

# Twitigation: Old Rules in a New World

Andrew C. Payne\*

## I. INTRODUCTION

As social-networking websites like Facebook and Twitter are taking a prominent place in our cultural reality, they are also becoming part of our legal reality.<sup>1</sup> The growth in social-networking websites has caused an explosion in the amount of electronic information and plays a large role in litigation.<sup>2</sup> In the criminal law context, both prosecutors and defendants have used social-networking information to arrive at the “truth.”<sup>3</sup> In the civil context, as the amount of electronic social-networking information increases, the legal system will face complex issues surrounding its application in the courtroom.

Recent cases have also demonstrated three areas in civil litigation in which social-networking information is relevant. Early cases indicate that social-networking information may play a role in family law, specifically in divorce and child welfare cases.<sup>4</sup> Social-networking informa-

---

\* B.A. 2007, University of Kansas; J.D. Candidate 2010, Washburn University School of Law. I would like to thank the editors of the law journal for their valuable insight. I would also like to thank those friends who shared their thoughts and ideas throughout the writing process. Follow me on Twitter at [www.twitter.com/andrewcpayne](http://www.twitter.com/andrewcpayne).

1. For instance, some countries allow service of process through social-networking sites. Andriana L. Schultz, *Superspoked and Served: Service of Process via Social-Networking Sites*, 43 U. RICH. L. REV. 1497, 1497 (2009); Rick C. Hodgin, *New Zealand Judge Allows Papers Served via Facebook*, TG DAILY, Mar. 16, 2009, available at <http://www.tgdaily.com/business-and-law-features/41733-new-zealand-judge-allows-papers-served-via-facebook>.

2. See THE NIELSEN COMPANY, GLOBAL FACES AND NETWORKED PLACES: A NIELSEN REPORT ON SOCIAL-NETWORKING'S NEW GLOBAL FOOTPRINT 1 (2009), available at [http://blog.nielsen.com/nielsenwire/wp-content/uploads/2009/03/nielsen\\_globalfaces\\_mar09.pdf](http://blog.nielsen.com/nielsenwire/wp-content/uploads/2009/03/nielsen_globalfaces_mar09.pdf).

3. Clark v. Indiana, 915 N.E. 2d 126, 131 (Ind. 2009) (allowing evidence from a defendant's MySpace page as character evidence); Damiano Beltrami, *I'm Innocent. Just Check My Status on Facebook*, N.Y. TIMES, Nov. 11, 2009, at A27, available at <http://www.nytimes.com/2009/11/12/nyregion/12facebook.html>. In November 2009, police accused Rodney Bradford of a robbery that occurred in Brooklyn, New York at 11:50 a.m. *Id.* Bradford alleged that he could not have been in Brooklyn at the time because he had made a Facebook status update at 11:49 a.m. from his father's home across town in Harlem. *Id.* The Facebook status read “ON THE PHONE WITH THIS FAT CHICK...WHERE MY IHOP.” Posting of Ravi Somaiya to Gawker, *Papers Find Facebook Status Too Risque to Print*, <http://gawker.com/5403874/papers-find-facebook-status-too-risque-to-print> (Nov. 13, 2009, 5:39 EST). Police subpoenaed the information from Facebook and released Bradford when the information revealed that the status update originated at Bradford's father's home. Beltrami, *supra*, at A27; see also Edward Marshall, *Burglar Leaves His Facebook Page on Victim's Computer*, THE JOURNAL, Sept. 16, 2009, available at <http://www.journal-news.net/page/content.detail/id/525232.html> (reporting that police were able to track down and arrest a burglar who used the victim's computer in her house to visit Facebook and did not log off).

4. Beltrami, *supra* note 3, at A27 (reporting that online communications “are often used as proof of cheating”).

tion is also rapidly emerging as key evidence in employment cases.<sup>5</sup> Lastly, social-networking information also looks to play a role in non-economic damage issues.<sup>6</sup> The amount of online-communication information will only increase and courts must be equipped to handle the rush. However, the current e-discovery rules are inadequate in managing the different issues that uniquely attach to social-networking information.

This Note argues that courts should be hesitant to analogize directly social-networking information with “Electronically Stored Information” (ESI) as defined in the 2006 Federal Rules of Civil Procedure Amendments. Courts should recognize that meaningful distinctions exist between traditional electronically stored information and social-networking information. There are four key differences.<sup>7</sup> First, social-networking information is permanently stored on third-party servers, which makes the information difficult to access. Second, the Advisory Committee on Civil Rules (Advisory Committee) designed the e-discovery amendments with business information in mind, not personal information. Third, social-networking information is inherently intimate and carries with it privacy implications. Fourth, social-networking information is not monolithic—internal controls allow users to choose who can view their information and what information to share. Courts should not only recognize these distinctions but also discern that they warrant treating social-networking information differently. A failure to acknowledge the distinctions may result in excessive discovery and create serious implications for privacy rights.

The following seeks to illuminate the distinctions by tracing the development of both social networking and the e-discovery rules and show how they have diverged. Part II tracks the rise of electronic data and the progression of social networking. Part III examines the history of e-discovery law, including the 2006 Amendments to the Federal Rules of Civil Procedure. Finally, in Part IV this Note argues, in light of these developments, that future rules should recognize the distinctions between traditional electronically stored information and social-networking information and that courts should adapt their rules accordingly.

---

5. See generally Laura L. Owens, *Electronic Discovery 2009: What Corporate and Outside Counsel Need to Know*, PRACTISING LAW INST., Oct. 6, 2009, Order No. 18525.

6. Tracey Tyler, *Facebook User Poked—By the Courts*, TORONTO STAR, Mar. 14, 2009, available at <http://www.thestar.com/News/GTA/article/602324>. In Canada, a court held that all information on a man’s Facebook page was relevant to his claim that a car accident “lessened his enjoyment of life.” *Id.* More specifically, the court stated that the Facebook page most likely contains information regarding how the plaintiff lived his life after his car accident. *Id.* Furthermore, the court rejected the plaintiff’s privacy assertions and maintained that the plaintiff could not “hide behind self-set privacy controls.” *Id.*

7. See *infra* Part IV.A.

## II. RISE OF SOCIAL NETWORKING: DATA IS THE NEW CURRENCY

As with any technology, the Internet has not remained stagnant since its introduction to the consuming public.<sup>8</sup> The Internet has transformed significantly with the increase of technological capabilities and the collective knowledge of the Internet.<sup>9</sup> In its brief history, the Internet developed in two distinct phases: “web 1.0” and “web 2.0.”<sup>10</sup> Web 1.0 describes the web in its infancy, which includes early Internet technologies such as static websites and email.<sup>11</sup> Web 2.0 illustrates the Internet’s move toward dynamic information sharing.<sup>12</sup> This dynamic information-sharing concept has allowed social-networking websites like Facebook and Twitter to develop, which allow people to share personal information through online communities.<sup>13</sup> The distinctions between web 1.0 and web 2.0 illustrate a major shift in the character of the Internet, and an understanding of those distinctions is critical for crafting adequate litigation rules.

### A. *Web 1.0: Explaining the Difference Between the Internet and Email*

The flow of communication is the major attribute that defines both web 1.0 and web 2.0.<sup>14</sup> In the web 1.0 phase, communication only flowed from the website owner to the viewer—a one-way street.<sup>15</sup> Websites in this phase were static and not interactive.<sup>16</sup> Websites provided information but did not change or update.<sup>17</sup> Furthermore, a visitor was limited strictly to viewing the website and not allowed to contribute to or participate within the site.<sup>18</sup>

The wide adoption of email as a communication device also charac-

8. See Tim O’Reilly, *What Is Web 2.0*, O’REILLY, Sept. 30, 2005, available at <http://oreilly.com/lpt/a/6228>.

9. See *id.*

10. See Brian Getting, *Basic Definition: Web 1.0, Web 2.0, Web 3.0*, PRACTICAL ECOMMERCE, Apr. 18, 2007, available at <http://www.practicalecommerce.com/articles/464-Basic-Definitions-Web-1-0-Web-2-0-Web-3-0>. The separation of the phases of the Internet into Web 1.0, Web 2.0, and Web 3.0 is not entirely clear. *Id.* In fact, many continue to argue over the meanings and distinctions of the terms. O’Reilly, *supra* note 8. Even without precise meanings, these terms serve to illuminate the broad layout of the Internet. See Getting, *supra*.

11. See *infra* Part II.A.

12. See *infra* Part II.B.

13. See *infra* Part II.C.

14. See generally YouTube, Web 2.0, <http://www.youtube.com/watch?v=nsa5ZTRJQ5w> (last visited Apr. 23, 2010) (describing Web 2.0 as a renaissance in computer communication by moving away from isolated information on static websites to dynamic and interactive information sharing best described as a conversation).

15. Getting, *supra* note 10. Web 1.0 was merely a “read-only” web as described by Tim Berners-Lee, the director of the WC3 and so-called father of the Internet. *Id.* In the read-only web, the goal of most website owners was simply to make their information available so the viewing public could search for it and view it. *Id.* The read-only web did not feature user interaction or user data creation. *Id.*

16. Jonathan Strickland, *Is There a Web 1.0?*, HOWSTUFFWORKS, <http://computer.howstuffworks.com/web-101.htm> (last visited Apr. 23, 2010).

17. *Id.*

18. *Id.*

terizes web 1.0.<sup>19</sup> Emails are analogous to letters sent through the postal service but done electronically and stored on the sender's computer.<sup>20</sup> As the Internet became a normal personal and business tool, so did the use of email.<sup>21</sup> Although email is still widely used, further advancements of the Internet have largely turned email into a legacy application.<sup>22</sup> This stage demonstrates the Internet in its youth; the tech-savvy are likely to characterize it as a time when they had to explain the difference between the Internet and email to their parents.<sup>23</sup>

In the late 1990s and early 2000s, companies jumped on the Internet bandwagon and put their full faith in e-commerce.<sup>24</sup> This technological revolution led to the dot-com bubble that eventually burst in 2001.<sup>25</sup> Many in the technology industry lost confidence in the Internet as a viable form of commerce and labeled the technology as overhyped.<sup>26</sup> The burst bubble marked the end of the line for old and failing developments, labeled posthumously as web 1.0, but also led to the ascendance of new technologies that have defined the Internet ever since.<sup>27</sup> The concept of web 2.0 was born out of the rubble of the burst bubble, and its rise marked a turning point in the development of the Internet.<sup>28</sup>

### *B. Web 2.0: Explaining the Difference Between a Poke and a Tweet*

The goal of web 2.0, the phase that has dominated the web for much of the 2000s, is to facilitate the sharing of information among users.<sup>29</sup> This new chapter in the Internet's life envisions the web as a platform for services whose purpose is to harness collective intelligence.<sup>30</sup> The platform as a service model seeks to provide services to users over

---

19. See Joel S. Alleyne, *Email—Good Enough Isn't!*, 72 TEX. B. J. 344, 344 (2009).

20. 7 JAMES WM. MOORE ET AL., MOORE'S FEDERAL PRACTICE § 37A.04[1] (3d ed. 2009) ("In executing the transmission of an email message, a computer makes a copy of the message, retains the original, and sends a copy.")

21. *Id.* ("Email has rapidly become an essential tool in virtually all organizations and businesses.")

22. See Alleyne, *supra* note 19, at 344.

23. See Posting of David Gewirtz to AC360°, *The Dot-Com Bubble: How to Lose \$5 trillion*, <http://ac360.blogs.cnn.com/2009/11/24/the-dot-com-bubble-how-to-lose-5-trillion> (Nov. 24, 2009, 12:33 EST) ("This was a time before Google and YouTube . . . . It was a time when us techies found ourselves explaining to the less computer-savvy what '.com' meant, what those 'www' things were. . . . Twitter and Facebook were still years in the future.")

24. *Id.*

25. O'Reilly, *supra* note 8.

26. *Id.*; TIM O'REILLY & JOHN BATTELLE, *WEB SQUARED: WEB 2.0 FIVE YEARS ON 1* (2009), available at [http://assets.en.oreilly.com/1/event/28/web2009\\_websquared-whitepaper.pdf](http://assets.en.oreilly.com/1/event/28/web2009_websquared-whitepaper.pdf).

27. O'Reilly, *supra* note 8 ("[B]ubbles and consequent shakeouts appear to be a common feature of all technological revolutions. Shakeouts typically mark the point at which an ascendant technology is ready to take its place at center stage.")

28. O'Reilly, *supra* note 8.

29. See O'REILLY & BATTELLE, *supra* note 26, at 1.

30. *Id.* ("Collective intelligence applications depend on managing, understanding, and responding to massive amounts of user-generated data in real time.")

the web that used to be available only through software.<sup>31</sup> Additionally, this phase harnesses the collective intelligence by transforming the Internet into a “read-write” web by allowing the website viewer to participate in the information conversation presented by the website owner.<sup>32</sup> Platforms that follow the web 2.0 structure become more useful as more people use them and contribute information to them.<sup>33</sup> Web 2.0 platforms are merely frameworks for users to input information.<sup>34</sup> Companies literally outsource the creation of the information contained within their platforms to the users in a trend called “crowd-sourcing.”<sup>35</sup>

The flow of information in a web 2.0 environment is much more dynamic than the one-way-street flow in a web 1.0 environment.<sup>36</sup> In the new phase, information flows not only from website owner to website viewer, but also from viewer to owner and viewer to viewer.<sup>37</sup> This stage demonstrates the Internet’s maturity. The tech-savvy are likely to characterize it as a time when they moved beyond the basics and needed to explain the difference between a poke and a tweet to their parents.<sup>38</sup>

If data from individual contributors is the brick and mortar for web 2.0, social-networking websites are the prime contractors.<sup>39</sup> Users of social-networking websites like Facebook, Twitter, and MySpace create and store enormous amounts of information, especially personal information.<sup>40</sup> This information is beginning to play a larger role in civil litigation.<sup>41</sup> The uniqueness of social-networking information complicates the discovery-litigation framework. Accordingly, it is necessary to analyze the expanded use of social-networking sites as well as the fundamentals of popular services.

### *C. The Nuts and Bolts of Popular Social-Networking Websites*

Social-networking sites are “web-based services that allow individuals to (1) construct a public or semi-public profile within a bounded

---

31. See generally O’Reilly, *supra* note 8.

32. Getting, *supra* note 10.

33. O’REILLY & BATTELLE, *supra* note 26, at 1 (“[A]pplications . . . literally get better the more people use them, harnessing network effects not only to acquire users, but also to learn from them and build on their contributions.”).

34. See *id.*

35. John Winsor, *Crowdsourcing: What It Means for Innovation*, BUS. WEEK, June 15, 2009, available at [http://www.businessweek.com/innovate/content/jun2009/id20090615\\_946326.htm](http://www.businessweek.com/innovate/content/jun2009/id20090615_946326.htm) (arguing that mass participation through crowdsourcing will help solve societal problems like economic turmoil and global warming).

36. Getting, *supra* note 10.

37. *Id.*

38. See Gewirtz, *supra* note 23.

39. See O’REILLY & BATTELLE, *supra* note 26, at 2.

40. Social Media Optimization, Top Twenty Five Social Networking Sites – Feb 2009 (Feb. 17, 2009), <http://social-media-optimization.com/2009/02/top-twenty-five-social-networking-sites-feb-2009>. In January 2009, Facebook had more than 1.1 billion visits, MySpace had more than 810 million visits, and Twitter had more than 54 million visits. *Id.*

41. See *supra* notes 4–6 and accompanying text.

system, (2) articulate a list of other users with whom they share a connection, and (3) view and traverse their list of connections and those made by others within the system.”<sup>42</sup> Social-networking sites began to emerge in the late 1990s, but did not gain mainstream recognition until the mid-2000s.<sup>43</sup> To understand fully the details, it is important to understand how users create information, how users are able to place privacy restrictions on the information they create through internal controls, how information is stored, and how popular the use of these sites is becoming. This Note will primarily focus on two popular social-networking sites, Facebook and Twitter, but the fundamentals apply to similar sites.

### 1. How Social-Networking Websites Work

Facebook is the most popular social-networking website.<sup>44</sup> Facebook is a website-based network that allows users to create online profiles that display information about themselves.<sup>45</sup> Users then can connect with others users and share that information.<sup>46</sup> There are many types of information that users can create and share through Facebook.<sup>47</sup> Facebook members can share text with multiple people through a “status update” or through information placed on the user’s profile.<sup>48</sup> A completed profile contains approximately forty different ways to express information.<sup>49</sup> Users can also share text with another user individually through a direct message to the user or a wall post to the user’s profile, or users can have a direct conversation with another user through Facebook’s chat feature.<sup>50</sup> Social-networking patrons can also

---

42. danah m. boyd & Nicole B. Ellison, *Social Network Sites: Definition, History, and Scholarship*, 13 J. COMPUTER-MEDIATED COMM. (Issue 1) (2007), available at <http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html>.

43. *Id.*

44. NIELSEN, *supra* note 2, at 1.

45. See Facebook, Help Center: Profile, <http://www.facebook.com/help/?page=402> (last visited Apr. 23, 2010); Susan Whelan, *An Introduction to Facebook for Beginners: An Overview of the Facebook Social Network*, SUITE101.COM, Jan. 15, 2008, [http://social-networking-tagging.suite101.com/article.cfm/facebook\\_for\\_beginners](http://social-networking-tagging.suite101.com/article.cfm/facebook_for_beginners).

46. Whelan, *supra* note 45; see Facebook, Help Center: Friends, <http://www.facebook.com/help/?page=441> (last visited Apr. 23, 2010).

47. A status allows a user to share with others in a short block of text what they are doing, how they feel, or what they think. See generally Whelan, *supra* note 45.

48. Whelan, *supra* note 45; see Facebook, *supra* note 45.

49. James Grimmelmann, *Saving Facebook*, 94 IOWA L. REV. 1137, 1149 (2009) (identifying the possible information on a user’s profile as “name; birthday; political and religious views; online and offline contact information; gender, sexual preference, and relationship status; favorite books, movies, and so on; educational and employment history; and, of course, picture”).

50. A “wall post” is a message that a user can leave on another user’s profile and is often viewable by either the entire Facebook community or a user’s friends, depending on the user’s privacy settings. See LYONDELL BASELL, FACEBOOK 101: INSTRUCTIONS 2, available at <http://www.lyondellbasell.com/NR/rdonlyres/70EF661F-0074-42F4-B342-13D91DE6B9FB/0/Facebook.pdf> (last visited Apr. 23, 2010); Susan Ng, *A Beginner’s Guide to Facebook: Learn the Basics of Facebook*, HUBPAGES, <http://hubpages.com/hub/facebookforbeginners> (last visited Apr. 23, 2010); Facebook, Help Center: Wall: How to Use the Wall Feature and Wall Privacy, <http://www.facebook.com/help/?page=820> (last visited Apr. 23, 2010).

share pictures and videos.<sup>51</sup> A user's "news feed" displays all the information that his or her friends create, change, or share.<sup>52</sup>

Twitter is a much simpler social-networking website that allows users to share messages composed of 140 characters or less.<sup>53</sup> Twitter lets users share their answer to the question "What's happening?" with either specified people or the public at large.<sup>54</sup> The users can send a short message—also known as a "tweet"<sup>55</sup>—or view the messages of others through the web or a mobile phone.<sup>56</sup> Twitter users can also share pictures with other users.<sup>57</sup>

## 2. Internal Controls Create Different Types of Information

Social networks have internal controls that give users broad power over who can view their information and what types of information to share. This generally results in three types of information: public information released to anyone, semi-private information released only to friends, and mostly private information released to one person or a select few. Facebook has a very intricate privacy and security policy.<sup>58</sup> Users must confirm a third party as a friend for the third party to view information created by the user.<sup>59</sup> Users can specifically identify what types of people are able to view their information, which can range from allowing no one to view any information the user creates to allowing any one who accesses Facebook to view the information.<sup>60</sup> Similarly, a Twitter user may choose to have a private account or a public account.<sup>61</sup> Users with private accounts only display their tweets to specifically authorized persons.<sup>62</sup> Users with public accounts display their tweets to the public.<sup>63</sup>

---

51. See LYONDELL BASELL, *supra* note 50, at 1.

52. *Id.* at 2 (The news feed feature is a tickertape of all of a user's friends' activities, including their status updates, wall posts, and picture uploads.).

53. Twitter, About, <http://twitter.com/about> (last visited Apr. 23, 2010).

54. *Id.*

55. The Associated Press Stylebook has entries for the word "Twitter" as both a noun and a verb and also includes the variation "tweet" and verb form "to tweet." Press Release, Associated Press, New Edition of AP Stylebook Adds New Entries and Helpful Features (June 11, 2009), [http://www.ap.org/pages/about/pressreleases/pr\\_061109a.html](http://www.ap.org/pages/about/pressreleases/pr_061109a.html).

56. Mobile devices are increasingly integrating with online social-networking websites allowing users to interact with the sites in the same manner as if the user was on a computer. B. Garrie et al., *Mobile Messaging Making E-Discovery Messy: Mobile Messaging and Electronic Discovery*, 32 HASTINGS COMM. & ENT. L.J. 103, 105 (2009).

57. Posting of Josh Catone to Mashable, 5 Ways to Share Images on Twitter, <http://mashable.com/2009/05/19/twitter-share-images/> (May 19, 2009, 09:27 AST).

58. Facebook, Privacy Policy <http://www.facebook.com/policy.php> (last visited Apr. 23, 2010).

59. See Whelan, *supra* note 45.

60. See Facebook, *supra* note 58.

61. Twitter, Twitter Support: Guidelines for Law Enforcement, <http://help.twitter.com/forums/26257/entries/41949> (last visited Apr. 23 2010).

62. *See id.*

63. *See id.*

### 3. How Social-Networking Information Is Stored and Subpoenaed

All of the information created by social-network users is not stored permanently on a user's computer, but rather is stored on the social network's own servers.<sup>64</sup> Facebook has 30,000 servers located in several data centers across the United States.<sup>65</sup> The amount of data handled per day by Facebook's servers is equivalent to "1,000 times the volume of mail delivered daily by the U.S. Postal Service."<sup>66</sup> The amount of data stored includes eighty billion pictures—600,000 of which Facebook users receive every second.<sup>67</sup> Twitter operates a 15,000-square-foot data center to accommodate its storage needs.<sup>68</sup>

Getting access to this stored information is not easy. Facebook maintains in its privacy policy that it will share "information pursuant to subpoenas, court orders, or other requests (including criminal and civil matters) if we have a good faith belief that the response is required by law."<sup>69</sup> Twitter's privacy policy specifically indicates that although Twitter stores information, it will not release information unless required by a subpoena, court order, or legal process document.<sup>70</sup> The storage of information often lasts for a short time, but a data preservation request can extend the period for which data is stored.<sup>71</sup>

### 4. The Prevalence of Social Networking

In the past year, social-networking websites have become the preferred form of communication.<sup>72</sup> In 2009, social networking surpassed email in worldwide reach.<sup>73</sup> The time spent on social-networking sites and the amount of information created has grown exponentially.<sup>74</sup> More specifically, Facebook has moved from a limited college audience

---

64. See Rich Miller, *Facebook Now Has 30,000 Servers*, DATA KNOWLEDGE SERVERS, Oct. 13, 2009, <http://www.datacenterknowledge.com/archives/2009/10/13/facebook-now-has-30000-servers/>.

65. *Id.*

66. *Id.* (quoting Jeff Rothschild, Vice-President of Technology at Facebook). The amount of data per day is roughly twenty-five terabytes. *Id.* To put the amount of data in perspective, one terabyte is equivalent to 500 million typewritten pages or 1 million books and 10 terabytes would encompass all of the printed works in the Library of Congress. SHIRA A. SCHEINDLIN, *MOORE'S FEDERAL PRACTICE: E-DISCOVERY: THE NEWLY AMENDED FEDERAL RULES OF CIVIL PROCEDURE 2* (2006); CoolTechBlog.com, *Perspective on Storage; Powers of 10*, <http://www.cooltechblog.com/?p=43> (last visited Apr. 23, 2010).

67. See Miller, *supra* note 64.

68. Justin Lee, *Twitter's Growth Drives NTT Data Center*, WEB HOST INDUS. REVIEW, Sept. 1, 2009, [http://www.thewhir.com/web-hosting-news/090109\\_Twitter's\\_Growth\\_Drives\\_NTT\\_Data\\_Center](http://www.thewhir.com/web-hosting-news/090109_Twitter's_Growth_Drives_NTT_Data_Center).

69. Facebook, *supra* note 58.

70. Twitter, *supra* note 61.

71. *Id.* (Twitter will only store data pursuant to a preservation request if a court order or subpoena sent by law enforcement accompanies the request.).

72. Posting of Adam Ostrow to Mashable, *Social Networking More Popular than Email*, <http://mashable.com/2009/03/09/social-networking-more-popular-than-email/> (Mar. 9, 2009, 8:45 AST).

73. *Id.*

74. See *id.* Users spent 63% more time on social-networking websites than they did the year before. *Id.* Furthermore, the time spent on Facebook increased 566% by users worldwide. *Id.*

to a worldwide reach in a few short years.<sup>75</sup> In December 2009, Facebook surpassed 350 million active users, which is larger than the population of the United States.<sup>76</sup> Fifty percent of the 350 million active users visit the site on any given day.<sup>77</sup> One-third of Facebook's users are between the ages of thirty-five and forty-nine and one-quarter are over the age of fifty.<sup>78</sup> From December 2007 to December 2008, the time spent on Facebook increased 566%, compared to an increase of only 18% of time spent on the Internet in general.<sup>79</sup>

Twitter experienced a 752% growth in 2008 and saw an even larger increase in the first half of 2009.<sup>80</sup> Users tweeted approximately seven billion times since the inception of Twitter and over twenty-seven million times per day in November 2009.<sup>81</sup> In June 2009, Twitter planned a critical upgrade of its facilities to accommodate its rapid growth.<sup>82</sup> Twitter delayed the upgrade after receiving pressure from outside sources like the United States government because the outage caused by the upgrade would hamper the role the service was playing in communicating protests during the Iranian election.<sup>83</sup> With the widespread adoption and reliance on sites like Facebook and Twitter, social-networking sites across the Internet are sending the message that they are here to stay—so plan accordingly.

\* \* \*

The terminology and background of web 1.0, web 2.0, and social networking are important in understanding the landscape of electronic discovery. This Note contends that the 2006 e-discovery amendments and the incorporation of the term “electronically stored information” in the Rules of Civil Procedure was a reaction, in part, to the rise of web 1.0. Thus, this Note defines the term “traditional ESI” as web 1.0 technology. Additionally, this Note uses the terms “social-networking in-

---

75. NIELSEN, *supra* note 2, at 4. Approximately 70% of the users on Facebook are located outside of the United States, and there are more than seventy language translations available on the site. Facebook, Statistics, <http://www.facebook.com/press/info.php?statistics> (last visited Apr. 23, 2010).

76. Facebook, Timeline, <http://www.facebook.com/press/info.php?timeline> (last visited Apr. 23, 2010). An “active user” is a user who has visited the site in the previous thirty days. Facebook, Factsheet, <http://www.facebook.com/press/info.php?factsheet> (last visited Apr. 23, 2010).

77. Facebook, *supra* note 75. Additionally, more than sixty-five million users access Facebook through their mobile phones. *Id.*

78. NIELSEN, *supra* note 2, at 4. Facebook's fastest growing demographic is users ranging from age thirty-five to forty-nine. *Id.*

79. NIELSEN, *supra* note 2, at 3.

80. Lee, *supra* note 68.

81. Kim-Mai Cutler, *Updated: Twitter to Deliver “Several Billion Tweets” an Hour Next Year*, DIGITAL BEAT, Dec. 28, 2009, <http://digital.venturebeat.com/2009/12/28/twitter-billion>. Co-Founder of Twitter, Biz Stone, anticipates that in 2010, Twitter will receive over one billion searches each day and users will make “several billion tweets an hour.” *Id.*

82. Lee, *supra* note 68.

83. Posting of @Biz (Biz Stone) to Twitter Blog, Down Time Rescheduled, <http://blog.twitter.com/2009/06/down-time-rescheduled.html> (June, 15, 2009, 16:17 PST).

formation” and “web 2.0” interchangeably as applied to the civil discovery rules. The next Part will address how the legal field has sought to address the web 1.0 and web 2.0 information waves. Just as courts adopted new frameworks and rules to address the onslaught of web 1.0 information, courts are now facing the reconciliation of their new rules and frameworks with web 2.0 information.

### III. E-DISCOVERY: A CONFLICTING HISTORY

In the realm of electronic information in civil discovery, courts and rule drafters have struggled to keep pace with technology.<sup>84</sup> Despite the intent of rule drafters to create longstanding rules, frequent advances in technology have impeded this goal. Old rules are often incompatible with new technology because of the inability of rule drafters to foresee future problems. The Advisory Committee has amended the discovery rules twice—in 1970 and 2006—to keep pace with new situations created by technology.<sup>85</sup> When technology has advanced too far beyond the scope of the amended rules, courts have stepped in to fill the gaps and reconcile the old rules with the new technology.<sup>86</sup>

This system of technological rulemaking has created three different phases of rules governing electronic information. In the first phase, the rapid expansion of electronic information during the web 1.0 wave in the 1990s forced courts to develop new rules pertaining to electronic information.<sup>87</sup> Courts entered the second phase in 2006 with amendments to the Federal Rules of Civil Procedure that specifically incorporated ESI rules and procedures.<sup>88</sup> Courts are currently in the third phase and face reconciling web 2.0 information with the 2006 Amendments.<sup>89</sup>

There are several areas in which distinctions between old rules and new technology are present: the scope of discovery, the allocation of costs, the application of the duty of preservation, and the protection of privacy.<sup>90</sup> The following sections will address the three rule-changing phases and the reaction to technological advancements in those areas in which courts could find distinctions.

---

84. See 7 JAMES WM. MOORE ET AL., *supra* note 20, § 37A.01[1] (“[I]t is doubtful whether the development of a jurisprudence will ever keep pace with new inventions and technological advancements.”).

85. FED. R. CIV. P. 34 advisory committee’s note (1970 & 2006 amendments) (clarifying that Rule 34 applies to electronic data complications). See generally SCHEINDLIN, *supra* note 66 (outlining the text of the 2006 e-discovery amendments and describing the changes).

86. See *infra* Part III.A.

87. See *infra* Part III.A.

88. See *infra* Part III.B.

89. See *infra* Part III.C.

90. See generally Kenneth J. Withers, *Electronically Stored Information: The December 2006 Amendments to the Federal Rules of Civil Procedure*, 4 NW. J. TECH. & INTELL. PROP. 171, 173-91 (2006) (describing the distinctions between traditional discoverable documents and electronic information).

### A. Phase I: Courts Step in to Fill the Electronic Discovery Rule Gaps

Before the adoption of the recent formal e-discovery rules, courts accepted the basic principle that “computerized data is discoverable if relevant.”<sup>91</sup> As the creation and use of electronic data increased through the 1990s, litigation transformed so that virtually all cases involved electronic data.<sup>92</sup> With electronic data becoming increasingly commonplace, courts addressed the issues of scope, accessibility, and preservation. However, courts could not agree on how to address those issues.<sup>93</sup> Some judges and scholars acknowledged that “digital is different” from traditional discovery, but the legal community lacked consensus regarding those differences.<sup>94</sup> Some courts asserted that the Federal Rules, as they currently existed, could incorporate electronic discovery.<sup>95</sup> Furthermore, judges possessed the widespread view that, although differences may exist between electronic and traditional discovery, the existing rules could accommodate those differences.<sup>96</sup>

In the early 2000s, the landmark *Zubulake v. UBS Warburg, LLC*<sup>97</sup> opinions cemented the common law rules for e-discovery before the enactment of the 2006 amendments.<sup>98</sup> The *Zubulake* case arose from discovery disputes concerning emails that were only located on backup

91. *Anti-Monopoly, Inc. v. Hasbro, Inc.*, No. 94 Civ. 2120, 1995 WL 649934, at \*2 (S.D.N.Y. Nov. 3, 1995) (stating that the rule was “black letter law”); *Bills v. Kennecott Corp.*, 108 F.R.D. 459, 463-64 (D. Utah 1985) (stating “information stored in computers should be as freely discoverable as information not stored in computers”); see also MICHAEL R. ARKFELD, *ARKFELD ON ELECTRONIC DISCOVERY AND EVIDENCE* § 1.3(A) (2d ed. 2009).

92. ARKFELD, *supra* note 91, § 1.3(A); David S. Isom, *Electronic Discovery: New Power, New Risks*, 16 UTAH B. J. 8, 10 (2003). In the late 1990s, studies suggested that as much as 97% of information was electronic and much of that data never appeared in printed form. ARKFELD, *supra* note 91, § 1.3(A) (citing an article from 2000).

93. Withers, *supra* note 90, at 172.

94. *Id.*

95. *Jones v. Goord*, No. 95 Civ. 8026, 2002 WL 1007614, at \*6 (S.D.N.Y. May 16, 2002) (“[The Federal Rules of Civil Procedure], albeit for the most part drafted in an earlier era, deal perfectly well with the problems occasioned by discovery of electronic ‘documents.’”).

96. Withers, *supra* note 90, at 172 (noting that in the few decisions regarding electronic discovery, courts analogized the discovery of electronic information to traditional discovery information).

97. United States Magistrate Judge Shira Scheindlin wrote seven opinions in the *Zubulake* case; three of the opinions addressed relevant electronic discovery issues. *Zubulake v. UBS Warburg, L.L.C. (Zubulake V)*, 229 F.R.D. 422 (S.D.N.Y. 2004) (sanctions); *Zubulake v. UBS Warburg, L.L.C. (Zubulake IV)*, 220 F.R.D. 212 (S.D.N.Y. 2003) (duty of preservation); *Zubulake v. UBS Warburg, L.L.C. (Zubulake I)*, 217 F.R.D. 309 (S.D.N.Y. 2003) (describing the scope of electronic discovery and cost shifting).

98. See Sean M. Georges, *Zubulake and E-Discovery: Did You Get Your Wake-Up Call?*, RES GESTAE, Oct. 18, 2006, at 12 (“*Zubulake* should be viewed as nothing less than a serious ‘wake-up call’ to counsel and clients across the country, as it attempts to clarify some of the many difficult issues concerning the obligation to preserve, maintain and produce discoverable electronic records . . . .”); John S. Wilson, Comment, *Myspace, Your Space, or Our Space? New Frontiers in Electronic Evidence*, 86 OR. L. REV. 1201, 1211 (2007) (“The final evolutionary progression in the common law rules governing e-discovery came in *Zubulake* . . . .”). The *Zubulake* litigation arose from a gender discrimination claim asserted by Laura Zubulake against her employer UBS Warburg. *Zubulake I*, 217 F.R.D. at 311. Ms. Zubulake sought the discovery of emails that were only available on backup tapes. *Id.* at 311-12. UBS alleged that the cost of restoring the emails from the back-up tapes would cost \$175,000 and would take five days to restore unless the backup tapes were taken to an expensive third-party vendor. *Id.* at 312, 314.

tapes, setting up what the court called “a textbook example of the difficulty of balancing the competing needs of broad discovery and manageable costs.”<sup>99</sup> In the course of the decisions, the *Zubulake* court confronted several of the most problematic issues with electronic information: the extent of discoverability of electronic data, the distribution of the costs of e-discovery, and the application of the duty of preservation.<sup>100</sup>

In addressing the issue of the extent of discovery of electronic data, the *Zubulake I*<sup>101</sup> opinion applied a very broad approach to the discovery of electronic documents.<sup>102</sup> The court inferred that electronic data is no different in its discoverability from data contained on paper under Federal Rule of Civil Procedure 34.<sup>103</sup> Rule 34 stated that parties could request discovery of documents “including writings, drawings, graphs, charts, photographs, phonorecords, and other data compilations.”<sup>104</sup> The court held that this description was broad enough to cover electronic documents because the Advisory Committee stated that the description “accord[s] with changing technology.”<sup>105</sup> Accordingly, the court gave electronic documents the same treatment as paper documents—electronic documents are discoverable if relevant.<sup>106</sup>

In addressing the issue of accessibility, the court’s primary motive was to determine which party would bear the cost of discovering electronic information.<sup>107</sup> The *Zubulake I* court sought to provide a framework to answer two questions: (1) whether production would impose an undue burden or expense on the responding party; and (2) in cases in

99. *Zubulake I*, 217 F.R.D. at 311.

100. See *infra* Part III.B.1-3.

101. 217 F.R.D. 309 (S.D.N.Y. 2003).

102. See *id.* at 317.

103. *Id.* at 311 (“Broad discovery is a cornerstone of the litigation process contemplated by the Federal Rules of Civil Procedure.” (citing *Jones v. Goord*, No. 95 Civ. 8026, 2002 WL 1007614, at \*1 (S.D.N.Y. May 16, 2002))).

104. *Id.* at 316-17 (quoting Fed R. Civ. P. 34(a)).

105. *Id.* (quoting Fed R. Civ. P. 34 advisory committee’s comment (1970 amendment)). The advisory committee comment to the 1970 amendment to Rule 34 further states that:

It makes clear that Rule 34 applies to electronics data compilations from which information can be obtained only with the use of detection devices, and that when the data can as a practical matter be made usable by the discovering party only through respondent’s devices, respondent may be required to use his devices to translate the data into usable form.

FED R. CIV. P. 34 advisory committee note (1970 amendment).

106. *Zubulake I*, 217 F.R.D. at 317. The court concluded that not only are electronic documents that currently exist discoverable, but that deleted documents that reside on backup disks are also discoverable. *Id.*

107. Before the *Zubulake* litigation, two decisions laid early groundwork for accessibility and cost allocation issues. The court in *McPeck v. Ashcroft*, 202 F.R.D. 31 (D.D.C. 2001), applied a marginal utility approach to cost allocation stating that “[t]he more likely it is that [ESI] contains information that is relevant to a claim or defense, the fairer it is that the [requestee] search at its own expense.” *Id.* at 34. Furthermore, the court in *Rowe Entertainment, Inc. v. William Morris Agency, Inc.*, 205 F.R.D. 421 (S.D.N.Y. 2002), set forth eight factors for deciding whether to shift the cost of discovering electronic data to the requestor. *Id.* at 429. The *Rowe* factors were hailed by some commentators as the “gold standard” for resolving discovery disputes until the *Zubulake* factors supplanted them. James M. Evangelista, *Polishing the “Gold Standard” on the E-Discovery Cost-Shifting Analysis: Zubulake v. UBS Warburg*, L.L.C., 9 J. TECH. L. & POL’Y 1, 3 (2004).

which production would impose an undue burden, when courts should apply cost shifting.<sup>108</sup>

The *Zubulake I* opinion stated that courts should apply cost shifting only when e-discovery imposes an “undue burden or expense” on the responding party.<sup>109</sup> According to the court, production of electronic data is unduly burdensome when inaccessible.<sup>110</sup> The accessibility of electronic data corresponds with how the information is stored.<sup>111</sup> The court identified five types of stored information: (1) active, online data; (2) near-line data; (3) offline storage/archives; (4) backup tapes; and (5) erased, fragmented, or damaged data.<sup>112</sup> The *Zubulake I* opinion maintained that the first three categories are typically accessible because the data “is stored in a readily usable format.”<sup>113</sup> The court deemed the last two categories to be typically inaccessible because they cannot be produced in a “readily useable format” without extensive recovery processes.<sup>114</sup>

Recognizing that courts should not apply the cost-shifting analysis simply because data is inaccessible, the court established a seven-factor test for determining whether to apply cost shifting. The factors are:

- (1) The extent to which the request is specifically tailored to discover relevant information;
- (2) The availability of such information from other sources;
- (3) The total cost of production, compared to the amount in controversy;
- (4) The total cost of production, compared to the resources available to each party;
- (5) The relative ability of each party to control costs and its incentive to do so;
- (6) The importance of the issues at stake in the litigation; and
- (7) The relative benefits to the parties of obtaining the information.<sup>115</sup>

The court maintained that the factors do not have equal weight and di-

---

108. See *Zubulake I*, 217 F.R.D. at 317-18.

109. *Id.* at 318. A burden is undue if it “outweighs its likely benefit, taking into account the needs of the case, the amount in controversy, the ‘parties’ resources, the importance of the issues at stake in the litigation, and the importance of the proposed discovery in resolving the issues.” *Id.* (quoting FED. R. CIV. P. 26(b)(2)(iii) (prior to the 2006 amendment)). The court was quick to point out that courts should not apply cost shifting in every electronic discovery case. *Id.* at 317. The court pointed to the fact that often times electronic discovery is cheaper than traditional discovery because of search functions, key word search capabilities, and the elimination of mass photocopying. *Id.* at 318. The court also reestablished the presumption that the responding party will bear the full cost of expenses and that an e-discovery issue did not automatically rebut that presumption. *Id.* at 324.

110. *Id.* at 318 (stating that the distinction between accessible and inaccessible “corresponds closely to the expense of production”).

111. *Id.*

112. *Id.* at 318-19. For a detailed description of the classifications of electronic storage, see ARKFELD, *supra* note 91, § 3.6(B).

113. *Zubulake I*, 217 F.R.D. at 319-20.

114. *Id.* at 320.

115. *Id.* at 322. The test established in *Zubulake I* eliminates two factors from the test established in *Rowe* and adds factor number seven. See *id.* at 321-22.

vided them into three levels of importance. The most important factors are (1) and (2); the second most important group of factors includes (3), (4), (5), and (6); and the factor with the least importance is (7).<sup>116</sup>

The court in *Zubulake IV*<sup>117</sup> also outlined the common-law duty of preservation as it applied to electronic information.<sup>118</sup> Under the duty of preservation, a party must preserve potential evidence in its possession, control, or custody if the evidence is potentially relevant.<sup>119</sup> The duty has two relevant parts: the time when the duty applies and the scope of the duty.<sup>120</sup> The duty arises when either “the party has notice that the evidence is relevant to litigation or when a party should have known that the evidence may be relevant to future litigation.”<sup>121</sup> Under this standard, the duty may arise well before the opposing party files a lawsuit.<sup>122</sup> A party’s duty may arise even before any notice by the opposing party.<sup>123</sup>

When the duty begins, it does not necessarily extend to all electronic information.<sup>124</sup> Rather, the scope of the duty is limited to electronic data “that might be useful to an adversary.”<sup>125</sup> The court further restricted the scope by including the preservation of documents made by or for individuals who are “likely to have relevant information”—“the key players.”<sup>126</sup> Once the duty attaches because a party reasonably anticipates litigation, the party should institute a “litigation hold” to preserve meaningfully the evidence.<sup>127</sup>

In addition to scope, accessibility, and preservation, courts also faced the issue of privacy rights in electronic information. The discovery rules offer parties a chance to assert privacy rights to limit discovery despite the lack of a privacy privilege.<sup>128</sup> Under Rule 26(c), courts can grant a protective order “to protect a party or person from annoyance,

116. *Id.* at 323.

117. *Zubulake v. UBS Warburg, L.L.C. (Zubulake IV)*, 220 F.R.D. 212 (S.D.N.Y. 2003).

118. *Id.* at 216; Douglas L. Rogers, *A Search for Balance in the Discovery of ESI Since December 1, 2006*, 14 RICH. J.L. & TECH. (ISSUE 3) 4-8 (2008); THE SEDONA CONFERENCE, THE SEDONA PRINCIPLES: BEST PRACTICES RECOMMENDATIONS & PRINCIPLES FOR ADDRESSING ELECTRONIC DOCUMENT PRODUCTION 28-30 (2d ed. 2007) (“The common law duty to preserve evidence clearly extends to electronically stored information.”).

119. See 7 JAMES WM. MOORE ET AL., *supra* note 20, § 37A.10[1].

120. *Zubulake IV*, 220 F.R.D. at 216; THE SEDONA CONFERENCE, *supra* note 118, at 29.

121. *Zubulake IV*, 220 F.R.D. at 216; Kenneth J. Withers, “*Ephemeral Data*” and the Duty to Preserve Discoverable Electronically Stored Information, 37 U. BALT. L. REV. 349, 349-50 (2008).

122. See 7 JAMES WM. MOORE ET AL., *supra* note 20, § 37A.10[3][a].

123. *Id.*

124. *Zubulake IV*, 220 F.R.D. at 217.

125. *Id.*

126. *Id.* at 218.

127. SCHEINDLIN, *supra* note 66, at 10 (stating “litigation hold[s] [have] three essential components: (1) a notice to all custodians of records—which may include not only information technology (IT) people but key employees; (2) a protocol for retrieving and preserving relevant ESI; and (3) monitoring procedures to ensure that employees are actually implementing the litigation hold”).

128. *Hecht v. Pro-Football, Inc.*, 46 F.R.D. 605, 607 (D.C. Cir. 1969); *United States v. Bell*, 217 F.R.D. 335, 343 (M.D. Pa. 2003).

embarrassment, oppression, or undue burden or expense.”<sup>129</sup> Courts may consider the privacy of a party to determine whether a request for discovery is “oppressive or unreasonable” under the rule.<sup>130</sup> If a court identifies a privacy right, the court will balance that right against the value of producing the information.<sup>131</sup> Early cases involving privacy and electronic information revolved around e-mails in the workplace.<sup>132</sup> Largely, courts have held that employees have no expectation of privacy in their emails, and, therefore, employees’ emails are discoverable.<sup>133</sup>

\* \* \*

The Advisory Committee began conferring in 2000 regarding potential amendments to the Federal Rules of Civil Procedure to incorporate ESI.<sup>134</sup> The committee indicated that prior to the amendments court application of the Federal Rules to ESI was difficult because “most rules had not been drafted with electronic information in mind.”<sup>135</sup> The committee spent five years aiming to answer three questions: (1) what are the differences between conventional and electronic discovery; (2) if there are distinctions, do they warrant changes in the Federal Rules of Civil Procedure; and (3) how could changes in the rules solve litigation problems.<sup>136</sup> The committee crafted amendments after recognizing that fundamental differences between traditional discovery documents and ESI existed.<sup>137</sup>

#### *B. Phase II: “Digital Is Different”—The 2006 E-Discovery Amendments*

The e-discovery amendments to the Federal Rules of Civil Procedure went into effect on December 1, 2006. The Advisory Committee claimed that the rules needed amendments because of four key distinctions between paper documents and electronic information.<sup>138</sup> First, the volume of electronic information dwarfed the amount of traditional paper documents.<sup>139</sup> Second, the drafters emphasized that ESI includes

---

129. FED R. CIV. P. 26(c)(1).

130. *Bell*, 217 F.R.D. at 343.

131. 6 JAMES WM. MOORE ET AL., MOORE’S FEDERAL PRACTICE § 26.101[1][c] (3d ed. 2010).

132. *See* 7 JAMES WM. MOORE ET AL., *supra* note 20, § 37A.04[4][a].

133. *Id.*

134. SCHEINDLIN, *supra* note 66, at 1.

135. *See* 7 JAMES WM. MOORE ET AL., *supra* note 20, § 37A.01[1].

136. Withers, *supra* note 90, at 192.

137. *Id.* at 192-94.

138. SCHEINDLIN, *supra* note 66, at 2.

139. *Id.* The enormous volume of ESI led the Advisory Committee to conclude that it was undisputed that the costs of civil discovery would drastically increase. *Id.* To illuminate the vastness of ESI, an average employee will write or receive fifty emails a day equating to 1.5 billion emails per year for a company with 100,000 employees. *Id.* *See generally* 7 JAMES WM. MOORE ET AL., *supra* note 20, § 37A.01[2].

information “not contained within its four corners.”<sup>140</sup> Third, ESI is difficult to delete permanently from a computer as compared with the ease of shredding paper documents.<sup>141</sup> Fourth, ESI may require costly retrieval, restoration, or translation from its storage device before a party can review it.<sup>142</sup> The Advisory Committee maintained that these distinctions created the risk of excessive discovery.<sup>143</sup>

The amendments sought to address these technological distinctions by grafting specific discovery procedures for ESI into the rules.<sup>144</sup> The codified rules address the issues that courts had struggled with regarding ESI: scope, accessibility, and preservation.<sup>145</sup> The following subsections outline how the Advisory Committee drafted the amendments to address those concerns.

### 1. Rule 34: Electronically Stored Information Is Discoverable

The amended Rule 34 established the scope of discoverable electronic data.<sup>146</sup> The rule put the term “electronically stored information” on equal grounds with the term “documents.”<sup>147</sup> The Advisory Committee notes specify that the term “electronically stored information” is expansive and forward-looking.<sup>148</sup> The committee included the phrase

140. 7 JAMES WM. MOORE ET AL., *supra* note 20, § 37A.01[2]; *see also* SCHEINDLIN, *supra* note 66, at 2-3 (“Computers automatically create information without the direction or often the knowledge of the operator.”). Electronic documents contain information that is not located on the printed copy of the document. 7 JAMES WM. MOORE ET AL., *supra* note 20, § 37A.01[2]. This information is commonly known as “metadata.” *Id.* A common definition of metadata is “data about data.” *Id.* § 37A.03[1]. A computer’s operating system or an individual user affixes metadata to ESI. *Id.* Metadata commonly contains information regarding the document’s file name, author of the document, when a user created and modified the document, the length of time a user spent on modifications to the document, and the document’s storage information. *Id.* For a detailed description of metadata, *see Williams v. Sprint/United Management Co.*, 230 F.R.D. 640, 646-47 (D. Kan. 2005) (articulating the common definitions of metadata).

141. SCHEINDLIN, *supra* note 66, at 3. Deleted electronic documents remain recoverable on a computer’s hard drive until a new file overwrites it. *See* 7 JAMES WM. MOORE ET AL., *supra* note 20, § 37A.03[3]. Oftentimes, only pieces of an original document remain while other parts of the document become overwritten. *Id.* Retrieval of deleted documents may require extensive time and money. SCHEINDLIN, *supra* note 66, at 3.

142. SCHEINDLIN, *supra* note 66, at 3. ESI located on outdated technology or in inaccessible formats requires significant and expensive restoration activities to be useable. *Id.* Such restoration activities permit review of ESI before a party can produce it. *Id.*

143. *See* 7 JAMES WM. MOORE ET AL., *supra* note 20, § 37A.01[2].

144. *Id.* The whole package of amendments included changes to Rules 16, 26, 33, 34, 37, and 45. *See generally* SCHEINDLIN, *supra* note 66. This Note will only address those relevant to scope, accessibility, and preservation.

145. SCHEINDLIN, *supra* note 66, at 3 (“Preservation of potentially relevant evidence is more of a problem now than ever before.”).

146. The amended rule reads:

A party may serve on any other party a request within the scope of Rule 26(b): (1) to produce . . . (A) any designated documents or *electronically stored information*—including writings, drawings, graphs, charts, photographs, sound recordings, images, and other data or data compilations—stored in any medium from which information can be obtained either directly or, if necessary, after translation by the responding party into a reasonably usable form . . . .

FED. R. CIV. P. 34(a) (emphasis added).

147. FED. R. CIV. P. 34(a)(1)(A); Withers, *supra* note 90, at 195.

148. FED. R. CIV. P. 34 advisory committee’s note (2006 amendment) (“The rule covers—either

“‘stored in any medium’ to encompass future developments in computer technology.”<sup>149</sup>

The motivating factor behind the committee’s adoption of such a broad term was to have one rule that addresses both present and future technologies.<sup>150</sup> In the rulemaking process, the Advisory Committee considered adding electronic devices such as tapes, floppy disks, and hard drives to the list of discoverable items in Rule 34.<sup>151</sup> As the committee debated the rules, new electronic items like iPods and thumb drives hit the shelves, while floppy disks vanished.<sup>152</sup> The committee determined that the rules needed an expansive view of technology to prevent the need for constant amendments to keep pace with technology.<sup>153</sup> The committee eventually arrived at inserting “electronically stored information” alongside documents as discoverable items.<sup>154</sup>

## 2. Rule 26(b)(2)(B): Inaccessible ESI

The amendment to Rule 26 addresses the issue of accessible and inaccessible ESI.<sup>155</sup> The amended Rule 26(b)(2) moves away from the cost-shifting approach and adopts a “two tier approach”<sup>156</sup> The first tier maintains that a party must produce ESI from sources that are reasonably accessible.<sup>157</sup> The second tier addresses ESI from sources that are “not reasonably accessible because of undue burden or cost.”<sup>158</sup> Instead of adopting a strict cost-shifting paradigm, the rule maintains that ESI from sources not reasonably accessible is not within the scope of discovery and, therefore, not discoverable.<sup>159</sup> The rule further maintains that a court may order discovery of ESI from sources not reasonably accessible on a showing of good cause and provides the court with the power to

---

as documents or as electronically stored information—information ‘stored in any medium,’ to encompass future developments in computer technology. Rule 34(a)(1) is intended to be broad enough to cover all current types of computer-based information, and flexible enough to encompass future changes and developments.”).

149. *Id.*

150. *Id.*; Withers, *supra* note 90, at 194-95.

151. Withers, *supra* note 90, at 194.

152. *Id.*

153. *Id.* at 195.

154. *Id.*

155. FED. R. CIV. P. 26(b)(2)(B). The amended rule reads:

*Specific Limitations on Electronically Stored Information.* A party need not provide discovery of electronically stored information from sources that the party identifies as not reasonably accessible because of undue burden or cost. On motion to compel discovery or for a protective order, the party from whom discovery is sought must show that the information is not reasonably accessible because of undue burden or cost. If that showing is made, the court may nonetheless order discovery from such sources if the requesting party shows good cause, considering the limitations of Rule 26(b)(2)(C). The court may specify conditions for the discovery.

*Id.*

156. *Id.*; Withers, *supra* note 90, at 199.

157. See FED. R. CIV. P. 26(b)(2)(B).

158. *Id.*; Withers, *supra* note 90, at 199.

159. Withers, *supra* note 90, at 199.

limit discovery.<sup>160</sup>

### 3. Duty of Preservation Under the 2006 Amendments

The 2006 amendments do not specifically address the duty of preservation, but changes to the rules have implications for this duty.<sup>161</sup> Under the new system, a party is not always required to produce information that is not reasonably accessible.<sup>162</sup> However, a party may be required to preserve inaccessible information if the party “believes that the information on such sources is likely to be discoverable and not available from any reasonably accessible sources.”<sup>163</sup> Furthermore, the amendment to Rule 37 limits the court’s ability to issue sanctions on a party who fails to produce ESI.<sup>164</sup> The amended rule prohibits sanctions on a party for failing to produce ESI if the information was lost in “the routine, good-faith operation of an electronic information system.”<sup>165</sup>

#### *C. Phase III: Courts Address Whether Social-Networking Information Is Different*

Courts have only recently begun to analyze social-networking information under the 2006 amendments—and the field is neither clear nor defined.<sup>166</sup> The decisions in the few cases that do address social

160. FED. R. CIV. P. 26(b)(2)(B). Furthermore, Rule 26(b)(2)(C) provides limits on the discoverability of ESI. FED. R. CIV. P. 26(b)(2)(C). Courts can limit discovery if:

- (i) the discovery sought is unreasonably cumulative or duplicative, or can be obtained from some other source that is more convenient, less burdensome, or less expensive;
- (ii) the party seeking discovery has had ample opportunity to obtain the information by discovery in the action; or
- (iii) the burden or expense of the proposed discovery outweighs its likely benefit, considering the needs of the case, the amount in controversy, the parties’ resources, the importance of the issues at stake in the action, and the importance of the discovery in resolving the issues.

*Id.* These limitations resemble the accessibility factors that emerged out of *Zubulake I*. See *supra* note 115. The notable exception is factor (5)—“[t]he relative ability of each party to control costs and its incentive to do so”—which is not included in the rule. See *Zubulake v. UBS Warburg, L.L.C.*, (*Zubulake I*), 217 F.R.D. 309, 322 (S.D.N.Y. 2003); FED. R. CIV. P. 26(b)(2)(C).

161. See SCHEINDLIN, *supra* note 66, at 6.

162. See 7 JAMES WM. MOORE ET AL., *supra* note 20, § 37A.10[1].

163. FED. R. CIV. P. 37 advisory committee’s note (2006 amendment); 7 JAMES WM. MOORE ET AL., *supra* note 20, § 37A.10[1].

164. FED. R. CIV. P. 37(e). The amended rule reads:

Failure to Provide Electronically Stored Information. Absent exceptional circumstances, a court may not impose sanctions under these rules on a party for failing to provide electronically stored information lost as a result of the routine, good-faith operation of an electronic information system.

*Id.*

165. *Id.*

166. *Dahl v. Bain Capital Partners*, 655 F. Supp. 2d 146, 148 (D. Mass. 2009) (“The proper handling of electronic discovery is a new and developing area of law practice. The Federal Rules first addressed electronic discovery in 2006 . . . the court appreciates that it treads in what still are largely unknown waters . . .”); Steven C. Bennett, *Look Who’s Talking: Legal Implications of Twitter Social-Networking Technology*, 81 N.Y. ST. B. J. 10, 12-13 (2009). *Columbia Pictures, Inc. v. Bunnell*, 245 F.R.D. 443 (C.D. Cal. 2007), however, may be the best indicator of the path courts will take in evaluating the discoverability of social-networking information. Bennett, *supra*, at 12-13 (arguing that most likely, the discoverability of social-networking information will hinge on how the informa-

networking illustrate two early tendencies by the courts.<sup>167</sup> First, courts have interpreted ESI broadly and have allowed discovery of social-networking information as ESI if parties narrowly tailor their discovery requests.<sup>168</sup> Second, courts have firmly rejected privacy arguments asserted by parties producing social-networking information.<sup>169</sup> The following section will address these two early tendencies.

### 1. Courts Have Applied the ESI Rules Broadly to Encompass Web 2.0

Generally, courts have defined ESI very broadly to encompass large amounts of electronic data. The first indication of broad application is that courts consider “ephemeral data” as ESI.<sup>170</sup> Ephemeral data is data that is not permanent or may exist for only a short period, such as random access memory (RAM).<sup>171</sup> Although the data may be fleeting, courts have given a broad interpretation to the amended Rule 34’s language that ESI is discoverable if “stored in any medium” from which information can be translated into a useable form.<sup>172</sup>

In *Columbia Pictures, Inc. v. Bunnell*,<sup>173</sup> the court decided as a matter of first impression that information in a computer’s RAM is discoverable as ESI.<sup>174</sup> In this case, the plaintiff movie studio alleged that the defendants operated a website that facilitated illegal downloading of the studio’s movies.<sup>175</sup> The studio sought discovery of the defendants’ server log data contained within the RAM, which contained information about the users of the website.<sup>176</sup> The defendants asserted that RAM is not ESI because RAM is not stored for later retrieval—it is merely fleeting and non-permanent information.<sup>177</sup>

However, the court held that RAM was ESI under Rule 34 because the rule did not have a requirement of “for later retrieval,” but only for stored data.<sup>178</sup> Furthermore, the court stated that the ephemeral nature

---

tion is used in a particular case).

167. See Shannon Awsumb, *Social Networking Sites: The Next E-Discovery Frontier*, 66 BENCH & B. OF MINN. 22, 25-26 (2009).

168. See *id.*

169. See *id.*

170. Thomas Y. Allman, *Conducting E-Discovery After the Amendments: The Second Wave*, 10 SEDONA CONF. J. 215, 216 (2009).

171. See *id.*

172. *Id.*

173. 245 F.R.D. 443 (C.D. Cal. 2007).

174. *Id.* at 448-49. Compare *Phillips v. Netblue, Inc.*, No. C-05-4401 SC, 2007 WL 174459, at \*2-3 (N.D. Cal. Jan. 22, 2007) (holding that hyperlinks within emails do not fall within the duty to preserve); *Healthcare Advocates, Inc. v. Harding, Earley, Follmer & Frailey*, 497 F. Supp. 2d 627, 641-42 (E.D. Pa. 2007) (holding that files that are only temporarily located on a user’s computer—cache files—do not fall within the duty to preserve); *Convolv, Inc. v. Compaq Computer Corp.*, 223 F.R.D. 162, 177 (S.D.N.Y. 2004) (holding that ephemeral data does not fall within the duty to preserve), with *Columbia Pictures*, 245 F.R.D. at 448-49.

175. *Columbia Pictures*, 245 F.R.D. at 445.

176. *Id.* at 447 n.3.

177. *Id.* at 446.

178. *Id.* at 447.

of RAM does not hinder its discoverability because the information is located within a tangible enough medium to allow reproduction.<sup>179</sup> The court relied on the Advisory Committee's assertion that the term "ESI" was intended to be interpreted as broadly as possible in order to encompass future advances in technology.<sup>180</sup>

The trend in broad interpretation of ESI has also led courts to the conclusion that information located on a third party's device may be discoverable.<sup>181</sup> Specifically, courts have maintained that ESI is not limited to information on a hard drive, but includes information within a party's control.<sup>182</sup> Accordingly, parties can discover ESI found in operating systems, dynamic databases, websites,<sup>183</sup> voicemail, or networked hard drives, and parties can even discover text messages or pictures in cell phones,<sup>184</sup> or PDAs.<sup>185</sup>

One early case illustrates how the rules apply to ESI located on a third party social-networking site's servers. In *Mackelprang v. Fidelity National Title Agency*,<sup>186</sup> a sexual harassment defendant subpoenaed MySpace "to produce all records for [the plaintiff's MySpace] accounts, including private email communication exchanged between Plaintiff and others."<sup>187</sup> MySpace produced public information but refused to produce the private emails.<sup>188</sup> Although the court denied the defendant's discovery request because it was too broad, the court maintained that the defendant could subpoena MySpace to produce private emails that contain information about the party's claim.<sup>189</sup>

## 2. Courts Reject Any Right of Privacy in Social-Networking Information

In recognizing the trend that social-networking information may be discoverable, parties have asserted a right to privacy—but that argument has largely failed. Much of the information located on a social-networking site is personal and, therefore, carries with it implications on

---

179. *Id.* at 448-49.

180. *Id.* at 447.

181. Allman, *supra* note 170, at 216.

182. 7 JAMES WM. MOORE ET AL., *supra* note 20, § 37A.10[1].

183. *Arteria Prop. PTY Ltd. v. Universal Funding V.T.O., Inc.*, No. 05-4896, 2008 WL 4513696, at \*5 (D.N.J. Oct. 1, 2008). When parties have control over the content posted on a website, a court will not treat a website differently than any other electronic files. *Id.* at \*5. This is still the case if an intermediary runs the website for a party. *Id.* If the party has the ultimate authority or control to add, delete, or modify the website's content, then courts should treat the information like any other ESI. *Id.*

184. *McClain v. Norfolk S. Ry. Co.*, No. 3:07CV2389, 2009 WL 701001, at \*2 (N.D. Ohio Mar. 16, 2009) (holding that photos on a cell phone are discoverable); *Flagg v. City of Detroit*, 252 F.R.D. 346, 354 (E.D. Mich. 2008) (holding that text messages are discoverable under Rule 34(a)(1)).

185. Allman, *supra* note 170, at 216.

186. No. 2:06-cv-00788, 2007 WL 119149 (D. Nev. Jan. 9, 2007).

187. *Id.* at \*2.

188. *Id.*

189. *Id.* at \*8.

privacy rights.<sup>190</sup> Accordingly, parties have attempted to secure protective orders under Rule 26(c) to protect their private social-networking information, but courts have not been receptive to their arguments.

Early cases indicate three reasons why courts have not acknowledged any privacy right in social-networking information in the area of discovery. First, the courts are unwilling to give any privacy protection to information deliberately placed in the public sphere.<sup>191</sup> One court specifically noted that social-networking information should not get protection because “privacy concerns are far less where the beneficiary herself chose to disclose the information.”<sup>192</sup>

Second, courts balance relevant evidence against privacy in favor of production.<sup>193</sup> This balancing in favor of production occurs even in admitted private areas of social-networking sites.<sup>194</sup> One court held that private information on a social-networking site should be produced because “the information sought within the four corners of the subpoenas issued to [social-networking sites] is reasonably calculated to lead to the discovery of admissible evidence as is relevant to the issues in this case.”<sup>195</sup>

Third, one court has held that a person has no reasonable expectation of privacy for information posted on a social-networking site.<sup>196</sup> The California Fifth District Court of Appeals stated that the affirmative act of putting information onto social-networking sites removes any expectation of privacy to that information because social-networking sites are very popular and the information could be viewable by anyone with a computer.<sup>197</sup>

These early cases are merely indications of how courts may proceed in the future. The following Part argues that courts should diverge from the path set forward by these cases and recognize the uniqueness

190. *Cf.* ARKFELD, *supra* note 91, § 7.10(D).

191. Awsumb, *supra* note 167, at 25.

192. *Id.* In *Beye v. Horizon Blue Cross Blue Shield*, No. 06-5377 (D.N.J. Dec. 12, 2007) and *Foley v. Horizon*, No. 06-6219 (D.N.J. Nov. 11, 2007), the plaintiffs sued the defendant insurance company for denying coverage for their eating disorders. Awsumb, *supra* note 167, at 25. The insurance company sought production of “emails, journals, diaries, and communications concerning the minor children’s eating disorders.” *Id.* The court ordered the plaintiffs to produce such discovery including Facebook and MySpace information. *Id.*

193. See *Ledbetter v. Wal-Mart Stores, Inc.*, No. 06-cv-01958, 2009 WL 1067018 (D. Colo. Apr. 21, 2009).

194. *Id.* at \*1; Awsumb, *supra* note 167 at 25 (stating “[defendants] subpoenaed information from the social networking sites regarding the private areas of the plaintiffs’ accounts”). In *Ledbetter*, plaintiffs sought damages from Wal-Mart arising out of an electrical fire. *Ledbetter*, 2009 WL 1067018, at \*1. Wal-Mart subpoenaed Facebook, Myspace, and Meetup.com for information in private areas of those social-networking sites that related to the plaintiffs’ damage claims. *Id.*

195. *Ledbetter*, 2009 WL 1067018, at \*2.

196. *Moreno v. Hanford Sentinel, Inc.*, 91 Cal. Rptr. 3d 858, 862-63 (Cal. Ct. App. 2009).

197. *Id.* at 862. *Moreno v. Hanford Sentinel, Inc.*, involved a girl who posted an entry onto her MySpace page, which contained negative remarks about her hometown. *Id.* at 861. The girl later removed the entry but not before the principal of the local high school submitted the entry to the local newspaper. *Id.* The newspaper published the entry, and the community reacted violently against the girl and her family. *Id.* The girl subsequently sued for invasion of privacy. *Id.*

of social-networking information.

#### IV. SOCIAL-NETWORKING INFORMATION SHOULD BE TREATED DIFFERENTLY THAN TRADITIONAL ESI

As the amount of social-networking information increases and plays a larger role in litigation, courts will face the challenge of determining how social-networking information fits within the current discovery scheme.<sup>198</sup> Courts have yet to reconcile the e-discovery rules with social networking.<sup>199</sup> Yet some courts and commentators argue that courts should directly treat social-networking information under the rules of traditional ESI.<sup>200</sup> The arguments for traditional ESI treatment point out that the Advisory Committee intended ESI to be a broad and expansive term to encompass future technologies.<sup>201</sup> Despite the Advisory Committee's desire to create a longstanding rule, courts should be hesitant to apply directly the e-discovery rules to social-network information. Instead, courts should recognize that social-networking information is distinct from traditional ESI, which would allow them to escape the bonds of the outdated e-discovery amendments and traditional ESI framework.

This Part will first show that technological advances will always push the limits of the rules.<sup>202</sup> Next, following the method of the *Zubulake* court and the Advisory Committee in the early 2000s, this Part will identify the distinctions between new technology and the technology that the old rules addressed and identify areas within the discovery rules in which the distinctions make a difference. There are four key distinctions between social-networking information and the ESI that the Advisory Committee contemplated.<sup>203</sup> Those distinctions warrant different treatment in three key areas: accessibility, the duty of preservation, and privacy-protection orders.<sup>204</sup>

---

198. See Bennett, *supra* 166, at 12-13.

199. Martha A. Mazzone, *The New E-Discovery Frontier—Seeking Facts in the Web 2.0 World (and Other Miscellany)*, 53 BOSTON B. J. 1, 8 (2009).

200. Katherine Minotti, Comment, *The Advent of Digital Diaries: Implications of Social Networking Websites for the Legal Profession*, 60 S.C. L. REV. 1057, 1062-63 (2009). Minotti gives three reasons why courts should treat social-networking information as traditional ESI:

(1) the Advisory committee intended the rule on ESI to be flexible, (2) social networking web site components are similar in structure and function to traditional forms of ESI, and (3) case law on traditional forms of evidence provides guidance for any differences between social networking web sites and other forms of ESI.

*Id.*

201. FED. R. CIV. P. 34 advisory committee's note (2006 amendment) ("Rule 34(a)(1) is intended to be . . . flexible enough to encompass future changes and developments.").

202. See *infra* Part IV.A.

203. See *infra* Part IV.A.

204. See *infra* Part IV.B-C.

A. *Broadly Applying the Scope of the Old Rules to New Technology Is Unworkable: Four Relevant Distinctions Exist Between Social-Networking Information and Traditional ESI*

Contrary to the Advisory Committee's wish, concrete rules are not suitable for advances in technology. The Advisory Committee promised time-tested, concrete rules once before—and failed.<sup>205</sup> In 1970, Congress first amended the Rules of Civil Procedure specifically to include electronic data.<sup>206</sup> Over two decades later, the rise of the Internet and electronic information boom in the 1990s forced courts to adapt and create new rules and frameworks for electronic data.<sup>207</sup> The change in information was so drastic that the Advisory Committee sought further to amend the rules to incorporate directly electronic data.<sup>208</sup>

The recentness of the 2006 amendments should not convince courts that the rules have kept pace with technology. Judges should not measure the age of the rules in years, but in terms of how far technology has progressed. The amount of information on the Internet has grown exponentially since the time of the amendments' drafting, and the landscape is entirely different.<sup>209</sup> The Advisory Committee acknowledged that the constant change in technology would pose a problem, so it created rules that it thought would withstand the test of time and apply to changes in technology.<sup>210</sup> Only a few years after the change, technology has already outpaced the 2006 amendments.

Courts should abandon the Advisory Committee's wish to apply the e-discovery rules to advances in technology. Instead, courts should recognize the four key distinctions between traditional ESI under the 2006 amendments and social-networking information. Each of these distinctions plays a role in illustrating why social-networking information should receive different treatment than traditional ESI.<sup>211</sup>

The first key distinction is that social-networking information is permanently stored on a third-party server and not on a party's own computer.<sup>212</sup> Social-networking information, such as the information on Facebook or Twitter, is not permanently stored on the user's hard drive. Rather, the only permanent storage for social-networking data resides

---

205. FED. R. CIV. P. 34(a) advisory committee's note (1970 amendment).

206. *Id.* ("The inclusive description of 'documents' is revised to accord with changing technology. It makes clear that Rule 34 applies to electronics data compilations.")

207. *See* *Zubulake v. UBS Warburg, L.L.C. (Zubulake I)*, 217 F.R.D. 309 (S.D.N.Y. 2003).

208. Withers, *supra* note 90, at 192; *see supra* notes 134-143.

209. *See supra* Part II.A-B.

210. FED. R. CIV. P. 34(a) advisory committee's note (2006 amendment); Withers, *supra* note 90, at 192-94.

211. *See infra* Part IV.B-C.

212. *Pupo-Leyvas v. Bezy*, No 2:08-cv-207, 2009 WL 1810337, at \*1 (S.D. Ind. June 24, 2009) (holding that a party does not have a right to control documents if the party merely has the "practical ability to obtain"); *see* Owens, *supra* note 5, at \*216-17.

on the servers in the data centers of the social-networking companies.<sup>213</sup> Accordingly, users are neither able to control how the information is stored nor control the costs of obtaining the information. This leaves users subject to the policies and methods of social-networking storage facilities. In terms of scope, the word “stored” in “electronically stored information” is either an outdated term or excessively broad considering how social-networking information is compiled and saved.

Second, the Advisory Committee designed the 2006 e-discovery amendments with corporate web 1.0 information in mind. The rules do not contemplate the hundreds of millions of individual social-networking users.<sup>214</sup> The Advisory Committee specifically addressed corporate practices, cutting costs for businesses in discovery, and how businesses can best utilize the rules.<sup>215</sup>

The third key distinction is that social-networking information carries with it strong privacy implications that traditional ESI does not. Web 1.0 communications have little privacy implications because they flow from a website creator to a website viewer and remain static.<sup>216</sup> Web 2.0 social-networking information implicates privacy because it involves the communication of personal information based on individual expression, relationship building, and a sense of community.<sup>217</sup> The extra layer of personal information attached to social-networking information ought to carry with it extra privacy protections under the discovery rules.<sup>218</sup>

Fourth, not all social-networking information is the same. Courts need to apply a more nuanced analysis because the internal controls that a user can implement change the character of each piece of information.<sup>219</sup> Privacy, and the ability to limit access to information, has become one of the largest issues in the social-networking community.<sup>220</sup> Social-networking sites have responded by implementing broad privacy policies.<sup>221</sup> For example, on Facebook, a user can limit not only who can

---

213. See Carlos Armas, *MySpace Replaces Storage with Solid-State Drive Technology in 150 Standard Load Servers*, INFOQ, Dec. 14, 2009, <http://www.infoq.com/news/2009/12/myspace-ssd>; Lee, *supra* note 68; Miller, *supra* note 64.

214. See Posting of Dean Gonsowski to E-Discovery 2.0, Top 5 Cases That Shaped Discovery in 2008, <http://www.clearwellsystems.com/e-discovery-blog/2008/12/12/top-5-cases-that-shaped-electronic-discovery-in-2008/> (Dec. 12, 2008, 14:40 PST) (asserting that the rules “[focus] somewhat myopically on email”).

215. See generally SCHEINDLIN, *supra* note 66 (noting throughout the deliberations that the Advisory Committee was concerned with addressing the e-discovery issues that businesses faced, not individuals as litigants); Withers, *supra* note 90.

216. See *supra* Part II.A.

217. See Grimmelmann, *supra* note 49, at 1151-60.

218. See *infra* Part IV.C.

219. See *supra* Part II.C.2.

220. See Rick Whiting, *Facebook's Zuckerberg: Face It, No One Wants Online Privacy Anymore*, CHANNELWEB, Jan. 11, 2010, <http://www.crn.com/security/222300279;jsessionid=QQ1WQCNEBBROMFQE1GHPSKHWATMY32JVN>.

221. See Facebook, *supra* note 58; Twitter, *supra* note 61; Myspace, MySpace Safety Tips & Settings, [http://www.myspace.com/index.cfm?fuseaction=cms.viewpage&placement=safety\\_pagetips](http://www.myspace.com/index.cfm?fuseaction=cms.viewpage&placement=safety_pagetips)

see his or her information—ranging from only the user to everyone—but also limit the type of information visible to other specific users.<sup>222</sup> A stranger can obtain some social-networking information very easily, while other information may be more difficult or even impossible to obtain.<sup>223</sup>

The items addressed above are meaningful distinctions. Courts should recognize these distinctions and move away from applying the discovery rules to social-networking information. Viewing the rules through the lens of these distinctions will help courts catch up with technology. There are many areas in which these distinctions should play a role. This Note addresses three of those areas. First, the accessibility and cost-shifting rules are not suitable for social-networking information because of the lack of control that the user has over the information. Second, the duty of preservation as applied to traditional ESI is not fit for application to social networking without deviation.<sup>224</sup> Third, the non-uniform nature of social-networking information and the privacy implications warrant consideration for privacy protection under Rule 26(c).<sup>225</sup>

#### *B. Courts Should Narrow the Scope of ESI to Exclude Social-Networking Information and Apply a Separate Analysis*

Because of the dynamic distinctions between ESI and social-networking information, courts should bypass the old ESI rules. A separation from the ESI amendments will free courts to apply separate and more applicable discovery rules to social-networking information. Reliance on the ESI rules will result in undue costs and burdens on producing parties in two areas: accessibility and the duty of preservation.

The accessibility of social-networking information represents a large departure from traditional ESI because social-networking users cannot control the storage or retrieval of their information.<sup>226</sup> Under the ESI amendments' two-tiered approach, a party must produce reasonably accessible information or produce inaccessible information upon a showing of good cause by the requesting party.<sup>227</sup> The limits placed on the production of ESI under Rule 26(b)(2)(C) resemble the cost-shifting factors from *Zubulake I*, yet leave out any consideration of a party's ability to control costs.<sup>228</sup>

---

(last visited Apr. 23, 2010).

222. Facebook, *supra* note 58.

223. *See supra* Part II.C.2.

224. *See infra* Part IV.B.

225. *See infra* Part IV.C.

226. *See supra* notes 212-213.

227. FED. R. CIV. P. 26(b)(2)(B).

228. *See supra* note 115 and accompanying text. Factor five of the *Zubulake I* cost-shifting factors is “[t]he relative ability of each party to control costs and its incentive to do so.” *Zubulake v.*

This rule may impose an undue burden on parties who produce social-networking information because the parties have no control over how their information is stored or retrieved.<sup>229</sup> Parties cannot devise cheaper methods of retrieval or plan for discovery expenses but remain subjects of social-network storage facilities. The costs of discovering social-networking information lay solely at the hands of the social-networking companies, causing the cost of discovery to be unpredictable and uncontrollable. Under the ESI rules, this factor has no weight.<sup>230</sup> The language in Rule 26(b)(2)(B)-(C) may be appropriate for traditional ESI because parties have direct control over the information stored on their servers but inappropriate for social-networking information because producing parties lack that control.

Courts should be more willing to return to the *Zubulake I* cost-shifting analysis for determining accessibility and assigning costs for social-networking information.<sup>231</sup> If discovery of social-networking information is ordered, especially when inaccessible, courts should apply the *Zubulake I* cost-shifting factors, including factor five, which allows courts to consider the ability of a party to control discovery costs. Under this framework, courts will be able to protect producing parties from undue and unpredictable production expenses that lay outside of the producing party's control and shift some of those costs to the requesting party.

A similar problem emerges regarding the duty of preservation of social-networking information. There is no firmly established precedent regarding the duty to preserve social-networking information.<sup>232</sup> However, the risk of courts adopting the traditional ESI framework for the preservation duty threatens to place a large burden on producing parties.<sup>233</sup>

The duty to preserve electronic data arises when a party reasonably anticipates litigation.<sup>234</sup> That duty applies not only to businesses with large amounts of electronic data, but also to individuals who have small amounts of personal electronic data. Courts offer no distinction between sophisticated parties and unsophisticated parties. In a web 2.0

---

UBS Warburg, L.L.C. (*Zubulake I*), 217 F.R.D. 309, 322 (S.D.N.Y. 2003).

229. See *supra* note 213 and accompanying text.

230. FED. R. CIV. P. 26(b)(2)(B)-(C).

231. See *Zubulake I*, 217 F.R.D. at 322. Courts have applied the cost shifting under the *Zubulake I* factors even after the 2006 amendments. See, e.g., *Major Tours, Inc. v. Colorel*, No. 05-3091, 2009 WL 3446761, at \*5 (D.N.J. Oct. 20, 2009); *Sue v. Milyard*, No. 07-cv-01711, 2009 WL 1504747, at \*1 (D. Colo. May 26, 2009); *Ex parte Cooper Tire & Rubber Co.*, 987 So. 2d 1090, 1106 (Ala. 2007); see also Withers, *supra* note 90, at 200 (“[T]he cost shifting analysis from *Zubulake I* may come back into the picture if discovery is ordered.”).

232. See Withers, *supra* note 121, at 352.

233. See Minotti, *supra* note 200, at 1062-63 (“Although the Federal Rules Advisory Committee may not have had social networking web sites in mind when drafting the rules on ESI, courts should apply the Federal Rules to social networking web sites just as other types of ESI.”).

234. *Zubulake v. UBS Warburg, L.L.C. (Zubulake IV)*, 220 F.R.D. 212, 216 (S.D.N.Y. 2003).

world, the duty shifts from a party's duty not to delete information on its own hard drive, to a positive duty to take steps to preserve information located on a third party's server.<sup>235</sup> Social-networking sites like Twitter and Facebook require court orders for information to be preserved.<sup>236</sup>

In the coming years, as the amount of social-networking information expands and results in discovery issues, unsophisticated parties will unknowingly fall victim to this duty. The duty to preserve social-networking information should apply only to parties who are experienced in litigation and in fact able to anticipate litigation. The court should analyze the experience and sophistication of the producing party before pronouncing a violation of the broad duty to preserve.

### *C. Courts Should Consider a Social-Network User's Privacy Rights Under Rule 26(c)*

The distinctions between traditional ESI and social-networking information also emerge in the realm of privacy. In the limited case law that has developed thus far, courts have refused to acknowledge any expectation of privacy for social-networking information when issuing protective orders under Rule 26(c).<sup>237</sup> Courts cite the Advisory Committee's desire to cast a broad net with the term "ESI" and the nature of privacy on social-networking sites.<sup>238</sup>

However, future courts should consider two distinctions. First, social-networking information carries a perceived sense of privacy. Second, different types of social-networking information may have different levels of privacy implications. By recognizing these distinctions, courts should apply a nuanced approach in analyzing social-network privacy under Rule 26(c). Courts should consider determining whether a social-network user has an expectation of privacy by looking at the type of information and whether it is reasonable to expect that information to remain private.

Social-networking information is very different than traditional ESI because it is set in the backdrop of an entirely different social dynamic. The difference lies at the core of the division between web 1.0 and web 2.0.<sup>239</sup> Traditional ESI, or web 1.0 information, involves communication

---

235. Twitter, *supra* note 61 ("Data preservation requests must be accompanied by a subpoena or court order."); Posting of Sam Glover to Lawyerist.com, Subpoena Facebook Information, <http://lawyerist.com/subpoena-facebook-information/> (July 10, 2009) (stating that in civil matters, Facebook will only preserve user information through a subpoena or court order from the state of California); Posting of Sam Glover to Lawyerist.com, Subpoena MySpace Information, <http://lawyerist.com/subpoena-myspace-information/> (July 17, 2009) (indicating that MySpace requires personal service on its registered agent and will only accept out-of-state subpoenas "if [litigants] have been properly domesticated through a California court").

236. See *supra* Part II.C.4.

237. See *supra* Part III.B-C and accompanying text.

238. See *supra* Part III.C.1-2.

239. See *supra* Part II.

from one person to another—a one-way street.<sup>240</sup> On the other hand, web 2.0, or social-networking information, involves communication that results from many people participating in a community or a group of friends.<sup>241</sup>

Social networks, by their very nature, are social instruments. Social networks have become incredibly popular because people are inherently social beings.<sup>242</sup> The information shared goes far beyond the unilateral communication information of web 1.0 such as electronic spreadsheets and corporate email. Participation in social networking encourages the revelation of intimate details about the participant's life.<sup>243</sup> Despite the warnings and potential privacy dangers, users reveal intimate personal information through social networks to fulfill their innate human social needs.<sup>244</sup> Whether online or offline, the sharing of intimate knowledge is the building block for establishing personal and community relationships.<sup>245</sup>

The sharing of intimate knowledge lets a user accomplish three social goals: express users' identity, build relationships, and demonstrate community value. First, users are able to express their identity by revealing details about themselves.<sup>246</sup> What users choose to reveal on their Facebook profile pages or what they choose to tweet about is as much an expression of their identity as their choice in hairstyle.<sup>247</sup> Second, the sharing of personal information creates and nurtures relationships.<sup>248</sup> A user's decision to "friend" or "follow" another user signals that the user trusts the other user enough to share personal information.<sup>249</sup> Third, sharing personal information allows a user to establish a

240. See *supra* note 15 and accompanying text.

241. See Getting, *supra* note 10.

242. See A. H. Maslow, *A Theory of Human Motivation*, 50 PSYCHOL. REV. 370, 381 (1943), available at <http://psychclassics.yorku.ca/Maslow/motivation.htm>. In his famous 1943 work, Maslow ranked basic human needs from highest to lowest. See *id.* Maslow ranks the social need to feel love and affection just below physiological and safety needs. *Id.*

243. Grimmelmann, *supra* note 49, at 1151.

244. *Id.*

245. See Lior Jacob Strahilevitz, *A Social Networks Theory of Privacy*, 72 U. CHI. L. REV. 919, 923 (2005) ("Sharing our most intimate information with those who we expect to keep it secret promotes further friendship and intimacy.").

246. See generally Grimmelmann, *supra* note 49, at 1151-60 (discussing the social motivations of Facebook users to reveal intimate information to their Facebook friends).

247. *Id.* at 1152 ("Each additional datum is a strategic revelation, one more daub of paint in your self-portrait."). According to Grimmelmann, a user's decision to share information such as a profile picture, favorite music and movies, to what groups the user belongs, and who is on their friends list are all expressions of individual identity. See *id.* at 1152-53. For example, if a user shares that he or she belongs to the "Darfur Action Group," the user's motivation is not solely to save Darfur, but also to indicate to other users that he or she is the kind of person who wants to save Darfur. *Id.* at 1153. See also danah boyd & Jeffery Heer, *Profiles as Conversation: Networked Identity Performance on Friendster*, in PROCEEDINGS OF THE HAWAII INTERNATIONAL CONFERENCE ON SYSTEM SCIENCE § 3 (2006), available at <http://www.danah.org/papers/HICSS2006.pdf> (stating that sharing information on a social-network profile is a dialogue and encourages other users to communicate back by sharing their own information).

248. Grimmelmann, *supra* note 49, at 1154.

249. danah boyd, *Friends, Friendsters, and MySpace Top 8: Writing Community into Being on*

social status within the community.<sup>250</sup> By establishing connections with a variety of people, users can draw on those connections to find information, form friendships, or organize groups.<sup>251</sup> All of the information expressed on social-networking sites is social expression.<sup>252</sup>

Social-network information builds its foundation upon intimate details. The social goals that Facebook and Twitter members pursue are the same goals that everyone seeks to achieve every day—the Internet just makes it easier.<sup>253</sup> However, relationships built on intimate information sharing cannot exist without some degree of privacy.<sup>254</sup> A blanket judicial interpretation that users have no expectation of privacy in social-networking information threatens the social benefits of the websites.

The federal rules recognize the value in protecting intimate information under Rule 26(c).<sup>255</sup> For intimate information shared offline, courts can protect privacy by granting a protection order.<sup>256</sup> Courts apply a balancing test and weigh the hardship of the party seeking to keep the information private against the information’s probative value.<sup>257</sup> Under the case law that has developed so far, courts will not afford social-networking information the same protection despite it being intimate and personal information.<sup>258</sup>

Courts should also recognize that not all social-network information is the same.<sup>259</sup> Users are able to utilize internal controls to limit

*Social Network Sites*, 11 FIRST MONDAY (NUMBER 12), Dec. 4, 2006, <http://firstmonday.org/htbin/cgi-wrap/bin/ojs/index.php/fm/article/view/1418/1336> (analyzing the concept of “friending” on the social-networking sites of MySpace and Friendster).

250. See generally Grimmelmann, *supra* note 49, at 1157-59 (“[Y]ou can signal your coolness by having cool friends.”).

251. Nichole B. Ellison et al., *The Benefits of Facebook “Friends”: Social Capital and College Students’ Use of Social Online Network Sites*, 12 J. COMPUTER-MEDIATED COMM. (ISSUE 4) (2007), available at <http://jcmc.indiana.edu/vol12/issue4/ellison.html>. A person’s capacity to access a network of relationships for resources is referred to as social capital. *Id.* Individuals possessing social capital contribute to the overall well-being of society. *Id.* For example, studies indicate that social capital is associated with “better public health, lower crime rates, and more efficient financial markets.” *Id.* An absence of social capital reduces civic participation and creates mistrust within the community. *Id.*

252. A user’s decision to share intimate details by posting pictures of their latest party or tweeting about Lil Wayne all indicate the user’s desire to connect socially. The information is meant to communicate: (1) you should define me as a person by the information I choose to reveal to you; (2) I am revealing this information to you because you matter to me; and (3) your knowledge of this information should make you think I am a valued member of the community and, consequently, we should help each other.

253. Grimmelmann, *supra* note 49, at 1159 (“Identity, relationship, and community are not unique to social network sites. They’re basic elements of social interaction, offline and on. . . . [Social interaction has] always been central to the human experience, and it always will be.”)

254. Strahilevitz, *supra* note 245, at 924.

255. ARKFELD, *supra* note 91, § 7.4(I)(8)(2) (“Protective orders are often sought in electronic discovery cases on the basis that retrieval of computer data is unreasonably burdensome or costly and to protect privacy . . .”).

256. FED R. CIV. P. 26(c)(1).

257. 6 JAMES WM. MOORE ET AL., *supra* note 131, § 26.101[1][c].

258. See *supra* Part III.C.2.

259. See *supra* Part IV.B.

who is able to view their information.<sup>260</sup> Conceptually, users are able to gate off information to specific users and gate off specific types of information to specific users.<sup>261</sup> To acknowledge fully this distinction, courts should refuse to state without further analysis that social-networking information carries no reasonable expectation of privacy. Instead, courts should apply an objective test to determine whether a social-networking user should have expected the information to remain private.

Courts should take cues from social-network theory and Fourth Amendment cases by looking at the flow of communication and the structure of the social network.<sup>262</sup> The relevant factors that courts should consider are where the information exists, what types of people have access to the information, and whether any social dynamics exist that constrain or facilitate dissemination.<sup>263</sup> Specifically, courts should look at the nuts and bolts of the social-networking website: where the information was located, who is the receiver of the information, how the information was stored, and whether any internal policy or norm created an expectation that other users would not disseminate the information. Only by looking at the internal workings of the sites can courts truly gauge privacy.

## V. CONCLUSION

Courts must remain vigilant in keeping litigation rules on pace with advances in technology. In doing so, courts must recognize and understand the technology involved. The transition from web 1.0 to web 2.0 illustrates a change in the character of the Internet. The 2006 e-discovery amendments do not embrace this change of character because the Advisory Committee crafted the rules to address web 1.0 issues. Social-networking information presents the largest challenges to courts because of the distinct nature of the information. The four key distinctions between social-networking information and traditional ESI demand separate treatment of social-networking information in the areas of the accessibility, preservation duty, and protection orders based on privacy. Without acknowledging that social-networking technology has outpaced the discovery rules, courts are doomed to produce the same inconsistencies they produced in the early e-discovery cases as well as fail to give parties adequate protection of their privacy rights.

---

260. See *supra* Part IV.B.

261. Facebook, *supra* note 58; Twitter, *supra* note 61.

262. See *Quon v. Arch Wireless Operating Co.*, 529 F.3d 892, 906 (9th Cir. 2008); Strahilevitz, *supra* note 245, at 970-71.

263. See Strahilevitz, *supra* note 245, at 970-71.