JOHN S. WILSON*

MySpace, Your Space, or Our Space? New Frontiers in Electronic Evidence

What began as a back-room experiment between government and university computer programmers has revolutionized the world as we know it.[1] The Internet now

* J.D. Candidate, University of Oregon School of Law, 2008. Operations Editor, *Oregon Law Review*, 2007–08. Law Clerk, U.S. Attorneys Office, 2006–08. First and foremost, I would like to thank Missi Wilson for being a loving and supportive wife as I have pursued my dream of going to law school. I am thankful to have a partner who "lives the adventure" with me. We are also blessed with two wonderful children, Andrew and Samantha, who are constant sources of joy and inspiration. I am indebted to Jeff Evans, an excellent lawyer and an even better friend, for his friendship and helpful comments on this paper. I am also grateful to Assistant U.S. Attorneys William "Bud" Fitzgerald, Sean Hoar, Chris Cardani, Frank Papagni, Kirk Engdall, and John Ray for mentoring me and giving me the best job a law student could ask for. Our country is lucky to have such excellent lawyers working for it. I am tremendously appreciative of the members of *Oregon Law Review* who helped "sand down" the numerous rough edges of this Article, particularly Executive Editor Megan Thompson, Systems/Managing Editor Harvey Rogers (and his crack team of Staff Editors), and Editor-in-Chief Kirk Neste. Finally, I would be remiss if I did not acknowledge the encouragement I have received during law school from my extended family: the Hilliers, Palmblads, Wilsons, and Gotters.

[1] *See generally* J.R. OKIN, THE INTERNET REVOLUTION: THE NOT-FOR-DUMMIES GUIDE TO THE HISTORY, TECHNOLOGY, AND USE OF THE INTERNET 54–111 (2005) (describing the genesis of the World Wide Web from the Defense Advance Research Project Agency's "ARPANET"); CHRISTOS J.P. MOSCHOVITIS ET AL., HISTORY OF THE INTERNET: A CHRONOLOGY, 1843 TO THE PRESENT 98–137 (1999) (discussing the technological evolution from ARPANET to computer networks such as Usenet, BITnet, FidoNet, and the growth of online communities such as Cleveland Free-Net); STEPHEN SEGALLER, NERDS 2.0.1: A BRIEF HISTORY OF THE INTERNET 99–157 (1999) (describing the same in greater detail and with more emphasis on the many eccentric personalities that were involved in the formation of the Internet).

affects nearly every facet of our daily lives. It connects individuals, facilitates economic transactions, fosters the exchange of information, and serves as a vibrant commercial marketplace.[2] This technological revolution also has left its mark on the practice of law. In civil cases, corporate America's increased reliance on electronic communications has had a profound impact on discovery, with discovery requests of several million pages becoming commonplace.[3] In criminal cases, law-enforcement agencies and attorneys are turning in increasing numbers to social-networking web sites such as MySpace and Facebook to gather evidence. Yet the legal profession's response to electronic evidence in both the civil and criminal contexts can be described as advancing in fits and starts. The recent promulgation of new Federal Rules of Civil Procedure responded to the influx of burdensome electronic discovery requests by placing some limits on what types of electronic evidence are discoverable.[4]

---

[2] *See generally* MICHAEL D. SCOTT, SCOTT ON COMPUTER LAW §§ 1.01–.02 (2d ed. 2002) (claiming that the advent of the computer is one of the most important discoveries in history and that "there has never been an invention with a more profound effect on every aspect of society than the computer"); CENTRAL INTELLIGENCE AGENCY, THE WORLD FACTBOOK: FIELD LISTING—INTERNET USERS (2008), https://www.cia.gov/library/publications/the-world-factbook/fields/2153.html (noting that as of 2006 the United States had over 208 million regular Internet users).

> Our Nation's critical infrastructures are composed of public and private institutions in the sectors of agriculture, food, water, public health, emergency services, government, defense industrial base, information and telecommunications, energy, transportation, banking and finance, chemicals and hazardous materials, and postal and shipping. Cyberspace is their nervous system—the control system of our country. Cyberspace is composed of hundreds of thousands of interconnected computers, servers, routers, switches, and fiber optic cables that allow our critical infrastructures to work.

The White House, *The National Strategy to Secure Cyberspace*, at vii (2003), *available at* http://www.whitehouse.gov/pcipb/cyberspace_strategy.pdf.

[3] *See, e.g.*, Rowe Entm't, Inc. v. William Morris Agency, 205 F.R.D. 421, 425 (S.D.N.Y. 2002) (noting that the estimated cost to retrieve all email on corporate backup tapes would have been $9.75 million); *In Re* Brand Name Prescription Drugs Antitrust Litig., 1995 WL 360526, at *1 (N.D. Ill. 1995) (noting defendant's contention that responding to plaintiff's document demands would require a review of 30 million pages of email data).

[4] For further discussion of how the recent revisions to the Federal Rules of Civil Procedure affected electronic discovery, see *infra* Part I.B.

The trend toward the importance of digital information in the practice of law raises important and timely questions: How effectively do the revised Federal Rules of Civil Procedure address the myriad challenges that electronic discovery presents? To what extent is information posted on a personal web page protected by the Fourth Amendment right to freedom from unreasonable searches? What legal issues arise with respect to evidence gathered not through crime-scene investigations, but through electronic surveillance in the online world?

This Comment argues that traditional legal rules are generally ineffective in addressing the new challenges that electronic evidence poses and that such challenges require new solutions. Many of the lessons learned from the increased use of electronic evidence in civil litigation—"e-discovery," in the parlance of litigators—may be applied to the burgeoning use of social-networking sites to gather evidence in criminal cases. This Comment also suggests some shortfalls in the newly revised Federal Rules of Civil Procedure governing e-discovery and offers suggestions for closing existing loopholes.

The discussion unfolds in three parts. Part I analyzes the increased reliance on e-discovery in civil litigation by describing its historical evolution and important common law developments. It also focuses on recent revisions to the Federal Rules of Civil Procedure that will force judges, attorneys, and clients to take notice of digital evidence in litigation. Part II turns to the rise of social-networking web sites such as MySpace and Facebook and discusses how such online communities are changing the way prosecutors, defense attorneys, and law-enforcement officers investigate crimes and prepare for trial. It traces the development of online communities and gives examples of the potential use, or misuse, of social-networking sites for gathering evidence. Part III presents the heart of the argument—namely, that while some of the legal concepts developed through the evolution of e-discovery can and should be applied to the use of social-networking sites to gather evidence, meeting the challenges of emerging technologies requires new approaches.[5] It is only by combining the lessons

[5] *See* Zubulake v. UBS Warburg LLC, 217 F.R.D. 309, 311 (S.D.N.Y. 2003) (quoting Henry David Thoreau's maxim that "[t]he process of discovery is very

learned from past successes and failures with new legal strategies that the law governing evidence gathered online will gain uniformity.

At the outset, some definitions are in order. Electronic information, by its nature, is somewhat amorphous. Parties other than original authors often can manipulate files, and many computer systems have processes by which files are automatically revised based on changing variables within the system. Beyond this, the sheer scope of modern information systems defies easy definition. For the purposes of this Comment, it is enough to note that the terms "electronic evidence" and "digital evidence" will be used interchangeably and generally will refer to information stored or transmitted in digital form that a party to a legal action may use to further his or her case.[6] This Comment defines social-networking sites as interactive web sites that connect users based on common interests and that allow subscribers to personalize individual web sites.[7] Examples include MySpace,[8] Facebook,[9] Xanga,[10] and LinkedIn.[11]

simple," but concluding that this statement has "given way to rapid technological advances, requiring new solutions to old problems").

[6] A more comprehensive definition of electronic media that comprises "electronic evidence" includes: (1) data files on office desktop computers and workstations, notebook computers, home computers, computers of personal assistants and staff, palmtop and handheld devices, and network file servers and mainframes; (2) backup tapes including system-wide backups (monthly, weekly, or incremental), disaster-recovery backups that are stored off-site, and personal backups that can be on diskettes or other portable media; and (3) other media sources such as tape archives, replaced or removed drives, and portable media (e.g., floppy diskettes, CDs, and Zip disks). Joan E. Feldman & Rodger I. Kohn, *The Essentials of Computer Discovery*, 564 PLI/PAT 51, 57 (1999); *see also* Hon. Shira A. Scheindlin & Jeffrey Rabkin, *Electronic Discovery in Federal Civil Litigation: Is Rule 34 up to the Task?*, 41 B.C. L. REV. 327, 333 (2000) (describing electronic evidence as "any electronically-stored information subject to pretrial discovery," which includes all information stored digitally, optically, or in analog form); MANUAL FOR COMPLEX LITIGATION (THIRD) § 21.446 (1995) (noting that computerized data includes "operating systems (programs that control a computer's basic functions), applications (programs used directly by the operator, such as word processing or spreadsheet programs), computer generated models, and other sets of instructions residing in computer memory"); Int'l Journal of Digital Evidence, http://www.ijde.org (last visited Apr. 1, 2008); Int'l Organization on Computer Evidence, http://www.ioce.org (last visited Apr. 1, 2008).

[7] *See generally* Brad Stone, *Social Networking's Next Phase*, N.Y. TIMES, Mar. 3, 2007, at C1 (describing the increased use of social-networking web sites by private enterprises like the Portland Trailblazers and organizations such as Barack Obama's presidential campaign).

At first blush, electronic evidence subject to discovery in civil litigation cases and electronic evidence in the context of criminal investigations may seem to defy conflation. A more nuanced analysis, however, reveals that both are cut from the same cloth: these forms of evidence are the unavoidable byproducts of the information age in which we live. Gone are the days when legal practitioners could ignore digital information or even hire computer experts to translate "electronic gibberish" for them. The tidal wave of technological change has reached the legal shore, bringing with it new challenges and opportunities. By applying the lessons learned from the evolution of e-discovery to the expanding use of social-networking sites for gathering evidence, the legal community can develop new approaches to such technological advances.

I
E-DISCOVERY: CHANGING THE PRACTICE OF CIVIL LITIGATION

Throughout the past half-century, technological developments such as the personal computer,[12] online legal-research services,[13]

[8] MySpace, http://www.myspace.com (last visited Apr. 1, 2008). See text accompanying notes 103–13 *infra* for an in-depth discussion of MySpace.

[9] Facebook, http://www.facebook.com (last visited Apr. 1, 2008). See text accompanying notes 95–102 *infra* for discussion of Facebook.

[10] Xanga, http://www.xanga.com (last visited Apr. 1, 2008). Xanga is an online community that differs slightly from MySpace and Facebook in that it allows users to post content in various "blog" forms. For example, Xanga hosts weblogs, photoblogs, videoblogs, and audioblogs for its users.

[11] LinkedIn, http://www.linkedin.com (last visited Apr. 1, 2008). LinkedIn is a hybrid social-networking web site that aims to connect working professionals throughout the world. Rather than allowing users to post photos, blogs, and their favorite music, as MySpace and Facebook do, LinkedIn users "create a profile that summarizes [their] professional accomplishments." LinkedIn: About LinkedIn, www.linkedin.com/static?key=company_info (last visited Apr. 1, 2008); *see also* Bob Tedeschi, *Listing Top Jobs but Charging Candidates to Seek Them*, N.Y. TIMES, June 4, 2007, at C5 (describing how LinkedIn has "emerged as a favorite trolling ground for corporate recruiters across the spectrum of job levels").

[12] *See generally* David C. Tunick, *Has the Computer Changed the Law?*, 13 J. MARSHALL J. COMPUTER & INFO. L. 43 (1994) (describing the various effects of the computer on the practice of law).

[13] *See generally* Richard M. Georges, *Impact of Technology on the Practice of Law—2010*, 71 FLA. B.J. 36 (1997) (attempting to predict how technology will affect a lawyer practicing in 2010, with discussion of such technological innovations as the

and most recently, electronic court filing systems[14] have changed the way attorneys practice law. In the same way, corporate America's increased reliance on electronic information has revolutionized how civil litigators practice law. While discovery has always been meant to make trials "less a game of blind man's [bluff] and more a fair contest with the basic issues and facts disclosed to the fullest practicable extent,"[15] the immense volume of electronically stored information has forced litigators to engage discovery in new and different ways. Given the storage capacity of average computers today, even the most modest mom-and-pop businesses may have electronic storage space equivalent to 2,000 four-drawer file cabinets.[16] Throughout the nation, email is becoming the principal means of communication in the workplace.[17] This pervasive reliance on electronic media led one pundit to claim that "[c]orporate

Internet, e-mail, "Internet Real Time Communications," legal research, and "Dispute Settlement in Cyberspace").

[14] *See* ABA Legal Technology Resource Center Electronic Filing Resource Page, http://www.abanet.org/tech/ltrc/research/efiling/ (last visited Apr. 1, 2008) (noting that "[b]y reducing courier and copying fees, use of paper, and staff time, E-Filing can be a tremendous cost savings" for practicing attorneys). A recent *New York Times Magazine* article posits that neuroscience evidence, or "neurolaw"—yet another technological advance in the legal forum—represents a significant divergence from the status quo by arguing that defendants should not be held responsible for criminal acts that may be the result of a neurological flaw. *See* Jeffrey Rosen, *The Brain on the Stand*, N.Y. TIMES MAG., Mar. 11, 2007, at 49.

[15] United States v. Proctor & Gamble Co., 356 U.S. 677, 682 (1958) (citing Hickman v. Taylor, 329 U.S. 495, 501 (1947)).

[16] GEORGE L. PAUL & BRUCE H. NEARON, THE DISCOVERY REVOLUTION 5 (2006); *see also* MANUAL FOR COMPLEX LITIGATION (FOURTH) § 11.446 (2004) (stating that one CD can contain the equivalent of 325,000 typewritten pages; one gigabyte of storage can hold 20 million pages; and one terabyte—the storage unit used to measure corporate backups—can hold 500 billion typewritten pages); Linda G. Sharp, *Restoration Drama: The Complexity of Electronic Discovery Requires Practitioners to Master New Litigation Skills*, L.A. LAW., Oct. 2005, at 31, 31, *available at* http://www.lacba.org/showpage.cfm?pageid=5787 (noting that a single personal hard drive can contain up to 1.5 million pages of data, and one corporate backup tape can contain 4 million pages of data); Patricia Nieuwenhuizen, *E-Mail: The Smoking Gun of the Future*, NAT'L L.J., Dec. 11, 2000, at B9 (noting that office workers exchange 5 billion email messages each day); Geanne Rosenberg, *Electronic Discovery Proves an Effective Legal Weapon*, N.Y. TIMES, Mar. 31, 1997, at D5 (noting the assertion that, even in 1997, it was possible to store more documents on a ten-square-inch hard drive than could have been kept as hard copies in an entire story of a building).

[17] Hon. Jacob P. Hart & Anna Marie Plum, *Litigating the Production of Electronic Media*, PRAC. LITIGATOR, July 2001, at 31, 33. This article provides a complete, well-reasoned discussion of the issues surrounding e-discovery.

America has lost control of its electronic data."[18] When the average employee sends twenty and receives thirty emails per day,[19] and over eighty percent of all corporate data is created and stored electronically without ever being converted to paper,[20] the volume of electronic information created within any given organization can be overwhelming.[21]

These technological advances have significant ramifications for civil litigators. In general, digital-era discovery has increased the cost and time of civil litigation.[22] Voluminous electronic information retrievals and productions are often very expensive,[23] and the producing party usually bears the costs.[24] Perhaps even more discouraging to corporate litigants is the reality that they may be paying to produce "smoking guns"—damaging electronic information that should have been

---

18 Ashby Jones, *What a Mess! For Corporations, Pileup of Electronic Data Could Be Trouble Waiting to Happen*, NAT'L L.J., Dec. 2, 2002, at C6.

19 Peter Lyman & Hal R. Varian, *How Much Information? 2003*, http://www2.sims.berkeley.edu/research/projects/how-much-info-2003/ (last visited Apr. 1, 2008) (study of electronic information by faculty and students at the University of California at Berkley School of Information Management and Systems).

20 Jones, *supra* note 18; *see also* Michele C.S. Lange, *Sarbanes-Oxley Has Major Impact on Electronic Evidence*, NAT'L L.J., Jan. 2, 2003, *available at* http://www.law.com/jsp/article.jsp?id=1039054510969 (noting that "93 percent of all business documents [are] created electronically and only 30 percent [are] ever printed to paper").

21 Paul H. Luehr, *Real Evidence, Virtual Crimes: The Role of Computer Forensic Experts*, CRIM. JUST., Fall 2005, at 14, 14 (noting that "[i]n sheer volume, digital evidence often overwhelms the testimonial, physical, or documentary evidence in the possession of the trial lawyer").

22 Mark Ballard, *Digital Headache: E-Discovery Costs Soar into the Millions, and Litigants Seek Guidance*, NAT'L L.J., Feb. 10, 2003, at A18.

23 *See, e.g.*, Murphy Oil USA, Inc. v. Fluor Daniel, Inc., 2002 WL 246439, at *3 (E.D. La. 2002) (noting that the cost of digital discovery in the case topped $6.2 million).

24 *See, e.g.*, Daewoo Elecs. Co. v. United States, 650 F. Supp. 1003, 1006 (Ct. Int'l Trade 1986).

> It would be a dangerous development in the law if new techniques for easing the use of information became a hindrance to discovery or disclosure in litigation. . . .
>
> . . . .
>
> . . . The normal and reasonable translation of electronic data into a form usable by the discovering party should be the ordinary and foreseeable burden of a respondent in the absence of a showing of extraordinary hardship.

Id.

destroyed or should not have been created in the first place.[25] Corporate litigants have even been fined for failing to produce emails in the course of a Securities and Exchange Commission investigation[26] and where their experts had difficulty locating sought-after emails from backup tapes.[27]

Electronic information also has played a central role in several well-known cases beyond the battlefields of corporate litigation. In the Iran-Contra scandal, investigators found deleted incriminating communications between President Reagan's former national security advisors.[28] Similarly, during Kenneth Starr's investigation of President Clinton, the special prosecutor's legal team uncovered a "talking points" memo in a computer file that Monica Lewinsky thought she had deleted from her computer.[29]

Beyond the challenges of increased costs and time, parties to civil litigation also must confront the inherent uncertainty in e-discovery. Just what forms of electronic media are discoverable? How deep must the producing party dig to find discoverable materials? When does the burden of electronic discovery shift to the defendant? In a series of decisions over the past decade or

25 *See* Jones, *supra* note 18. Jones described how a series of emails played a central role in a "very good" settlement of a shareholder stock-fraud suit brought against Boeing. *Id.* While these documents should have been destroyed under the company's document-retention plan, they instead were included on 14,000 backup tapes stored in a company warehouse where they were subject to discovery. *Id.*

Interoffice electronic communications also created a "smoking gun" in a $150 million securities-fraud case brought by the Siemens Corporation against ARCO. Patrick R. Grady, *Discovery of Computer Stored Documents and Computer Based Litigation Support Systems: Why Give Up More Than Necessary?*, 14 J. MARSHALL J. COMPUTER & INFO. L. 523, 524 (1996). Emails found in the computer system of an ARCO subsidiary acquired by Siemens suggested that ARCO employees had expressed concern about the flaws in one of the subsidiary's products. *Id.* Among the more-damaging emails was one that read: "[T]he whole basis of our plan is almost invalid due to the fact that we have been operating under the wrong assumptions for ten years." *See id.*

26 Jones, *supra* note 18.

27 *See* Residential Funding Corp. v. DeGeorge Fin. Corp., 306 F.3d 99, 102–04, 113 (2d Cir. 2002) (ordering the trial court to impose sanctions on a corporation for failing to produce email evidence in time for trial even after the corporation claimed that its expert was having difficulty finding the desired emails in the backup tapes).

28 Rosenberg, *supra* note 16.

29 Scheindlin & Rabkin, *supra* note 6, at 329.

so, American courts have attempted to provide answers to these important questions.

A. Providing Guidance Through the Electronic "Roadblock":[30] The Courts Enter the Fray

As the courts began to fill with litigants requesting electronic discovery, members of the judiciary were forced to feel their way through this emerging area of the law.[31] As with other areas of the law, the result has been a slow progression, with each successive advance ostensibly improving on the preceding one. Because of the potentially prohibitive cost of e-discovery, the question of cost shifting, or whether the requesting or producing party should pay for discovery of electronically stored information, has taken center stage. In response, courts have adopted three alternative approaches to the cost-shifting analysis.

First, the "marginal utility approach" to balancing the costs of e-discovery has its roots in *McPeek v. Ashcroft*.[32] In *McPeek*, the fight over which side should bear the costs of discovery began when an employee of the Federal Bureau of Prisons accused his supervisor of sexual harassment.[33] After the parties reached a confidential settlement agreement, the plaintiff was transferred to another department within the Department of Justice.[34] Despite his transfer, the plaintiff contended that his co-workers knew about his past claims of sexual harassment and that he experienced humiliation and retaliation as a result.[35] He further contended that he suffered renewed retaliation efforts after

30 *See* Zubulake v. UBS Warburg LLC, 217 F.R.D. 309, 311 (S.D.N.Y. 2003) ("[T]he reliance on broad discovery has hit a roadblock. As individuals and corporations increasingly do business electronically . . . the more expensive it is to discover all the relevant information until, in the end, 'discovery is not just about uncovering the truth, but also about how much of the truth the parties can afford to disinter.'") For further discussion of the Zubulake case, see *infra* text accompanying notes 49–68.

31 Responding to the increase in requests for electronic information, U.S. Magistrate Judge Peck remarked, "[I]t is black letter law that computerized data is discoverable if relevant." Anti-Monopoly, Inc. v. Hasbro, Inc., 1995 WL 649934, at *2 (S.D.N.Y. Nov. 3, 1995).

32 202 F.R.D. 31 (D.D.C. 2001).

33 *Id.* at 31.

34 *Id.* at 32.

35 *Id.*

hiring counsel to pursue formal legal remedies.[36] During the discovery phase of *McPeek*, the plaintiff sought to force the Department of Justice to search its backup systems for data that had been deleted but was stored on backup tapes.[37] After acknowledging that "[t]he Federal Rules of Civil Procedure do not require such a search, and the handful of cases are idiosyncratic and provide little guidance,"[38] Magistrate Judge Facciola imposed a "test run."[39] The court required the Department of Justice to perform a backup restoration of emails from one specific computer over a period of one year.[40]

The marginal utility approach reasons that the more likely it is that a resource, such as a backup tape, contains relevant information, the more fair it is to impose the costs of production on the producing party.[41] Thus, if the trier of fact finds any evidence pointing to the existence of relevant data that has not been produced because it allegedly is not reasonably accessible, the court will require the producing party to bear the cost of producing it. Several other cases have also followed this approach.[42]

The second foundational decision addressing which party should bear the expense of complying with e-discovery requests was *Rowe Entertainment, Inc. v. William Morris Agency, Inc.*[43] In *Rowe Entertainment*, African American concert promoters brought suit against booking agencies and other promoters, contending that the defendants' discriminatory and anticompetitive practices froze the plaintiffs out of the market for promoting events with white musicians.[44] The court noted that despite the presumption that the responding party must

36 *Id.*

37 *Id.*

38 *Id.* at 33.

39 *Id.* at 34.

40 *Id.*

41 *See id.*

42 *See* Medtronic Sofamor Danek, Inc. v. Michelson, 2003 WL 21468573, at *5–6 (W.D. Tenn. 2003) (applying the marginal utility approach as part of the cost-shifting analysis); Byers v. Illinois State Police, 2002 WL 1264004, at *11–12 (N.D. Ill. 2002) (applying the marginal utility approach to shift costs to the requesting party).

43 205 F.R.D. 421 (S.D.N.Y. 2002).

44 *Id.* at 423.

bear the expense of complying with discovery requests,[45] the court has the ability to protect the producing party from "undue burden or expense" by shifting some or all costs to the requesting party.[46] The court listed eight factors that had been used in other cases to determine when this undue burden or expense justified shifting the burden of discovery.[47] Applying these factors, the court ordered the plaintiff's counsel to "formulate a search procedure for identifying responsive emails and . . . notify each defendant's counsel of the procedure chosen, including any specific word searches."[48]

The final evolutionary progression in the common law rules governing e-discovery came in *Zubulake v. UBS Warburg LLC*.[49] Many practitioners and legal scholars consider the *Zubulake* decisions to be the lodestar of e-discovery rulings. U.S. Magistrate Judge Shira Scheindlin has illuminated her opinions through several articles on the topic coauthored with her law clerks.[50] In the first of several opinions and written

45 *Id.* at 428 (citing Oppenheimer Fund, Inc. v. Sanders, 437 U.S. 340, 358 (1978)).

46 *Id.* (citing FED. R. CIV. P. 26(c)).

47 *See id.* at 429. The eight factors were: (1) the specificity of the discovery request (the less specific the requesting party's demands, the more appropriate it is to shift the costs of production to that party); (2) the likelihood of discovering critical information; (3) the availability of such information from other sources; (4) the purpose for which the responding party retained the requested data (if a party actively uses the data, that party must respond to the discovery request at its own expense); (5) the relative benefit to the parties of obtaining the data (if the responding party reaps a substantial benefit, there is little justification for shifting the burden to the requesting party); (6) the total cost of production (if insubstantial, there is no justification for deviating from the presumption that the responding party will bear the expense); (7) the relative ability and incentive of each party to control costs ("[W]here the discovery process is going to be incremental, it is more efficient to place the burden on the party that will decide how expansive the discovery will be."); and (8) the parties' available resources (where the cost of discovery might go beyond the resources of one of the parties, shifting the burden to the other party may be justified). *Id.* at 429–32.

48 *Id.* at 433.

49 Zubulake v. UBS Warburg LLC (*Zubulake V*), 229 F.R.D. 422 (S.D.N.Y. 2004). The long and drawn-out *Zubulake* case produced a series of written opinions relating to sparring by the parties over discovery issues. *See* Zubulake v. UBS Warburg LLC (*Zubulake I*), 217 F.R.D. 309 (S.D.N.Y. 2003); Zubulake v. UBS Warburg LLC (*Zubulake II*), 230 F.R.D. 290 (S.D.N.Y. 2003); Zubulake v. UBS Warburg LLC (*Zubulake IV*), 220 F.R.D. 212 (S.D.N.Y. 2003); *Zubulake V*, 229 F.R.D. 422. *Zubulake II*, *Zublake III*, and *Zubulake IV* are not cited in this Comment because they discuss inapplicable matters.

50 *See, e.g.*, Shira A. Scheindlin & Kanchana Wangkeo, *Electronic Discovery Sanctions in the Twenty-First Century*, 11 MICH. TELECOMM. & TECH. L. REV. 71

orders in the *Zubulake* case, Judge Scheindlin described her view of electronic evidence, noting:

> Many courts have automatically assumed that an undue burden or expense may arise simply because electronic evidence is involved. This makes no sense. Electronic evidence is frequently cheaper and easier to produce than paper evidence because it can be searched automatically, key words can be run for privilege checks, and the production can be made in electronic form obviating the need for mass photocopying.[51]

In *Zubulake*, Judge Scheindlin addressed the important questions of what electronic evidence was discoverable,[52] how the cost of discovering electronic evidence should be shared among parties,[53] and whether sanctions should be imposed on a party for failing to produce evidence.[54]

The plaintiff, Laura Zubulake, was an equities trader at UBS Warburg.[55] After leaving the company, Zubulake sued her former employee for gender discrimination.[56] Following a protracted two-year period of discovery, Zubulake moved to sanction UBS Warburg for its failure to produce relevant information.[57] The question before the U.S. District Court for the Southern District of New York was whether UBS failed to

(2004); Scheindlin & Rabkin, *supra* note 6. U.S. District Court Judge Shira A. Scheindlin is recognized as one of the leading jurists considering electronic discovery issues. From 1998 to 2005, Judge Scheindlin also served on the U.S. Advisory Committee on Civil Rules, where she was active in helping draft the e-discovery amendments to the Federal Rules of Civil Procedure. *See* Advisory Committee on Civil Rules, http://www.uscourts.gov/rules/Committee%20Membership%20Lists/ST_Roster_2004.pdf (last visited Apr. 21, 2008) (listing membership of that committee).

51 *Zubulake I*, 217 F.R.D. at 318 (citations omitted).

52 *See id.* at 316–17.

53 *See id.* at 317–18.

54 See *Zubulake V*, 229 F.R.D. at 437–41 (discussing whether sanctions should be imposed for discovery violations, and ultimately imposing an adverse-jury instruction against UBS Warburg and forcing that company to pay for any depositions or redepositions that may be required by the late production).

55 *See Zubulake I*, 217 F.R.D. at 312.

56 *See id.*

57 *See Zubulake V*, 229 F.R.D. at 425–26 (reviewing the procedural history of *Zubulake*). Specifically, the plaintiff requested "[a]ll documents concerning any communication by or between UBS employees concerning Plaintiff," including, "without limitation, electronic or computerized data compilations." *Zubulake I*, 217 F.R.D. at 312 (footnote omitted).

"preserve and timely produce relevant information and, if so, did it act negligently, recklessly, or willfully?"[58]

The *Zubulake* court favored a broad approach to discoverability, stating that "in the world of electronic data . . . any data that is retained in a machine readable format is typically accessible."[59] The court further recognized that "broad discovery is a cornerstone of the litigation process contemplated by the Federal Rules of Civil Procedure."[60]

The *Zubulake* case is somewhat unique in that the plaintiff was seeking an adverse-inference jury instruction.[61] In its analysis, the court considered the *Rowe Entertainment* factors, but ultimately criticized the test for not taking into account "the amount in controversy or the importance of the issues at stake in the litigation."[62] The court eliminated or modified two prongs of the *Rowe Entertainment* test and developed a new test comprised of seven factors.[63] It noted that the seven factors should not be weighted equally, and that the central question is whether the request imposes an undue burden or expense on the responding party, or, "[p]ut another way, 'how important is the

---

[58] *Zubulake V*, 229 F.R.D. at 424.

[59] *Zubulake I*, 217 F.R.D. at 318.

[60] *Id.* at 311 (quoting Jones v. Goord, 2002 WL 1007614, at *1 (S.D.N.Y. May 16, 2002)).

[61] *See Zubulake V*, 229 F.R.D. at 430. The court explained that for a plaintiff to be entitled to such an instruction, she must prove:

> (1) that the party having control over the evidence had an obligation to preserve it at the time it was destroyed; (2) that the records were destroyed with a "culpable state of mind" and (3) that the destroyed evidence was "relevant" to the party's claim or defense such that a reasonable trier of fact could find that it would support that claim or defense.

Id. (citing Byrnie v. Town of Cromwell, 243 F.3d 93, 107–12 (2d Cir. 2001)).

[62] *Zubulake I*, 217 F.R.D. at 321.

[63] *See id.* at 322. The seven *Zubulake* 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.

Id.

sought-after evidence in comparison to the cost of production?'"[64]

Applying the seven factors to the case at hand, the *Zubulake* court ordered the defendant to produce, at its expense, all responsive emails residing on its optical disks, active servers, and any five backup tapes to be selected by Zubulake.[65] The court ruled that it would make a final cost-shifting decision after reviewing those backup tapes and the defendant's cost of production.[66] It imposed the sanction of an adverse-inference jury instruction in order to "restore [the plaintiff] to the position she would have been in had UBS faithfully discharged its discovery obligations."[67] The adverse-inference jury instruction apparently had a strong effect on the jury, which subsequently awarded Laura Zubulake more than $29 million in damages.[68]

---

[64] *Id.* at 322–23 (footnote omitted).

[65] *Id.* at 324.

[66] *Id.*

[67] *See* Zubulake v. UBS Warburg LLC (*Zubulake V*), 229 F.R.D. 422, 437 (S.D.N.Y. 2004). The adverse-inference jury instruction read as follows:

> You have heard that UBS failed to produce some of the e-mails sent or received by UBS personnel in August and September 2001. Plaintiff has argued that this evidence was in defendants' control and would have proven facts material to the matter in controversy.
>
> If you find that UBS could have produced this evidence, and that the evidence was within its control, and that the evidence would have been material in deciding facts in dispute in this case, you are permitted, but not required, to infer that the evidence would have been unfavorable to UBS.
>
> In deciding whether to draw this inference, you should consider whether the evidence not produced would merely have duplicated other evidence already before you. You may also consider whether you are satisfied that UBS's failure to produce this information was reasonable. Again, any inference you decide to draw should be based on all of the facts and circumstances in this case.

Id.

[68] Eduardo Porter, *UBS Ordered to Pay $29 Million in Sex Bias Lawsuit*, N.Y. TIMES, Apr. 7, 2005, at C4.

B. Moving Toward Uniformity: The Rules Respond

Proving the old maxim that "the only constant is change,"[69] the rules of discovery were subject to revisions well before the issue of e-discovery arose. Indeed, as one commentator noted, "The Federal Rules of Civil Procedure change with the telephone directory. Every year, something is tweaked, torn, wrenched, or rewritten. Most of this is merely annoying. Sometimes, though, buried amid the clutter is an amendment that carries a real wallop for major aspects of practice."[70] After many years of observing the courts apply the traditional paper-discovery rules to electronic discovery with disparate results, the Committee on Rules of Practice and Procedure responded in 2006 with something akin to a "real wallop": a revision of the Rules that directly addressed electronically stored information.

The full package of revisions[71] includes changes to Rules 16,[72] 26,[73] 33,[74] 34,[75] 37,[76] and 45,[77] as well as Form 35. These changes

[69] *See, e.g.*, Michael Bürgi, Editor's Note, *The Only Constant Is Change*, MEDIAWEEK, June 4, 2007, http://www.mediaweek.com/mw/departments/columns/article_display.jsp?vnu_content_id=1003593172 ("[D]epending on which Web source you believe . . . [the maxim] was first uttered either by Greek philosopher Heraclitus, or slightly more contemporary sci-fi author Isaac Asimov.").

[70] Richard Marcus, *Only Yesterday: Reflections on Rulemaking Responses to E-Discovery*, 73 FORDHAM L. REV. 1, 18 (2004) (quoting Gregory P. Joseph, *Rule Traps*, LITIG., Fall 2003, at 6, 6).

[71] In-depth discussion of all the changes to the Rules included in this most recent revision falls outside the ambit of this Comment. The full text of the amendments is available on the U.S. Supreme Court's web site at http://www.supremecourtus.gov/orders/courtorders/frcv06p.pdf (last visited Apr. 4, 2008). For a brief summary of the changes, see *infra* notes 72–77. For a more complete description, see Kenneth J. Withers, *Electronically Stored Information: The December 2006 Amendments to the Federal Rules of Civil Procedure*, 4 NW. J. TECH. & INTELL. PROP. 171 (2006), *available at* http://www.law.northwestern.edu/journals/njtip/v4/n2/3/J.%20Withers.pdf.

[72] FED. R. CIV. P. 16(b). The revised Rule 16(b) now sets forth provisions that parties must meet in advance of trial to discuss discovery issues related to electronically stored information. *See id.*

[73] FED. R. CIV. P. 26. The revised Rule 26(a)(1) states that a party must provide the names of holders of its relevant information and a copy or description of the data it will use to the other parties in the litigation, without awaiting a discovery request. *See* FED. R. CIV. P. 26(a)(1). Rule 26(b)(2)(B) deals with the issue of discovery of information that is not reasonably accessible because of undue burden or cost. *See* FED. R. CIV. P. 26(b)(2)(B). The amended Rule 26(f) touches on a wide range of issues including discussion of issues relating to preserving discoverable information at pretrial meetings. *See* FED. R. CIV. P. 26(f).

were the result of over five years of consideration by the Advisory Committee on Civil Rules ("Advisory Committee").[78] At the dawn of the twenty-first century, there was a limited recognition that "digital is different," but little consensus as to the specific differences between traditional paper documents and electronically stored information. At that time, the prevailing view among judges was that the current civil rules could accommodate whatever differences might exist. Members of the Advisory Committee did not share this view, and in 1999 Advisory Committee Chairman Judge Paul V. Niemayer said:

> [T]he committee recognizes that electronic storage and retrieval of information are changing the opportunities for discovery and the dangers of excessive discovery. Anecdotes abound. The committee is just beginning to study the need to devise mechanisms that will ensure continued access to useful information without overwhelming the parties by burdens far beyond anything justified by the interests of litigation.[79]

[74] FED. R. CIV. P. 33. The amended Rule 33 makes clear that the option to produce business records includes electronically stored information. *See* FED. R. CIV. P. 33(d).

[75] FED. R. CIV. P. 34. The revised Rule 34 adds "electronically stored information" as a category subject to production. *See* FED. R. CIV. P. 34(a)(1)(A). Rule 34(b) permits a requesting party to "specify the form or forms in which electronically stored information is to be produced." *See* FED. R. CIV. P. 34(b)(1)(C).

[76] FED. R. CIV. P. 37. Rule 37 has been amended to address the problem of the destruction of records resulting from the "routine, good-faith operation of an electronic information system." *See* FED. R. CIV. P. 37(e). The rule may "protect a corporation from sanctions for inadvertently permitting a backup tape to be automatically overwritten, but not for failing to prevent employees from deleting relevant e-mails." Elaine Ki Jin Kim, *The New Electronic Discovery Rules: A Place for Employee Privacy?*, 115 YALE L.J. POCKET PART 161, 164 (2006), http://www.thepocketpart.org/2006/08/kim.html.

[77] FED. R. CIV. P. 45. The revised Rule 45 provides for subpoenas regarding electronically stored information as well as paper documents. *See* FED. R. CIV. P. 45(a)(1)(A)(iii).

[78] The Advisory Committee on Civil Rules is comprised of judges, legal professors, and practitioners. The current reporter is Professor Edward Cooper of the University of Michigan Law School. *See* Advisory Committee on Civil Rules (2006), http://www.uscourts.gov/rules/Memb1206.pdf.

[79] Withers, *supra* note 71, at 192 (quoting Letter from Paul V. Niemeyer to the Chief Justice of the United States and Member of the Judicial Conference of the United States (Sept. 1, 1999) (reprinted in meeting materials of the Advisory Committee on Civil Rules, Oct. 14–15, 1999)).

Recognizing that the traditional rules were incompatible with new technologies, the Advisory Committee embarked on a five-year project to answer three basic questions:

> [W]hat are the differences between conventionl and electronic discovery? . . . [D]o these differences create problems that can or need to be addressed through changes in the Rules of Civil Procedure? And finally, if there are problems that rulemaking can or should address, what rules can be crafted to serve that purpose?[80]

The process of developing these new Rules required the Advisory Committee to evaluate the very nature of electronically stored information and the practical needs of litigators. But perhaps the most important consideration was the ad hoc rule-making process that had sprung up as local courts responded to e-discovery requests. The changes to Rule 26 illustrate this point.

Rule 26 sets forth certain required disclosures that a party must provide before receiving a discovery request.[81] Prior to the revisions to the Rules, many federal district courts faced with e-discovery requests had realized that the traditional discovery-avoidance tactic of "hiding the ball," when applied to e-discovery, resulted in increased costs, delays, and needless disputes. In response, federal courts in Wyoming and Arkansas adopted local rules requiring disclosure of electronic records and discussion of electronic discovery plans before formal discovery could begin.[82] Federal courts in New Jersey continued the trend, requiring not only disclosure and a pretrial conference, but also that counsel for both parties investigate their clients' information systems and assist with computer-based discovery.[83] Federal courts in Delaware and Kansas took a slightly different path by

---

[80] *Id.*

[81] *See* FED. R. CIV. P. 26(a)(1)(B) (requiring, among other things, initial disclosures of "a copy of, or a description by category and location of, all documents, electronically stored information, and tangible things that are in the possession, custody, or control of the party and that the disclosing party may use to support its claims or defenses, unless solely for impeachment").

[82] U.S. District Court for the Eastern District of Arkansas, Local Rule 26.1, *available at* http://www.are.uscourts.gov/rules/r26-1.cfm (last visited Apr. 10, 2008); U.S. District for the District of Wyoming, Local Rule 26.1(e), *available at* http://www.wyd.uscourts.gov/pdfforms/localrules-cv.pdf (last visited Apr. 10, 2008).

[83] U.S. District Court for the District of New Jersey, Local Civil Rule 26.1(d), *available at* http://pacer.njd.uscourts.gov/rules/05-0901-Rules.pdf (last visited Apr. 10, 2008).

foregoing the adoption of local rules, and instead promulgating standards or guidelines for attorneys to follow when conducting electronic discovery. These guidelines have the effect of standing orders and are more detailed than the local rules of Arkansas, Wyoming, and New Jersey.[84]

The emergence of local rules, standards, and guidelines for e-discovery provided the Advisory Committee with objective experience on which to draw. But these local experiments also highlighted the necessity for federal rule making, if for no other reason than to prevent further divergence from the ideal of a national, uniform set of civil procedure rules in all federal courts.[85]

Although the new Rules represent a good effort to regulate e-discovery, their language is still general enough that many remaining questions of interpretation and application will be resolved only through litigation. The Advisory Committee drafted the revisions so that they can be applied to any source of information potentially subject to discovery, as long as a court can determine whether the source may contain information that is potentially relevant to a particular case. However, the revisions fail to address several important e-discovery issues. Specifically, the new Rules avoid discussing which types of file formats litigants are required to produce when they receive a preservation order.[86] Also, the new Rules do not address the

[84] U.S. District Court for the District of Delaware, *Default Standard for Discovery of Electronic Documents ("E-Discovery")*, *available at* http://www.ded.uscourts.gov/Announce/Policies/Policy01.htm (last visited Mar. 5, 2007); The U.S. District Court for the District of Kansas, *Guidelines for Discovery of Electronically Stored Information (ESI)*, *available at* http://www.ksd.uscourts.gov/guidelines/electronicdiscoveryguidelines.pdf (last visited Apr. 10, 2008).

[85] *See* Charles E. Clark & James Wm. Moore, *A New Federal Civil Procedure: I. The Background*, 44 YALE L.J. 387, 387 (1935) (describing the rationale for new rules of procedure for civil actions as "unit[ing] the federal law and equity procedure").

[86] *See* Jason Krause, *Fear of the 'Native': How E-Discovery Data Is Delivered Can Be a Costly Decision*, A.B.A. J., Jan. 2008, at 59, 59. The article describes how under the revised Rule 34 parties are allowed to request "native" file formats as well as copies of the original files. *Id.* The "native" format is that in which the file was created. Because of the uncertainty of how to proceed, some litigants "keep native files and copies, doubling their inventory." *Id.* The article also notes that "aggressive use of the rule is causing some headaches because many vendors still can't handle native formats." *Id.*

significant issue of how to handle discovery of metadata.[87] Metadata may be discoverable, but absent guidance from the Rules, it will be up to the courts to decide when and how it can be used.

Thus, a broad examination of the evolution of e-discovery reveals several unique developments in the process. First, litigants present courts with novel questions of law where easy answers from the Rules or case law are lacking. Second, courts carefully consider the issues and develop laws on an ad hoc basis that not only decide the case at bar but also provide guidance to the legal community and future litigants. Courts often decide questions of law on a case-by-case basis only after protracted ancillary litigation defines the scope of the issue. Based on the localized nature of many of these decisions, the law often develops a "patchwork quilt" appearance at this stage: each jurisdiction may have its own unique rules. Finally, this judge-made common law is codified in a formal set of rules or a statute.

The history of e-discovery shows that applying traditional rules to emerging technological advances produces, at best, disparate results. It was only through innovative judge-made law and a revision to the Federal Rules of Civil Procedure that this area of the law achieved a measure of uniformity. To explore this idea in a different and timelier context, this Comment will turn to the burgeoning use of social-networking sites by examining the history of such web sites and the legal issues that arise when law-enforcement officers use them to gather evidence.

II

SOCIAL-NETWORKING WEB SITES: "SODA FOUNTAINS" FOR THE TWENTY-FIRST CENTURY

In a bygone era, members of a community would gather at the local soda fountain to "chew the fat"—discuss matters of local

[87] Metadata can be described as the computer-generated, invisible "headers" that accompany most computer files. ALAN M. GAHTAN, ELECTRONIC EVIDENCE 7 (1999). *See also* Luehr, *supra* note 21, at 15 (describing metadata as "data about the data" that can "help determine who wrote a smoking-gun memo; who received, opened, edited, copied, moved, or printed the memo; and when these actions occurred").

politics, share the latest gossip, or complain about the weather.[88] These days, millions of people are engaged in the same conversations not over root beer floats at soda fountains, but over keyboards in online communities known as social-networking web sites.

At a fundamental level, social-networking sites are online networks of individuals linked through personalized Internet web pages.[89] These web sites typically allow users to customize their own personal web pages (often known as "profiles"), post photographs or videos, add music, or write a journal or blog that is published to the online world. Social-networking sites also facilitate interpersonal communications through email systems that allow users to exchange messages. These web sites allow users to compile lists of "friends" who are "ostensibly" part of one's social network.[90] Users may also create and join groups based on common interests, such as Oregon Duck Fans[91] or Alaskan Malamute Owners.[92] The emergence of these popular services is the result of ingenuity, slick marketing, and tapping into our society's intense interest in customization.[93]

88 *See generally* ANNE COOPER FUNDERBURG, SUNDAE BEST: A HISTORY OF SODA FOUNTAINS 101 (2002) (describing how soda fountains acted as "community social center[s]" in the early twentieth century).

89 *See, e.g.*, John W., http://www.myspace.com/johnswilson (last visited Apr. 10, 2008) (MySpace profile of the Author).

90 The use of quotation marks on "friends" and "ostensibly" is appropriate here because often a user's "friends list" includes many people with whom the user has little or no affiliation. For example, Tom Anderson, one of the founders of MySpace, lists 230,321,585 people in his "friends list." *See* Tom, http://www.myspace.com/tom (last visited Apr. 10, 2008).

91 *See Duck Nation (Home of the Oregon Ducks)*, http://groups.myspace.com/ducknation (last visited Apr. 10, 2008) (Oregon Ducks fans MySpace group).

92 *See* Alaskan Malamutes Rock!, http://groups.myspace.com/alaskanmalamutesrock (last visited Apr. 10, 2008) (Alaskan Malamute owners' MySpace group). MySpace currently hosts over two million user groups. *See* Groups Home, http://groups.myspace.com (last visited Apr. 10, 2008).

93 *See, e.g.*, Diane Brady et al., *Customizing for the Masses*, BUS. WK., Mar. 20, 2000, at 130, *available at* http://www.businessweek.com/2000/00_12/b3673136.htm (describing how today's consumers seek the ability to customize their products—from Dell computers to NikeiD shoes).

A. Clicking on a Phenomenon: The History of Social Networking[94]

As an undergraduate at Harvard, Mark Zuckerberg created what was to become one of the most popular web sites on the Internet. Originally called "thefacebook," the site was named for the paper facebooks that universities often distribute to incoming students, faculty, and staff depicting members of the campus community.[95] Zuckerberg launched thefacebook in February of 2004, and it was an immediate hit.[96] Within months, the user base had spread from the dorm rooms of Harvard to Stanford and Yale, where the site's popularity grew.[97] Fellow Harvard students Dustin Moskovitz and Chris Hughes aided Zuckerberg in his venture,[98] and as the site grew to a national student-network phenomenon, Zuckerberg and Moskovitz dropped out of Harvard and began to run the site full time.[99] In August 2005, the site was officially renamed "Facebook" and the domain name facebook.com was purchased for a reported $200,000.[100] Originally the site was only open to those with a

[94] Because of the relatively recent emergence of social-networking sites, information about this technological advance in the traditional forms of print sources is scarce. Therefore, this Comment, and this Part in particular, must rely to some degree upon online sources such as Mashable, Alexa.com, and Valleywag. Where possible, material taken from these sources has been corroborated with research by more traditional sources such as the New York Times and Los Angeles Times.

[95] John Markoff, *An Internet Darling's Tangled Roots*, INT'L HERALD TRIB., Sept. 2, 2007, at 13. This version of events is not without its critics. Three founders of ConnectU, a different social-networking site, have claimed that Zuckerberg stole the idea from them. Aaron Greenspan, who was Zuckerberg's Harvard classmate, has argued that he actually developed the idea. *See* John Markoff, *Who Found the Bright Idea?*, N.Y. TIMES, Sept. 1, 2007, at C1. Facebook ultimately settled the lawsuit that had been filed by the founders of ConnectU against the company and Mark Zuckerberg. *See* Brad Stone, *Facebook to Settle Thorny Lawsuit over Its Origins*, N.Y. TIMES, Apr. 7, 2008, *available at* http://bits.blogs.nytimes.com/2008/04/07/facebook-to-settle-thorny-lawsuit-over-its-origins/. For Zuckerberg, the settlement could not have come soon enough. The discovery phase of the case made public such embarrassing documents as his online diary and application to Harvard University. *See* The Facebook Files, http://www.02138mag.com/magazine/article/1764.html (last visited Apr. 21, 2008).

[96] Sid Yadav, *Facebook—The Complete Biography*, MASHABLE, Aug. 25, 2006, http://mashable.com/2006/08/25/facebook-profile/.

[97] *Id.*

[98] *Id.*

[99] *Id.*

[100] *Id.*

valid university email address, but in 2006 Facebook opened registration to anyone with a valid email address.[101] Today, Facebook boasts more than "70 million active users" across "over 55,000 regional, work-related, collegiate, and high school networks."[102]

But despite this popularity, Facebook is dwarfed by the social-networking behemoth MySpace.[103] MySpace offers similar features such as allowing users to create or join groups, post photos or videos, post "bulletins," and write personal blogs. MySpace also offers users an instant-messaging system that allows them to exchange messages in real time.[104] Unlike Facebook, however, the corporate history of MySpace is not so cut and dry.

The company line states that MySpace was founded in July 2003 by two friends, Tom Anderson and Chris DeWolfe.[105] Anderson and DeWolfe were connected through the same Silicon Valley circles and were inspired to start MySpace by the success of other social-networking sites such as Ryze and Friendster.[106] This version of events, however, is not without its critics. An investigative report by journalist Trent Lapinski claims that MySpace is actually the brainchild of three of Silicon Valley's biggest spammers,[107] Brad Greenspan,[108] Chris

101 Anick Jesdanun, *Facebook to Open to All Internet Users*, PANTAGRAPH.COM, Sept. 12, 2006, http://www.pantagraph.com/articles/2006/09/12/news (click on title of article).

102 Facebook Press Room, http://www.facebook.com/press/info.php?statistics.php (last visited Apr. 11, 2008).

103 MySpace, http://www.myspace.com. The capitalization of both the 'M' and 'S' within MySpace reflects the accurate corporate moniker. *See also MySpace Gains Top Ranking of U.S. Websites*, USA TODAY, July 11, 2006, *available at* http://www.usatoday.com/tech/news/2006-07-11-myspace-tops_x.htm (stating that MySpace has been ranked the most popular web site in the United States).

104 MySpace Instant Messaging, http://www.myspace.com/myspaceim (last visited Apr. 21, 2008).

105 MySpace—Wikipedia, http://en.wikipedia.org/wiki/MySpace (last visited Apr. 11, 2008).

106 *See generally* Joseph Menn, *The Personal Links of Three Social-Networking Sites*, L.A. TIMES, Dec. 29, 2003, at C1 (describing the early social-networking sites Ryze, Tribe, and Friendster).

107 *See, e.g.*, BLACK'S LAW DICTIONARY 1430 (8th ed. 2004) (defining "spam" as "[u]nsolicited commercial e-mail"). *But see* Andy Greenberg, *Don't Call It Spam*, FORBES, Feb. 22, 2007, *available at* http://www.forbes.com/2007/02/21/spam-lawsuit-marketing-tech-cx_ag_0222spam.html (quoting a spam-law analyst from the

DeWolfe, and Tom Anderson, who built the site's popularity through an intense unsolicited mass-email campaign.[109] The site continued to exhibit meteoric growth, and Rupert Murdoch's News Corporation acquired it in 2005 for a reported $580 million.[110]

Regardless of whether MySpace is the result of a "happy accident that began in [Tom] Anderson's bedroom or garage"[111] or the result of an insidious mass-marketing campaign, one fact cannot be denied: MySpace is currently the most popular web site in the United States[112] and the fifth most popular web site in the world, trailing only Yahoo, MSN, Google, and YouTube.[113]

The broad appeal of social-networking sites such as MySpace and Facebook seems to have its roots in a successful twist on the age-old concept of self-promotion. By allowing, let alone encouraging, the solicitation and promotion of anything and everything, social-networking sites have tapped into society's

Electronic Frontier Foundation as stating, "There's no legal definition [for spam] . . . . Spam is in the eye of the beholder.").

108 Brad Greenspan plays a central role in the controversy surrounding MySpace's corporate history. Originally one of the cofounders of the site, he has since had a falling out with the company and now leads a crusade against MySpace by calling on the Securities and Exchange Commission, the U.S. Department of Justice, and the U.S. Senate to investigate News Corporation's acquisition of MySpace as "one of the largest merger and acquisition scandals in U.S. history." Dawn C. Chmielewski, *MySpace Founder Seeks Inquiry*, L.A. TIMES, Oct. 6, 2006, at C1. In 2006, Greenspan's suit against MySpace and News Corp. was dismissed after a Los Angeles Superior Court judge found that the acquisition was lawful. *Suit over Sale of MySpace Dismissed*, SEATTLE POST-INTELLIGENCER, Oct. 10, 2006, *available at* http://seattlepi.nwsource.com/business/ 28111_myspace10.html. Greenspan also runs his own web site at http://www .freemyspace.com (last visited Apr. 11, 2008) where he lists his litany of complaints against MySpace and News Corporation.

109 Dan Mitchell, *The Story Behind MySpace*, N.Y. TIMES, Sept. 16, 2006, at C5; *see also* Trent Lapinski, *MySpace: The Business of Spam 2.0 (Exhaustive Edition)*, VALLEYWAG, Sept. 11, 2006, http://www.valleywag.com/tech/myspace/myspace-the-business-of-spam-20-exhaustive-eition-199924.php (describing MySpace's alleged "re-imagining and repackaging of spam").

110 *See* Richard Siklos, *News Corporation Buys an Internet Company*, N.Y. TIMES, July 19, 2005, at C6, *available at* http://www.nytimes.com/2005/07/19/ business/media/19online.html.

111 Lapinski, *supra* note 109.

112 *See MySpace Gains Top Ranking of U.S. Websites, supra* note 103 (reporting that MySpace captured 80% of all visits to social-networking sites, and that Facebook was a distant second at 7.6%).

113 Alexa Top 500 Sites, http://www.alexa.com/site/ds/top_sites?ts_mode=global &lang=none (last visited Apr. 11, 2008).

infatuation with customization and drawing attention to one's self.[114] The problem, of course, arises when users draw attention to themselves through criminal activities.

B. Patrolling the Information Superhighway: The Point-and-Click Police Add MySpace to Their "Friends Lists"

Law-enforcement officers are increasingly working a new beat, turning to social-networking sites such as MySpace and Facebook to gather evidence of crimes. These members of the "point-and-click" police are finding a great deal of helpful information because of the extremely personal[115] nature of social-networking sites.[116]

---

114 *See generally* B. JOSEPH PINE II, MASS CUSTOMIZATION: THE NEW FRONTIER IN BUSINESS COMPETITION 8 (1993) (noting that companies that produce or supply "automobiles, apparel, lighting controls, power tools, refrigerated warehouses, travel services, midrange computers, watches, power supplies, [and] pagers . . . [are] increas[ing] their variety and customization—all to satisfy more closely the individual wants and needs of their customers"). While written from a business management perspective, Pine's book does an excellent job of describing the transition in American business from mass production to mass customization. *See also* LISA JOHNSON, MIND YOUR X'S AND Y'S: SATISFYING THE 10 CRAVINGS OF A NEW GENERATION OF CONSUMERS (2006). Johnson lists five criteria for how consumers operate in today's market, including "Shine the Spotlight," where she describes how today's young consumers are "itching to stand out, stand up, and be celebrated with their names in lights (or print, or pixels)." *Id.* at 18. Interestingly, Johnson cites a certain university athletic department that touched on these desires by sending football recruits a customized comic book where the recruit is the hero of the story. The school is none other than the University of Oregon. *See id.* at 15–18. Johnson also describes how companies that offer such products as customizable M&M's candies or personalized comics are able to "tap into this powerful need with highly creative and customized efforts." *Id.* at 18–19.

115 An example of just how "personal" content posted on MySpace can be is seen in the infamous case of the "MySpace Mayor," Carmen Kontur-Gronquist. *See* Mike Celizic, *Ousted Mayor Makes No Apologies for Lingerie Photos*, MSNBC.COM, Mar. 3, 2008, http://www.msnbc.msn.com/id/23445683/. Kontur-Gronquist was recalled from her position as mayor of the tiny town of Arlington, Oregon, after several photos of her in "an opaque black bra and matching boy-short panties" were discovered on MySpace. *Id.* She was recalled by a vote of 142 to 139. *Id.* Kontur-Gronquist does not make any apologies for the photos, and in fact is selling poster-size, autographed prints, with a portion of the proceeds going to charity. *Id.*

116 During the course of researching this Comment, the Author learned that MySpace had written and distributed a set of guidelines for investigations by law enforcement officers. In the guidelines, MySpace states that the service "supports the vision of providing a safer and more secure environment for all MySpace users. Accordingly, MySpace is committed to a high level of cooperation with law enforcement to assist in investigating and identifying those involved in activity that

For example, police detectives in Tacoma, Washington used MySpace to prove a motive, confirming that the victims and suspects in a triple homicide knew each other after learning that at least two of the victims were on one another's "friends lists."[117] In the same vein, the Attorney General of Utah filed sexual-exploitation charges against a twenty-seven-year-old man after investigators discovered a photo on his MySpace profile that featured the man and two boys with whom he had been court-ordered not to have contact.[118] The man's MySpace friends list included many teenage boys.[119] In another case, a former elementary school teacher was sent back to jail for violating the terms of her probation after she contacted her rape and sexual-battery victim through MySpace's blog feature.[120] And in Boulder, Colorado, a tech-savvy detective assembled a "police lineup" of suspects in a sexual-assault case from the portrait photos displayed on their MySpace profiles.[121]

Sometimes MySpace can also assist law-enforcement agencies in preventing serious crimes before they occur, as in the case of the sixteen-year-old boy who was arrested after posting photographs of himself holding handguns on his MySpace profile.[122] Police were alerted by concerned parents who kept

undermines this vision." MySpace.com Law Enforcement Investigators Guide (on file with Author). This "cooperation," however, is not entirely voluntary. The Electronic Communications Privacy Act of 1986 mandates that services functioning as "electronic communications" and "remote computing" services must disclose certain user information in response to specific types of government requests, including subpoenas, court orders, and search warrants. *See* 18 U.S.C. § 2703(c) (2006).

117 Paul Sand, *MySpace: Meet People, Talk Music, Fight Crime*, NEWS TRIB. (Tacoma, Wash.), Mar. 12, 2006, *available at* http://dwb.thenewstribune.com/news/crime/story/5583552p-5021349c.html.

118 *Id.*

119 *Id.*

120 *MySpace Page Puts Teacher Back in Jail*, MSNBC.COM, Apr. 12, 2006, http://www.msnbc.msn.com/id/12289591/. Authorities accused the twenty-eight-year-old former teacher of issuing a cryptic message to the victim through the MySpace page by referring to him by his basketball jersey number, calling him her hero, and saying that she would not fall in love again for three years. *Id.*

121 Andrew Romano, *Walking a New Beat: Surfing MySpace.com Helps Cops Crack the Case*, NEWSWEEK, Apr. 24, 2006, at 48. The article also stated that MySpace assists police officers with 150 investigations per month and that the company's "20-member, 24/7 law-enforcement team fields 350 calls a week from its Rolodex of nearly 800 agencies." *Id.*

122 *Teen Arrested After Showing Handguns on Blog*, MSNBC.COM, Feb. 23, 2006, http://www.msnbc.msn.com/id/11514585/. Perhaps most disturbingly, one photo

their children home from school after the photos began circulating throughout the community.[123] Police arrested the boy at his home and charged him with three counts of juvenile possession of a handgun.[124]

Some people act as something akin to "MySpace vigilantes," using the site to ferret out potential sex abusers. For example, a group of boys in Fontana, California, created a fake profile of a fifteen-year-old girl on MySpace to cheer up a friend who had recently broken up with his girlfriend.[125] Before long, however, the "girl" was receiving messages from an adult male and the conversations began to have sexual overtones.[126] The older man also sent the "girl" his picture and made arrangements to meet at a local public park.[127] The group of boys went to the park, saw the man, and called the police.[128] When the police arrived, they arrested the forty-eight-year-old man for felony attempted lewd and lascivious conduct with a child and for an outstanding warrant.[129]

allegedly showed the boy lying on the floor surrounded by nine rifles with the caption, "Angel o' death on wings o' lead." *Id.* The parents' heightened concern after seeing the photos is certainly understandable, given that this case occurred in the same school district as Columbine High School, where a tragic 1999 high school shooting spree by two students claimed thirteen lives. *Id.*

123 *Id.*

124 *Id.* For a more recent example that hit closer to home for Oregon residents, see Jessica Bruder, *Student Detained After 'Killing Spree' Postings*, OREGONIAN, Feb. 16, 2008, at D1. The twenty-three-year-old student in question had posted statements on his MySpace profile including, "'Ave Maria' . . . would be my soundtrack for a killing spree," and, "It's getting harder to not just start shooting." *Id.* Although no charges have been filed in the case, police did revoke the student's concealed-handgun license. *Id.*

125 *Boys' MySpace Prank Results in Sex Crime Arrest*, MSNBC.COM, Mar. 8, 2006, http://www.msnbc.msn.com/id/11708746/.

126 *Id.*

127 *Id.*

128 *Id.*

129 *Id.* In this case, friends assumed an online identity through the creation of a fake MySpace profile in the hope that they could encourage one of their despondent peers. In at least one well-publicized case, however, the anonymity provided by MySpace allowed for harassment and ultimately led to a tragic consequence. *See* Steve Pokin, *Pokin Around: A Real Person, a Real Death*, ST. CHARLES J., Nov. 10, 2007, *available at* http://stcharlesjournal.stltoday.com/articles/2007/11/10/news/sj2tn20071110-1111stc_pokin_1.ii1.txt. Megan Meiers was a thirteen-year-old girl who lived outside St. Louis, Missouri. *Id.* After Megan had signed up for a MySpace account with a friend under a false name (ostensibly as a way to talk with boys online), her mother found out and deleted her profile. *Id.* As Megan's fourteenth birthday approached, she pleaded with her mother to allow her

Police officers, detectives, and self-appointed vigilantes are not the only ones patrolling online social-networking sites to catch wrongdoers. Principals and school administrators have also begun to realize that such sites can be effective tools for enforcing school-wide bans on smoking or drinking.[130] Some schools have also suspended athletes from participating in practices or games after photographs showing the athletes breaking team rules appeared on MySpace.[131]

While law-enforcement officers and school administrators have realized that social-networking sites can represent a treasure trove of evidence, at least two significant legal issues arise when the police begin to gather evidence from such sites. First, much of the evidence gathered online faces admissibility

to sign-up for MySpace again. *Id.* Her mother relented, but told Megan that she would carefully monitor all of her daughter's online activities. *Id.* To this end, Megan's mother kept the profile password secret and logged Megan on to MySpace upon request. *Id.* Megan met "Josh," a sixteen-year-old boy who was new to the area on MySpace and quickly added him to her friends list. *Id.* As Megan and Josh's friendship flourished, her self-esteem seemed to improve. *Id.* This changed abruptly, however, when Josh sent Megan a message saying that he did not want to be friends with her because he had heard that she was not nice to her friends. *Id.* According to Megan's father, Josh sent Megan a message through MySpace stating, "Everybody in [town] knows how you are. You are a bad person and everybody hates you. Have a [expletive] rest of your life. The world would be a better place without you." *Id.* Extremely distraught, Megan ran to her bedroom, and when her parents came to check on her twenty minutes later, they found that she had hung herself in the closet. *Id.* She was three weeks shy of her fourteenth birthday. *Id.* It turns out that "Josh" had been created by a mother of one of Megan's friends, purportedly to find out what was being said about her daughter online. *Id.* No charges were ever filed in the case. *Id.*; *see also* Christopher Maag, *A Hoax Turned Fatal Draws Anger but No Charges*, N.Y. TIMES, Nov. 28, 2007, at A23, *available at* http://www.nytimes.com/2007/11/28/us/28hoax.html.

130 *See* Maria Sacchetti, *To Catch Rule-Breakers, Schools Look Online*, BOSTON GLOBE, Dec. 22, 2006, at 1A.

131 *Id.*; *see also* Jane Gordon, *MySpace Draws a Questionable Crowd*, N.Y. TIMES, Feb. 26, 2006, at C14. *But see Cops Bust Teens' Root-Beer Kegger*, MSNBC.COM, Mar. 28, 2008, http://www.msnbc.msn.com/id/23851011/. In Wausau, Wisconsin, several members of sports teams from D.C. Everest High School had been suspended after school administrators saw photographs of the athletes drinking from red cups. *Id.* In order to show their displeasure with the suspensions, students staged a party complete with all of the requisite indicia of underage debauchery—a keg, drinking games, and cars lining the street outside of a packed house. *Id.* However, instead of beer, the keg was filled with "1919 Classic American Draft Root Beer," a fact that the police discovered after they administered nearly ninety breath tests to suspected underage drinkers. *Id.* A video of the incident has gained prominence on the popular site YouTube. *See* Police Bust High School Kegger, http://youtube.com/watch?v=vfQCE2917NE.

problems under the Federal Rules of Evidence. Second, because individual users' profiles may be considered their personal property, gathering evidence can implicate Fourth Amendment privacy protections.

C. The Tale of Detective Smith and Chris Jones: Evaluating the Admissibility of Evidence from Social Networking Sites

Suppose that Detective Smith of the Anytown Police Department reads an article in a law-enforcement magazine describing MySpace as a fertile ground for evidence gathering. Intrigued, Detective Smith signs up and logs onto MySpace using a pseudonym. During a slow day around the station, Detective Smith begins entering names of known offenders into MySpace's "search" function. After failing to find any user profiles for the first three names she enters, Detective Smith enters the name "Christopher Jones" into the search box. Detective Smith has a long history with "Chris" Jones, having investigated a crime spree several years ago that resulted in multiple felony convictions for Jones. After narrowing her search results to those within a fifty-mile radius of her postal zip code, Detective Smith locates what she believes is Jones's MySpace profile. Because Jones is a felon, Detective Smith is surprised to see several pictures on Jones's MySpace page[132] showing him brandishing multiple firearms in violation of his probation and local laws prohibiting felons from owning or possessing firearms.[133] Can Detective Smith use these photos as evidence in

[132] To further prove the point, suppose that the website address showing the photographs of Jones is http://www.myspace.com/ChrisJones420, so that there is little dispute that Jones is indeed the user who controls the page.

[133] Although the tale of Detective Smith and Chris Jones is a fiction included for illustrative purposes, it is not far from the truth. In the summer of 2007, after writing the first drafts of this Comment, the Author worked as a law clerk for the U.S. Attorney's Office in Eugene, Oregon. Agents from the Bureau of Alcohol, Tobacco, and Firearms ("ATF") contacted the Author for assistance investigating an individual who had posted several videos and photographs of himself holding and firing automatic weapons or "machine guns," which are closely regulated by federal law. The subject of the investigation, known by the online pseudonym "Crazy Kermie," had uploaded the materials onto his MySpace page and the online video host YouTube. Besides the digital photographs of various automatic weapons, he had posted videos showing large explosions of homemade bombs. A concerned citizen who came across the photos and videos while online alerted the ATF to the materials. The opinions contained in this Article, of course, are the author's alone and not necessarily reflective of the U.S. Department of Justice or the U.S. Attorney's Office.

a criminal case against Jones? There are at least two significant admissibility issues that arise when police officers gather evidence on social-networking sites such as MySpace and Facebook: authentication and the evidentiary rules' prohibition on hearsay.[134]

First, Detective Smith will have to overcome authentication issues. In general, evidence can be categorized into evidence that self-authenticates and evidence that requires authentication before it may be admitted. The basic rule is that "authentication or identification as a condition precedent to admissibility is satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims."[135] For self-authenticating exhibits, Rule 902 provides that "[e]xtrinsic evidence of authenticity as a condition precedent to admissibility is not required."[136] Self-authenticating exhibits generally fall into one of the enumerated categories set forth in Rule 902.[137] Based on the specific nature of the self-authenticating exhibits listed in Rule 902, it seems unlikely that evidence gathered on social-networking sites could be described as self-authenticating.

---

134 A third admissibility issue that may be implicated with these situations is the Best Evidence Doctrine, which is covered by Federal Rules of Evidence 1001–08 and requires, in the most simple terms, that the contents of a writing be proven by the writing itself. Although this situation is likely to be implicated only in very narrow factual situations with respect to evidence gathered on social-networking sites, the Federal Rules of Evidence expressly address the issue by stating that "[i]f data are stored in a computer or similar device, any printout or other output readable by sight, shown to reflect the data accurately, is an 'original.'" FED. R. EVID. 1001(3). *See also* Doe v. United States, 805 F. Supp. 1513, 1517 (D. Haw. 1992) (stating that "[t]he best evidence rule applies where a party attempts to introduce evidence to prove what the contents of a document are, and is more properly thought of as an original document rule").

135 FED. R. EVID. 901(a) (the evidence must be "sufficient to support a finding that the [evidence] in question is what its proponent claims"); *see also* United States v. Simpson, 152 F.3d 1241, 1250 (10th Cir. 1998) (allowing for the admission of a computer printout of a chat-room discussion between the defendant and a detective, even over the defendant's objection that the evidence was not authenticated because the government could not prove that the statements were attributable to the defendant through "handwriting, writing style, or his voice").

Some of the acceptable bases for authentication under Rule 901(b) include: (1) testimony of witness with knowledge, (2) nonexpert opinion on handwriting, (3) comparison by the trier or an expert witness, and (4) distinctive characteristics. FED R. EVID. 901(b).

136 FED. R. EVID. 902.

137 Some of the self-authenticating items enumerated in Rule 902 include: (1) domestic public documents under seal, (2) domestic public documents not under seal, (3) foreign public documents, and (4) certified copies of public records. *Id.*

Further, any such evidence would likely be lacking the indicia of reliability that characterize the self-authenticating items listed in Rule 902. The Fontana, California, youths who created a profile by posing as a teenage girl provide a clear example of MySpace users' ability to adopt fake identities.[138] Because evidence gathered on social-networking sites would not be self-authenticating, the question becomes whether Detective Smith can authenticate the evidence under any of the methods set forth in Rule 901.[139]

Second, Detective Smith will have to overcome the Rules' prohibition on hearsay. Suppose that Detective Smith is reading the "comments" section of Chris Jones's MySpace page when she finds that a friend has written, "I had fun grabbing the $5K of 'lettuce' from the Main Street 'grocery store' with you last October. Ha Ha!" This information corresponds with an unsolved bank robbery that occurred last October. Detective Smith and the district attorney prosecuting the case will need to overcome the Rules' prohibition on hearsay in order to admit this evidence in a criminal case against Jones.

Under the Federal Rules of Evidence, hearsay is an out-of-court statement, made by a party other than the declarant while testifying at trial, offered to prove the truth of the matter asserted.[140] Rule 801(a) defines a statement as "(1) an oral or written assertion or (2) nonverbal conduct of a person, if it is intended by the person as an assertion."[141] Rule 802 bluntly states that hearsay is not admissible except when provided by the Rules.[142] In the hypothetical case of Detective Smith and Chris

138 *See supra* notes 125–29 and accompanying text.

139 *See* Orin S. Kerr, *Computer Records and the Federal Rules of Evidence*, U.S. ATTORNEYS' USA BULL., Mar. 2001, at 25, 26, *available at* http://www.usdoj.gov/usao/eousa/foia_reading_room/usab4902.pdf ("The standard for authenticating computer records is the same as for authenticating other records. The degree of authentication does not vary simply because a record happens to be (or has been at one point) in electronic form." (footnote omitted)). *But see* United States v. Scholle, 553 F.2d 1109, 1125 (8th Cir. 1982) (stating in dicta that "the complex nature of computer storage calls for a more comprehensive foundation").

140 FED. R. EVID. 801.

141 FED. R. EVID. 801(a).

142 FED. R. EVID. 802. In an oft-quoted passage, Professor Wigmore characterized the rule against hearsay as "that most characteristic rule of the Anglo-American law of evidence—a rule which may be esteemed, next to jury trial, the greatest contribution of that eminently practical legal system to the world's

Jones, any statements or photos posted online will likely be inadmissible hearsay.[143] To use the MySpace evidence, a valid hearsay exception will have to apply.

Rules 803 to 807 contain the exceptions to the hearsay rule, and determining which exception to apply first requires an inquiry into whether a hearsay declarant is available or unavailable to testify under oath and in the face of "the greatest legal engine ever invented for the discovery of truth":[144] cross-examination. Rule 803 provides twenty-three enumerated exceptions to the bar on hearsay when the declarant is available as a witness;[145] however, none seem to provide sufficient grounds for admitting evidence gathered on a social-networking site.[146]

Perhaps the strongest basis for admission is found in Rule 803(21), which allows for hearsay when it reflects on the "[r]eputation of a person's character among associates or in the community."[147] Rule 804 provides hearsay exceptions for those situations where the declarant is unavailable,[148] but such

jurisprudence of procedure." John H. Wigmore, *The History of the Hearsay Rule*, 17 HARV. L. REV. 437, 458 (1904).

143 If Jones had authored the statement about "grabbing $5K of lettuce," it may have been admissible as an admission of a party-opponent. Similarly, if Detective Smith wished to introduce emails or messages authored by Jones and sent through MySpace's mail service, these messages may be admissible as nonhearsay admissions or adopted admissions under Rule 801(d)(2). *See* Sea-Land Serv. Inc. v. Lozen Int'l, 285 F.3d 808, 821 (9th Cir. 2002); Luehr, *supra* note 21, at 21.

144 Coleman v. Southwick, 9 Johns. 50 (N.Y. 1812).

145 Examples include present-sense impression, FED. R. EVID. 803(1); excited utterances, FED. R. EVID. 803(2); statements of then existing mental, emotional, or physical condition, FED. R. EVID. 803(3); and statements made for purposes of medical diagnosis or treatment, FED. R. EVID. 803(4).

146 Although no hearsay exception clearly applies to content gathered on social-networking websites, a creative lawyer may try to argue that the evidence could fall within the business-records exception. This exception is more pliable than most realize, as the term "business" includes "business, institution, association, profession, occupation, and calling of every kind, whether or not conducted for profit." FED. R. EVID. 803(6). Courts will generally admit computer records if they were kept pursuant to a routine procedure for motives that tend to assure their accuracy. *But see* United States v. Jackson, 208 F.3d 633 (7th Cir. 2000) (holding that postings by a white-supremacist group on a website were hearsay and could not be admitted as business records of the Internet service providers that hosted the sites).

147 FED. R. EVID. 803(21).

148 Rule 804(a) defines when a witness is considered to be "unavailable." *See* FED. R. EVID. 804(a).

exceptions, which include former testimony,[149] statements made under the belief of impending death,[150] statements against pecuniary interests,[151] and statements of personal or family history,[152] also do not provide satisfactory grounds for the evidence Detective Smith has gleaned from her visits to Jones's MySpace page. Perhaps the last resort is Rule 807, the residual or "catch-all" exception to the hearsay rule.[153] Such evidence, however, may be barred by Rule 807's requirement that such exhibits be characterized by "equivalent circumstantial guarantees of trustworthiness,"[154] a trait that seems lacking in evidence gathered on social-networking sites. However, courts have seemed more amenable to the application of the residual hearsay exception in recent times,[155] so even without the "guarantees of trustworthiness," Rule 807 seems to provide the strongest basis for admission of this type of evidence.

It is beyond the scope and purpose of this Comment to provide conclusive answers to the authentication and hearsay questions posed by the fictitious allegory of Detective Smith and Chris Jones. Rather, the goal is merely to illuminate the evidentiary admissibility issues that may arise when "point-and-

149 FED. R. EVID. 804(b)(1).

150 FED. R. EVID. 804(b)(2).

151 FED. R. EVID. 804(b)(3).

152 FED. R. EVID. 804(b)(4).

153 FED. R. EVID. 807.

154 *Id.*

155 *See, e.g.*, United States v. Laster, 258 F.3d 525, 529–30 (6th Cir. 2001), *cert. denied*, 122 S. Ct. 1116 (2002). In *Laster*, the Sixth Circuit affirmed the district court's decision to admit evidence under Rule 807 "if it is 'material,' 'more probative on the point for which it is offered than any other evidence which the proponent can procure through reasonable efforts,' and its admission best serves the interest of justice." *Id.* at 530 (quoting FED. R. EVID. 807); *see also* Randolph N. Jonakait, *The Subversion of the Hearsay Rule: The Residual Hearsay Exceptions, Circumstantial Guarantees of Trustworthiness, and Grand Jury Testimony*, 36 CASE W. RES. L. REV. 431, 445–62 (1986) (concluding that the Fourth Circuit has stretched the boundaries of specific exceptions by resorting to the residual exception); Myrna S. Raeder, Commentary, *A Response to Professor Swift: The Hearsay Rule at Work: Has It Been Abolished De Facto by Judicial Discretion?*, 76 MINN. L. REV. 507, 514–19 (1992) (stating that the hearsay rule is being eroded by judicial discretion through use of the catchall exceptions); Faust F. Rossi, *The Silent Revolution*, LITIG., Winter 1983, at 13, 13–17 (stating that courts are now routinely admitting probative hearsay through the application of the catchall provisions of the Federal Rules of Evidence).

click" police officers begin working the cyber beat to gather evidence of criminal activity.[156]

D. Pleading the Fourth: Privacy Concerns over Evidence Gathering Online

More than a century ago, Justice Brandeis argued that the progress of science, especially in the area of communication technology, requires that the focus shift from the letter to the spirit of the law to protect the individual from privacy invasions.[157] This argument still rings true today. More recently, the Supreme Court has admitted that "[t]he law, though jealous of individual privacy, has not kept pace with these advances in scientific knowledge."[158] Modern privacy law holds that a reasonable expectation of privacy in a communication medium is a condition precedent to investing it with Fourth Amendment protection.[159] In the context of social-networking web sites, the question becomes whether people have a reasonable expectation

156 Interestingly enough, the Federal Rules of Evidence have also taken notice of the challenges of electronic discovery, and the proposed Rule 502 is aimed at reducing the cost of electronic discovery. However, at least one commentator has argued that the proposed rule is duplicative and "the cost and burden of electronic discovery will persist." Dimo Michailov, *Proposed FRE 502 Is Good for Electronic Discovery, but It Is Not Going to Drastically Reduce the Cost of Litigation as the Authors Are Hoping*, Dec. 16, 2007, http://www.cybercrimelaw.org/2007/12/16/proposed-fre-502-is-good-for-electronic-discovery-but-it-is-not-going-to-drastically-reduce-the-cost-of-litigation-as-the-authors-are-hoping/.

157 Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 196 (1890).

158 Berger v. New York, 388 U.S. 41, 49 (1967); *see also* Olmstead v. United States, 277 U.S. 438, 479 (1928) (Brandeis, J., dissenting).

> Experience should teach us to be most on our guard to protect liberty when the government's purposes are beneficent. Men born to freedom are naturally alert to repel invasion of their liberty by evil-minded rulers. The greatest dangers to liberty lurk in insidious encroachment by men of zeal, well-meaning but without understanding.

Id.

159 Katz v. United States, 389 U.S. 347, 360–61 (1967) (Harlan, J., concurring). Justice Harlan's concurrence in *Katz* set forth the modern two-part test for privacy intrusions. First, the individual alleging the privacy violation must have had a subjective expectation of privacy, and second, this expectation must be one that society is "prepared to recognize as 'reasonable.'" *Id.* at 361. A court confronting this question would be faced with an interesting and novel issue as it attempted to answer the second question. As the use of social-networking web sites become more widespread, it seems likely that society would find a reasonable expectation of privacy in one's personal "space" on the Internet.

of privacy for the information they post to their individual profiles. To answer this question, we must consider two variables: (1) whether there is a reasonable expectation of privacy on a personal web site accessible by anyone, and (2) whether there is a reasonable expectation of privacy on a personal web site that has been secured by some form of privacy protection.[160] For the following reasons, the former presents a relatively easy answer that there is no reasonable expectation of privacy for information posted on one's personal web site, while the latter involves a more nuanced analysis that fails to reveal a clear answer.

Because social-networking sites are of a relatively recent vintage, analyzing the impact on individual privacy rights when law enforcement gathers evidence online requires analogies to other situations that have come before the courts.[161] *Katz v. United States*,[162] where the Court found that the warrantless wiretapping of standard landline telephones constituted an unreasonable search, is generally considered the leading case in modern privacy law.[163] Relying on *Katz*, the Court has frequently taken the position that the mere possibility of exposure to the public eye diminishes and sometimes obviates one's privacy expectation.[164] Given this, it seems likely that

160 MySpace and other social-networking sites offer users several levels of privacy protections. When a user does not elect to apply these protections, anyone with an Internet connection can view that user's photos, videos, blogs, and other limited personal information. Users who apply protections generally must "approve" those who are seeking to view their page or may require visitors to enter in some form of a password such as the user's last name or email address.

161 *See generally* Kyllo v. United States, 533 U.S. 27, 33–34 (2001) ("It would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology."); Lopez v. United States, 373 U.S. 427, 441 (1963) (C.J. Warren, concurring) (noting that "the fantastic advances in the field of electronic communication constitute a great danger to the privacy of the individual; . . . indiscriminate use of such devices in law enforcement raises grave constitutional questions under the Fourth and Fifth Amendments").

162 *Katz*, 389 U.S. at 352 (recognizing a reasonable expectation of privacy in "the words [one] utters into the mouthpiece" of a telephone in an enclosed booth).

163 *See, e.g.*, *Kyllo*, 533 U.S. at 32–35 (discussing the *Katz* test, its application to various factual situations, and offering a rejoinder to some of the test's critics).

164 *Katz*, 389 U.S. at 351 (noting that "[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection" (quoting California v. Ciraolo, 476 U.S. 207, 213 (1986)); *see also* Kee v. City of Rowlett, 247 F.3d 206, 217 (5th Cir. 2001) (finding no reasonable expectation of privacy at a memorial service where investigators had placed a

courts would not find a reasonable expectation of privacy where someone places photographs or other personal information on a social-networking site that could be accessed by anyone.

More difficult questions arise, however, when a personal web site is protected by a password. If by locking a container one creates a reasonable expectation of privacy in its contents,[165] does it follow that by "locking" access to one's web site one creates an expectation of privacy?[166] May confidential informants, government or private investigators, or defense attorneys gather evidence from a MySpace profile by posing as an "approved friend?"[167] A similar issue is whether a law-

recording device in a funeral urn); United States v. Longoria, 177 F.3d 1179, 1182 (10th Cir. 1999) (finding no Fourth Amendment protection where the defendant knowingly exposed inculpatory information); United States v. Padin, 787 F.2d 1071, 1076 (6th Cir. 1986) (concluding that defendant, who telephoned his own home, had no "subjective expectation of privacy in the incriminating telephone conversation" he unwittingly had with police officers).

165 *See* United States v. Jacobsen, 466 U.S. 109, 114 (1984) ("Letters and other sealed packages are in the general class of effects in which the public at large has a legitimate expectation of privacy; warrantless searches of such effects are presumptively unreasonable."); *Ex parte* Jackson, 96 U.S. 727, 733 (1877) ("Letters and sealed packages . . . in the mail are as fully guarded from examination and inspection, except as to their outward form and weight, as if they were retained by the parties forwarding them in their own domiciles.").

166 *See generally* Lieutenant Colonel LeEllen Coacher, *Permitting Systems Protection Monitoring: When the Government Can Look and What It Can See*, 46 A.F. L. REV. 155 (1999) (describing, in part, the Fourth Amendment issues that arise in the context of systems protection monitoring); Chris J. Katopis, *"Searching" Cyberspace: The Fourth Amendment and Electronic Mail*, 14 TEMP. ENVTL. L & TECH. J. 175 (1995); Orin S. Kerr, *The Fourth Amendment in Cyberspace: Can Encryption Create a "Reasonable Expectation of Privacy?"*, 33 CONN. L. REV. 503 (2001).

167 *See, e.g.*, Stephanie Francis Ward, *MySpace Discovery*, A.B.A. J., Jan. 2007, at 34. The article describes how Eugene, Oregon, lawyer Laura Fine found evidence on MySpace when representing a teenager accused of forcible rape. *See id.* The alleged victim had told police that she would never willingly have had sex, but Fine came to a different conclusion after viewing the girl's MySpace page. *Id.* The page "displayed provocative photos of the young woman . . . and a lascivious screen name." *Id.* Although the page was meant to be private, Fine viewed it over the shoulder of another witness, who gained access through a MySpace group that he and the girl belonged to. *Id.* Based on what she saw on MySpace, Fine had a sense of how the young woman would present to the grand jury. *Id.* After hearing the girl's testimony, the grand jury dismissed the charges. *Id.*

But see Gouled v. United States, 255 U.S. 298 (1921). In *Gouled*, a private in the U.S. Army pretended to make a friendly visit to the defendant. *Id.* at 304. While the defendant was not present, and without an authorizing warrant, the Army private seized and took with him several documents belonging to the defendant. *Id.* These documents were later turned over to the U.S. Attorney as evidence. *Id.* The

enforcement officer could log onto a MySpace page to gather evidence as a warrantless search incident to arrest by invoking either of the twin rationales of *Chimel v. California*.[168] As with the evidentiary issues raised by the hypothetical of Detective Smith and Chris Jones, it is beyond the purview of this Comment to fully discuss and resolve these questions. For purposes of identifying problems with evidence gathering on social networking sites, it is enough to recognize the issues.

III
HINDSIGHT IS ALWAYS 20/20: APPLYING THE LESSONS OF THE PAST TO THE CHALLENGES OF THE FUTURE

This Comment has thus far traced the history of e-discovery and the development of new rules and described the challenges that arise when law-enforcement agencies gather evidence online. It now turns to applying the lessons of the past to the emerging practice of gathering evidence on social-networking web sites. As the experience of e-discovery reveals, there are three distinct steps in the evolution of an unsettled area of the law: first, there are unsuccessful attempts to apply traditional legal rules to new challenges; second, innovative judge-made law provides short-term answers, but those answers lack uniformity across jurisdictions; and third, federal law codifies judge-made law through revision and promulgation of new Federal Rules of Civil Procedure.[169] In addressing evidence gathering on social-networking sites, the law is currently positioned somewhere between the first and second steps in the process.

---

defendant did not realize the documents had been surreptitiously taken until the Army private took the stand and testified about how he had procured them. *Id.* at 304–05. The court held the seizure of the documents to be a violation of the Fourth Amendment; thus, the documents' admission was improper. *Id.* at 309–10, 312–13.

168 Chimel v. California, 395 U.S. 752 (1969). The well-known "twin rationales of *Chimel*" are (1) officer safety, and (2) preservation of evidence. *See id.* at 763. In *United States v. Reyes*, the court upheld a warrantless search of a wireless pager that could receive "numerical codes that could be interpreted as coded messages" as a container search incident to a valid arrest. United States v. Reyes, 922 F. Supp. 818, 832 (S.D.N.Y. 1996). Some have argued, however, that the exception under *Chimel* allowing evidence obtained in a warrantless search is inapplicable in this situation because a pager, unlike a closed box, cannot be used to hide a dangerous instrument or deadly weapon. *See, e.g.*, Megan Connor Bertron, *Home Is Where Your Modem Is: An Appropriate Application of Search and Seizure Law to Electronic Mail*, 34 AM. CRIM. L. REV. 163, 179–92 (1996).

169 *See supra* Part I.B.

By drawing upon both the successes and failures in the history of e-discovery, the legal community can expedite the process by which this recent development is defined and standardized. Specifically, the legal community must understand and apply two important lessons. First, the onus is on the courts to clearly define the scope of permissible use for such evidence. The experience of e-discovery, and particularly the failure of the revised Federal Rules of Civil Procedure to address the significant issue of metadata,[170] shows that the lack of precise definitions can create loopholes. Such loopholes are generally closed only after extensive litigation or subsequent revisions to the Rules. In the context of evidence gathered on social-networking web sites, these definitions must include the appropriate parameters for usage. That is, the definitions must specify which types of evidence may be obtained: written statements in a blog, photographs, videos, or communications directed solely toward a third party. Further, courts must consider whether evidence may be gathered against a party by searching other third-party social-networking sites, or if such practices should be cabined to allow evidence gathering only on the specific user's profile.

Second, courts must develop innovative and practical tests or factors to analyze the circumstances under which evidence gathered online might be admissible. For example, the decisions in *Rowe Entertainment* and *Zubulake* are essentially based on the touchstone concept of proportionality embodied in the Federal Rules of Civil Procedure. The Federal Rules of Evidence also reflect a concern for proportionality between prejudice and probative value.[171] Likewise, the Fourth Amendment requires a balance between personal privacy interests and the legitimate law-enforcement purposes of the state.[172] Any evaluative factors for deciding whether evidence

170 *See supra* note 87 and accompanying text.

171 *See* FED. R. EVID. 403 ("Although relevant, evidence may be excluded if its probative value is substantially outweighed by the danger of unfair prejudice, confusion of the issues, or misleading the jury, or by considerations of undue delay, waste of time, or needless presentation of cumulative evidence.").

172 *See* Berger v. New York, 388 U.S. 41, 60–63 (1967) (describing the importance of electronic eavesdropping to law enforcement, but ultimately concluding that "it is not asking too much that officers be required to comply with the basic command of the Fourth Amendment before the innermost secrets of one's home or office are invaded").

gathered on social-networking web sites may be used in a criminal case must similarly reflect this concern for proportionality.

Some factors that courts should consider in developing such analyses include: (1) whether the personal web site is protected by a password or other form of privacy protection; (2) whether the affected party might have had a reasonable expectation of privacy even if no password protection was applied; (3) whether the police had a reasonable suspicion or probable cause to investigate the social-networking site or whether the evidence was gleaned through an evidentiary "fishing expedition"; (4) whether the evidence is accompanied by some indicia of reliability; (5) whether the police have the ability to gather the evidence through other means; (6) whether the probative value is substantially outweighed by the prejudicial effect of the evidence; and (7) the "strength" of the evidence, that is, the potential nexus between the alleged criminal activity and the evidence gathered.

Some argue that there is a greater need for uniformity in procedural rules than in the legal issues surrounding evidence gathered on social-networking sites. While there is truth in such a proposition, law-enforcement agencies' increasingly widespread use of social-networking sites to gather evidence also justifies the creation of clear, standardized rules. As the use of these sites continues to grow, it would be wise for the courts to proactively engage this issue before a jurisdictional "patchwork quilt" of rules results.

CONCLUSION

The evolution of e-discovery teaches that the application of traditional legal rules to novel challenges can be ineffective. For many years, judges attempted to apply the established discovery procedures to e-discovery requests with only limited success. Meaningful change occurred only after several innovative judges began to clearly define the issues and develop practical tests. While these tests certainly represented a new level of understanding in terms of the unique characteristics of electronically stored information, the unpredictable nature of ad hoc rule making on a case-by-case basis is ineffective over the long term. Realizing this, the Advisory Committee on Civil

Rules undertook the challenge of standardizing this unsettled area of the law. The result is a less-than-perfect but nonetheless helpful set of revisions to the Federal Rules of Civil Procedure that reflect the unique characteristics of electronically stored information.

The recent trend toward gathering evidence on social-networking sites presents the law with a new set of challenges. Such practices implicate difficult questions of evidence admissibility as well as privacy. The time is ripe for judges and rule makers to recognize this development and to define the scope of permissible use and develop practical tests that will provide guidance to lawyers, law-enforcement agencies, and the public.

These unprecedented issues require broader thinking—thinking by judges, rule makers, and practitioners that transcends merely trying to "fit a square peg into a round hole." By learning from both the successes and failures of the past and applying these lessons to future challenges, the legal profession can develop innovative principles that effectively address the unique characteristics of technological advances such as social-networking sites.