THE YALE LAW JOURNAL

COMMENT

The New Electronic Discovery Rules: A Place for Employee Privacy?

In 2002, the world's computer users generated approximately five exabytes of data, the informational equivalent of a half a million libraries the size of the Library of Congress. Ninety-two percent of that new information was stored magnetically.[1] Since then, our appetite for electronic information, and for hardware that can store greater amounts of it, has grown exponentially.

The law has struggled to keep pace with the proliferation and stockpiling of electronic data. In particular, this trend has placed severe strains on the existing framework for discovery, prompting the Civil Rules Advisory Committee of the U.S. Judicial Conference to recommend amendments to the Federal Rules of Civil Procedure. As the Advisory Committee has acknowledged, the traditional paper rules cannot simply be stretched to deal with unprecedented problems such as the automatic creation of metadata, the retrieval of "deleted" data, and, most urgently, the sheer volume of electronic information.[2]

A package of proposed amendments on electronic discovery, or "e-discovery," has recently been approved by the Judicial Conference and now awaits consideration by the U.S. Supreme Court. Although the amendment process appears to be in the final stages, it will be some time before the new rules go into effect.[3] Meanwhile, courts continue to formulate their own e-

1. PETER LYMAN ET AL., SCH. OF INFO. MGMT. & SYS., UNIV. OF CAL. AT BERKELEY, HOW MUCH INFORMATION? 2003 (2003), http://www.sims.berkeley.edu:8000/research/projects/how-much-info-2003/printable_report.pdf.

2. *See* REPORT OF THE CIVIL RULES ADVISORY COMMITTEE 40 (amended July 25, 2005), *reprinted in* COMM. ON THE RULES OF PRACTICE & PROCEDURE OF THE JUDICIAL CONFERENCE OF THE U.S., SUMMARY OF COMMITTEE ON RULES OF PRACTICE AND PROCEDURE: AGENDA E-18 app. C (Sept. 2005) [hereinafter PROPOSED AMENDMENTS].

3. If the Court promulgates the proposed amendments by May 1, 2006, the new rules will take effect on December 1, 2006, unless Congress enacts legislation to reject, modify, or defer the

discovery rules. One recent case, *Zubulake v. UBS Warburg LLC*,[4] has intensified corporations' anxiety about their e-discovery obligations. In this employment discrimination case, the district court treated data stored on magnetic backup tapes as broadly discoverable, eventually instructing the jury that it could infer bad faith on the part of the corporation for its e-discovery failures.[5]

While *Zubulake* and recent commentary on e-discovery have emphasized balancing the interests of the litigants, this Comment shifts the focus to the collateral effects that e-discovery may have on everyday employment relations. Specifically, this Comment contends that the e-discovery framework offered by *Zubulake* increases incentives for employers to implement intrusive forms of electronic surveillance. While the Judicial Conference's proposed rules may reduce these incentives indirectly by easing the discovery burdens on employers, courts applying the new rules can and should engage the issue of employee privacy directly. This Comment suggests how courts can shape e-discovery procedures to discourage the abuse of surveillance technologies and protect privacy in the workplace.

I. THE *ZUBULAKE* STANDARD

In *Zubulake*, a former employee sued UBS Warburg for gender discrimination and illegal retaliation. During the discovery phase, the plaintiff requested "[a]ll documents concerning any communication by or between UBS employees concerning Plaintiff," including internal e-mails stored on the firm's active and archived media.[6] The court took the discoverability of the disaster recovery tapes as given,[7] but ordered a sample restoration of five tapes to assess the cost of producing all the relevant data. It was only later, when ruling on UBS's cost-shifting motion, that the court gave special consideration to the

rules. *See* U.S. Courts, Federal Rulemaking, http://www.uscourts.gov/rules/#judicial0905 (last visited Oct. 2, 2005); *see also* 28 U.S.C. § 2074 (2000).

4. Zubulake v. UBS Warburg LLC (*Zubulake I*), 217 F.R.D. 309 (S.D.N.Y. 2003); Zubulake v. UBS Warburg LLC (*Zubulake III*), 216 F.R.D. 280 (S.D.N.Y. 2003); Zubulake v. UBS Warburg LLC (*Zubulake IV*), 220 F.R.D. 212 (S.D.N.Y. 2003); Zubulake v. UBS Warburg LLC (*Zubulake V*), 229 F.R.D. 422 (S.D.N.Y. 2004).

5. *Zubulake V*, 229 F.R.D. at 436-37.

6. *Zubulake I*, 217 F.R.D. at 312.

7. *Id.* at 317 ("Thus, '[e]lectronic documents are no less subject to disclosure than paper records.' This is true not only of electronic documents that are currently in use, but also of documents that may have been deleted and now reside only on backup disks." (quoting Rowe Entm't, Inc. v. William Morris Agency, Inc., 205 F.R.D. 421, 428 (S.D.N.Y. 2002))).

inaccessible nature of the requested information.[8] As part of a multifactor cost-shifting test, the court analyzed whether the plaintiff's request for inaccessible data was specifically tailored to discover relevant information and whether the information was available from more accessible sources.[9] Evaluating sixty-eight e-mails from the sample production that the plaintiff had pinpointed as "highly relevant to the issues," the court concluded that the sample restoration sufficiently "demonstrated that Zubulake's discovery request was narrowly tailored,"[10] while admitting that it was "speculative" that the backup tapes contained the smoking-gun email that Zubulake sought.[11] The court eventually ordered UBS to restore and produce the remaining tapes and to bear seventy-five percent of the production costs.[12]

In subsequent rulings in the case, the court turned its attention to whether UBS had committed spoliation—the destruction of discoverable evidence. Restoration of the backup tapes revealed that key players had deleted relevant e-mails from their computers after the lawsuit was filed. Furthermore, UBS had recycled some tapes in violation of its retention policy, and UBS's counsel had failed to inform two employees to turn over responsive e-mails stored in their active files.[13] Although the corporation's failures were arguably only negligent,[14] the court found that the employees' deletions of e-mails had been willful and granted the plaintiff's motion for an adverse inference instruction to

8. *Zubulake I*, 217 F.R.D. at 324 ("A court should consider cost-shifting *only* when electronic data is relatively inaccessible, such as in backup tapes."). Under *Zubulake*, data is inaccessible if some process, such as restoration or reconstruction, is necessary to render the information humanly intelligible. *Id.* at 320.

9. These are the two most important factors in *Zubulake*'s seven-part cost-shifting test. *See Zubulake III*, 216 F.R.D. at 284. The other factors are:

> the total cost of production, compared to the amount in controversy; the total cost of production, compared to the resources available to each party; the relative ability of each party to control costs and its incentive to do so; the importance of the issues at stake in the litigation; and the relative benefits to the parties of obtaining the information.

Id.

10. *Id.* at 285-87 (internal quotation marks omitted).

11. *Id.* at 286-87.

12. *Id.* at 291.

13. *Zubulake V*, 229 F.R.D. at 426-30.

14. *Zubulake IV*, 220 F.R.D. at 220-21.

the jury.[15] Ultimately, the jury awarded the plaintiff $9.1 million in compensatory damages and $20.1 million in punitive damages.[16]

II. *ZUBULAKE* AND EMPLOYEE PRIVACY

Zubulake has had an impact far beyond the Southern District of New York, influencing courts in other jurisdictions[17] and alarming corporations (and their counsel) across the country.[18] *Zubulake* poignantly demonstrates that a court can order the production of old disaster recovery tapes even if no one knows exactly what they contain. Given the broad relevance standard of the Federal Rules, the scope of discoverable evidence may encompass hundreds, even thousands, of difficult-to-restore tapes.[19] Moreover, under *Zubulake*, a corporation may face stiff sanctions if it inadvertently recycles a tape that a court later decides should have been preserved, or if employees delete relevant e-mails despite corporate counsel's reasonable care to enforce a litigation-hold.[20] Multiply these costs by the number of lawsuits a corporation faces every year, and e-discovery could wind up dictating the outcome in many instances, as companies choose to settle rather than face extensive e-discovery costs.[21]

---

15. *Zubulake V*, 229 F.R.D. at 436.

16. *See* Eduardo Porter, *UBS Ordered To Pay $29 Million in Sex Bias Lawsuit*, N.Y. TIMES, Apr. 7, 2005, at C4.

17. *See, e.g.*, Wiginton v. CB Richard Ellis, Inc., 229 F.R.D. 108 (N.D. Ill. 2004); OpenTV v. Liberate Techs., 219 F.R.D. 474 (N.D. Cal. 2003).

18. *See* Wendy Davis, *The* Zubulake *Road Show: Lawyers Are Traveling to Conferences, Companies To Explain E-Discovery Opinions*, 91 A.B.A. J. 22 (2005) ("[*Zubulake*] has lawyers across the country hitting the road to lecture corporations, speak on panels and reassure skittish clients."); David W. Garland & William R. Horwitz, *Avoiding Sanctions in Electronic Discovery*, METROPOLITAN CORP. COUNS., Oct. 2004, at 18.

19. The process of restoring and searching through tapes, removing duplicates, and conducting privilege review can be extremely expensive. *See* McPeek v. Ashcroft, 212 F.R.D. 33, 35 (D.D.C. 2003) ("The frustration of electronic discovery as it relates to backup tapes is that backup tapes collect information indiscriminately, regardless of topic. One, therefore, cannot reasonably predict that information is likely to be on a particular tape."); Medtronic Sofamor Danek, Inc. v. Michelson, 229 F.R.D. 550, 557-58 (W.D. Tenn. 2003) (noting that it could cost "several million" dollars for Medtronic to search through 996 backup tapes and an additional $16.5 to $70 million to conduct privilege review).

20. *See Zubulake V*, 229 F.R.D. at 435; *see also* Thomas Y. Allman, *Ruling Offers Lessons for Counsel on Electronic Discovery Abuse* 2 (Wash. Legal Found., Legal Backgrounder Vol. 19, No. 34, 2004) http://www.wlf.org/upload/101504LBAllman.pdf (arguing that "[t]here is no room for error, carelessness or preoccupation with other responsibilities in this regard").

21. *See Conference on Electronic Discovery: Panel Four: Rule 37 and/or a New Rule 34.1: Safe Harbors for E-Document Preservation and Sanctions*, 73 FORDHAM L. REV. 71, 77 (2004)

In short, by combining a low bar for the discoverability of inaccessible data with the possibility of severe sanctions for negligent destruction, the *Zubulake* framework places a heavy burden on employers with large information systems. Systematic electronic surveillance thus becomes an attractive option, because it enables employers to (1) keep employees from using company networks for personal reasons, thereby reducing the amount of data captured on backup tapes; (2) detect improper employee behavior before a lawsuit is lodged against the company; and (3) prevent key players from erasing evidence from their computers once litigation is anticipated. With *Zubulake* on the books, and increasingly sophisticated surveillance technologies flooding the market, employee privacy is in serious jeopardy.[22]

But why should we care about employee privacy? Private-sector employees have neither a federal constitutional right nor a statutory right to privacy in the workplace. Under the Electronic Communications Privacy Act[23] and the law of most states, a private employer may freely monitor employees' electronic activities when they are using firm property, so long as the employer has some plausible business justification, such as enhancing worker productivity.[24]

The fact remains, however, that many employees continue to hold onto a subjective expectation of privacy, at least with regard to extreme intrusions. Evidence of this subjective expectation can be found in studies showing that workers who are aware of constant surveillance exhibit higher levels of anxiety and fatigue.[25] These studies also indicate that surveillance may lower worker productivity, spawning widespread dissatisfaction and increasing the corporation's liability exposure. For example, if management intercepts or retrieves sexually harassing e-mails but fails to take steps to ameliorate the situation, the corporation could be held liable for tolerating a hostile work

(quoting Laura Lewis Bird, Partner, Alston & Bird LLP, stating that a corporation may need to budget $500,000 for electronic retention and retrieval for a case worth that dollar amount).

22. AM. MGMT. ASS'N, 2001 AMA SURVEY: WORKPLACE MONITORING & SURVEILLANCE: SUMMARY OF KEY FINDINGS 1 (2001), http://www.amanet.org/research/pdfs/ems_short2001.pdf (reporting that, as of 2001, 36.1% of firms monitor computer files, and 46.5% monitor e-mails).

23. 18 U.S.C. §§ 2511-2520, 2701-2707 (2000).

24. *See, e.g.*, Smyth v. Pillsbury Co., 914 F. Supp. 97 (E.D. Pa. 1996) (applying Pennsylvania law); McLaren v. Microsoft Corp., No. 05-97-00824-CV, 1999 WL 339015 (Tex. App. May 28, 1999).

25. *See, e.g.*, NAT'L WORKRIGHTS INST., PRIVACY UNDER SIEGE: ELECTRONIC MONITORING IN THE WORKPLACE 5 (2004), http://www.workrights.org/issue_electronic/NWI_EM_Report.pdf.

environment.[26] Thus, while corporations may have previously believed that spot checks or searches based on individual suspicion were sufficient to meet legal and business requirements and that the higher expenses and lower employee morale associated with continuous surveillance outweighed any additional benefits,[27] *Zubulake* has altered this balance.

III. THE NEW E-DISCOVERY RULES

The adoption of the new e-discovery rules provides an opportunity to recalibrate the balance between employers' interests in reducing their e-discovery burdens and employees' interests in protecting against invasive forms of surveillance. The proposed rules offer two features designed to alleviate e-discovery burdens: (1) a two-tier structure of discoverability, with different procedures for accessible and inaccessible electronic data; and (2) a safe harbor for the loss of electronic evidence. I will discuss each of these features in turn.

The two-tier structure appears in proposed Rule 26, which requires parties to produce all reasonably accessible electronic data without further prompting, but relieves them from producing information from sources that the party identifies as "not reasonably accessible because of undue burden or cost."[28] If a party's designation of inaccessibility is challenged, it must persuade the court that the extreme burden or cost of production makes the withheld data "not reasonably accessible." If that showing is made, the burden shifts to the requesting party to show that "good cause" nonetheless warrants discovery.[29]

Proposed Rule 26 incorporates the consideration of costs and the balancing of burdens, which *Zubulake* confined to the cost-shifting analysis, into the threshold inquiry of whether information should be discoverable at all. Thus, in contrast to the *Zubulake* framework—which treats all relevant, nonprivileged data as uniformly discoverable—the proposed model removes electronic data

26. *See* Peter J. Bezek et al., *Employer Monitoring of Employee Internet Use and E-Mail: Nightmare or Necessity?*, 2-11 Mealey's Cyber Tech Litig. Rep. 27 (2001) (discussing the costs of electronic monitoring, including increased risk of liability, low employee morale, and direct expenses).

27. *See* Christopher Pearson Fazekas, 1984 *Is Still Fiction: Electronic Monitoring in the Workplace and U.S. Privacy Law*, 2004 DUKE L. & TECH. REV. 15, ¶¶ 22-28, http://www.law.duke.edu/journals/dltr/articles/PDF/2004DLTR0015.pdf (arguing that employers are unlikely to abuse their right to monitor employees because it would dampen employee morale).

28. PROPOSED AMENDMENTS, *supra* note 2, Rule 26(b)(2)(B).

29. *Id.*

from the scope of discoverability if the court finds that production would be overly burdensome and no good cause exists to override that determination.

Whether the new model will actually cut e-discovery costs for companies, however, depends on how strictly or liberally courts decide to interpret the good cause requirement. Proposed Rule 26 directs courts to consider the general proportionality limitations contained in current Rule 26(b)(2)(i)-(iii) in determining whether the requesting party has established good cause.[30] Because these factors already govern the discovery of inaccessible evidence (as they do all types of evidence), a straight reapplication of these standards under the guise of a good cause analysis would frustrate the motivating purpose behind the amendments to alleviate the burdens posed by e-discovery. If the line drawn in the proposed rules between accessible and inaccessible data is to be a meaningful one, the limitations in Rule 26(b) must have sharper bite in the context of inaccessible data.[31] Courts should in all cases require the party seeking the discovery of inaccessible data to establish a high likelihood that the requested evidence does not exist in more accessible locations. In addition, the requesting party should be required to show that the inaccessible data likely contains evidence relevant to a claim or defense, as opposed to evidence relating to the general subject matter of the litigation.[32] In determining whether a request is framed with sufficient specificity, courts should carefully analyze the characteristics of the storage media and information system at issue. A seemingly narrowly worded request—for example, one that seeks all e-mails in a one-year span that mention the plaintiff's name—should be rejected if the respondent cannot locate such e-mails without first having to restore its entire inventory of backup tapes. Strengthened in this way, the good cause requirement would actually ease e-discovery burdens.

If the two-tier model reduces compliance costs for employers, it could indirectly benefit employee privacy by making aggressive methods of electronic

30. The committee note to proposed Rule 26 adopts *Zubulake*'s seven-part structure, *see supra* note 9, for the good cause analysis, but replaces the factors dealing with amount-in-controversy and relative ability to control costs with factors that expand upon the relevance of the inaccessible data and the existence of relevant data in more accessible sources. PROPOSED AMENDMENTS, *supra* note 2, Rule 26(b)(2)(B) committee note.

31. Because proposed Rule 26 makes the consideration of costs a factor in defining the scope of discoverability, it may completely displace the need for apportioning production costs. Consequently, if Rule 26(b)(2) limitations are not applied more stringently in the context of inaccessible data, corporations may wind up paying more for e-discovery under the proposed model than under the existing *Zubulake* framework.

32. *See* FED. R. CIV. P. 26(b)(1) ("Parties may obtain discovery regarding any matter, not privileged, that is relevant to the claim or defense of any party. . . . For good cause, the court may order discovery of any matter relevant to the subject matter involved in the action.").

surveillance less cost-effective and desirable. However, instead of simply hoping that the proposed Rule 26 will prompt employers to voluntarily protect employee privacy, courts could directly promote employee privacy by considering invasion of privacy as an additional cost that weighs against the expected benefit of e-discovery.[33] To illustrate, a request for all relevant e-mails written by a minor player in the case should be considered overly burdensome if it would require the company to read through all of the employee's personal e-mails to ascertain which, if any, are relevant to the suit.

Moreover, courts should acknowledge employee privacy only to the extent that the employer has done so itself. If the corporation has utilized extensive surveillance technology to monitor employees, then it should be precluded from offering its employees' nonexistent privacy as a reason for limiting its discovery obligations—thereby providing an incentive for the company to protect employee privacy. As one court has remarked: "To permit a corporation . . . to reap the business benefits of such technology and simultaneously use that technology as a shield in litigation would lead to incongruous and unfair results."[34]

The second innovation introduced by the proposed amendments is a safe harbor for the loss of electronic data. Proposed Rule 37 shields a party from sanctions if it has lost discoverable data due to the "routine, good-faith operation" of its electronic information system.[35] As the committee note explains, the concept of a routine operation includes "the alteration and overwriting of information, often without the operator's specific direction or awareness, a feature with no direct counterpart in hard-copy documents."[36] In other words, proposed Rule 37 would 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. Thus, even with this safe harbor in place, many companies may still decide that electronic surveillance is necessary to thwart willful spoliation by employees.

To avoid this result, courts could interpret proposed Rule 37 to promote employee privacy by varying the application of the safe harbor according to the

33. *See* Michael Marron, Comment, *Discoverability of "Deleted" E-Mail: Time for a Closer Examination*, 25 SEATTLE U. L. REV. 895, 897 (2002) (arguing that "[p]ublic policy concerns such as communication efficiency, individual privacy, and free speech should outweigh the rights of a litigant to access deleted e-mail correspondence without some showing of particular relevance or need").

34. Linnen v. A.H. Robins Co., No. 97-2307, 1999 WL 462015, at *6 (Mass. Super. Ct. June 16, 1999).

35. PROPOSED AMENDMENTS, *supra* note 2, Rule 37(f).

36. *See id.*, Rule 37(f) committee note.

level of employee surveillance a company maintains. For example, courts could impose harsher spoliation sanctions on companies that have instituted continuous or blanket forms of electronic surveillance, as opposed to limited surveillance confined to key players after the preservation duty has attached. Such a policy is certainly reasonable: A corporation that has adopted extensive surveillance measures has a greater technological capacity to prevent employees from deleting relevant evidence, and should therefore be held to a higher standard of preservation. Courts could also broaden the scope of discoverable backup tapes if evidence shows that employees have deleted relevant e-mails, on the theory that there is good cause to believe that a corporation that closely monitors its employees probably knew about and condoned the spoliation.[37] If the corresponding backup data has been lost in a routine operation, courts could consider the extent of a corporation's surveillance as evidence tending to support a finding of bad faith, which would render the safe harbor of Rule 37(f) inapplicable.

CONCLUSION

The two-tier model of electronic discovery, with its good cause requirement and safe harbor, could have the unintended effect of benefiting employee privacy if it alleviates the pressure on companies to turn to data-mining and tracking programs as ways of managing e-discovery. However, there is ample room in the new e-discovery framework to more fully protect employee privacy, and this Comment has suggested some practical ways in which the new rules, and the courts that will apply them, can actively discourage companies from adopting intrusive forms of surveillance. While technology advances with frightening speed, our notions of privacy appear to be stuck in the nineteenth century. The time has come to reexamine the value of privacy and update it to fit the world we live in.

ELAINE KI JIN KIM

37. *See id.*, Rule 26(b)(2) committee note (stating that "the failure to produce relevant information that seems likely to have existed but is no longer available on more easily accessed sources" is an appropriate consideration for construing good cause).