Sewell Testimony

04-CV-016

Request to Testify 1/12 San Francisco

RECEIVED 12/16/04

"Thumma, Sam-PHX" <SThumma@phx.perkinscoie.com>
12/15/2004 11:56 PM

To <Peter_McCabe@ao.uscourts.gov>
cc "Thumma, Sam-PHX" <SThumma@phx.perkinscoie.com>
Subject Written Testimony of Bruce Sewell-Intel Corporation

> Peter G. McCabe
> Secretary
> Committee on Rules of Practice and Procedure
> Administrative Office of the United States Courts
>
> Dear Mr. McCabe,
>
> Attached in Word format is Written Testimony of Bruce Sewell, General Counsel and Vice President of Intel Corporation Before the Committee on Rules of Practice and Procedure of the Judicial Conference of the United States, in anticipation of his oral testimony at the January 12, 2005 San Francisco, California public hearing on proposed amendments to the Federal Rules of Civil Procedure regarding electronic discovery. We would greatly appreciate it if you would confirm receipt of this Written Testimony.
> We understand that your office will provide to us logistical details applicable to Mr. Sewell's testimony well in advance of January 12, 2005. Should you have any questions or need any additional information, please contact us.
>
> Very truly yours,
> Sam Thumma
>

****
Samuel A. Thumma
Perkins Coie Brown & Bain P.A.
2901 North Central Avenue
Phoenix, Arizona 85012
T 602.351.8338
F 602.351.8516
sthumma@perkinscoie.com
****

<<Bruce Sewell Written Testimony (12/15/04).DOC>>

Bruce Sewell Written Testimony (12_15_04).DOC

Intel Corporation
2200 Mission College Blvd.
P.O. Box 58119
Santa Clara, CA 95052-8119
(408) 765-8080
www.intel.com

October 28, 2004

Peter G. McCabe
Secretary
Committee on Rules of Practice and Procedure
Administrative Office of the United States Courts
Thurgood Marshall Federal Judicial Building
Washington, D.C. 20544

Re: Testimony on Proposed Amendments to the Federal Rules of Civil Procedure Regarding Electronic Discovery

Dear Mr. McCabe:

The Intel Corporation has reviewed the Proposed Amendments to the Federal Rules of Civil Procedure regarding electronic discovery that were circulated for public comment in August 2004. I understand that the Judicial Conference Advisory Committee on Civil Rules is holding public hearings on these Proposed Amendments next year, including a public hearing on January 12, 2005 in San Francisco, California.

On behalf of Intel Corporation, I hereby request the opportunity to testify at the January 12, 2005 San Francisco public hearing. If there are any relevant protocols applicable to my testimony, please let me know at your earliest opportunity. In addition, if there is anything in addition to providing this notice that I need to do to testify at this public hearing, please let me know at your earliest opportunity.

Should you have any questions, or need any additional information, please contact me.

Very truly yours,

Bruce Sewell
V.P. & General Counsel
Intel Corporation

04-CV-054
Request to Testify 1/12 San Francisco
RECEIVED 12/16/04

"Thumma, Sam-PHX"
<SThumma@phx.perkinscoie.com>
12/15/2004 11:56 PM

To <Peter_McCabe@ao.uscourts.gov>
cc "Thumma, Sam-PHX" <SThumma@phx.perkinscoie.com>
Subject Written Testimony of Bruce Sewell-Intel Corporation

> Peter G. McCabe
> Secretary
> Committee on Rules of Practice and Procedure
> Administrative Office of the United States Courts
>
> Dear Mr. McCabe,
>
> Attached in Word format is Written Testimony of Bruce Sewell, General Counsel and Vice President of Intel Corporation Before the Committee on Rules of Practice and Procedure of the Judicial Conference of the United States, in anticipation of his oral testimony at the January 12, 2005 San Francisco, California public hearing on proposed amendments to the Federal Rules of Civil Procedure regarding electronic discovery. We would greatly appreciate it if you would confirm receipt of this Written Testimony.
> We understand that your office will provide to us logistical details applicable to Mr. Sewell's testimony well in advance of January 12, 2005. Should you have any questions or need any additional information, please contact us.
>
> Very truly yours,
> Sam Thumma
>
****
Samuel A. Thumma
Perkins Coie Brown & Bain P.A.
2901 North Central Avenue
Phoenix, Arizona 85012
T 602.351.8338
F 602.351.8516
sthumma@perkinscoie.com
****

<<Bruce Sewell Written Testimony (12/15/04).DOC>>

Bruce Sewell Written Testimony (12_15_04).DOC

Intel Corporation
2200 Mission College Blvd.
SC4-203
Santa Clara, CA 95052

Testimony of Bruce Sewell
General Counsel and Vice President of Intel Corporation
Before the Committee on Rules of Practice and Procedure
of the Judicial Conference of the United States
January 12, 2005
San Francisco, California

My name is Bruce Sewell and I am Vice President and General Counsel of Intel Corporation. I am honored to appear before this Committee on Intel's behalf to comment on important proposed changes to the Federal Rules of Civil Procedure regarding the discovery of electronically stored information.

I come before the Committee with nearly two decades of experience in civil litigation. My comments today primarily draw on my perspective as an in-house attorney at Intel, where I have worked since 1995. But my experience before Intel includes a decade in private civil practice, first with the law firm of Schnader, Harrison, Segal & Lewis, and then as a partner with Brown & Bain. In both my in-house and outside counsel capacities—I say without any fondness—I have become intimately familiar with requests for production covering millions of documents—and more recently—multi-gigabytes of information.

In my testimony today, I will summarize Intel's recommendations on two areas of the proposed amendments:

First, on the proposed two-tiered approach for discovery of electronically stored information, Intel requests that the Committee: (a) confirm that the rules do not require a party to alter or suspend the routine operation of a disaster recovery system; and (b) provide for a presumption of cost sharing—not cost shifting, but cost sharing—when a party requests electronic information that is not reasonably accessible.

Second, Intel requests that the proposed safe harbor provision be clarified so that the proposal is not read to require the suspension of a pre-existing disaster recovery system absent a specific court order.

Before turning to the specifics of Intel's recommendations, it should help to explain the perspective and experience from which those recommendations flow. So I'll begin with a brief discussion of how Intel creates and stores electronic information.

I. INTEL'S USE AND STORAGE OF ELECTRONIC INFORMATION.

For more than 35 years, Intel has developed technology that has supported and enabled the computer and Internet revolution. In 1971, Intel introduced the world's first microprocessor. Today, it is the world's largest chip maker. We supply the computing and communications industries with products—including chips, boards, systems and software—that are the building blocks of those industries.

Intel has more than 78,000 employees in nearly 300 different offices and facilities on several continents. That includes over 7,000 researchers and scientists in labs around the world.

Given Intel's size and technology base, it is no surprise that the company creates and uses an enormous amount of electronically stored information. This data resides on tens of thousands of notebook computers, personal computers and servers around the world.

Intel also maintains a disaster recovery system for some, but not all, of its computer systems. The limited purpose of this system is to back up enough data—but only enough data—sufficient to return some computers or data storage systems to a functional state in the event of a disaster. Disasters can include a variety of natural and man-made events—from earthquakes to hard drive crashes—that make the data resident on an active computer unusable.

For purposes of the proposed rules, it is critical to emphasize the limits of disaster recovery systems such as Intel's. Information stored on these systems is very

difficult and expensive to search—in the parlance of the proposed rules, that information is demonstrably not "reasonably accessible."

Disaster recovery systems "are by their nature indiscriminate. They capture all information at a given time and from a given server," depending on how the system is configured.[1] These systems are ***not*** built to be used and cannot be used like a storage facility in which documents are organized by subject matter, and from which specific documents can be easily identified and retrieved.

Importantly, the limited information stored on Intel's disaster recovery system is not word-searchable. For example, we couldn't simply type the words "Pentium 4" into a search program, and then hope to retrieve all of the email messages, documents, spreadsheets, CAD programs and other electronic data using that term that were on the system.

Rather, to search for information in our disaster recovery system, we depend on electronic catalogues. These electronic catalogues contain information—but very limited information—about the data in our disaster recovery backup tapes, such as the name of a directory, subdirectory or file, its author, and the date the file was created. But these catalogues do not identify the subject or contents of the data in any given file, unless it happens to be referred to in the file name itself.

Needless to say, with such limited information to use as a roadmap, finding even the smallest piece of any particular file on a backup tape is extremely time-consuming. That process can take dozens of employee hours and involve several people. Moreover, once the data is found, it often is not readable without taking further steps to identify and load the software that was used to create the data.[2]

---

[1] *McPeek v. Ashcroft*, 202 F.R.D. 31, 33 (D.D.C. 2001).

[2] The costs of searching for data on backup tapes are well known. In a just-issued opinion, the California Court of Appeal observed that "'finding relevant data requires restoring a tape, viewing its directories, and searching within the directories for specific files. If the file is not on the tape, the process must be repeated for each backup tape.'" *Toshiba Am. Elect. Components, Inc. v. Superior Court*, 2004 WL 2757873, at *3 (Cal. Ct. App. Dec. 3, 2004). Evidence in that case showed that "[p]rocessing a

Not only are backup tapes difficult to search, but any such search has only a marginal chance of success. Backup tapes only capture information on the server at the very moment that the backup occurred. Backup tapes will not capture data that had not yet been created or that had been deleted at the time of the backup. Moreover, as *The Sedona Principles* on electronic discovery observe, "backup tapes generally are not retained for substantial periods, but are instead periodically overwritten when new backups are made." *See The Sedona Principles: Best Practices & Principles for Addressing Elec. Document Production* (Jan. 2004), Cmt. 5b. That feature of backup tapes only compounds the difficulty of finding information on them.

II. INTEL'S COMMENTS ON SPECIFIC PROPOSALS.

With that background, I'll now address two aspects of the proposed rule amendments: (1) the two tiered discovery system in proposed Rule 26(b)(2); and (2) the safe harbor provision proposed for Rule 37(f).

A. The Two-Tiered System.

In setting forth procedures for electronic discovery, the proposal adds three sentences to Rule 26(b)(2):

> "A party need not provide discovery of electronically stored information that the party identifies as not reasonably accessible. On motion by the requesting party, the responding party must show that the information is not reasonably accessible. If that showing is made, the court may order discovery of the information for good cause and may specify terms and conditions for such discovery."

As an initial matter, Intel strongly endorses the basic concept underlying this proposal: a party should not be required to produce data that is not "reasonably accessible" absent a showing of good cause. As I've just discussed, the burden of searching for information stored in disaster recovery systems—which by definition are

---

selection of 130 [backup] tapes surrounding 15 key dates would cost at least $211,250." *Id.* at *1. Processing approximately 800 backup tapes was estimated to cost between $1.5 and $1.9 million. *Id.*

not "reasonably accessible"—is enormous. In contrast, the benefits of such searches in the ordinary case are negligible. If the electronic information in question was created or used in the ordinary course of business and relevant to the operations of the company, it likely still exists on a party's active computer system. *See The Sedona Principles*, Cmt. 9b (noting that if information no longer exists on an active computer system, "the data will be marginal at best in most cases"). And if the information is relevant to issues in litigation, case law already addresses the duty to preserve that information.[3] If there is any additional concern about whether that information would or should be preserved, the proposed amendment to Rule 26(f) rightly directs the parties to discuss these issues at the outset of the litigation, and they are free to stipulate or move for an appropriate preservation order.

It is the rare case when important information is available only on a disaster recovery system, and in that rare case, the "good cause" standard of proposed Rule 26(b)(2) permits the requesting party to seek an order directing a search for the information. But absent a "good cause" requirement, it is simply too easy for a requesting party to fire off a scatter-shot discovery request demanding the costly search and production of "all" electronic and other information on an issue, regardless of how marginally relevant the information might be, regardless of whether the information is "reasonably accessible," and regardless of whether it is available through other, accessible, sources. Unfortunately, some courts have tolerated these blunderbuss and potentially abusive sorts of discovery demands, apparently without imposing any good cause requirement on the requesting party. Reform in the direction of the Committee's two-tiered approach clearly is needed.

---

[3] *See, e.g., Kucala Enters., Ltd. v. Auto Wax Co.*, No. 02 C 1403, 2003 WL 21230605, at *1 (N.D. Ill. May 27, 2003) (sanctions imposed where party intentionally destroyed computer files); *Proctor & Gamble Co. v. Haugen*, 179 F.R.D. 622, 632 (D. Utah 1998) (imposing sanctions for failure to preserve emails of key witnesses); *Residential Funding Corp. v. DeGeorge Fin. Corp.*, 306 F.3d 99, 108 (2d Cir. 2002) (sanctions may be imposed for failure to disclose emails).

Notwithstanding Intel's general support for the approach set forth in proposed Rule 26(b)(2), we believe that this two-tiered discovery proposal needs to be clarified and modified to ensure that its objectives are realized. In particular, the proposal should be amended: (a) to ensure that a party may continue to operate a pre-existing disaster recovery system, absent a specific order to the contrary; and (b) to include a presumption for cost-sharing when a party requests and obtains discovery on information that is not reasonably accessible.

1. The Proposed Amendments Should Make Express That The Rules Do Not Require A Party To Suspend The Operation Of A Pre-Existing Disaster Recovery System, Absent A Specific Court Order.

Intel is concerned that, as currently written, proposed Rule 26(b)(2) may create an unreasonable risk for a company that allows the routine—and necessary—recycling of information in their disaster recovery systems to continue during the pendency of litigation, or even before litigation begins. This risk unduly weakens the benefits of the proposed safe harbor for information lost because of disaster recovery systems. To avoid this concern, the proposed rules should state explicitly that they do not require the suspension of disaster recovery systems absent a specific court order issued on good cause.

The proposed Committee Note to proposed Rule 26(b)(2) begins by appropriately recognizing that information stored on disaster recovery systems ordinarily would "not be considered reasonably accessible." The Note describes many of the practical difficulties that we at Intel and other entities face when attempting to restore and retrieve data that appear on disaster recovery systems. These concerns are reflected again in proposed Rule 37(f), which provides a safe harbor from sanctions for information lost "because of the routine operation of the party's electronic information system," provided that the party "took reasonable steps to preserve the information after it knew or should have known the information was discoverable in the action."

The problem, however, is that proposed Rule 26(b)(2) states that a court ***may*** order discovery of information that is not reasonably accessible—presumably including information that exists on a disaster recovery system—for "good cause." And conceivably, under the "should have known" standard in proposed Rule 37(f), the safe harbor might be held inapplicable if a party could be charged with anticipating that a court might find "good cause" for ordering production of disaster recovery information under proposed Rule 26(b)(2).

The combined effect of these two proposed rules puts companies with disaster recovery systems in a quandary. As *The Sedona Principles* (Cmt. 5b) explain, disaster recovery systems are by nature dynamic—backup tapes "are periodically overwritten when new backups are made." Indeed, the *Principles* observe that "preserving backup tapes would require the time-consuming and costly process of reprogramming backup systems, manually exchanging backup tapes, and purchasing new tapes or hardware." *Id.* Despite that reality, does the possibility that a court ***might*** some day find good cause for ordering discovery of disaster recovery information create an undue risk for a company that leaves its disaster recovery system in place? This risk is particularly difficult to evaluate because critical components of the "good cause" determination—such as the extent of the requesting party's alleged need for the information—are inherently unpredictable, case-specific, and beyond the control of the party that uses the disaster recovery system. Indeed, the proposed Committee Note acknowledges that the proper application of the principles set forth in Rule 26(b)(2) are subject to development "through judicial decisions in specific situations."

This quandary may occur even before litigation begins. Courts have required parties to preserve information before a complaint is filed if the litigation can reasonably be anticipated and the information in question can reasonably be expected to be relevant. *E.g. Wm T. Thompson Co. v. Gen. Nutrition Corp.*, 593 F. Supp. 1443, 1455 (C.D. Cal. 1984) ("[s]anctions may be imposed against a litigant who is on notice that documents and information in its possession are relevant to . . . potential

litigation"). Given this precedent, does the language of the proposed rules mean that even before a complaint is filed, a potential litigant faces a risk of sanctions if it fails to suspend the operations of a disaster recovery system because a court might some day find "good cause" for production of information in that system?

The discovery rules should not present users of disaster recovery preservation systems with these sorts of risks. After all, the proposed Committee Note to Rule 26(f) rightly recognizes that "[w]holesale or broad suspension of the ordinary operation of computer disaster-recovery systems . . . is rarely warranted."

Intel, therefore, requests that the proposed rules be clarified to remove the risk that an entity may be sanctioned for continuing the operation of a pre-existing disaster recovery system, in the absence of a specific order that such system be halted. One of the proposals that has been presented to the Committee would provide just that clarification, by stating: "Nothing in these rules requires a party to suspend or alter the operation in good faith of disaster recovery or other [electronic data] systems . . . unless the court so orders for good cause . . ."

We strongly encourage the Committee to include such a provision in its proposed rules—either by including it in Rule 26(b) or by making it a separate rule. Doing so would avoid placing undue pressure to suspend disaster recovery systems. At the same time, where information in these systems is truly necessary and the burden can be justified, a court would be free to issue a discovery order to fit those circumstances.

2. Proposed Rule 26(b)(2) Should Contain A Presumption That Costs Incurred In Identifying And Producing "Not Reasonably Accessible" Information Should Be Shared.

Proposed Rule 26(b)(2) authorizes a court to order production of information that is not reasonably accessible "for good cause" and on such "terms and conditions" as the court may specify. The proposed Committee Note states that these "terms and conditions" may include "provisions regarding the cost of production." Intel agrees with this direction of the Rule, but requests that it go one step further. Given the enormous time and expense required in producing information that demonstrably is "not

reasonably accessible," it should be the unusual case in which the responding party is forced to bear all the costs of identifying and producing this information. Intel therefore requests that the proposed Rule include a rebuttable presumption that the costs of retrieving and producing information that is not "reasonably accessible" will be shared between the parties.

The concept of cost sharing properly allows the parties by agreement or court order to allocate costs to both the requesting and the responding party. This concept is designed to allow for legitimate, relevant discovery of information that cannot be obtained anywhere other than in data that is not reasonably accessible. Moreover, this presumption could be overcome if justified by the facts and circumstances of a particular case.

Cost sharing also would help ensure that information which is not "reasonably accessible" is sought only in appropriate instances and not as a fishing expedition or—as some have called it—a "weapon of mass discovery." As the California Court of Appeal has just recognized:

> "If the respondent is expected to bear its own expense, the demanding party has no incentive to demand anything less than all electronic data in any form. . . . [S]uch an unlimited demand can result in a stronomical costs to the responding party, which in turn inflates the settlement value of even meritless cases. If the demanding party were required to bear the expense, then presumably that party would only demand what it really needs."

Toshiba Am. Elect. Components, Inc. v. Superior Court, 2004 WL 2757873, *5 (Cal. Ct. App. Dec. 3, 2004).

The concept of cost sharing and cost shifting is not new. Texas provides that when a court (over objection) orders production of information that is not accessible "through reasonable efforts," "the court must also order that the requesting party pay the reasonable expenses of any extraordinary steps required to retrieve and produce the information." Tex. R. Civ. P. 196.4. Likewise, California requires a requesting party to

pay necessary costs incurred in "translat[ing] any data compilations included in the demand into reasonably usable form," a requirement that applies to the costs involved in retrieving data on backup tapes. Cal. Code Civ. P. § 2031(g)(1); *see Toshiba*, 2004 WL 2757873. The respected group of judges, scholars, and practitioners that generated *The Sedona Principles* on electronic discovery also recognize the unfairness of forcing the responding party to bear the costs of searching for data that is not reasonably accessible. *See Sedona Principle* 13 ("If the data or formatting of the information sought is not reasonably available to the responding party in the ordinary course of business, then, absent special circumstances, the costs of retrieving and reviewing such electronic information should be shifted to the requesting party."); *cf.* Manual for Complex Litigation § 11.446 at 81 (4th ed. 2004) ("More expensive forms of production, such as production of word-processing files with all associated metadata, or production of data in a specified nonstandard format, should be conditioned upon a showing of need or sharing of expenses.") (citing authority).

In sum, Intel believes that cost sharing is a valuable deterrent against overbroad, marginally relevant discovery, and yet, at the same time, permits litigants to discover all the information that they need.

B. The Safe Harbor Provision in Proposed Rule 37(f) Should Be Clarified.

As I already discussed, proposed Rule 37(f) would limit sanctions for failing to provide electronically stored information lost "because of the routine operation of the party's electronic information system." But this safe harbor is subject to two limitations: It would not apply: (1) where a party failed to take "reasonable steps to preserve the information after it knew or should have known the information was discoverable in the action"; or (2) where "a party violated an order in the action requiring [a party] to preserve electronically stored information." Intel believes that this proposal needs to be clarified in two respects.

First, the Committee should make clear that the first limitation on the safe harbor—i.e., the "should have known" test—is not intended to require the suspension of the operation of a pre-existing electronic data retention or disaster recovery system unless and until a court issues a specific preservation order requiring the system to be suspended. I addressed this need for clarification in my comments on proposed Rule 26(b)(2), and will not repeat them again here.

Second, and relatedly, the Committee should avoid a potential ambiguity in the second limitation on the safe harbor—the requirement that a party not violate an "order in the action requiring [a party] to preserve" electronic data. The notion that a party shouldn't destroy data in the face of an order not to do so is irrefutable. The question, however, is how specific must the preservation order be to subject a party to sanctions for failing to suspend the routine operation of its disaster recovery system? In Intel's view, the order should ***specifically require*** that such disaster recovery systems be suspended before sanctions can fairly be imposed.

General preservation orders have become commonplace in litigation. Such orders often are merely broad commands to preserve documents and information relevant to the litigation. These general orders often are entered in rubber-stamp fashion, without any regard to how they might apply to routine electronic information systems, and certainly without any specific showing of cause for suspending the systems. It would be especially unreasonable to view these general orders as prohibiting the suspension of electronic information systems, given the Committee's recognition that "[w]holesale or broad suspension of the ordinary operations of computer disaster-recovery systems . . . is rarely warranted." *See* Committee Note to Proposed Rule 26(f); *see also* Manual for Complex Litigation § 11.442 at 73 (4th ed. 2004) ("Routine system backups for disaster recovery purposes may incidentally preserve data subject to discovery, but recovery of relevant data from nonarchival backups is costly and inefficient, and a data-preservation order that requires the

accumulation of such backups beyond their usual short retention period may needlessly increase the scope and cost of discovery.").

Accordingly, Intel urges that the second limitation on the safe harbor be modified to apply only where a court ***specifically*** directs the suspension of "the routine operation of the party's electronic information system." *Cf.* Manual for Complex Litigation § 10.151 at 15 (4th ed. 2004) (noting that "a clear, specific, and reasonable management program, developed with the participation of counsel, will reduce the potential for sanctionable conduct because the parties will know what the judge expects of them").

III. CONCLUSION.

On behalf of Intel, it has been my pleasure to appear before this Committee to discuss this important aspect of civil litigation that promises to become even more important in the future. I appreciate this opportunity, wish the Committee well in its continuing work and deliberations and would be happy to entertain any questions that the Committee may have about my comments.