Legal Technology Group, Inc.

www.LegalTechnologyGroup.com

Main Office • Portland
1001 SW 5th Avenue, Suite 1100
Portland, OR 97204
Fax: (503) 697-3113

Seattle Area Office
313 Avenue D
Snohomish, WA 98290
Fax: (508) 448-5663

Office: (866) 883-2452 *toll free*

LARRY JOHNSON, Esq.
President
Johnson@LegalTechnologyGroup.com

TOM HOWE, Esq.
Chief Technology Officer
Howe@LegalTechnologyGroup.com

E-mail: Where the Good Stuff Is

Most of us are now familiar with the irony of Bill Gates being hoisted on his own petard when many of his emails were used to impeach him during cross-examination in the federal antitrust case against Microsoft. This and other well-publicized cases where email "made the case"[1] underscore the fact that litigators cannot afford to overlook email in discovery.

Email has replaced the telephone as the most commonly used communication medium in business.[2] In addition, collaborative work environments made possible by networked computers guarantee that important documents inevitably become email attachments in the course of team reviews and approval by higher-ups.

And there's something about email that gets people telling the truth. Emails make possible a kind of "virtual water cooler" where gossip and candidly-expressed thoughts are only a click of the "SEND" button away.

When was the last time you had a case where an important document did *not* wind up somewhere as an attachment to somebody's email? To be sure, certain types of documents, such as medical records and accounting data, are unlikely candidates for emails, but in most commercial litigation emails and their attachments will take center stage among the evidence.

---

[1] For example, it cost one company a $250,000 settlement because of this email: "I want you to get that [expletive deleted] tight-assed bitch out of here. I don't care what you have to do." In the Rodney King case, emails, sent from patrol cars immediately after the event, conclusively established racial bias in the judge's mind ("Oops, I haven't beaten anyone so bad in a long time"; "Sounds almost [as] exciting as our last call.... It was right out of 'Gorillas in the Mist.'"). At Chevron, it took the offensive email messages of just 4 employees to create the basis for a $2,200,000 settlement in another sexual harassment case. In the Fen-Phen litigation that ultimately settled for $3.75 billion, an executive for the manufacturer of the product proudly thought he fooled the FDA into thinking a warning label wasn't necessary ("The meeting with the FDA yesterday was a tremendous success! No black box [warning]!").

[2] A recent 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 [2000] alone." "How Much Information?" assembled by Researchers: Peter Lyman and Hal R. Varian and published on the Web on October 20, 2000 at http://info.berkeley.edu/how-much-info/.

Email Attachments: Evidence Preserved in Amber

Not only will you usually find relevant documents among email attachments, there is a built-in "quality filter factor" in the business email context that should seem obvious: a document attachment's importance will tend to be directly proportionate to the number of people who read it and how far up the command structure it goes.

And here is the best part about email attachments: a user's email box *will preserve the actual document attached*. So there's never going to be a question about the authenticity or document version of the attachment. If I email you a spreadsheet today, what is attached to the email is the spreadsheet as it existed when I sent it. Tomorrow I can change the spreadsheet or delete it, but that will have no effect on the email and the attached spreadsheet that sits on your computer's hard drive, or the copy of it that resides in my "Sent Items" folder, or the backup tape on my network server that preserves a copy of the email I sent you.

Getting There Is Easier Than You Think

Electronic discovery is perceived by some to be too complicated and expensive, and the process introduces new and unique issues of scope, data exchange protocols and cost sharing that frequently require the use of experts like Legal Technology Group (for a discussion on these issues, see LTG's White Paper, *McPeek*: a "Try Before You Buy" Approach to Electronic Discovery).

But *email discovery* can be swift and relatively cheap, a kind of guerilla raid on the other side's electronic evidence that can give you the biggest bang for the buck. What you ask for (at least, initially) is a limited number of email boxes of the key people of interest to you. Since most enterprises use Microsoft Outlook for their email software, the technical name for a person's "email box" is his or her "PST file," a computer file with the extension .pst.[3] Your Rule 34 request can thus be fashioned as follows:

> Please produce the Microsoft Outlook .pst files of the following persons (i.e. their emails and email attachments in the "In", "Sent Items", "Out Box", "Deleted Items" folders, as well as any other folders containing email, to be produced on electronic data storage media in their native electronic format), for the dates between [date] and [date]:
>
> a. John Smith
> b. Sally Jones
> c. Ronald McDonald
> d. Peter Upton
> e. Jolene Piper

[3] Microsoft refers to .pst files as "Personal Folder Files;" why they are not called .pff files instead of .pst files is no doubt explained somewhere in an archived Microsoft email.

The producing party will, of course, want to exclude from production all emails that are privileged or irrelevant. That task will take time and effort, like any other discovery request requiring sifting through reams of paper or other electronic files, but often much less so. By limiting the scope of your initial discovery request to only certain emails from certain people in a given time frame, the opposing side cannot protest too loudly, and a judge will be more likely disposed to a motion to compel because of your modest shopping list.

To further counter burdensomeness objections from the producing party, you can suggest the use of a number of search and review software tools on the market that help expedite the review of emails and other electronic files (see LTG White Paper, Strategies and Software to Cull Privileged and Irrelevant Electronic Documents). And there's always the option of looking at each and every email subject to a discovery request and hand-picking the ones to be produced. Under either computer-assisted or manual review, however, there is an important point to keep in mind: you can create from a user's .pst file a subsidiary .pst file of only the responsive emails. That resultant .pst file can be reviewed directly in Outlook itself. Note, however, that the "Find" feature in Outlook searches only email message text but not the text in the attachments. To be able to search both message text and the text of the email attachments, you will need to convert the .pst files produced to a fully searchable database or spreadsheet. There are specialty vendors and software that can do that.

Having taken your first foray into electronic discovery by concentrating on the email boxes of the key witnesses or parties, you may find all the evidence you need to make your case.

by **Larry Johnson, Esq.**
President
Legal Technology Group, Inc.