



# E-Discovery News



## President's Note:

By: Mike Anderson

*E-Discovery News* is the first in a series of newsletters that we will send you to inform you of electronic discovery matters that may affect your practice. NTI is one of the leaders in providing electronic evidence discovery services to law firms, primarily through computer forensics and data conversion services.

Larry Johnson's article below discusses the importance of preserving evidence to avoid spoliation and points out that digital evidence may have a much shorter "shelf life" than you think. He indicates that "preserving evidence is just as important as disclosing it." Attorneys that do not adhere fully to Rule 26(a) may find that they are guilty of spoliation and subject to sanctions.

I would appreciate any feedback and comments you may have. If there is anything we can do to help you with these important legal discovery issues, please contact us at 503.661.6912 or e-mail [scott@dataforensics.com](mailto:scott@dataforensics.com).

**"...not all electronic evidence is created equal. Some of it has the life span of a June Bug."**



## Early Birds and Rule 26(a)

By Larry G. Johnson Esq.—Copyright © 2002, Legal Technology Group, Inc.

There are both technical and legal reasons why the old adage about the early bird and the worm is truer than ever for trial lawyers and their clients. If a lawyer doesn't aggressively move to preserve and obtain the relevant electronic evidence in a case, it could be gone forever. And now, thanks to a change in a court rule that governs civil litigation in the federal courts, Rule 26(a), lawyers don't even have a choice about it anymore: they must disclose the bulk of the evidence they have about their case or face sanctions, including the possibility of seeing their case thrown out of court.

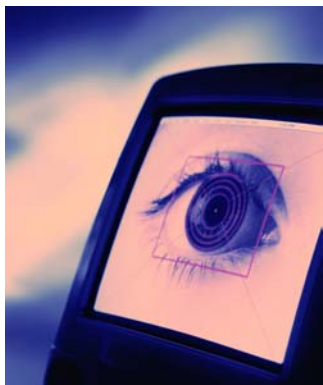
Lawyers who are used to doing electronic discovery sometimes get the feeling

that digital evidence is eternal, you can't get rid of the stuff, so why worry about when you have to start sifting through it all? Even if users "erase" data on hard drives, forensics experts can recover most of it, right? And as for emails, hey, they replicate like rabbits on backup tapes and on the hard drives of recipients and people to whom the emails are forwarded, and yet again on all those persons' backup tapes ad infinitum – so what's the rush?

Well, there are two kinds of rushes. First, not all electronic evidence is created equal. Some of it has the life span of a June Bug.[1] A key email may have existed briefly on the sender's and recipient's hard drives, but clever conspirators that they are, they were able to quickly remove all

*(Continued on page 2)*

## Early Birds and Rule 26(a)



traces of it. For a brief period of time, however, maybe as long as 60 days, that telltale email that could make or break a case might still reside on one or more servers of an Internet Service Provider.

These ISPs have full-time employees sitting at desks, waiting to receive subpoenas from tech-savvy lawyers. Most Terms of Service agreements between ISPs and their customers grant ISPs the right to respond to discovery demands from lawyers once they give their customers 15-day prior notice of a subpoena. But absent a court order, ISPs can and routinely do flush their servers of things like email and ftp logs which would help to prove when a user sent or received files via a server, and what those files were.

Also, data stored (increasingly, these days) on cell phones and PDA's (Personal Data Assistants, like PalmPilot or Blackberry) are not stored on hard drives (unless synched with a desktop computer) and are easily lost if users are not advised to preserve all digital information. For some top execs, their cell phones and PDAs are the only places they store any information of importance.

These are but a few examples of how ethereal some digital data can be, even if as a gross data phenomenon electronic evidence seems to be multiplying like The Sorcerer's Apprentice's brooms, bloating the nation's computer storage media.[2]

So much for the technical need for lawyers to be Early Birds, now on to the legal requirements.

The other important reason to do electronic evidence "due diligence" before or very early in litigation is not to run afoul of Federal Rule of Civil Procedure 26(a). This rule requires parties to exchange information "as soon as practicable and in any event at least 14 days before a scheduling conference," the first encounter counsel have in a case with the judge or magistrate.

Before December 1, 2000, it was possible for individual U.S. District Courts to opt out of this "early discovery" provision, something approximately two-thirds of all federal district courts had done. But no more. Now all district courts and the lawyers who try cases in them are subject to the new Rule 26(a).

The information that has to be exchanged is significant and broad in scope. And note: this is a required disclosure that must occur without the other side having to ask for it. Specifically, what each side has to turn over right away is the following:



"(A) the name and, if known, the address and telephone number of each individual likely to have discoverable information that the disclosing party may use to support its claims or defenses, unless solely for impeachment,[3] identifying the subjects of the information;

"(B) a copy of, or a description by category and location of, all documents, data compilations,[4] and tangible things that are in the possession, custody, or control of the party and that the disclosing party may use to support its claims or defenses, unless solely for impeachment;

"(C) a computation of any category of damages claimed by the disclosing party, making available for inspection and copying as under Rule 34 the documents or other evidentiary material, not privileged or protected from disclosure, on which such computation is based, including materials bearing on the nature and extent of injuries suffered; and

"(D) for inspection and copying as under Rule 34 any insurance agreement under which any person carrying on an insurance business may be liable to satisfy part or all of a judgment which may be entered in the action or to indemnify or reimburse for payments made to satisfy the judgment."

\



## Early Birds and Rule 26(a)

Complying with these requirements means basically disclosing your whole case against the other side – and now, not months later.

In addition, no lawyer should have to be reminded that, right from the start of the lawsuit, preserving evidence is just as important (if not more so) as disclosing it. Lawyers have to be especially careful that their clients are not negligently or purposely shredding evidence, let alone failing to disclose it under Rule 26(a). Deleting electronic files when a lawsuit is underway – or even before then, when a lawsuit can reasonably be anticipated – is called “spoliation.” Because ordinary use of computers inevitably leads to changes or loss of data, extraordinary efforts have to be taken to preserve data against spoliation, such as creating extraordinary backup tapes and image-copying (“cloning”) hard drives with potentially relevant information.

Failing to preserve evidence or disclose under Rule 26(a) can cause dire consequences. Under Rule 37 (which Rule 26(a) says applies to it), a judge can fine an offending party, limit what a party can present by way of evidence at trial, or even enter a judgment against an offending party before or during trial.[5]

A final, happier note: the need to gather, preserve and disclose evidence before or early in a lawsuit can result in significant savings. There are technologies and increasingly accepted protocols blessed by courts that can limit initial disclosures and discovery to a sampling of electronic data based on the probability of finding relevant data in relevant locations, to be balanced by cost and who should pay.

States like Texas have adopted court rules that state, essentially, that readily available information kept in the ordinary course of business should be made available by the owner of that information to any adversary requesting it. Anything else requiring unusual efforts has to be paid for by the requester and may be subject to court-imposed restrictions.[6]

Where both sides to a dispute have a lot of digital and other data, involving experts early to help shape and enforce protocols on sampling and disclosure of only the relevant information can significantly reduce the scope of electronic discovery.

###

Byline: Larry Johnson is an attorney and President of Legal Technology Group, Inc., with offices in Portland and Seattle, offering consulting, expert witness and due diligence services to law firms in their selection of litigation support technologies and services.

---

1 In case you didn’t grow up in a place like Minnesota, this is a flying insect that lives for one hot summer day, swarming in such numbers as to block the sun, and then it dies with its relatives in a sea of crunchy exoskeletons.

2 A UC Berkeley study indicates that “[o]ver 93 percent of the information produced in 1999 was in digital format,” and “[e]mail has become one of the most widespread ways of communication in today’s society. A white collar worker receives about 40 email messages in his office every day. Aggregately, based on different estimates, there will be from 610 billion to 1100 billion messages sent this year alone.” “How Much Information?” assembled by Researchers: Peter Lyman and Hal R. Varian.





## NEW TECHNOLOGIES INC.

2075 NE Division Street  
Gresham, OR 97030-5812

Phone: 503-661-6912  
Fax: 503-674-9145  
Email: [scott@dataforensics.com](mailto:scott@dataforensics.com)

The Ultimate in Computer  
Forensics

---

WE'RE ON THE WEB!  
[WWW.DATAFORENSICS.COM](http://WWW.DATAFORENSICS.COM)

---



### Early Birds and Rule 26(a)

3 “Impeachment” here is narrow and means “information you plan to use at trial to show somebody up as a liar (or at least inconsistent) during cross-examination.”

4 “Data compilations” include “information [that] can be obtained, translated, if necessary, by the respondent [person responding to a discovery request] through detection devices into reasonably usable form,” such as a computer. Leave it to lawyers to not just say “electronic evidence” when something more complicated will do.

5 Prudential, for example, had to pay \$1,000,000 in sanctions in a case where it rather lazily and clumsily told its employees not to destroy any evidence (which they continued to do due to lax supervision). In another case, Piper Aircraft, of Piper Cub fame, had a default judgment entered against it for selectively pruning from its files a number of documents that it thought might harm it in future litigation, even though no such litigation was pending at the time.

6 Tex. R. Civ. P. 196.4.