Johnson & Johnson

OFFICE OF
GENERAL COUNSEL

ONE JOHNSON & JOHNSON PLAZA
NEW BRUNSWICK, N.J. 08933-7002

04-CV-096
Request to Testify
2/11 DC

January 20, 2005

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

Dear Mr. McCabe:

I am Associate General Counsel, Litigation at Johnson & Johnson, responsible for the corporation's litigation worldwide. I will shortly be submitting our comments on the proposed amendments to the Federal Rules pertaining to electronic discovery and respectfully request the opportunity to amplify some of those comments at the hearing scheduled in Washington, DC on February 11.

Very truly yours,

Theodore B. Van Itallie, Jr.

Phone 732-524-2075
Fax 732-524-1277

Johnson & Johnson

04-CV-096
Testimony
2/11 DC

OFFICE OF
GENERAL COUNSEL

ONE JOHNSON & JOHNSON PLAZA
NEW BRUNSWICK, N.J. 08933-7002

January 31, 2005

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

Amendments to the Federal Rules of Civil Procedure

Dear Mr. McCabe:

I am Associate General Counsel, Litigation, for Johnson & Johnson, and write to comment on the proposed amendments to the Federal Rules of Civil Procedure relating to production and management of electronically stored information. We overwhelmingly support the need to update the civil rules to account for the changes wrought by the increase in the creation and storage of electronic data and thank the committee for its extremely thoughtful analysis of these issues.

Johnson & Johnson is vitally interested in the proposed amendments because its more than 200 operating companies world wide receive, generate and store vast quantities of electronic data while at the same time operating in business segments – pharmaceuticals, medical devices and consumer health care products – associated with significant amounts of on-going litigation both inside and outside the U.S.

In defending and prosecuting such litigation our focus is on outcomes based on the merits of the individual cases and we strive to preserve and produce all discoverable information. We work extremely hard to avoid any basis for a charge that we have failed to preserve or produce relevant information. We are acutely mindful of the expense, delay and impact on outcomes such a charge can have.

Johnson & Johnson and its operating companies have a vastly complex information architecture. We have certain enterprise systems that span multiple

operating companies such as email and human resources databases and many more at each of our operating companies tailored to their individual lines of business. Managing litigation preservation and production obligations against such a backdrop is already complex. Managing those obligations without adequate guidance and protection from up-to-date rules is highly problematic.

The proposed rules amendments respond precisely to that need and will prove invaluable to courts and litigants. We describe below several places where we believe that clarification would be helpful but we also want to stress that overall we applaud the committee's excellent work and leadership in this area.

Identifying Inaccessible Electronically Stored Information

First, we are concerned about the arguable lack of clarity attending the obligation in the proposed amendments to Rule 26(b)(2) that the party responding to a discovery request "identif[y]" inaccessible electronically stored information not being produced. If interpreted to require only that the party identify those repositories of inaccessible data located after reasonable investigation which are known or believed to contain discoverable materials, then the obligation is manageable. On the other hand, if interpreted to require a comprehensive inventory of all repositories of inaccessible data which might possibly contain discoverable information, then the rule significantly expands discovery obligations, becomes a snare for the unwary and will spawn satellite litigation.

The problem stems from the fact that the nature of a repository of inaccessible data makes it highly burdensome to determine whether or not it includes discoverable information. Furthermore, without regard to the diligence of the investigation, some systems and repositories undoubtedly will be missed creating the inducement for satellite "gotcha" litigation seeking to exploit the failure to identify the inaccessible data store.

The solution is to make it plain in the rule or the notes that the obligation is to identify general categories of inaccessible data known or believed to contain discoverable materials rather than to inventory all repositories of inaccessible data without regard to whether or not there is any basis to conclude they contain discoverable materials.

Instant Messenger Not Electronically Stored Information

Next, we are concerned that the terminology "electronically stored information" in Rules 33 and 34 might create controversy down the road. For example, Instant Messenger (IM) communications reside in RAM during the session but are not "stored" when the IM session is ended. It is therefore not "electronically stored information" and the note should clarify that such a form of communication is not intended to be included within the defined term.

If there is no business need to store IM sessions after they are concluded then there should be no litigation obligation to alter the configuration of such systems so that IM sessions are stored. This is no different than recognizing that businesses are not required to set up their phone systems such that phone conversations are stored even when phones are used to exchange information which in another form – such as email – would be required to be preserved and produced. It should be made clear in the notes or otherwise that residing in RAM is not "storage" under the Rule.

Form of Production

We are likewise concerned with potential confusion about Rule 34's terminology describing the default form of production of electronic material: "a form in which it is ordinarily maintained, or an electronically searchable form." If the first "form" is understood as precluding the movement of materials from the location where "ordinarily maintained" to another location – such as from dozens or hundreds of personal computers to a central storage area where it may be searched and produced – then real problems will occur as that is how large collections and productions typically occur. The rule or notes should clarify that no such restriction is intended.

The second form is similarly burdensome to the extent it suggests the materials must be converted into a searchable form if not already in such a form. The rule should indicate that the producing party need not make the material any more searchable than it currently is.

Safe Harbor

A. Broad Preservation Orders Should Not Trump the Safe Harbor

Finally, we are concerned that the "safe harbor" arising from the amendments to Rule 37 will be vitiated by the entry of broad preservation orders. Not only will the safe harbor be unavailable under such circumstances under the amended rule, but in addition our adversaries will claim that the rule requires in such circumstances (where a blanket preservation order exists) suspension of all routine computer operations such as recycling of backup tapes even where a highly effective litigation hold process exists. As the Committee comments in its Report (pp. 7-8): "suspension of all or a significant part of that [automatic deletion or overwriting] activity could paralyze a party's operations. "

We believe that the type of preservation order that should trump the safe harbor is exclusively one entered after the amended Rule 26(f) discussion about preservation and one carefully tailored to the case and the issues it presents. If either party believes that such routine operations should stop they have an obligation to surface the issue rapidly under Rule 26(f) and make a motion if no agreement is reached. It is not appropriate or fair for a large enterprise to stop recycling or the using data management programs required for on-going business based on the risk of a "gotcha" motion months after a lawsuit has

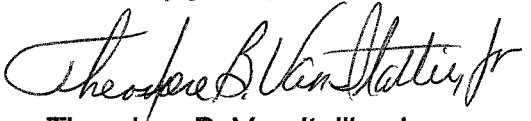
begun. The burden should be on the party seeking discovery rapidly to determine if a basis exists for shutting down the routine operation of computer systems and to obtain a precise court order resolving the issue before the producing party should face the risk of sanctions for pursuing essential business processes.

B. Level of Culpability for Sanctions

A related issue concerns the basis for a determination under the safe harbor rules that sanctions are appropriate for the elimination of discoverable evidence due to the routine operation of the computer system. We believe that a showing of mere negligence cannot be enough for sanctions in this setting because it will always be possible to show that more care would have preserved the materials in question. The entity at issue must actually know – or be so close to knowing as to be reckless – that discoverable data is being destroyed before sanctions can ever be applied for destruction through the "routine" operation of computer systems. Any other approach will be paralyzing for large data generators.

Thank you very much for the opportunity to comment on these Rules amendments and we appreciate very much the hard work the Committee has done in working towards dramatically improved guidance for parties, lawyers and courts in this important area.

Sincerely yours,



Theodore B. Van Itallie, Jr.