

Electronically Stored Information in Litigation

By Timothy J. Chorvat and Laura E. Pelanek*

I. INTRODUCTION

The law governing the discovery and use of electronically stored information (“ESI”) in litigation continues to evolve, through case law spanning *Zubulake*¹ to *Pension Committee*,² amendments to the rules of civil procedure,³ and court-based efforts to address the costs and burden of electronic discovery,⁴ in both state and federal systems.⁵ That evolution is driven in part by a need for litigation to adapt to new technologies and uses that continue to emerge, such as social media and cloud computing. In this survey, we review the cases that have addressed those new forms of ESI and then look briefly at recent developments in connection with what already can be regarded as more traditional forms of ESI.

II. SOCIAL MEDIA: DISCOVERY REQUESTS IN A FRIEND REQUEST WORLD

As social media sites like Facebook and Twitter have come to dominate aspects of many people’s lives, those sites have accumulated vast reservoirs of information that lawyers are seeking to tap in litigation. In cases as varied as

* Mr. Chorvat is a partner, and Ms. Pelanek is litigation counsel, in the Chicago office of Jenner & Block LLP.

1. *Zubulake v. UBS Warburg LLC*, 217 F.R.D. 309 (S.D.N.Y. 2003); *Zubulake v. UBS Warburg LLC*, 230 F.R.D. 290 (S.D.N.Y. 2003); *Zubulake v. UBS Warburg LLC*, 216 F.R.D. 280 (S.D.N.Y. 2003); *Zubulake v. UBS Warburg LLC*, 220 F.R.D. 212 (S.D.N.Y. 2003); *Zubulake v. UBS Warburg LLC*, 229 F.R.D. 422 (S.D.N.Y. 2004).

2. *Pension Comm. of the Univ. of Montreal Pension Plan v. Banc of Am. Sec., LLC*, 685 F. Supp. 2d 456 (S.D.N.Y. 2010).

3. See FED. R. CIV. P. 16, 26, 33, 34, 37, 45.

4. See, e.g., SEVENTH CIRCUIT ELEC. DISCOVERY PILOT PROGRAM COMM., SEVENTH CIRCUIT ELECTRONIC DISCOVERY PILOT PROGRAM: FINAL REPORT ON PHASE TWO, MAY 2010–MAY 2012, at 1 (2012), available at <http://www.discoverypilot.com/sites/default/files/Phase-Two-Final-Report-Appendix.pdf>.

5. For a summary of developments in the federal courts during 2009–2010, see Timothy J. Chorvat & Laura E. Pelanek, *Electronically Stored Information in Litigation*, 66 BUS. LAW. 183 (2010). For a summary of the developments in state courts during 2010–2011, see Timothy J. Chorvat & Laura E. Pelanek, *Electronically Stored Information in Litigation*, 67 BUS. LAW. 285 (2011).

personal injury actions⁶ and commercial litigation,⁷ opposing parties are using statements, photographs, and other materials posted online as evidence. Social media services like LinkedIn, Facebook, Twitter, and MySpace permit users to post information for viewing by the public or designated groups, including personal information in profiles, status updates about a user's activities, photographs, and more private direct messages.⁸ Upon joining a social media site, a user is encouraged to develop a profile, to provide personal information, and to encourage and accept requests for "connections," "friends," or "followers."⁹ Social media sites permit users to protect information to varying degrees through the use of privacy settings,¹⁰ so that adverse parties may not be able to access a user's information outside of discovery.

In recent years, courts have begun to address the discoverability of social media, primarily in connection with Facebook and MySpace postings. Courts tend to allow discovery of social media to proceed when requests are directed to a party after balancing the relevance of the data being sought against privacy and privilege interests.¹¹

A. DISCOVERY REQUESTS TO PARTIES CONCERNING SOCIAL MEDIA

One of the first cases to address the discoverability of social media content was *Bass v. Miss Porter's School*, a 2009 federal district court decision from Connecticut, in which the defendant served discovery requests seeking social media data relating to the conduct and pleadings at issue in the action.¹² Based on an *in camera* review, the court concluded that the defendant had demonstrated that the plaintiff's production of social media information had been vastly underinclusive and ordered the plaintiff to provide her complete Facebook profile to the defendant.¹³

Similarly, *EEOC v. Simply Storage, LLC*, a 2010 federal case from Indiana, addressed a request for the production of two claimants' social media profiles and

6. See, e.g., *Tompkins v. Detroit Metro. Airport*, 278 F.R.D. 387 (E.D. Mich. 2012) (denying motion to compel in a slip-and-fall case); *Offenback v. L.M. Bowman, Inc.*, No. 1:10-CV-1789, 2011 U.S. Dist. LEXIS 66432 (M.D. Pa. June 22, 2011); *Zimmerman v. Weis Mkts., Inc.*, No. CV-09-1535, 2011 Pa. Dist. & Cnty. Dec. LEXIS 187 (Pa. D. & C. May 19, 2011); *McMillen v. Hummingbird Speedway, Inc.*, No. 113-2010 CD, 2010 Pa. Dist. & Cnty. Dec. LEXIS 270 (Pa. D. & C. Sept. 9, 2010).

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

8. See, e.g., *Basics, Facebook Help Center*, FACEBOOK.COM, <https://www.facebook.com/help/basics> (last visited May 28, 2012); *Profile*, MYSPACE.COM, http://www.myspace.com/help?pm_cmp=ed_footer (last visited May 28, 2012); *Learning Center*, LINKEDIN.COM, <http://learn.linkedin.com/> (last visited May 28, 2012); *Twitter Basics*, TWITTER.COM, <https://support.twitter.com/> (last visited May 28, 2012).

9. See *supra* note 8.

10. See *supra* note 8.

11. See, e.g., *Offenback*, 2011 U.S. Dist. LEXIS 66432, at *10; *EEOC v. Simply Storage Mgmt., LLC*, 270 F.R.D. 430, 435–36 (D. Ind. 2010); *Bass v. Miss Porter's School*, 2009 U.S. Dist. LEXIS 99916, at *1 (D. Conn. 2009); *Largent v. Reed*, No. 2009-1823 (Pa. D. & C. Nov. 8, 2011); *Zimmerman*, 2011 Pa. Dist. & Cnty. Dec. LEXIS 187, at *9–10; *McMillen*, 2010 Pa. Dist. & Cnty. Dec. LEXIS 270, at *11.

12. See *Bass*, 2009 U.S. Dist. LEXIS 99916, at *1.

13. *Id.* at *4.

communications.¹⁴ The defendant sought that information, contending that the claimants had put their emotional health at issue, because the Facebook and MySpace accounts contained probative information.¹⁵ The court noted that, although social media provides a novel context, basic discovery principles apply.¹⁶ The court explained that social media content is not privileged from discovery merely because the user has deemed it “private,” and concluded that privacy concerns can be addressed through a protective order.¹⁷ Citing *Bass*, the court decided that complete production of social media information is not required in the first instance.¹⁸ Rather, social media materials must be relevant to the claims at issue.¹⁹ “[T]he simple fact that a claimant has *had* social communications is not necessarily probative of the . . . issue in the case.”²⁰

In *McMillen v. Hummingbird Speedway, Inc.*, a Pennsylvania state court considered a defendant’s motion to compel the plaintiff to produce log-in information for social media sites.²¹ In response, the plaintiff asked the court to conclude that social media communications are essentially privileged; however, the court declined to do so, ordering the production of usernames and passwords to opposing counsel.²² The court noted that while both Facebook and MySpace “do guarantee a modicum of privacy insofar as users may, with the exception of certain basic information, choose what information and posts to make public . . . reading 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 anyone else.”²³

The defendant in another Pennsylvania case, *Zimmerman v. Weis Markets, Inc.*, also sought user name and password information to access non-public portions of the plaintiff’s social media profiles for information probative on damages issues.²⁴ The court there agreed with the *McMillen* rationale that no privilege protects social media postings under Pennsylvania law and accordingly granted the motion to compel.²⁵ The court “flatly rejected” the plaintiff’s suggestion that the court should conduct an *in camera* review of the social media, as doing so would impose an unfair burden on the court.²⁶ Most recently, a third Pennsylvania court reiterated in *Largent v. Reed* that no general privacy or social media privilege

14. *Simply Storage Mgmt.*, 270 F.R.D. at 432.

15. *Id.* at 432–33.

16. *Id.* at 434.

17. *Id.*

18. *Id.* at 435.

19. *Id.*

20. *Id.*

21. No. 113-2010 CD, 2010 Pa. Dist. & Cnty. Dec. LEXIS 270, at *1 (Pa. D. & C. Sept. 9, 2010).

22. *Id.* at *3–4; *see also* *Gallion v. Gallion*, No. FA114116955S, 2011 Conn. Super. LEXIS 2517, at *1 (Super. Ct. Sept. 30, 2011) (ordering the exchange of parties’ Facebook usernames and passwords between counsel only).

23. *McMillen*, 2010 Pa. Dist. & Cnty. Dec. LEXIS 2517, at *6.

24. *Zimmerman v. Weis Mkts., Inc.*, No. CV-09-1535, 2011 Pa. Dist. & Cnty. Dec. LEXIS 187, at *6 (Pa. D. & C. May 19, 2011).

25. *Id.* at *3–4.

26. *Id.* at *3 n.2. *Compare* *Offenback v. L.M. Bowman, Inc.*, No. 1:10-CV-1789, 2011 U.S. Dist. LEXIS 66432, at *7–10 (M.D. Pa. June 22, 2011) (citing *Simply Storage* for the scope of social media

protects Facebook profile information, even when designated as “private,” including photographs, applications, posts, and status updates, from production.²⁷ The court wrote that “Facebook’s foremost purpose is to ‘help you connect and share with the people in your life.’ That can only be accomplished by sharing information with others. Only the uninitiated or foolish could believe that Facebook is an online lockbox of secrets.”²⁸

In 2012, a Michigan federal court held similarly in *Tompkins v. Detroit Metropolitan Airport* that claims of privilege generally do not protect information posted on social media sites, although the court also recognized that the protections provided by Rule 26(b) apply to social media discovery.²⁹ In *Tompkins*, the plaintiff claimed that a back injury had impaired her ability to work and enjoy life.³⁰ Citing *McMillen*, the defendant moved to compel production of the plaintiff’s entire Facebook account.³¹ The court agreed with the holding of *McMillen* but stated that “the Defendant does not have a generalized right to rummage at will through information that Plaintiff has limited from public review. Rather, consistent with Rule 26(b) . . . there must be a threshold showing that the requested information is reasonably calculated to lead to the discovery of admissible evidence.”³² As the court warned, “[o]therwise, the Defendant would be allowed to engage in the proverbial fishing expedition in the hope that there *might* be something of relevance in Plaintiff’s Facebook account.”³³ The court denied the motion to compel, distinguishing the factual setting from *McMillen* and noting that none of the pictures the defendants attached as exhibits were inconsistent with the plaintiff’s injury claims.³⁴

The case law to date has not addressed one potential complication from orders directing parties to turn over social media passwords: contractual issues arising from the sites’ terms of use.³⁵ Sites’ terms of use, such as Facebook’s Statement of Rights and Responsibilities, purport to preclude users from sharing their passwords with others.³⁶ A court order directing a Facebook user to provide sign-on

discovery and conducting an *in camera* review, using the plaintiff’s username and password, to determine a limited list of materials that were discoverable from the plaintiff’s Facebook account).

27. No. 2009-1823, slip op. at 9–10 (Pa. D. & C. Nov. 8, 2011).

28. *Id.* at 10; see generally *Juror No. One v. Superior Ct.*, No. C067309, slip op. at 15–16 (Cal. Ct. App. May 31, 2012) (dismissing challenge to order directing juror to consent to disclosure of Facebook postings in connection with investigation of juror misconduct).

29. 278 F.R.D. 387, 388 (E.D. Mich. 2012).

30. *Id.* at 387.

31. *Id.* at 388.

32. *Id.*

33. *Id.*

34. *Id.* at 389.

35. The courts in both *Largent* and *McMillen* cite to Facebook’s privacy policy in their privilege analysis but do not address the issue of compelling production of usernames and passwords. See *Largent v. Reed*, No. 2009-1823, slip op. at 9 (Pa. D. & C. Nov. 8, 2011); *McMillen v. Hummingbird Speedway, Inc.*, No. 113-2010 CD, 2010 Pa. Dist. & Cnty. Dec. LEXIS 270, at *6–9 (Pa. D. & C. Sept. 9, 2010).

36. See, e.g., Facebook Statement of Rights and Responsibilities, FACEBOOK.COM, <http://www.facebook.com/legal/terms> (last visited Feb. 14, 2012) (“Registration and Account Security . . . 8. You will not share your password, . . . let anyone else access your account, or do anything else that might jeopardize the security of your account.”).

information to an opposing party or counsel appears to compel the party to violate Facebook's terms of use. Although it is not clear at this point what consequences (if any) follow from the discrepancy between a court order and sites' terms of use, courts likely will have to confront that issue. By contrast, orders directing a user to turn over the contents of his or her social media postings do not seem to raise similar concerns.³⁷

B. DISCOVERY REQUESTS TO SOCIAL MEDIA PROVIDERS

In contrast to courts' receptiveness to social media discovery directed to parties, litigants have been largely unsuccessful in seeking to compel entities that host social media sites to produce information data. In response to subpoenas requesting such data, those entities have relied on a 1986 federal statute, the Stored Communications Act (the "SCA"), as a shield against production.³⁸ The SCA prevents providers of communication services from disclosing private communications under specified circumstances. The statute restricts providers from voluntarily disclosing information in their possession about their users, and limits the government's ability to compel providers to divulge such information.³⁹

A 2010 federal case from California, *Crispin v. Christian Audigier, Inc.*, provides a careful analysis of the SCA's provisions in the social media context.⁴⁰ *Crispin* arose out of a dispute concerning an oral license to use art in connection with the manufacture of certain apparel.⁴¹ The defendants served subpoenas on Facebook, MySpace, and other third parties, seeking the plaintiff's communications and subscriber information.⁴² The defendants contended that the information sought was relevant to the nature and terms of the alleged oral agreement.⁴³ The plaintiff filed an *ex parte* motion to quash the subpoenas, arguing, *inter alia*, that they sought information that the social media sites were prohibited from disclosing under the SCA.⁴⁴ The magistrate judge denied the motion to quash.⁴⁵

37. See *Facebook Data Use Policy, Sharing and Finding You on Facebook*, FACEBOOK.COM, <https://www.facebook.com/about/privacy/your-info-on-fb#controlprofile> (last visited Feb. 14, 2012) (explaining that users' control over access to their information is not absolute and can be modified by other users to a certain extent); *Facebook Statement of Rights and Responsibilities*, FACEBOOK.COM, <https://www.facebook.com/legal/terms?ref=pf> (last visited Feb. 15, 2012) ("2. Sharing Your Content and Information. You own all of the content and information you post on Facebook . . ."); see also *McMillen*, 2010 Pa. Dist. & Cnty. Dec. LEXIS 270, at *7 ("Facebook users are thus put on notice that regardless of their subjective intentions when sharing information, their communications could nonetheless be disseminated by the friends with whom they share it, or even by Facebook at its discretion.").

38. 18 U.S.C. §§ 2701–2712 (2006 & Supp. III 2009).

39. *Id.* §§ 2702–2703.

40. 717 F. Supp. 2d 965 (C.D. Cal. 2010).

41. *Id.* at 968.

42. *Id.*

43. *Id.* at 969.

44. *Id.*

45. *Id.*

The plaintiff moved for reconsideration before the district court on the issue of whether social media sites are subject to the SCA.⁴⁶ The district court granted that motion, and noted that the SCA prohibits communication service providers from disclosing private communications to specified entities.⁴⁷ The SCA “creates a set of Fourth Amendment-like privacy protections by statute, regulating the relationship between government investigators and service providers in possession of users’ private information.”⁴⁸

As an initial matter, the court determined that the plaintiff had standing to challenge the subpoenas due to the personal information at stake.⁴⁹ The court then turned to the SCA, noting that the statute distinguishes between providers of remote computing services (“RCS”) and electronic communication services (“ECS”).⁵⁰ The SCA defines RCS to be “the provision to the public of computer storage or processing services by means of an electronic communications system,” while an ECS is defined to be “any services which provides to users thereof the ability to send or receive wire or electronic communications.”⁵¹ The SCA restricts disclosures by both RCS and ECS providers, under different legal tests.⁵²

Recognizing that social media sites provide services beyond the contemplation of Congress in 1986, the court looked to legislative history as well as the application of the SCA to other technologies like text messages.⁵³ The court divided its analysis between messages that have been read and retained by a user on the social media site and those that have not been read.⁵⁴ The court concluded that the sites’ unread private message services qualify the sites as ECS providers under the SCA.⁵⁵ The court also concluded that the social media sites qualify as RCS providers with respect to messages that have been opened and retained by a user.⁵⁶ The court decided that Facebook and MySpace are not ECS providers in connection with wall postings or comments; the court held that the social media sites were SCA-protected RCS providers with respect to such messages.⁵⁷ However, the record before the court did not indicate whether the plaintiff’s

46. *Id.* at 971.

47. *Id.* at 970–71.

48. *Id.* at 972 (citing Orin S. Kerr, *A User’s Guide to the Stored Communications Act, and a Legislator’s Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1213 (2004)).

49. *Id.* at 976.

50. *Id.* at 978–79 (citing 18 U.S.C. § 2511(2)).

51. *Id.* at 972 (citing 18 U.S.C. § 2510(15)).

52. See 18 U.S.C. § 2702 (2006). An ECS is prohibited from disclosing “the contents of a communication while in electronic storage by that service.” *Id.* § 2702(a)(1). An RCS is prohibited from disclosing the content of any communication received by electronic transmission that is carried or maintained on its service for a customer “solely for the purpose of providing storage or computing processing services to [the] subscriber or customer, if the provider is not authorized to access the contents of [the] communications for the purpose of providing . . . services other than storage or computer processing.” *Id.* § 2702 (a)(2).

53. *Crispin*, 717 F. Supp. 2d at 979.

54. *Id.* at 987.

55. *Id.* at 982.

56. *Id.* at 987.

57. *Id.* at 990. However, the court in *Juror No. One v. Superior Court* attempted to discount the conclusion of *Crispin*: “*Crispin* . . . did not establish as a matter of law that Facebook is either an ECS or an RCS or that the postings to that service are protected by the SCA. The findings in *Crispin*

privacy settings allowed the general public to view his wall postings and MySpace comments. As a result, the court reversed the magistrate judge's order with respect to private social media messages and remanded for further proceedings with respect to the plaintiff's Facebook wall postings and MySpace comments.⁵⁸

C. RULE 34: THE CLOUD'S SILVER LINING

Although lawyers may find the idea of retrieving data from the cloud to be a fuzzy concept, cloud computing simply refers to storing data on a third party's infrastructure and using internet-based software to access that data.⁵⁹ For purposes of discovery, the principles resemble those controlling social media information: users typically will be found to have "possession, custody or control" of data that they upload to the cloud.⁶⁰

In re NTL Inc. Securities Litigation, a 2007 decision in a securities action from the Southern District of New York, laid out the principles involved.⁶¹ The defendant entity issued a document hold memorandum to a selected group of its employees.⁶² Shortly after the plaintiffs brought suit, the defendant filed a Chapter 11 petition and its principal assets were divided between two new entities, only one of which became a defendant in the securities action.⁶³ The defendant successor entity did not produce any documents to the plaintiffs, on the ground that it did not have possession of the original defendant's documents because those materials were in the possession of the non-party successor.⁶⁴ The court disagreed, holding that the successor defendant had control for purposes of Rule 34(a).⁶⁵ "Under Rule 34, 'control' does not require that the party have legal ownership or actual physical possession of the documents at issue; rather, documents are considered to be under a party's control when that party has the right, authority, or practical ability to obtain the document from a non-party to the action."⁶⁶ Because the defendant entity had a contractual right to access data owned by the non-party successor, the court found that the defendant successor had committed spoliation and imposed an adverse inference sanction.⁶⁷

A 2009 decision from a federal court in Maryland illustrates the flip side of the control analysis.⁶⁸ In *Goodman v. Praxair Services, Inc.*, the plaintiff filed a

were based on the stipulations and evidence presented by the parties in that case." No. C067309, slip op. at 12 (Cal. Ct. App. May 31, 2012).

58. *Crispin*, 717 F. Supp. 2d at 991.

59. For a brief background on cloud computing, see, for example, Mark L. Austrian & W. Michael Ryan, *Cloud Computing Meets E-Discovery*, *CYBERSPACE LAW.*, July 2009, at 1.

60. *In re NTL, Inc. Sec. Litig.*, 244 F.R.D. 179 (S.D.N.Y. 2007).

61. *Id.* at 181.

62. *Id.* at 182–83.

63. *Id.* at 181.

64. *Id.* at 184, 195.

65. *Id.* at 195.

66. *Id.* (internal citations omitted).

67. *Id.* at 201.

68. *Goodman v. Praxair Servs., Inc.*, 632 F. Supp. 2d 494, 514 (D. Md. 2009).

spoliation motion that argued that the defendant had failed to preserve evidence when it knew or should have known of the potential for litigation.⁶⁹ One issue concerned whether the defendant was under a duty to preserve data in the possession of third-party consultants.⁷⁰ The plaintiff contended that the consultants were the defendants' agents, while the defendant argued that the consultants were independent contractors who were beyond its control.⁷¹ Citing *NTL*, the court undertook a fact-intensive control analysis and concluded that the defendant did not have "sufficient legal authority or practical ability to ensure the preservation of documents prepared [by the third-party consultants]."⁷² The court found that the plaintiff had failed to show the existence of a relationship comparable to the contractual file-sharing relationship found in *NTL*.⁷³ Accordingly, the court denied the portion of the motion relating to the third-party consultants.⁷⁴

Future disputes over access to data stored in the cloud are likely to turn on the same kind of control analysis. If a party has the legal or practical ability to retrieve data stored on third-party computers, then a court likely will impose on the party the responsibility to preserve and produce that data.

III. NEW DEVELOPMENTS IN OLD ESI

Even as developments in connection with social media and the cloud capture attention, the law governing more traditional forms of electronically stored information like e-mail continues to change with the technological times as well. We focus here on developments in connection with predictive coding and privacy issues.

A. PREDICTIVE CODING: BREAKING THE CODE?

Both courts and commentators have bemoaned the expense involved reviewing the large volumes of data retained by modern computer systems.⁷⁵ We previously have noted that court-based projects like the Seventh Circuit Electronic Discovery Pilot Program are addressing that problem from a legal perspective, encouraging cost-reduction through approaches that include cooperation and

69. *Id.* at 505.

70. *Id.* at 512.

71. *Id.* at 514.

72. *Id.* at 515.

73. *Id.*

74. *Id.* at 525.

75. See, e.g., *Zubulake v. UBS Warburg LLC*, 217 F.R.D. 309, 311 (S.D.N.Y. 2003) ("As individuals and corporations increasingly do business electronically—using computers to create and store documents, make deals, and exchange e-mails . . . the universe of discoverable material has expanded exponentially. The more information there is to discover, the more expensive it is to discover all the relevant information until, in the end, 'discovery is not just about uncovering the truth, but also about how much of the truth the parties can afford to disinter.');" Steven C. Bennett, *Are E-Discovery Costs Recoverable by a Prevailing Party?*, 20 ALB. L.J. SCI. & TECH. 537, 538 n.1 (2010) (noting that a mid-size case can cost between \$2.5 and \$3.5 million for the collection, review, and production of electronic information).

respect for proportionality.⁷⁶ Technological approaches also are coming to the fore, including predictive coding—a software-based approach that uses sophisticated algorithms to locate relevant materials—in lieu of document-by-document review or a mechanical application of search terms.⁷⁷

Case law addressing predictive coding is now beginning to appear. In *Da Silva Moore v. Publicis Groupe*,⁷⁸ Magistrate Judge Peck issued an opinion that “recognize[d] that computer-assisted review is an acceptable way to search for relevant ESI in appropriate cases.”⁷⁹ As Judge Peck explained, “every person who uses email uses predictive coding, even if they do not realize it. The ‘spam filter’ is an example of predictive coding.”⁸⁰ Unlike traditional document review, predictive coding involves attorneys coding a small set of documents, which the computer uses to code other documents, until the system’s predictions and reviewers’ coding are sufficiently aligned.⁸¹

Da Silva Moore was a gender discrimination case, in which five female plaintiffs asserted claims against a large advertising conglomerate.⁸² As part of a phased discovery process, the parties agreed to employ predictive coding to create a random sample of e-mail data and to use that collection to train the predictive coding software.⁸³ The defendants agreed to provide the entire sample set, with coding, to the plaintiffs for their review prior to running the predictive coding on the remaining e-mail collection.⁸⁴

After the parties submitted an ESI protocol to the court,⁸⁵ the plaintiffs objected to the protocol in three primary respects. First, the plaintiffs asserted that predictive coding “provides unlawful ‘cover’” for defendants’ counsel to escape their Rule 26(g) duty to certify that production is complete and correct.⁸⁶ Judge Peck rejected that contention, noting that in “large-data cases like this, involving over three million emails, no lawyer using any search method could honestly certify its production is ‘complete’—but more importantly, Rule 26(g)(1)

76. See Timothy J. Chorvat & Laura E. Pelanek, *Electronically Stored Information in Litigation*, 67 BUS. LAW. 285, 291 (2011); Timothy J. Chorvat & Laura E. Pelanek, *Electronically Stored Information in Litigation*, 66 BUS. LAW. 183, 188–89 (2010). The Pilot Program recently completed its second phase and is now expanding to additional courts and cases in Phase Three. See SEVENTH CIRCUIT ELEC. DISCOVERY PILOT PROGRAM COMM., SEVENTH CIRCUIT ELECTRONIC DISCOVERY PILOT PROGRAM: FINAL REPORT ON PHASE TWO, MAY 2010–MAY 2012, at 1 (2012), available at <http://www.discoverypilot.com/sites/default/files/Phase-Two-Final-Report-Appendix.pdf>. The Pilot Program’s website, www.discoverypilot.com, includes discussions of recent cases involving ESI as well as links to further web-based ESI resources.

77. *Da Silva Moore v. Publicis Groupe*, No. 11 Civ. 1279 (ALC) (AJP), 2012 U.S. Dist. LEXIS 23350, at *3 (S.D.N.Y. Feb. 24, 2012) (citing Andrew Peck, *Search, Forward*, L. TECH. NEWS, Oct. 2011, at 25, 29).

78. *Id.*

79. *Id.*

80. *Id.* at *7 n.2.

81. *Id.* at *6.

82. *Id.* at *4.

83. *Id.* at *14, *16.

84. *Id.* at *16.

85. *Id.* at *20 n.6.

86. *Id.* at *20.

does not require that.”⁸⁷ Second, the plaintiffs objected that predictive coding violates the “gatekeeping function” of Federal Rule of Evidence 702.⁸⁸ However, Judge Peck concluded that Rule 702 does not apply because the e-mails located by predictive coding are “not being offered into evidence at trial as the result of a scientific process or otherwise. The admissibility of specific emails at trial will depend upon each email itself.”⁸⁹ Third, the plaintiffs objected to the ESI protocol on the basis that it lacks a standard to determine whether the method is reliable.⁹⁰ Judge Peck described this objection as premature.⁹¹

Judge Peck observed that his opinion appeared to be the first to endorse the use of predictive coding, but specifically noted that it was not intended to mandate predictive coding.⁹² Judge Peck specifically stated that predictive coding does not have to be used in all cases.⁹³ Similarly, the court recognized that the ESI protocol approved in *Da Silva Moore* may not be appropriate in other situations.⁹⁴ Judge Peck concluded that “[w]hat the Bar should take away from this Opinion is that computer-assisted review is an available tool and should be seriously considered for use in large-data-volume cases where it may save the producing party (or both parties) significant amounts of legal fees in document review.”⁹⁵

B. PRIVACY CONCERNS

In *Corsair Special Situations Fund, L.P. v Engineered Framing Systems, Inc.*,⁹⁶ a collection action, a defendant and judgment debtor filed a motion to quash a subpoena directed to Verizon Wireless that sought information relating to her account.⁹⁷ The defendant argued that the subpoena violated her right to privacy and would be duplicative of other disclosed information.⁹⁸ The defendant did not cite any authority supporting her privacy argument, but the court analyzed what it saw as analogous claims of a right to privacy in billing information.⁹⁹ The court concluded that no right to privacy protects the account information contained in invoices, such as dates of account and roaming fees.¹⁰⁰ Noting a circuit split on the right to a protected privacy interest in the contents of text messages, the court found that the defendant failed to carry her burden to show that she had standing to challenge the subpoena.¹⁰¹ Accordingly, the court denied the

87. *Id.* at *21.

88. *Id.* at *23.

89. *Id.* at *24.

90. *Id.*

91. *Id.* at *25.

92. *Id.* at *39–40.

93. *Id.* at *40.

94. *Id.*

95. *Id.*

96. No. 09-1201-PWG, 2011 U.S. Dist. LEXIS 91770, at *3 (N.D. Md. Aug. 17, 2011).

97. *Id.*

98. *Id.*

99. *Id.* at *7–10.

100. *Id.* at *7–8.

101. *Id.* at *10.

motion to quash, although the court ordered that information produced in response to the subpoena could be used only for the limited purpose of collecting the judgment. Once the judgment was satisfied, all copies of the information were to be destroyed or returned within thirty days.¹⁰²

IV. CONCLUSION

As in past years, recent developments in the law of electronically stored information are noteworthy—principally for the application of existing principles to new technologies, rather than for the creation of novel legal doctrines. The rule that a party must preserve and produce information within its possession, custody, or control will continue to provide the starting point for a determination of whether data are producible, without regard to what individual or entity owns the machine on which the data reside.

102. *Id.* at *11.

