04-CV-209

Kroll Ontrack®

February 11, 2005

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

RE: PROPOSED CHANGES TO THE FEDERAL RULES OF CIVIL PROCEDURE

Dear Mr. McCabe,

On behalf of Kroll Ontrack Inc., a leading provider of electronic discovery, paper discovery, and computer forensics services, we would like to commend the Committee on its much anticipated draft amendments to the Federal Rules of Civil Procedure ("Rules") concerning electronic discovery. Electronic discovery has become routinely accepted in today's legal arena, and courts are increasingly requiring counsel to actively engage in directing and managing the electronic discovery process. With the release of these Rules, federal courts and lawmakers take a great step forward in setting e-discovery standards for litigators, corporations and courts. In addition to lending our support, Kroll Ontrack would like to offer a response to your request for further comments on the Rules and contribute to the revision process.

Early Discussion of Electronic Data
We commend the Committee on amending Rules 26(f) and 16(b) and Form 35 to prompt early discussion of issues relating to electronically stored information. With this amendment, parties will be required to discuss relevant electronic information – such as preservation obligations, discovery time frames, costs, and production format – during the meet and confer conference. These amendments will also put courts on notice that a need to address electronic information early in the litigation exists. This is a solid addition to the Rules that reflects best practices by competent litigators.

Definition of Electronically Stored Information
Proposed Rule 34(a) clarifies and modernizes the definition of discoverable material by specifically indicating that electronically stored information is subject to discovery. However, Rule 34(a)(1)(A) may require further clarification.

First, the Rule could clarify whether the term "images" simply includes document images (such as tiff images, PDF images, graphical images, etc.) or if it indicates "mirror images" – that is, forensically sound, bit-by-bit copies of hard drives. The discovery burden placed on a party may be much greater and more complicated if a court construes this language to mean hard drive mirror images since a hard drive mirror image captures all information contained on a hard drive, including active data, deleted data, Internet files, etc.

In addition, the Rule does not address whether metadata is included in the definition of "any designated electronically stored information of any designated documents." We suggest including metadata in the text of the Rule. Metadata describes computer-based information, explaining the "who, what, when, where, and how" of an electronic document,

and provides crucial information when authenticating an electronic document in court. In the context of litigation, an electronic document is incomplete without proper metadata documentation. Because metadata is not included in standard printed documents, attorneys engaged in litigation involving e-documents will not produce or receive a complete document if the electronic documents are simply printed. Based on these factors, we recommend the Committee expressly include metadata in Rule 34(a)(1)(A).

Production Format

Rule 34(b) allows a requesting party to designate the form in which it wishes to have electronic information produced. We support the Committee's method of allowing parties to specify their desired production format. This allows for a variety of production formats, including native, tiff and text productions.

However, the Rule could clarify definitions pertaining to the default production option, which states that if a production format is not specified, parties must produce information in the form in which it is "ordinarily maintained, or in an electronically searchable form." We recommend clarifying the definition of "ordinarily maintained." Some practitioners and courts may read the term to imply that production must be exclusively in native format. The term could also be construed to mean merely producing data electronically, in which case the responding party could potentially produce in an electronic format that might be virtually unusable by the demanding party.

Option to Produce Electronically Stored Information in Response to Interrogatories

The current version of Rule 33 allows a party responding to an interrogatory to produce business records as an option for responding to an interrogatory. The proposed Rule 33 allows the responding party to produce electronic information when responding to interrogatories as long as the requesting party can fairly locate and identify the information. While we support this addition, we also suggest clarifying the scope of the responding party's burden – the Rule could identify what the responding party must provide to ensure the demanding party can use the information as easily as the responding party. For example, comments to the Rule could give examples of the degree of technical support a demanding party may be required to offer (*i.e.*, the responding party needs to provide technical support for a relevant but proprietary computer database).

Reasonably Accessible Information

Rule 26(b)(2), absent good cause, requires production of data which is "reasonably accessible." We are concerned that the "reasonably accessible" requirement may result in unintended consequences. The Rule, as drafted, puts the producing party in the sole position of determining what information is inaccessible. Such a Rule may be susceptible to self-serving evaluations of data accessibility. For instance, critical case data may reside on backup tapes or other media, which in some cases will be easily accessible by a party. However, that party has an incentive to claim that accessing such storage or backup data is inaccessible simply because it is less convenient than accessing active data. Certainly, a party should not be able to avoid properly complying with discovery by claiming that data is inaccessible, without an objective standard or set of criteria against which the court can weigh the accessibility of the data.

We also recommend, as others have also suggested, that the Rule shed light on what constitutes "reasonably accessible" data. For example, the Rule could give guidance on whether deleted data, archived data, embedded data, or legacy data is included in this definition. In some cases recovering deleted computer files, accessing legacy data, or recovering antiquated backup tapes may be inconvenient; at the same time, however, it may not necessarily constitute "inaccessible" data. Without further objective guidance or clarification, parties may attempt to exclude data

and documents that could go to the very heart of the legal matter based upon their subjective assessment of a definition.

In addition, the Rule could articulate what is meant by the "good cause" required to overcome the presumptive standard and offer examples of the factors a court should weigh when determining if "good cause" exists to access inaccessible data. For instance, a court might consider a variety of factors including the necessity of the data, the availability of the data from other sources, and the ability of the parties to bear the production costs. More specifically, the court could consider a factual record based upon a showing that certain hardware or software, which would allow access to the data, is still in business use. If the software is currently in use, a claim of inaccessibility would be less appropriate than if the hardware or software was a legacy system or program (*i.e.*, from a system which had been decommissioned a number of years prior to the request).

We also recommend that the Committee take into account the host of reported electronic discovery case decisions requiring parties seeking inaccessible information to pay for it. *See Zubulake v. UBS Warburg*, 217 F.R.D. 309 (S.D.N.Y. 2003) (Court should consider cost shifting when electronic data is relatively inaccessible); *OpenTV v. Libertate Technologies*, 219 F.R.D. 474 (N.D.C.A. 2003) (Court shifted part of the costs of accessing inaccessible source code data to the requesting party); *Wiginton v. CB Richard Ellis, Inc.*, 2004 WL 1895122 (N.D.Ill. Aug. 10, 2004) (Court ordered the plaintiff to pay 75 percent of the costs of restoring the backup tapes, searching the data, and transferring it to an online review tool). Frameworks set forth and reiterated in case law could form the basis of Rule-based solutions to the definitional questions of data accessibility.

Belated Assertion of Privilege

Rule 26(b)(5)(B) offers a method for a party to assert the privilege claim when privileged information is inadvertently produced. Under Rule 26(b)(5)(B), the producing party must notify the parties who received the information of its claim of privilege within a "reasonable time." Given the ease of inadvertent privileged electronic productions, we support this amendment as it is a practical solution to managing inadvertent productions. We also agree that the privilege return request should be reasonably prompt to be effective.

Safe Harbor Provision

Finally, in Rule 37(f), the Committee proposes limiting sanctions – absent a court preservation order – to the loss of electronically stored information that results from routine operation of a party's computer system if the party took reasonable steps to preserve the information. As a threshold matter, Rule 37(f) limits the court's discretion to impose sanctions by requiring the court to impose sanctions only when a party does not act reasonably and the information is not destroyed during routine business operations.

We submit that the Rule also consider conduct that violates a reasonable preservation letter as equally sanctionable as conduct that violates a preservation court order. The effect of the Rule's current wording may likely be an increase in the number of attorneys seeking preservation orders because they may want to ensure that the court has the discretion to issue sanctions should the opposing party spoliate data. This rule may have an adverse impact by failing to encourage litigants to manage discovery-related issues among themselves without unnecessary court intervention.

In this context, we suggest that the Rule offer some examples in the Comments of what constitutes "reasonable" preservation steps. For instance, acting reasonably might require a party to suspend automated document

destruction policies, notify opponents and third parties of the obligation to preserve data, and formulate a "preservation response team" to develop a plan for responding to the new or impending litigation. Or, the requirement might be tempered by the specific facts of the case, limiting preservation to key individuals, time periods or subjects.

Finally, the Committee could provide further clarification as to what is meant by "routine operation." The Rule and Comments could state whether "routine operation" applies exclusively to functions that require human intervention – such as backup tape recycling, where people and processes are involved – or whether it also applies to technology operations not requiring human intervention such as spam filtering, automatic email archiving and deletion, the routine booting of a computer, or data written to a hard drive. For example, a party could argue against the imposition of spoliation sanctions claiming that it took reasonable preservation steps even though data was lost through an automatic email archiving and destruction operation. The party could argue this data was not destroyed during "routine operation" because it was not a process handled by people but rather it was the result of an automatic technological operation that was out of the party's control.

Conclusion

In conclusion, we applaud the Committee's efforts to update the Rules to reflect the changing times. We also sincerely appreciate the opportunity to participate in the rule-making process and eagerly await the adoption of the discovery rule changes. If we can clarify any of our comments or be of further assistance, do not hesitate to contact us.

Respectfully,

Kristin M. Nimsger, Esq.
Vice President, Legal Technologies
Kroll Ontrack Inc.
9023 Columbine Road
Eden Prairie, MN 55347
(952) 906-4913
knimsger@krollontrack.com

Michele C.S. Lange, Esq.
Staff Attorney, Legal Technologies
Kroll Ontrack Inc.
9023 Columbine Road
Eden Prairie, MN 55347
(952) 906-4927
mlange@krollontrack.com