

RECEIVED  
1/10/05

**SochaConsulting** LLC

*Informing digital discovery decisions<sup>sm</sup>*

**George J. Socha Jr., Esq**  
1374 Lincoln Avenue  
St. Paul MN 55105  
Tel 651.690.1739  
Cell 651.336.3940  
Fax 651.846.5920  
george@sochaconsulting.com

January 10, 2004

04-CV-094  
Request to Testify  
2/11 DC

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:

Please accept this correspondence as my formal request to testify on the proposed electronic discovery rules in Washington, D.C. on February 11, 2005. I look forward to and appreciate the opportunity to participate in this process.

If you would like any further information from me regarding this request, please contact me via email at [george@sochaconsulting.com](mailto:george@sochaconsulting.com) or by phone at 651.690.1739.

Sincerely,



George J. Socha, Jr.



04-CV-094  
Testimony  
2/11 DC

## SochaConsulting LLC

*Informing digital discovery decisions<sup>sm</sup>*

George J. Socha Jr., Esq  
1374 Lincoln Avenue  
St. Paul MN 55105  
Tel 651.690.1739  
Cell 651.336.3940  
Fax 651.846.5920  
george@sochaconsulting.com

January 31, 2005

The Honorable 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: Proposed Amendments to the Federal Rules of Civil Procedure Regarding  
Electronic Discovery

To the Honorable Members of the Advisory Committee:

Thank you for this opportunity to provide comment on the proposed amendments to the Federal Rules of Civil Procedure regarding electronic discovery. Even a cursory review of the proposed amendments and draft comments show the enormous amount of effort and thought that you all have put into this endeavor, for which you should be commended.

### Background Information

By way of background and to provide some perspective on my comments, following is some background information. I am an attorney and electronic discovery consultant. I began seeking the discovery of electronically stored information in the early 1990's. My first reluctant brushes with electronic discovery consisted of depositions of persons most knowledgeable about systems used to generate, store and retrieve information located on electronic mail systems and backup tapes. The scope of my electronic discovery activities soon expanded to include restoration of data from outdated storage media, collection and analysis of information stored in normal-course-of-business databases, and collection and analysis of information stored on end-user computers, server computers and backup systems.

After nearly sixteen years in private practice, in July of 2003 I launched a consulting practice focusing on electronic discovery. As an electronic discovery consultant, I assist consumers of electronic discovery services and software in their efforts to craft and

implement effective electronic discovery strategies, identify and select appropriate electronic discovery services and software providers, and manage the electronic discovery process. I also have been appointed as a special master and technical advisor to the court. For electronic discovery providers, I provide insights into market trends; evaluate existing solutions, determine shortcomings and recommend improvements; prepare strategies for increasing the profile of their offerings; and assist with the development of new services, software, and strategies. Along with Thomas Gelbmann, I publish the 2003 and 2004 Socha-Gelbmann Electronic Discovery Surveys, which examined the size, scope and growth of the electronic discovery market in the preceding year. We are in the process of gathering data for the 2005 survey.

I have written and spoken extensively on issues relating to electronic discovery, including seven years as co-chair of the Glasser Legal Works Electronic Discovery and Records Retention Conference.

### **Rule 26(b)(2)**

The Committee has proposed adding new language at the end of Rule 26(b)(2) that offers a two-tiered approach for electronic discovery, built around the concept of reasonable accessibility of data:

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.

This approach appears to be consistent with existing practices for the discovery of information stored on paper as well as with the more effective practices for the discovery of electronically stored information. To better assist bench and bar in their application of this approach, the following revisions to the Committee Note for Rule 26(b)(2) may be of value.

#### ***Consider changing wording of example in Note***

The third sentence in the first paragraph of the Committee Note for Rule 26(b)(2) states:

For example, some information may be stored solely for disaster-recovery purposes and be expensive and difficult to use for other purposes.

I suggest changing “solely” to “primarily”:

For example, some information may be stored primarily for disaster-recovery purposes and be expensive and difficult to use for other purposes.

The reason for this suggestion is to avoid leaving the impression that even a single use of a disaster-recovery system for reasons other than recovering from a disaster would mean

that all of the information stored on that systems was presumptively “reasonably accessible” and hence subject to discovery without the need for a showing of good cause.

### ***Consider adding comment on range of disasters***

While the Note for Rule 26(b)(2) mentions disaster-recover purposes, it says nothing of what might constitute a disaster for which electronically stored information might be recovered. It might be useful to add a comment explicitly acknowledging systems used to backup electronically stored information for disaster recovery purposes are intended to address a broad range of disasters, not just the most extreme ones.

I regularly encounter attorneys who assume that only catastrophic events qualify as disasters for purposes of electronic discovery. For examples they offer destruction of a facility by fire, flood, or similar happenstance, or a situation where the entire contents of a server computer have been deleted because of equipment malfunction.

Backup systems are intended to allow for restoration of electronically stored information should these types of disaster occur, but they also are used for smaller but equally valid disasters, such as the corruption of a file so that it no longer can be accessed by an end user, damage to the hard drive of a backed-up computer so that information stored on at least a portion of the drive no longer can be readily accessed by the end user, or problems caused by malicious computer programs such as virus, worms and Trojan horses, especially where those problems are not immediately identified.

### ***Consider revising the discussion of “reasonably accessible” in Note***

The last full paragraph on the second page of the Committee Note for Rule 26(b)(2) states:

Whether given information is “reasonably accessible” may depend on a variety of circumstances. One referent would be whether the party itself routinely accesses or uses the information. If the party routinely uses the information - sometimes called “active data” - the information would ordinarily be considered reasonably accessible. The fact that the party does not routinely access the information does not necessarily mean that access requires substantial effort or cost.

I suggest that the Committee modify this paragraph to recognize that although a party routinely uses information, that does not necessarily mean that the information is “reasonably accessible” for discovery purposes.

At first blush this may sound like nonsense. Actually it makes a lot of sense, as I hope the following example demonstrates. Organizations of all sizes routinely rely on databases in order to accomplish a vast range of tasks. Rare is the organization today that does not depend on databases to meet its needs in areas such as accounting, human resources, customer complaints, contact management, product development. Typically users of these databases enter information into the databases using predefined electronic

forms and get information out of the databases in a limited number of preset ways. Often the users of the databases have no practical way of bypassing those forms to look at the full body of information stored in the databases, to evaluate that information in ways other than the ones provided by the makers of the database programs, or to report out information in ways other than provided by the software the end users work with on a routine basis.

My organization is like many others in this way. I use QuickBooks to keep track of the finances for my consulting practice. I use preset forms to enter information into QuickBooks, such as contact information for a new client or time spent working on a project. I also use preset forms to get information out of QuickBooks so that I can create invoices, balance my checkbook, or determine my year-to-date finances. The program allows me to make a limited number of modifications to the preset forms. From time to time, I want to look at the data in ways that as far as I can tell were not envisioned by the people who wrote the program. When this happens, I often find myself stymied and may eventually decide that the potential benefit of obtaining that information in that format is not worth the cost. Were I to be asked to go into this "active data" – information I routinely access and use – in ways that I have not done and which were not provided for by the makers of the software, I most likely would have to turn to expensive outside assistance to accomplish this in a reliable fashion.

Analogous challenges exist with respect to information stored in electronic form on end user computers, server computers, backup tapes and other storage devices.

In any event, the clause "sometimes called 'active data'" should be removed from this paragraph. The distinction between "active data" and "inactive data" is a murky one at best, and not one mentioned elsewhere in the proposed rule changes or the notes to the proposed changes. Among practicing lawyers, the term "inactive data" often seems to be used to describe any electronic information stored on backup tapes and the term "active data" to describe all other electronically stored information. This may accurately describe the situation for some organizations or individuals, but for many others it is not just inaccurate but misleading.

There is another way in which reasonably accessible can become an issue – capacity. Should a party be required to attempt to locate "reasonably accessible" information within much or all of its computer network or on many or all of its backup systems, as a practical matter it may not be able to muster the capacity to accomplish this. Consider backup tapes as an example. To the best of my knowledge, most providers of electronic discovery services who purport to be able to restore information from backup tapes reach the limits of their capacity well before 100 tapes. I know of only three electronic discovery service providers who purport to have the capacity to handle truly large volumes of tapes. One recovered information from a collection of approximately 10,000 tapes, a second from a grouping of approximately 14,000 tapes, and a third from a set of over 100,000 tapes. If a party in a lawsuit were required to attempt to located information in a collection of 50,000 tapes, as of today there appears to be only one vendor in the industry claiming to be able to accomplish that. The same limitations exist

with respect to information on other types of backup systems as well as on active servers and end user computers, but are more difficult to describe.

I have heard some argue that we do not need to concern ourselves with backup tapes in the rules or the notes to the rules because in short order backup tapes will disappear. In my estimation, this is unlikely to happen for some time. First, organizations that have invested in backup tape systems and made those systems an integral part of their business operations are likely to switch to some type of tape-less backup system when (a) the pain of continuing to use a tape-based system becomes substantial, (b) affordable tape-less systems are available at a price the organization feels is in line with the benefit derived from replacing the old system with a new one, and (c) the organization determines that it is willing to suffer the disruption of replacing systems. This is akin to replacing your furnace at home; you generally do not do it until you really, really need to. The second reason tapes are likely to be here for a while is that the tape industry does not want to go away. Providers of tape systems are busily working to be able to offer less expensive, more powerful systems to prevent their customers from abandoning tape systems in favor of tape-less ones, and in many cases appear to be succeeding. Finally, litigation generally is a backward-looking process. Ten years hence we could well be trying to get information off tapes created today; so long as the tapes exist and have the potential to contain relevant damning or exculpatory information, parties will have an interest in determining what they contain and whether that information is useful.

***Consider revising the comment about “actually accessing” requested information***

That last sentence in the first full paragraph of the third page of the Committee Note for Rule 26(b)(2) states:

But if the responding party has actually accessed the requested information, it may not rely on this rule as an excuse from providing discovery, even if it incurred substantial expense in accessing the information.

This provision is subject to the same problems described above. The mere fact that a party has accessed the requested information in some fashion does not mean that the party has ready or even any access to the information in the fashion sought by the requesting party.

**Rule 26(f) and Rule 34(b)**

Rule 26(f) and Rule 34(b) discuss, among other things, the form of production. As currently worded, the Committee Notes for those subsections might be interpreted to suggest that for a single production of electronically stored information, all the information must be produced in a single form. This could cause problems for requesting and producing parties alike, as there are times when multiple forms would be more appropriate. A single production might contain both (a) spreadsheet files containing privileged materials where the need for redaction requires that the spreadsheet file be converted from its native format to a quasi-paper format such as TIFF or PDF and (b)

relational database files that are meaningful only if produced as an electronic database and that become unusable if converted to TIFF or PDF. In such a situation, a single form of production would be counter-productive for all involved.

Accordingly, I suggest the following changes:

***Consider revising references to “form” and “format” in the Note for Rule 26(f)***

The paragraph at the top of the second page of the Committee Note for Rule 26(f) refers to “form” and “format.” Change those to the plurals “forms” and “formats.”

***Consider adding a comment at the end of the Note for Rule 34(b)***

Consider adding the following comment at the end of the Committee Note for Rule 34(b), after the paragraph ending “Advance communication about the form that will be used for production might avoid that difficulty.”

A party may be asked to produce a range of types of electronically stored information, so that a single production might include word processing documents, email messages, electronic spreadsheets, complete databases and subsets of other databases. Requiring that such diverse ranges of electronically stored information all be produced in one single form may reduce meaningful access to the information while at the same time increasing the costs of producing and working with the information. The amendment therefore permits the requesting party to choose different forms of production for different types of electronically stored information and provides the same option for the producing party.

**Rule 34(a)**

The Committee Note to Rule 34(a) states, at the bottom of the first page:

A reference to “images” is added to clarify their inclusion in the listing already provided.

It is not clear to me what is meant by “images.” Is this intended to address image files (JPEG, GIF, TIFF, PDF, etc.) used by parties in the normal course of their activities, or is it intended to address image files created by or for attorneys for the parties during litigation? A clarification would be useful. If the latter is what the Committee intends, I would caution that this opens a whole new area of dispute that so far as I know has not been contemplated as part of this rule-making process.

**Rule 45**

The Committee Note to Rule 37(f) states, in the first full paragraph on the fourth page of the Note:

Rule 37(f) does not apply if the party's failure to provide information resulted from its violation of an order in the action requiring preservation of the information. An order that directs preservation of information on identified topics ordinarily should be understood to include electronically stored information. Should such information be lost even though a party took "reasonable steps" to comply with the order, the court may impose sanctions. If such an order was violated in ways that are unrelated to the party's current inability to provide the electronically stored information at issue, the violation does not deprive the party of the protections of Rule 37(f). The determination whether to impose a sanction, and the choice of sanction, will be affected by the party's reasonable attempts to comply. (Emphasis added.)

The underlined sentence seems to be designed to discourage parties from entering into preservation orders. It also suggests that parties may be required to take "unreasonable" steps once a preservation order is in place. These can hardly be the intent of the Committee.

Thank you again for the opportunity to participate in this process.

Sincerely,

  
George J. Socha, Jr.



RECEIVED  
2/15/05

## SochaConsulting LLC

*Informing digital discovery decisions<sup>sm</sup>*

George J. Socha Jr., Esq

1374 Lincoln Avenue  
St. Paul MN 55105  
Tel 651.690.1739  
Cell 651.336.3940  
Fax 651.846.5920  
george@sochaconsulting.com

January 31, 2005

04-CV-094  
Supplement to  
2/11 Testimony

The Honorable 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: Proposed Amendments to the Federal Rules of Civil Procedure Regarding  
Electronic Discovery

To the Honorable Members of the Advisory Committee:

Thank you for this opportunity to provide comment on the proposed amendments to the Federal Rules of Civil Procedure regarding electronic discovery. Even a cursory review of the proposed amendments and draft comments show the enormous amount of effort and thought that you all have put into this endeavor, for which you should be commended.

### Background Information

By way of background and to provide some perspective on my comments, following is some background information. I am an attorney and electronic discovery consultant. I began seeking the discovery of electronically stored information in the early 1990's. My first reluctant brushes with electronic discovery consisted of depositions of persons most knowledgeable about systems used to generate, store and retrieve information located on electronic mail systems and backup tapes. The scope of my electronic discovery activities soon expanded to include restoration of data from outdated storage media, collection and analysis of information stored in normal-course-of-business databases, and collection and analysis of information stored on end-user computers, server computers and backup systems.

After nearly sixteen years in private practice, in July of 2003 I launched a consulting practice focusing on electronic discovery. As an electronic discovery consultant, I assist consumers of electronic discovery services and software in their efforts to craft and

implement effective electronic discovery strategies, identify and select appropriate electronic discovery services and software providers, and manage the electronic discovery process. I also have been appointed as a special master and technical advisor to the court. For electronic discovery providers, I provide insights into market trends; evaluate existing solutions, determine shortcomings and recommend improvements; prepare strategies for increasing the profile of their offerings; and assist with the development of new services, software, and strategies. Along with Thomas Gelbmann, I publish the 2003 and 2004 Socha-Gelbmann Electronic Discovery Surveys, which examined the size, scope and growth of the electronic discovery market in the preceding year. We are in the process of gathering data for the 2005 survey.

I have written and spoken extensively on issues relating to electronic discovery, including seven years as co-chair of the Glasser Legal Works Electronic Discovery and Records Retention Conference.

## **Rule 26(b)(2)**

The Committee has proposed adding new language at the end of Rule 26(b)(2) that offers a two-tiered approach for electronic discovery, built around the concept of reasonable accessibility of data:

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.

This approach appears to be consistent with existing practices for the discovery of information stored on paper as well as with the more effective practices for the discovery of electronically stored information. To better assist bench and bar in their application of this approach, the following revisions to the Committee Note for Rule 26(b)(2) may be of value.

### ***Consider changing wording of example in Note***

The third sentence in the first paragraph of the Committee Note for Rule 26(b)(2) states:

For example, some information may be stored solely for disaster-recovery purposes and be expensive and difficult to use for other purposes.

I suggest changing “solely” to “primarily”:

For example, some information may be stored primarily for disaster-recovery purposes and be expensive and difficult to use for other purposes.

The reason for this suggestion is to avoid leaving the impression that even a single use of a disaster-recovery system for reasons other than recovering from a disaster would mean

that all of the information stored on that systems was presumptively “reasonably accessible” and hence subject to discovery without the need for a showing of good cause.

### ***Consider adding comment on range of disasters***

While the Note for Rule 26(b)(2) mentions disaster-recover purposes, it says nothing of what might constitute a disaster for which electronically stored information might be recovered. It might be useful to add a comment explicitly acknowledging systems used to backup electronically stored information for disaster recovery purposes are intended to address a broad range of disasters, not just the most extreme ones.

I regularly encounter attorneys who assume that only catastrophic events qualify as disasters for purposes of electronic discovery. For examples they offer destruction of a facility by fire, flood, or similar happenstance, or a situation where the entire contents of a server computer have been deleted because of equipment malfunction.

Backup systems are intended to allow for restoration of electronically stored information should these types of disaster occur, but they also are used for smaller but equally valid disasters, such as the corruption of a file so that it no longer can be accessed by an end user, damage to the hard drive of a backed-up computer so that information stored on at least a portion of the drive no longer can be readily accessed by the end user, or problems caused by malicious computer programs such as virus, worms and Trojan horses, especially where those problems are not immediately identified.

### ***Consider revising the discussion of “reasonably accessible” in Note***

The last full paragraph on the second page of the Committee Note for Rule 26(b)(2) states:

Whether given information is “reasonably accessible” may depend on a variety of circumstances. One referent would be whether the party itself routinely accesses or uses the information. If the party routinely uses the information - sometimes called “active data” - the information would ordinarily be considered reasonably accessible. The fact that the party does not routinely access the information does not necessarily mean that access requires substantial effort or cost.

I suggest that the Committee modify this paragraph to recognize that although a party routinely uses information, that does not necessarily mean that the information is “reasonably accessible” for discovery purposes.

At first blush this may sound like nonsense. Actually it makes a lot of sense, as I hope the following example demonstrates. Organizations of all sizes routinely rely on databases in order to accomplish a vast range of tasks. Rare is the organization today that does not depend on databases to meet its needs in areas such as accounting, human resources, customer complaints, contact management, product development. Typically users of these databases enter information into the databases using predefined electronic

forms and get information out of the databases in a limited number of preset ways. Often the users of the databases have no practical way of bypassing those forms to look at the full body of information stored in the databases, to evaluate that information in ways other than the ones provided by the makers of the database programs, or to report out information in ways other than provided by the software the end users work with on a routine basis.

My organization is like many others in this way. I use QuickBooks to keep track of the finances for my consulting practice. I use preset forms to enter information into QuickBooks, such as contact information for a new client or time spent working on a project. I also use preset forms to get information out of QuickBooks so that I can create invoices, balance my checkbook, or determine my year-to-date finances. The program allows me to make a limited number of modifications to the preset forms. From time to time, I want to look at the data in ways that as far as I can tell were not envisioned by the people who wrote the program. When this happens, I often find myself stymied and may eventually decide that the potential benefit of obtaining that information in that format is not worth the cost. Were I to be asked to go into this “active data” – information I routinely access and use – in ways that I have not done and which were not provided for by the makers of the software, I most likely would have to turn to expensive outside assistance to accomplish this in a reliable fashion.

Analogous challenges exist with respect to information stored in electronic form on end user computers, server computers, backup tapes and other storage devices.

In any event, the clause “sometimes called ‘active data’” should be removed from this paragraph. The distinction between “active data” and “inactive data” is a murky one at best, and not one mentioned elsewhere in the proposed rule changes or the notes to the proposed changes. Among practicing lawyers, the term “inactive data” often seems to be used to describe any electronic information stored on backup tapes and the term “active data” to describe all other electronically stored information. This may accurately describe the situation for some organizations or individuals, but for many others it is not just inaccurate but misleading.

There is another way in which reasonably accessible can become an issue – capacity. Should a party be required to attempt to locate “reasonably accessible” information within much or all of its computer network or on many or all of its backup systems, as a practical matter it may not be able to muster the capacity to accomplish this. Consider backup tapes as an example. To the best of my knowledge, most providers of electronic discovery services who purport to be able to restore information from backup tapes reach the limits of their capacity well before 100 tapes. I know of only three electronic discovery service providers who purport to have the capacity to handle truly large volumes of tapes. One recovered information from a collection of approximately 10,000 tapes, a second from a grouping of approximately 14,000 tapes, and a third from a set of over 100,000 tapes. If a party in a lawsuit were required to attempt to located information in a collection of 50,000 tapes, as of today there appears to be only one vendor in the industry claiming to be able to accomplish that. The same limitations exist

with respect to information on other types of backup systems as well as on active servers and end user computers, but are more difficult to describe.

I have heard some argue that we do not need to concern ourselves with backup tapes in the rules or the notes to the rules because in short order backup tapes will disappear. In my estimation, this is unlikely to happen for some time. First, organizations that have invested in backup tape systems and made those systems an integral part of their business operations are likely to switch to some type of tape-less backup system when (a) the pain of continuing to use a tape-based system becomes substantial, (b) affordable tape-less systems are available at a price the organization feels is in line with the benefit derived from replacing the old system with a new one, and (c) the organization determines that it is willing to suffer the disruption of replacing systems. This is akin to replacing your furnace at home; you generally do not do it until you really, really need to. The second reason tapes are likely to be here for a while is that the tape industry does not want to go away. Providers of tape systems are busily working to be able to offer less expensive, more powerful systems to prevent their customers from abandoning tape systems in favor of tape-less ones, and in many cases appear to be succeeding. Finally, litigation generally is a backward-looking process. Ten years hence we could well be trying to get information off tapes created today; so long as the tapes exist and have the potential to contain relevant damning or exculpatory information, parties will have an interest in determining what they contain and whether that information is useful.

### ***Consider revising the comment about “actually accessing” requested information***

That last sentence in the first full paragraph of the third page of the Committee Note for Rule 26(b)(2) states:

But if the responding party has actually accessed the requested information, it may not rely on this rule as an excuse from providing discovery, even if it incurred substantial expense in accessing the information.

This provision is subject to the same problems described above. The mere fact that a party has accessed the requested information in some fashion does not mean that the party has ready or even any access to the information in the fashion sought by the requesting party.

### **Rule 26(f) and Rule 34(b)**

Rule 26(f) and Rule 34(b) discuss, among other things, the form of production. As currently worded, the Committee Notes for those subsections might be interpreted to suggest that for a single production of electronically stored information, all the information must be produced in a single form. This could cause problems for requesting and producing parties alike, as there are times when multiple forms would be more appropriate. A single production might contain both (a) spreadsheet files containing privileged materials where the need for redaction requires that the spreadsheet file be converted from its native format to a quasi-paper format such as TIFF or PDF and (b)

relational database files that are meaningful only if produced as an electronic database and that become unusable if converted to TIFF or PDF. In such a situation, a single form of production would be counter-productive for all involved.

Accordingly, I suggest the following changes:

***Consider revising references to “form” and “format” in the Note for Rule 26(f)***

The paragraph at the top of the second page of the Committee Note for Rule 26(f) refers to “form” and “format.” Change those to the plurals “forms” and “formats.”

***Consider adding a comment at the end of the Note for Rule 34(b)***

Consider adding the following comment at the end of the Committee Note for Rule 34(b), after the paragraph ending “Advance communication about the form that will be used for production might avoid that difficulty.”

A party may be asked to produce a range of types of electronically stored information, so that a single production might include word processing documents, email messages, electronic spreadsheets, complete databases and subsets of other databases. Requiring that such diverse ranges of electronically stored information all be produced in one single form may reduce meaningful access to the information while at the same time increasing the costs of producing and working with the information. The amendment therefore permits the requesting party to choose different forms of production for different types of electronically stored information and provides the same option for the producing party.

**Rule 34(a)**

The Committee Note to Rule 34(a) states, at the bottom of the first page:

A reference to “images” is added to clarify their inclusion in the listing already provided.

It is not clear to me what is meant by “images.” Is this intended to address image files (JPEG, GIF, TIFF, PDF, etc.) used by parties in the normal course of their activities, or is it intended to address image files created by or for attorneys for the parties during litigation? A clarification would be useful. If the latter is what the Committee intends, I would caution that this opens a whole new area of dispute that so far as I know has not been contemplated as part of this rule-making process.

**Rule 45**

The Committee Note to Rule 37(f) states, in the first full paragraph on the fourth page of the Note:

Rule 37(f) does not apply if the party's failure to provide information resulted from its violation of an order in the action requiring preservation of the information. An order that directs preservation of information on identified topics ordinarily should be understood to include electronically stored information. Should such information be lost even though a party took "reasonable steps" to comply with the order, the court may impose sanctions. If such an order was violated in ways that are unrelated to the party's current inability to provide the electronically stored information at issue, the violation does not deprive the party of the protections of Rule 37(f). The determination whether to impose a sanction, and the choice of sanction, will be affected by the party's reasonable attempts to comply. (Emphasis added.)

The underlined sentence seems to be designed to discourage parties from entering into preservation orders. It also suggests that parties may be required to take "unreasonable" steps once a preservation order is in place. These can hardly be the intent of the Committee.

Thank you again for the opportunity to participate in this process.

Sincerely,

  
George J. Socha, Jr.

# SochaConsulting LLC

Informing digital discovery decisions<sup>sm</sup>

George J. Socha Jr., Esq

1374 Lincoln Avenue  
St. Paul MN 55105  
Tel 651.690.1739  
Cell 651.336.3940  
Fax 651.846.5920  
george@sochaconsulting.com

February 14, 2005

## DRAFT

The Honorable 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: Proposed Amendments to the Federal Rules of Civil Procedure Regarding  
Electronic Discovery

To the Honorable Members of the Advisory Committee:

Thank you for once again for the opportunity to provide comment on the proposed amendments to the Federal Rules of Civil Procedure regarding electronic discovery.

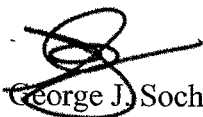
In my testimony before the Committee on February 11, 2005, I discussed as set of factors that might provide a useful framework for determining whether electronically stored information is "reasonably accessible." Following is a written version of that testimony.

Category	Description	Examples
Type	The information sought by the requesting party is of a type that the producing party routinely and knowingly uses, or that a reasonable entity in the producing party's circumstances would routinely and knowingly use. ("Routinely" is intended to denote normal-course-of-business usage, but not necessarily frequent usage.)	The text of a word processing document, but not necessarily the metadata associated with that file.  Active files on a computer hard drive, but not information stored in slack or swap space.



Category	Description	Examples
Form	The information sought by the requesting party is in a form that is consistent with the form or forms routinely and knowingly used by the producing party, of that a reasonable entity in the producing party's circumstances would routinely and knowingly use.	Information from an enterprise database system as provided through a report used by the producing party, but not information from that system that can be provided only by the creation of specialized reports that the producing party lacks the expertise to create.
Location	The information sought by the requesting party is stored in a location to which the producing party routinely and knowingly goes for business or similar purposes, or to which a reasonable entity in the producing party's circumstances would routinely and knowingly go for such purposes.	Online servers, but not disaster recovery systems.
Ability	The producing party has the hardware, software and expertise to gain access to the information sought by the requesting party, or a reasonable entity in the producing party's circumstances would have such hardware, software and expertise.	The ability to locate and copy a PST file, but not the ability to conduct computer forensics.
Effort	The effort required for the producing party to gain access to and produce the requested information is in line with the magnitude of the litigation.	

Sincerely,



George J. Socha, Jr.