2011-12 Sess. (Ca. 2011); Social Networking Safety Act, Assemb. 3757, 213th Leg., 2d Ann. Sess. (N.J. 2009).

5. See ADAM COHEN & DAVID LENDER, ELECTRONIC DISCOVERY: LAW AND PRACTICE ch. 6 (2003).

6. Thomas Y. Allman, *Federal E-Discovery Amendments*, 13 RICH. J.L. & TECH. 9, 36 (2007).

influence what technology lawyers and their experts will choose to deploy in civil cases.

Technical developments and the “how” of compliance with eDiscovery obligations aside, it is clear that such obligations exist with respect to social media—for parties (and even non-parties served with a subpoena or who reasonably anticipate such service) deemed to have “possession, custody and control” of social media content.⁷ The test for possession, custody, and control is whether a party has the legal right and the practical ability to access the information requested.⁸ The burden of establishing possession, custody, and control of the non-producing party lies with the requesting party.⁹ As with any other request under Rule 34 of the Federal Rules of Civil Procedure, whether the requesting party could obtain the same information elsewhere, e.g., from another party, does not excuse the duty to produce information within the possession, custody, and control of the target of the original request.¹⁰

The application of this threshold standard under a variety of easily plausible scenarios can raise unanswered questions when it comes to social media. Consider the following hypothetical situation under this standard:

1. A former employee of Company X brings an employment discrimination action against the Company when she is let go.
2. Former employee requests internal communications relating to the firing, including documents showing how the Company selected her for dismissal.
3. A manager who participated in the decision to lay off the former employee maintains a Facebook page using a laptop supplied by Company X.
4. Company X has no usage policies governing the use of computers it issues and has no policy regarding employee use of social media.

7. FED. R. CIV. P. 34.

8. *Id.* at 34(a)(1).

9. *Id.*

10. *Id.*

5. The manager occasionally uses the Facebook account to communicate with colleagues at the Company outside regular business hours.
6. The former employee issues document requests for the manager's Facebook communications with other employees.

It is unclear how a court would react to this set of facts in analyzing whether the Facebook communications fall within the possession, custody, and control of the Company. Variations on these facts could raise additional unanswered questions as to whether the analysis would change if the communications were transmitted using the manager's home computer, if the manager held an equity interest in the Company, or if the Company had a policy proscribing the use of social media through devices issued by the Company. The application of the possession, custody, and control standard to social media under these potential facts is as yet undetermined in any authoritative, much less precedential, way.

Assuming the standard is satisfied, the existence of further obligations is indicated, if not clearly delineated. Chronologically speaking, these obligations begin with preservation. Preservation is already the biggest stumbling block in eDiscovery. Cases involving allegations of spoliation—a curious sounding word for failure to comply with the duty to preserve—make up the lion's share of eDiscovery jurisprudence.¹¹

Even without having to worry about social media, preservation of electronic information is fraught with danger. This danger arises partly from the fuzzy legal requirements as to the timing and scope of the duty to preserve. The duty to preserve arises upon the “reasonable anticipation” of litigation and covers relevant data,¹² but it arises at a

11. See COHEN & LENDER, *supra* note 5, at ch. 3.

12. United States v. Ernstoff, 183 F.R.D. 148, 155 (D.N.J. 1998).

To determine whether a document was “prepared in anticipation of litigation,” the appropriate inquiry is “whether in light of the nature of the document and the factual situation in the particular case, the document can fairly be said to have been prepared or obtained because of the prospect of litigation.” To make this determination,

point in time where what is relevant has not yet been defined by expressly articulated claims or document requests. For business enterprises with multiple facilities, systems, and devices to worry about, implementation can be a further headache.

Injecting social media into this combustible mix can easily put the preservation effort in jeopardy. The problems can start with the flow of information from individual custodians or witnesses to counsel. As a general matter, employees who do not report to counsel facts leading to the reasonable anticipation of litigation risk the imputation of such knowledge to the corporate party even though the individuals responsible for compliance are not aware of such facts.¹³ More frequently, employees or individual parties, such as named plaintiffs in a putative class action, may not identify to counsel all potential sources of electronic information. Where this information resides on media disconnected from corporate systems or on the Internet, counsel's preservation and collection plan may fail to capture it—especially where employees are reticent to disclose ill-advised or embarrassing postings.

Social media exacerbates counsel's already vexing preservation worries. Employees and other individuals often assume that such content is either outside the scope of legal obligations or that it is always protected by privacy rights. Moreover, counsel may not specifically identify social media in providing preservation instructions to custodians.

Unfortunately, even with older forms of electronic information, such as e-mail or word processing files, many lawyers have unwittingly found themselves playing starring roles in public spoliation sanctions opinions.¹⁴ Sometimes this is due to lack of technical sophistication, hardly uncommon in the legal profession, and sometimes due to a failure to keep up with the ever-evolving law and practice of eDiscovery, which is not uniform even as between state and federal courts in the same jurisdiction. Precedent-setting opinions on eDiscovery disputes are rare, as appellate courts rarely pass on discovery decisions. Moreover, the

many courts have applied the "reasonable anticipation test" together with determining causation.

Id. (internal citations omitted); *see also* Pension Comm. of the Univ. of Montreal Pension Plan v. Banc of Am. Sec., LLC, 685 F. Supp. 2d 456, 466 (S.D.N.Y. 2010) ("It is well established that the duty to preserve evidence arises when a party reasonably anticipates litigation.").

13. *See* COHEN & LENDER, *supra* note 5, at ch. 3.

14. *Id.*

profession is still struggling to spread awareness of eDiscovery among practitioners. The New York State Bar Association, the largest bar association in the nation, published its eDiscovery Best Practices Guidelines for New York Attorneys in October of last year.¹⁵

Clearly, there is a time lag in the spreading of professional awareness of any developments in the law, especially when the law concerns constant changes in technology that impact legal obligations. But ignorance of the law, and in this case technology, is no excuse. Accordingly, where social media is within a party's possession, custody, or control and relevant to a reasonably anticipated or actually initiated lawsuit, it would be prudent to preserve it, at the risk of sanctions.

Lawyers should include social media when following the maxim "preserve broadly, produce narrowly."¹⁶ Arguments that a motion to compel the production of social media should be denied, whether on privacy or other grounds, are moot where the data has not been preserved and is therefore no longer available for production anyway. So far, relevance as the ultimate basis for discovery applies as equally to social media as it does to other forms of electronic information. "Discovery of SNS [social networking site] requires the application of basic discovery principles in a novel context."¹⁷

The fundamental touchstone of whether documents and electronically stored information are properly subject to Rule 34¹⁸ or Rule 45 of the Federal Rules of Civil Procedure¹⁹ requests is relevance and the likelihood of leading to admissible evidence.²⁰ However, as

15. E-DISCOVERY COMM., COMMERCIAL & FED. LITIG. SECTION OF N.Y. STATE BAR ASS'N, BEST PRACTICES IN E-DISCOVERY IN NEW YORK STATE AND FEDERAL COURTS (2011), available at <http://www.nysba.org/e-discovery/>.

16. "The first important electronic discovery principle thus becomes: 'Preserve Broadly, Produce Narrowly.' By preserving all potentially relevant documents, a litigator can fight the discovery battle as a series of staged retreats." Ramana Venkata, *How to Meet the New Electronic Discovery Challenge*, 25 OF COUNS. 5, 5 (2006).

17. *Equal Emp't Opportunity Comm'n v. Simply Storage Mgmt, LLC*, 270 F.R.D. 430, 434 (S.D. Ind. 2010).

18. FED. R. CIV. P. 34.

19. *Id.* at 45.

20. *See Gonzales v. Google, Inc.*, 234 F.R.D. 674 (N.D. Cal. 2006).

Any information sought by means of a subpoena must be relevant to the claims and defenses in the underlying case. More precisely, the information sought must be "reasonably calculated to lead to admissible evidence." Rule 26(b). This requirement is liberally construed to permit the discovery of information which ultimately

noted above, requests for discovery of social media may be met by objections on privacy grounds. Moreover, such requests often take the form of a Federal Rule of Civil Procedure 45 subpoena issued to the service provider, bringing with them the further complication of objections based on the Stored Communications Act (SCA or the “Act”).²¹

Crispin v. Audigier,²² one of the first notable civil cases involving social media discovery, presented just such a scenario. It involved an action for, inter alia, breach of contract and copyright infringement, in which the defendant issued a Federal Rules of Civil Procedure 45 subpoena to, inter alia, social media providers Facebook and MySpace.²³ Crispin, the plaintiff, moved ex parte to quash the subpoena.²⁴ The court rejected Crispin’s motion, finding that the subpoena sought relevant information that was neither protected by privacy rights nor the SCA.²⁵ Crispin then moved for reconsideration of that decision, “insofar as it conclude[d] that . . . Facebook, and MySpace are not subject to the SCA.”²⁶

The SCA was enacted in response to privacy issues raised by the Internet.²⁷ Social media providers such as Facebook and MySpace fall under the Act’s definition of an “Electronic Communications Service”

may not be admissible at trial. Overbroad subpoenas seeking irrelevant information may be quashed or modified.

Id. at 680.

In addition to the discovery standards under Rule 26 incorporated by Rule 45, Rule 45 itself provides that “on timely motion, the court by which a subpoena was issued shall quash or modify the subpoena if it . . . subjects a person to undue burden.” Rule 45(3)(A). Of course, “if the sought-after documents are not relevant, nor calculated to lead to the discovery of admissible evidence, then any burden whatsoever imposed would be by definition “undue.”

Id. (quoting *Compaq Computer Corp. v. Packard Bell Elec., Inc.*, 163 F.R.D. 329, 335-36 (N.D. Cal. 1995)).

21. 18 U.S.C. § 2701(a)(1) (2002).

22. *Crispin v. Christian Audigier, Inc.*, 717 F. Supp. 2d 965 (C.D. Cal. 2010).

23. *Id.* at 968.

24. *Id.* at 969.

25. *Id.* at 969-70.

26. *Id.* at 970.

27. *Id.* at 971 (quoting *Quon v. Arch Wireless Operating Co.*, 529 F.3d 892, 900 (9th Cir. 2008)).

(ECS) provider.²⁸ The Act prohibits an ECS provider from divulging “the contents of a communications while under electronic storage by [the ECS provider].”²⁹ “Electronic storage” is defined as: “(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication.”³⁰

Referencing Wikipedia—which the court derided as an unreliable source—Crispin described Facebook and MySpace as “companies which provide social networking websites that allow users to send and receive messages, through posting on user-created “profile pages” or through private messaging services.”³¹ According to the *Crispin* court, “no court appears to have decided whether a social networking site or a web hosting service is an ECS provider . . . at least one district court entered judgment on a jury verdict in favor of the plaintiff in a civil suit alleging improper retrieval of information from MySpace.”³²

Finding that the social networking sites provide messaging or email services, the court applied the case law holding that such services constitute ECSs under the SCA.³³ Additionally, noting that Facebook wall postings and MySpace comments are not “public” but rather only accessible to other users based on selection, the court held that case law designating *private* electronic bulletin board services as ECSs was “relevant, if not controlling.”³⁴ Private electronic bulletin board services are distinguished from services where messages are published to “the community at large,” the latter services not qualifying as ECSs under the SCA.³⁵

The court found a more difficult question in determining whether Facebook wall postings and MySpace comments qualify as the kind of “electronic storage” protected by the SCA. First, the court analyzed whether these social media communications qualify as “temporary,

28. *Id.* at 980.

29. *Id.* at 972 (quoting 18 U.S.C. § 2702(a)(1) (2008)).

30. 18 U.S.C. § 2510(17) (2002).

31. *Crispin*, 717 F. Supp. 2d at 976 (quoting Joint Stipulation at 14, 717 F. Supp. 2d 965 (C.D. Cal. 2010) (No. CV 09-09509 MMM (JEMx))).

32. *Id.* at 978 n.24.

33. *Id.* at 980.

34. *Id.*

35. *Id.* (quoting *MTV Networks v. Curry*, 867 F. Supp. 202, 204 n.3 (S.D.N.Y.1994)).

intermediate storage” included in the SCA’s definition of “electronic storage.”³⁶ After a thorough review of the SCA case law on other forms of electronic communications, the court found that they do not, because such storage covers only messages that have “not yet delivered to their intended recipient.”³⁷ In contrast to electronic mail, the Facebook postings and MySpace comments do not require opening by the user.

However, the Court found that Facebook and MySpace do use “electronic storage” under the SCA “for purposes of backup protection.”³⁸ These services, according to the *Crispin* court, keep copies of message on their servers after delivery in case the user decides to download it again.³⁹

The court also found in the alternative that the social media sites are Remote Computing Services (“RCS”) under the SCA.⁴⁰ It based this analysis at least in part on a case involving YouTube, another website considered by many to be social media.⁴¹ In that case, *Viacom International Inc. v. YouTube Inc.*, at issue were videos designated as *private* by the user uploading them.⁴² This designation on YouTube makes the videos accessible only to the users identified by the uploader.⁴³ The *Viacom* court held that YouTube is an RCS because it stores private videos on a web page “for the benefit of the user *and those the user designates.*”⁴⁴ Finding no distinction between the private YouTube videos and the Facebook and MySpace content at issue, the *Crispin* court likewise held that each of these social media is an RCS providing “electronic storage” under the SCA.⁴⁵

In conclusion, the court granted the plaintiff’s motion for reconsideration.⁴⁶ The only information in the record suggested that the plaintiff had restricted access to his Facebook wall postings and MySpace comments to select users.⁴⁷ Therefore, these communications

36. *Id.* at 985-87.

37. *Id.* at 982 (internal quotation marks omitted).

38. *Id.* at 987.

39. *Id.*

40. *Id.* at 990.

41. *Id.*

42. *Id.* (citing *Viacom Int’l Inc. v. YouTube Inc.*, 253 F.R.D. 256 (S.D.N.Y. 2008)).

43. *Id.*

44. *Id.* (emphasis added).

45. *Id.*

46. *Id.* at 991.

47. *Id.*

would be considered private and protected under the SCA. Based on its SCA analysis, the court remanded to the magistrate so that the record on plaintiff's privacy settings could be developed—the Wikipedia article relied upon by the magistrate being deemed ambiguous and insufficient to decide the issue.⁴⁸

Crispin deals with Federal Rule of Civil Procedure 45 subpoenas to non-parties. What of direct document requests to opposing parties of non-public social media information? In such cases courts may refer to relevance as the ultimate criteria and require production of social media content deemed relevant. In several cases, disclosure of social media is requested because personal injury or medical malpractice plaintiffs, in their less guarded moments, post content that contradicts their factual allegations.⁴⁹

Sometimes the revelations provided by social media in these cases border on the comical. In a Pennsylvania state court case, *Zimmerman v. Weis Markets, Inc.*, the plaintiff alleged that “‘his health in general has been seriously and permanently impaired and compromised’ and, that ‘he has sustained a permanent diminution in the ability to enjoy life and life’s pleasures.’”⁵⁰ Nevertheless, the defendant’s review of Zimmerman’s public Facebook page indicated that his interests included “ridin’” and “bike stunts.”⁵¹ Plaintiff’s MySpace page included recent photographs of him with a black eye posing next to his motorcycle before and after an accident.⁵² To make matters worse for the plaintiff, the page showed pictures of Zimmerman wearing shorts that made the scar from the accident giving rise to his claims clearly visible, despite his deposition testimony that “he never wears shorts because he is embarrassed by his scar.”⁵³

Similar state cases in which social media contradicted the plaintiff’s allegations and was held relevant and discoverable include *Romano v. Steelcase Inc.*, where the plaintiff claimed that her injuries had rendered her unable to travel, but she had posted pictures on her Facebook and MySpace pages depicting her recent travels to other states.⁵⁴ Another

48. *Id.*

49. *Sgambelluri v. Recinos*, 747 N.Y.S.2d 330 (Sup. Ct. 2002).

50. *Zimmerman v. Weis Mkts., Inc.*, No. CV-09-1535, 2011 Pa. Dist. & Cnty. Dec. LEXIS 187 (Pa. C. Ct. May 19, 2011).

51. *Id.* at *2.

52. *Id.*

53. *Id.*

54. *Romano v. Steelcase Inc.*, 907 N.Y.S.2d 650, 653 (Sup. Ct. 2010).

Pennsylvania court concluded that “[w]here there is an indication that a person’s social network sites contain information relevant to the prosecution or defense of a lawsuit . . . access to those sites should be freely granted.”⁵⁵ Federal courts have reached consistent holdings.⁵⁶

Obtaining discovery of social media does not guarantee that it will be useful in winning a case, however. For that purpose, you need *admissible* social media evidence. There are many cases involving the admissibility of web-based information. While early cases were skeptical of the authenticity of anything derived from the Internet, the trend has been to apply reasonable authenticity criteria while recognizing the potential for digital manipulation. Very few cases have examined specifically the admissibility of social media.

Litigants should expect that courts will apply similar criteria to social media as they have to proffers of other Internet evidence. The most exhaustive federal court analysis to date of admissibility criteria for electronic evidence, including websites, is in *Lorraine v. Markel American Insurance Co.*, a decision well in excess of one hundred pages occasioned by the attachment of e-mail printouts to a motion for summary judgment without any declaration supporting their admissibility.⁵⁷ An example of the application of evidentiary authenticity criteria to social media that tracks the criteria used for websites in general is found in the state criminal case *Griffin v. Maryland*.⁵⁸

In connection with the proffer of a MySpace profile page, the court found that there was “no reason why social media profiles may not be circumstantially authenticated in the same manner as other forms of electronic communication—by their content and context.”⁵⁹ In *Griffin*, the Court found that a printout of the MySpace page was sufficiently authenticated by the appearance on the printout of:

1. a photograph of the alleged owner of the profile;

55. *McMillen v. Hummingbird Speedway, Inc.*, No. 113-2010 CD, 2010 Pa. Dist. & Cnty Dec. LEXIS 270 (Pa. C. Ct. Sept. 9, 2010).

56. *See, e.g., Ledbetter v. Wal-Mart Stores, Inc.*, No. 06-cv-01958-WYD-MJW, 2009 WL 1067018 (D. Colo. Apr. 21, 2009) (social media discovery granted where public postings contradicted allegations of effects of injuries).

57. *Lorraine v. Markel Am. Ins. Co.*, 241 F.R.D. 534 (D. Md. May 4, 2007).

58. *Griffin v. Maryland*, 995 A.2d 791 (Md. Ct. Spec. App. 2010), *rev'd*, 19 A.3d 415 (Md. 2011).

59. *Id.* at 806.

2. her date of birth;
3. the number of children she had;
4. her boyfriend's nickname ("Boozy"); and,
5. the testimony of an officer that he believed the profile belonged to the alleged owner for the reasons previously listed.⁶⁰

As other courts have noted, the threshold for authenticity where there is no serious substantively-based challenge is a low one.⁶¹ Nonetheless, lawyers should not overlook the requirement in handling the evidence or risk eviscerating the value of hard won social media discovery through sloppy chain-of-evidence handling or other poor eDiscovery implementation.

Social media is a relatively new entrant in the ever-growing world of sources for eDiscovery. However, it is easily analogized to other forms of electronically stored information, which are discoverable as long as they are relevant (leaving aside burden objections), even when privacy concerns are implicated. Social media does present new opportunities and perils given the often imprudent and sometimes embarrassing nature of its content. Therefore, despite its relative novelty, social media should be handled with the same care in preservation, collection, production, and evidentiary integrity characteristically required in eDiscovery.

60. *Id.*

61. *See Baker v. Chrysler*, 901 N.E.2d 875 (Ohio Ct. App. 2008).