04-CV-010

"Middleton, Stephanie A ESQ TL48E" <Stephanie.Middleton@CIGNA.COM>
10/06/2004 02:19 PM

To "'Peter_Mccabe@ao.uscourts.gov'" <Peter_Mccabe@ao.uscourts.gov>
cc
Subject Electronic discovery hearing Wash, DC, Feb 11

I would like to sign up to testify at the Washington, DC hearing on February 11.

04-CV-010 Testimony 2/11 DC

Stephanie A. Middleton
Chief Counsel
Litigation
CIGNA Corporation

RECEIVED 2/9/05

CIGNA

Routing TL-48E
Two Liberty Place
1601 Chestnut St., TL-48E
Philadelphia, PA 19192
Telephone 215.761.4936
Facsimile 215.761.5511
stephanie.middleton@cigna.com

F A C S I M I L E T R A N S M I S S I O N

DATE: FEBRUARY 9, 2005

TO: PETER G. McCABE

FAX #: 202-502-1766

FROM: STEPHANIE A. MIDDLETON

PHONE #: (215) 761-4936

FAX #: (215) 761-5511

COMMENTS:

NUMBER OF PAGES INCLUDING COVER: 6

If transmittal is incomplete, please call:
Anne DiFabio
(215) 761-6232

Peter G. McCabe
Secretary
Committee on Rules of Practice and Procedure
of the Judicial Conference of the United States
Washington, DC 20544

Comments to the Committee Regarding Proposed Amendments to the Federal Rules of Civil Procedure Governing the Discovery of Electronically Stored Information

Introduction

I am Chief Litigation Counsel for CIGNA Companies. CIGNA's businesses are data-driven. CIGNA's health care businesses, for example, use vast systems to, among other things, process claims; apply data relating to contracts with customers and fee schedules with physicians, hospitals, and other health care providers; and create and maintain records for financial, regulatory, vendor management, and employment and benefits purposes. In addition, many of our 37,000 employees, for better or worse, spend much of their work day sending and receiving e-mails. In a recent month, there were approximately 10 million e-mails that came into and went out of CIGNA's electronic walls. Within those electronic walls, on an average day approximately 500,000 e-mails are circulated. CIGNA Companies may have several lawsuits pending at any one time; these disputes involve demands ranging from a few hundred dollars to hundreds of millions of dollars.

I first want to express my appreciation to the rules committees for so thoroughly and thoughtfully addressing the escalating problems related to electronic discovery. There is a genuine need to amend the Federal Rules to establish clear and consistent guidelines and to balance the benefits and burdens of preserving and producing electronically stored information. The current uncertainty resulting from variations in approach to this topic among jurisdictions and judges, leads to (1) the inability of parties to resolve discovery issues on their own, so that courts are forced to spend too much time as referees; (2) concern about sanctions, which forces attorneys to tell clients to "save everything." In extreme cases, businesses and other parties are forced to use unreasonable amounts of memory and take other steps that interfere with proper functioning of information systems and business processes, at least until a court gets heavily involved in discovery motions. Clients are stunned that the tail can wag the dog in this manner, as they do not believe that their lives or businesses exist primarily for the purpose of being able to respond to potential discovery requests. In addition to being wasteful and inefficient, this drives many parties from the courts or prevents them from ever reaching resolution on the merits.

In one case involving my client, a federal court, upon what must have seemed like a reasonable request from plaintiffs that all electronic information should be secured from any possibility of destruction, alteration or loss, signed an order requiring that all of our employees be informed that they could not delete, move or change any electronic or paper information that might possibly be relevant to what were, at the beginning of the case, broadly worded claims relating to essentially everything

connected with conducting the business. For the several days it took to get on the court's schedule to be heard, we had the choice of risking contempt sanctions, or essentially shutting down, as compliance with such an order was truly impossible. Other companies were subject to the same order. My comments below (for economy I am commenting only on the provisions or phrases that cause me concern, not those provisions that seem perfectly fine) are made in the context of this and other experiences. The expressed concerns are not based on hypotheticals.

My comments also are anchored in Rule 1 of the Federal Rules of Civil Procedure, which states that these rules "shall be construed and administered to secure the just, speedy, and inexpensive determination of every action." How do we keep that admonition from being lost in the sea of digital data that some would argue potentially could lead to potentially relevant evidence in any of the many hundreds of lawsuits that are filed against a government agency or large company, or in the few lawsuits that are served on a small business with limited resources for defense, or in the single suit filed against an individual who may own a personal computer, cell phone and a Blackberry?

Concerns

Reading the proposed changes together, I have the following concerns:

Rule 37

• The **safe harbor** is not a harbor when read in conjunction with the other changes. Imagine being handed the order described above, and applying the rule as proposed, especially as it relates to "inaccessible" or dynamic material. It is understandable that a court or party may tend toward overinclusiveness, but courts too often enter broad or vague preservation orders at the beginning of a case, based on broadly worded initial pleadings. (Consider the difference between the complaint and the consolidated first amended complaint typically filed in a shareholder class action.) When any data (eventually) sought by a requesting party has been lost, in hindsight and almost by definition, it is easily argued that a party did not take "reasonable steps" and was "negligent."

• Changes to Rule 37 should make it clear that taking **reasonable steps** means preserving or producing reasonably **accessible** information after the party knew or should have known the information was discoverable. Sanctions are appropriate only if a party is culpable, and a party is culpable only if it failed to take such steps and intentionally or recklessly violated an order to preserve **specific** and **material** information.

• Put another way, changes to Rule 37 do not make it clear that a party should not be sanctioned for failing to undertake the significant burden of preserving inaccessible data that they are rarely required to produce. In reality, and in widely recognized "best practices," discoverable information normally can be preserved and produced from active information retained for business purposes through **"litigation hold" memoranda**, and this renders unnecessary: (1) the routine preservation of massive

amounts of electronic information that is not reasonably accessible; (2) courts being mired in discovery disputes in every case; and (3) court ordered preservation.

• There should be clarification that agreements and stipulations regarding preservation, which may be approved by the court, are desirable; **court ordered preservation** is not, and should not become, the norm in most cases. Such orders are akin to TROs, and are normally necessary only when there is some evidence that a party is engaged in, or intends to engage in, inappropriate or prohibited acts. Further, the amendments should be made clear that any such orders must be specific and tailored to the circumstances of the case, after careful weighing of the burdens and benefits, and consideration of proportionality. This is key to having any meaningful safe harbor provision, and only **intentional or reckless** violation of a such court order merits sanctions.

• Some have expressed concern that **systems might be designed** to thwart legitimate discovery efforts and that parties have a predilection to destroy data. In reality, producing parties are highly motivated to make information needed for regulatory and business purposes readily or reasonably accessible, and do not have the time or the inclination, for numerous reasons, to do otherwise.

Rule 26(b)(5)

• With the massive volumes of electronic materials that are now turned over in litigation, there is bound to be inadvertent production of **privileged** or trade secret or other proprietary information. It is not burdensome for the requesting party to **certify** that such materials have been returned and all copies destroyed, and this may be one small step toward ensuring the material does not turn up on the internet.

• The rule or comment also should clarify that a party must act within a reasonable time after it learns of the inadvertent production, rather than a **reasonable time from production.**

Rule 34

• The proposed rules suggest a preference for production in **"native format."** Because of the dynamic nature of this format, Bates stamping, effective document management, protective order marking, use in depositions or motions or trial, and authentication may become serious problems if this suggestion remains. Production in native format also may unnecessarily increase the burdens of production as a result of the additional privilege review required, so it is not the preferred format in many or most cases. The rule should simply require the parties to discuss form of production at an early stage.

• The requirement to produce materials in a **"searchable"** format should be changed to a requirement to produce in a **"usable"** format. The apparent preference for a searchable format suggests, among other things, that in the many cases where paper documents are sufficient and acceptable to reasonable parties, a court should allow the requesting party to impose burdens of preserving, searching for, and producing

electronic evidence. In addition, some information, such as graphic or audio data, may not be searchable absent extreme steps, but is usable and useful.

• There should be clarification that none of the changes even remotely suggest that anyone other than the producing party has any discretion to require that party to give **direct access to its systems** to the requesting party.

Rule 26(b)(2)

The proposed amendment to Rule 26(b)(2) states that a producing party "need not provide discovery of electronically stored information that the party identifies as not reasonably accessible" without a court order based on a showing of good cause. The cost-benefit analysis and the proportionality concepts embodied in this amendment are welcome; however:

• As worded, this provision and the identification requirement may bog down courts in **excessive motion practice** over whether the information is actually inaccessible and may impose on a producing party unreasonable preservation and production obligations that do not exist under the current rules.

• The changes should make it clear that it is not necessary in all responses or cases for a producing party to **identify inaccessible information,** create a specific list of all places a party did not look (including places the party may not know about after reasonably searching accessible materials in response to appropriate requests), or specifically identify inaccessible data not produced in something akin to a privilege log. Only if the requesting party explains the need for additional information, should the producing party describe categories of inaccessible information and places or things not restored or searched, such as back-up tapes, legacy systems, meta-data, embedded data, and dynamic data bases. Otherwise, the rule could be read by some to require a producing party to create roadmaps to excessive discovery.

• The note should reflect that, in most cases and as has long been the presumption, the primary sources of discoverable materials are accessible records maintained for business and regulatory purposes, and other paper or electronically stored information that is active and purposely stored in a manner that anticipates future use in the normal course of business or daily life.

• The note should include, as examples of the type of information that may not be easily or reasonably accessible or presumptively and routinely to be produced, metadata, embedded date, and dynamic data bases.

• The note should state clearly that electronically stored information that is "not reasonably accessible" need not be produced or preserved absent agreement or court order. Under the changes as written, a party still may feel compelled to undertake to preserve vast quantities of inaccessible information that is of no use to them, and that interferes with memory and normal functioning of business, on the mere possibility that opposing party may at some point seek production of the data.

• The notes should clarify that, in the two-tiered approach, "reasonably accessible" for purposes of production does not necessarily or always include all **active and online or dynamic** data that may be **in use** for normal business transactions. Much active, online information is very difficult and costly to **preserve unaltered**, or retrieve and get into a format that is usable in litigation or is suitable for production. For example health care claims data resides on large mainframe claim engines, and broad requests may require extensive diversion of resources to program an extract of the information, which cannot be performed during most of the 24 hours a day because the engine is otherwise engaged in its intended work – paying health care claims. The note should recognize that active data generally should be considered accessible "unless obtaining such active data would be unduly costly or disruptive." In addition, the rules could be clearer that, merely because a backup tape has been accessed in the past, does not mean it is deemed accessible for all purposes for all time, or render all back up tapes of that party "accessible"; the extra steps of reviewing and producing information still present a substantial and often unwarranted additional burden upon the producing party that should not be imposed absent good cause.

• Examples of inaccessible information, in addition to back-up tapes and **obsolete and older systems**, could also include some reference to **meta-data**, embedded data, and dynamic data bases. The two-tiered approach is very good, but in reality there should be something akin to a **three-stage approach to production**, in which the producing party at the first stage provides accessible data in the form normally used in regular (i.e., non-litigation) activities. Only at a second stage, and upon request relating to specific documents or information, should a party produce, for example, the meta-data or embedded data related to those documents. And then, at a third stage or second tier, the parties can determine, or ask the court to determine, the appropriate extent and cost allocations for (further) discovery of inaccessible data.

• The rule or note should state a presumption of **cost allocation** for the preservation, retrieval, review and production of electronically stored information, especially where the information is not reasonably accessible. Cost shifting is an incentive for a party to be reasonable in, and focus on the burdens created by, its standard demands, even when the party is not consciously intending the discovery to be excessive or abusive. Put another way, cost shifting may be the only deterrent to the typical overbroad demands for marginally relevant materials of both sides.

• This **cost allocation presumption could be overcome** by specific, clear evidence of need and relevance, and demonstration that cost shifting would be unjust or otherwise inappropriate, and such a required showing is not unduly burdensome.

Stephanie A. Middleton