JAMES C. STURDEVANT*

MARK T. JOHNSON MONIQUE OLIVIER SYLVIA M. SOKOL

(方)

5

ELLEN M. CORBETT Of Counsel

THE STURDEVANT LAW FIRM

A PROFESSIONAL CORPORATION 475 SANSOME STREET, SUITE 1750 SAN FRANCISCO, CALIFORNIA 94111-3141

February 15, 2005

Peter G. McCabe, Secretary Committee on Rules of Practice and Procedure Of the Judicial Conference of the United States Thurgood Marshall Federal Judiciary Building Washington, DC 20544

Re: <u>Proposed Rules Relating to Electronic Discovery</u>

My name is Jim Sturdevant. I am the Principal of the Sturdevant Law Firm, PC in San Francisco. My small firm of five lawyers specializes in representing plaintiffs and plaintiff classes in the areas of consumer protection, unlawful business practices and employment discrimination. I have practiced for more than thirty years in both state and federal courts. I am the immediate past President of the Consumer Attorneys of California. I also serve on the Boards of Trial Lawyers for Public Justice, the National Association of Consumer Advocates and the San Francisco Trial Lawyers Association. I suggest making three clarifications to the proposal under Rule 26(b) (2) that "on motion by the requesting party, the responding party must show that the information is not reasonably accessible." First, the proposed amendment to Rule 26(b) (2) would essentially create a presumption that electronic information that can be characterized as not "reasonably accessible" need not be produced absent unusual circumstances. This is an enormous change from the current state of the law, which provides that information contained in places such as back-up tapes is discoverable unless the defendant establishes that it would be an "undue burden" to produce this information. The party identifying information as not reasonably accessible must establish that the production of the information would be unduly burdensome and costly. Thus, "not reasonably accessible" should be re-defined as "unduly burdensome and costly." Second, the party must submit

Telephone (415) 477-2410

Facsimile (415) 477-2420

email: 1stice@sturdevantlaw.com

04-CV-253

Peter G. McCabe, Secretary

Committee on Rules of Practice and Procedure Of the Judicial Conference of the United States Page 2

declarations under penalty of perjury establishing and providing sufficient detail for the court to assess whether the designation is appropriate. Third, the Court should consider whether the party seeking discovery should have the opportunity to depose the declarants to test the conclusion.

I endorse the Committee's requirement that the initial discovery conference include a discussion regarding the disclosure of electronically-stored information, including the form in which it should be produced. This discussion should require discussion of "the types of electronic information available, and the cost of producing that information." In addition, I recommend that the proposed language in 26(f) that the parties "discuss any issues relating to preserving discoverable information" be changed to "relating to preserving documents and electronically-stored information relevant to the subject matter of the litigation." This last suggestion makes clear that presentation of electronically-stored information is to be separately discussed, and also clarifies ambiguities in the meaning of "discoverable."

The proposed amendment to Rule 37 would create a new "safe harbor" provision, protecting responding parties from sanctions imposed for the destruction of digital and electronic information due to the "routine operation of the party's electronic information system." The proposal is likely to encourage the use of systems that routinely destroy electronic information at short intervals to protect parties and their counsel who share their duties to preserve and protect documents once litigation is commenced.

I recommend that proposed Rule 37(f)(i) be modified to read if "(1) the party took reasonable steps to preserve the information after it knew or should have known the information was <u>relevant to</u> the subject matter of the action." The phrase "relevant to the subject matter" is well established and relates directly to the "not reasonably accessible" standard.

As explained below, I submit that two of the proposed civil rule changes directed at electronic discovery would make it more difficult for persons harmed by corporate wrongdoing to obtain justice for their claims.

-2-

Peter G. McCabe, Secretary Committee on Rules of Practice and Procedure Of the Judicial Conference of the United States Page 3

There are numerous significant cases where governmental bodies or injured parties proved their cases largely through electronic and digital information. If the proposed rule is adopted, corporations facing potential legal challenges will have a significant incentive to put as much evidence as possible into media that they can, if not destroy, designate as not "reasonably accessible." Creating this incentive could easily hamstring important litigation. If would stifle a system that promises to provide justice.

I. ACCESS TO ELECTRONICALLY STORED INFORMATION IS EXTRAORDINARILY IMPORTANT TO PERSONS WITH CLAIMS IN THE CIVIL JUSTICE SYSTEM, AND NARROWING THAT ACCESS WILL HARM CONSUMERS AND ENCOURAGE CORPORATE WRONGDOING.

A. Today, Nearly All Information Is Kept and Stored In Electronic Form.

In today's economy, electronic information is universal. The information that is stored in digital or electronic form is frequently the only form in which vital information is stored. According to a University of California study, 93% of all information created during 1999 was first generated in digital form – on computers.¹ The trend towards maintaining data in electronic form has greatly accelerated since that study was completed, and will continue to increase in the coming years. In the business world, up to 70 percent of records may be stored in electronic form,² and an estimated 30 percent of all information is never printed on paper.³ Indeed, many forms of electronic information now routinely generated by businesses cannot be fully reduced to paper form at all. Electronic databases, for example, have no exact paper counterpart because a print-out cannot capture the

-3-

¹ John J. Hughes, One Judge's View of Electronic Information in the Courtroom, THE FEDERAL LAWYER, August 2002, at 41 (citing Kenneth J. Withers, Electronic Discovery: The Challenges and Opportunities of Electronic Evidence, Address at the National Workshop for Magistrate Judges (July 2001)).

² Lori Enos, *Digital Data Changing Legal Landscape*, E-COMMERCE TIMES, May 16, 2000, ¶ 1, *at* http://www.ecommercetimes.com/perl/story/3339.html.

³ Richard L. Marcus, *Confronting the Future: Coping with Discovery of Electronic Material*, 64-SUM LAW & CONTEMP. PROBS. 253, 280-81 (2001) (citations omitted).

Peter G. McCabe, Secretary Committee on Rules of Practice and Procedure Of the Judicial Conference of the United States Page 4

formulas defining cells and fields in the database, and often require a knowledgeable administrator to create a meaningful printed format. Other business records routinely available in hard copy in the past may now be available only on computer. Thus, vast amounts of today's business information can be found only in electronic form.

B. Electronic Information Has Repeatedly Proven Crucial In Significant Cases Involving Egregious Corporate Abuses.

Repeated examples demonstrate that crucial evidence of corporate misbehavior – often intentional misbehavior – is discovered only through electronic documents. In many cases, these electronic records directly contradict the stories offered to the public in connection with those events. Electronic evidence has become increasingly vital in cases of all kinds, particularly in cases involving businesses.⁴

In case after case in recent years, revelations from electronic materials have established that major national corporations have acted illegally and abused their power. Dozen of illustrations could be presented, but a quick summarizing demonstrates the extent to which electronic materials have been the leading proof in important cases:

• **Microsoft Antitrust Litigation.** The landmark litigation initiated by the Department of Justice and numerous state attorney generals depended heavily upon information stored in digital format. For example, when Microsoft Chairman Bill Gates offered self-serving explanations of the corporation's conduct, government lawyers relied heavily on Microsoft's and Gates' own e-mails to

⁴ One survey of case law examining only one type of electronic evidence – e-mail – found that between 1997 and the first half of 1999 there were more than 375 judicial decisions in which email played a significant role in resolving the issue. Samuel A. Thumma & Darrel S. Jackson, *The History of Electronic Mail in Litigation*, 16 SANTA CLARA COMPUTER & HIGH TECH. L. J. 1, 12 (1999); *see also* Shira A. Scheindlin & Jeffrey Rabkin, *Electronic Discovery in Federal Civil Litigation: Is Rule 34 Up to the Task?*, 41 B.C. L. REV. 327, 329 n.12 (2000) (listing cases involving incriminating e-mail).

Peter G. McCabe, Secretary Committee on Rules of Practice and Procedure Of the Judicial Conference of the United States Page 5

refute his remarks and to challenge numerous memory lapses.⁵ That case also involved crucial evidence from electronic materials that were not e-mails, and materials which the district court concluded should be produced despite the corporation's vigorous claims that it would be too burdensome to do so.⁶

• **Merrill Lynch Investment Scandal.** A number of shocking e-mails established that this huge Wall Street firm issued misleading stock analyses so as not to jeopardize its possible investmentbanking business.⁷ For example, an e-mail "from a Merrill Lynch analyst called the stock of a certain Internet company 'a piece of junk' and 'a powder keg.' At the same time, Merrill Lynch was giving the company, a Merrill Lynch client, the firm's highest stock rating. That e-mail, and others like it, led Merrill Lynch to announce the \$100 million settlement of civil enforcement proceedings last year."⁸ These revelations not only led to the return of millions of dollars to duped investors in successful litigation triggered by the Attorney General of New York, but also led to industry-wide reforms to prevent future recurrences. If the revealing e-mails had never been produced – either because they had been put on back-up tapes or overwritten after 30 days – it's entirely possible that these abuses would never have been exposed to the public.

• **Employment Discrimination.** In litigation over employment practices, the significance of e-

⁷ See, e.g., Randall Smith, *E-Mails Link CSFB Research with Banking*, THE WALL STREET JOURNAL, Nov. 27, 2002, at C1; Erik Portanger, *Now, Goldman Analysts Have E-Mail Issues*, THE WALL STREET JOURNAL, Nov. 26, 2002, at C1.

⁸ Lesley Friedman Rosenthal, *Electronic Discovery Can Unearth Treasure Trove of Information* or Potential Land Mines, 75 New York State Bar Ass'n Journal 32 (Sept. 2003)

-5-

⁵ James V. Grimaldi, *The Gates Deposition: 684 Pages of Conflict*, THE SEATTLE TIMES, March 16, 1999, at A1.

⁶ Kim S. Nash and Patrick Thibodeau, *What's in a Database?*, ComputerWorld (Oct. 19, 1998) ("As the government opens its antitrust case against Microsoft Corp. this week, state and federal lawyers will bring to court sales and pricing evidence fresh from Microsoft's own databases. Lawyers for the U.S. Department of Justice and 20 states visited the vendor's Redmond, Wash., headquarters last week with a court order allowing them to examine about 4 G bytes of sales data stored in Microsoft's own SQL Server databases. Microsoft had earlier said the databases were too complicated and proprietary to reproduce, as the government requested several weeks ago.")

Peter G. McCabe, Secretary Committee on Rules of Practice and Procedure

Of the Judicial Conference of the United States Page 6

mail evidence has grown exponentially, with plaintiffs often offering evidence of discrimination, harassment, or retaliation in the form of e-mail correspondence.⁹

• **Vioxx Products Liability Litigation.** By 2000, one email suggests Merck recognized that Vioxx didn't merely lack the protective features of old painkillers, but that something about the drug itself was linked to an increased heart risk. On March 9, 2000, the company's powerful research chief, Edward Scolnick, e-mailed colleagues that the cardiovascular events "are clearly there" and called it a "shame. . ." But the company's public statements after Dr. Scolnick's e-mail continued to reject the link between Vioxx and increased intrinsic risk.¹⁰

• Marsh & McLennan Kickbacks for Steering.¹¹ A Marsh & McLennan executive asked a manager of a big insurance company, in an e-mail message, to "send someone to a meeting to pretend to make a bid for an insurance policy being sought by a customer" – even though Marsh had already decided to steer the business to another insurer that agreed to pay a kickback to Marsh. The e-mail message – written in 2001 and disclosed last year as part of a New York State lawsuit asserting that Marsh, Inc., a unit of Marsh & McLennan, cheated customers – even made a joke about creating an illusion of competition."

The experiences of my firm confirm that electronic evidence is increasingly making a difference in litigation and is often crucial to the just outcome of a case.

-6-

⁹ Thumma & Jackson, *supra* note 6, at 13-15; *see also*, *e.g.*, *Knox v. Indiana*, 93 F.3d 1327, 1330 (7th Cir. 1996) (harassing e-mails from supervisor); *Strauss v. Microsoft Corp.*, No. 91 Civ. 5928, 1995 WL 326492, at *4 (S.D.N.Y. June 1, 1995) (e-mails manifesting discriminatory attitude on the part of a supervisor); *Aviles v. McKenzie*, No. C-91-2013-DLJ, 1992 WL 715248, at *2, 10 (N.D. Cal. Mar. 17, 1992) (e-mail messages showing that plaintiff engaged in whistleblowing activity).

¹⁰ Anna Wilde Matthews and Barbara Martinez, *E-Mails Suggest Merck Knew Vioxx's Dangers At Early Stage*, Wall Street Journal; Nov. 1, 2004 at A1.

¹¹ Alex Benenson, Spitzer's Latest Suit, Like Others, Cites Indiscreet E-Mail, New York Times (Oct. 18, 2004)

Peter G. McCabe, Secretary Committee on Rules of Practice and Procedure Of the Judicial Conference of the United States Page 7

II. THE PROPOSED AMENDMENTS WILL ENCOURAGE ABUSES THAT WILL MAKE IT HARDER FOR PLAINTIFFS TO OBTAIN IMPORTANT ELECTRONIC INFORMATION.

410

A. The Data Establishes that Stonewalling - the Concealment, Refusal to Produce or Even Destruction of Evidence - is the Greatest Problem With the Discovery System in both State and Federal Courts.

Despite an intense corporate lobbying campaign to create the impression, I am aware of no convincing empirical evidence to support the corporate view that excessive discovery requests for electronic information is a widespread problem; rather, empirical studies of discovery in general have concluded that "stonewalling" – the failure to respond to discovery requests adequately and in a timely manner – is by far the most common form of discovery abuse in document production. In *Ting v. AT&T*, U.S. District Court, Northern District of California, Case No. C 012969 BZ ADR, a class action lawsuit against AT&T on behalf of seven million California consumers, the district court found that the mandatory arbitration clause was illegal, unconscionable, and unenforceable. *Ting v. AT&T*, 182 F.Supp.2d 902 (N.D. Cal. 2002). It based its decision largely on emails and electronically stored documents detailing AT&T's staged effort to conceal the arbitration clause and its impact on its customers. The Ninth Circuit affirmed in most respects in a significant opinion, holding, among other things, that a clause prohibiting class action adjudication was a limitation on remedies and therefore unconscionable under California law. 319 F.3d 1126 (9th Cir.), *cert. denied*, 124 S. Ct. 53 (2003).

Overwhelming evidence establishes that the incentive to avoid culpability and the resulting behaviors of concealment and suppression and destruction of evidence, are at least as problematic with respect to electronic discovery as they are with respect to traditional paper discovery.

In the context of document discovery generally, a 1997 empirical study on discovery commissioned by the Advisory Committee established that stonewalling, not excessive requests, is the most widespread problem. It found that 84% of the attorneys in its sample used document requests in their cases, 28% of those complained that a party failed to respond to document requests adequately,

-7-

Peter G. McCabe, Secretary Committee on Rules of Practice and Procedure Of the Judicial Conference of the United States Page 8

and 24% reported that a party failed to respond in a timely manner.¹² Only 15% of respondents complained that an excessive number of documents were requested.¹³ In other words, nearly twice as many respondents complained of a failure to respond adequately (one form of stonewalling) than complained of excessive requests. Moreover, in a survey conducted in the early 1980's, one-half of 1,500 litigators surveyed believed that unfair and inadequate disclosure of material prior to trial was a "regular or frequent" problem.¹⁴

B. There is an Existing Problem With Major Corporations Repeatedly Getting Caught Destroying Crucial Electronic Evidence.

Neither empirical evidence nor common sense suggests that stonewalling would tend to be *less* of a problem when it comes to electronic discovery. Indeed, anecdotal evidence in the digital age suggests that responding parties routinely continue to refuse to produce discoverable materials or deny that they exist, construe what is "discoverable" in the most narrow way, and engage in dilatory tactics to delay or avoid production of unfavorable "documents," whether they are in paper or electronic form.¹⁵

Corporate defendants who have been sued or investigated in cases of serious wrongdoing have been repeatedly caught destroying or attempting to destroy crucial electronic records. In *Cortez v. Wells Fargo Bank*, San Francisco Superior Court Case No. 999072, we learned after the case had been pending for more than a year that Wells Fargo Bank was destroying documents daily based on its pre-

¹⁴ Deborah Rhode, Ethical Perspectives on Legal Practice, 37 STAN. L. REV. 589, 598-99 (1985).

¹⁵ Mark D. Robins, *Computers and the Discovery of Evidence – A New Dimension to Civil Procedure*, 17 J. MARSHALL J. COMPUTER & INFO. L. 411, 424-25 & nn. 58-60 (1999) (collecting cases addressing a failure to produce electronic data or evidence).

-8-

¹² Thomas E. Willging, Donna Stienstra, John Shapard & Dean Miletich, *An Empirical Study of Discovery and Disclosure Practice under the 1993 Federal Rule Amendments*, 39 B.C. L. REV. 525, 540, 574-75 (1998).

¹³ *Id.* at 575.

ه ،

Peter G. McCabe, Secretary Committee on Rules of Practice and Procedure Of the Judicial Conference of the United States Page 9

existing but undisclosed retention policy. We were forced to move for a temporary restraining order and preliminary injunctive relief to prevent continued destruction of documents relevant to the case. Similarly, in *Yu v. Signa Bank/Virginia*, Alameda County Superior Court Case No. H-184674-8, a case involving distant forum abuse against consumers in California, the credit card company's lawyers refused to enter into a stipulation to preserve documents necessitating motions to preserve records filed with both the Trial and Appellate Courts.

My firm's experience in this case is hardly unusual. Even a casual reader of both the mainstream and legal press has encountered numerous stories about corporate wrongdoers destroying important digital and electronic evidence for the evident purpose of concealing the truth about their conduct.

As one court concluded, a "haphazard and uncoordinated approach to document retention indisputably denies its party opponents potential evidence to establish facts in dispute."¹⁶ An astounding 68% of respondents to the ABA survey in 2000 said their clients rarely or never took steps to stop automatic overwriting of electronic data, even after notice of a filed lawsuit.¹⁷

C. The Proposed "Reasonably Accessible" Standard Will Encourage Corporations to Make Most Electronic Evidence "Inaccessible."

Under the proposed amendments to Rule 26(b)(2), a party not would not be required to provide electronically stored information in response to a discovery request if it decides that the information is not "reasonably accessible." The Note accompanying the proposed rule explains that this rule is required because of the staggering volume of electronically stored information and the variety of ways in which such information is maintained. If goes on to say that "reasonably accessible" electronic

-9-

¹⁶ In re Prudential Ins. Co. of America Sales Practices Litig., 169 F.R.D. 598, 615 (D. N.J. 1997) (drawing adverse inference and awarding sanctions of \$1,000,000 for repeated incidents of document destruction).

¹⁷ Enos, supra note 2, \P 6.

Peter G. McCabe, Secretary

Committee on Rules of Practice and Procedure Of the Judicial Conference of the United States Page 10

information would include information the party routinely uses – sometimes called "active data." The Note also gives examples of information generally not considered to be reasonably accessible: information stored solely for disaster-recovery purposes that may be expensive and difficult to use for other purposes (*e.g.*, back-up tapes); "legacy data" retained in obsolete systems that are no longer in use; and information deleted in a way that makes it inaccessible without resort to costly and uncertain computer forensic techniques.

Under the proposed rule, if the requesting party moves to compel the discovery of this information, the responding party would have to demonstrate that the information is not reasonably accessible. Once that showing is made, the court may still order the party to provide the information at issue if the requesting party shows good cause.

I am concerned that the responding party's ability to designate what's "accessible", or not gives responding parties the opportunity to throw up obstacles to discovery. I am also troubled by the fact that the proposed rule would change the existing presumption in the FRCP that *all* non-privileged information relevant to the claim or defense of a party is discoverable. Under the new rule, electronic information that is not "reasonably accessible" would be presumptively outside the scope of discovery. This differs from the approach in leading case law which applies a multi-factor test to determine whether cost-shifting is appropriate when dealing with a discovery request for inaccessible electronic data, but assumes that such data, to the extent relevant under Rule 26(b)(1), is at least discoverable.¹⁸ Finally, the proposed rule could pave the way to adoption in the future of a rule presumptively excluding from discovery paper documents that are not "reasonably accessible" because, for example, they are stored in a warehouse in some remote location together with a large volume of irrelevant documents.

Some advocates of the proposed "safe harbor" amendment have argued that companies adopting aggressive policies of overwriting computerized data are merely engaged in good business

¹⁸ See Zubulake v. UBS Warburg LLC, 217 F.R.D. 309, 318, 322 (S.D.N.Y. 2003)

Peter G. McCabe, Secretary Committee on Rules of Practice and Procedure Of the Judicial Conference of the United States Page 11

practices. In many cases, employees are directed not to keep materials that help them to remember and keep track of work because high-ranking corporate officials are concerned about revelations emerging in some future litigation. A particularly direct communication to this effect came to light in a recent lawsuit involving Microsoft:

- Microsoft Corp. developed policies stressing the systematic destruction of internal emails and other documents crucial to lawsuits it has faced in recent years, a California software company alleges.
- Burst.com, in court papers unsealed this week, also accuses Microsoft of destroying e-mails crucial to Burst's lawsuit against the software giant even after the trial judge ordered it to retain the documents....
- The Motion mentions an e-mail on Jan. 23, 2000, in which Jim Allchin, a Microsoft senior vice-president, told the Windows Division to purge e-mails every 30 days: "This is not something you get to decide. This is company policy.... Do not archive your mail. Do not be foolish. 30 days."¹⁹

This exchange is particularly revealing. Many Microsoft employees would clearly have preferred – in the routine performance of their work – to intake e-mails for some normal period of time. Instead, corporate managers directed them to destroy these materials. In light of the fact that many of Microsoft's serious past legal troubles were only exposed because of the existence of electronic evidence, this corporate policy of erasing shouldn't be sheltered under a veneer of good business practice.

D. The Proposed "Safe Harbor" Provision Will Encourage Corporations to Routinely Destroy Electronic Information At Short Intervals.

The proposed amendment to Rule 37 would create a new subdivision (f) to protect a party from sanctions under the FRCP for failing to provide electronically stored information lost because of

¹⁹ Foster Klug, *Microsoft Accused of E-Mail Scorched Earth Policy*, The Associated Press, Nov. 18, 2004.

Peter G. McCabe, Secretary Committee on Rules of Practice and Procedure Of the Judicial Conference of the United States Page 12

the "routine operation of the party's electronic information system." This "safe harbor" would not be available if the party violated a preservation order issued in the action, or if the party failed to take reasonable steps to preserve the information after it knew or should have known the information was discoverable in the action. The Note accompanying the proposed rule explains that the new section is intended to address the contention that suspension of the automatic recycling and overwriting functions of most computer systems can be "prohibitively expensive and burdensome." The proposed rule does *not* attempt to define the scope of the duty to preserve, and does *not* address the loss of electronically stored information that may occur before an action is commenced.

The proposed changes to Rule 37 taken together with the proposed changes to Rule 26 would mean that parties would be able to continue the routine destruction of inaccessible electronic data, even while an action is pending, without fear of sanctions. We are concerned that this "safe harbor" would encourage defendants to set up computer systems that "routinely" overwrite or purge data at very short intervals in order to thwart discovery in litigation.

As the foregoing makes clear, I strongly believe that no "safe harbor" rule should be created. If the Committee nevertheless decides to proceed with some rule, however, I urge the Committee not to adopt any rule that reduces the obligation of parties to preserve evidence. Under the proposed rule, it appears that no obligation to preserve evidence arises until after litigation formally commences. Under the leading case in this area, t6he *Zubulake* case, the duty to preserve electronic evidence may attach at the moment that litigation is "reasonably anticipated."²⁰ The *Vioxx* litigation described above gives one illustration of the importance of this point: in that case, the pharmaceutical manufacturer knew of evidence that the medicine might cause serious side-effects well before any potential victims knew of these issues. Under the "reasonably anticipated" standard of *Zubulake*, it would presumably be improper for any drug manufacturer to destroy key evidence. If a safe harbor rule is to be adopted, it should certainly reaffirm the duty to preserve and protect.

²⁰ Zubulake v. NBS, 220 F.R.D. 212, 217 (S.D.N.Y. 2003).

-12-

ł

Peter G. McCabe, Secretary Committee on Rules of Practice and Procedure Of the Judicial Conference of the United States Page 13

In conclusion, I strongly urge the Committee not to adopt the proposed amendments to Rule 26(b)(2) and Rule 37(f). In my firm's experience, the greatest problem with electronic discovery (like discovery generally) has been stonewalling and efforts to conceal or destroy crucial electronic evidence. We believe that the proposed amendments would encourage this abusive practice, without providing corresponding benefits to justify that harm.

Date: February 15, 2005

The Sturdevant Law Firm, PC

James C. Sturdevant 475 Sansome Street Suite 1750 San Francisco, California 94111 (415) 477-2410