GP|Solo
ABA General Practice, Solo & Small Firm Division

Technology eReport

Volume 5, Number 2
May 2006
Past Issues

Features

The New Federal Procedural Rules on Electronic Discovery: Writing Technology Into the Litigation Process
Find out about what to expect if you practice in federal court.

Metadata Management in Microsoft Office: How Firms Can Protect Themselves Against Unintentional Disclosure and Misuse of Metadata
Find out about metadata and how to protect your firm against the damage it can cause.

About GP|Solo

Find out about the benefits of being a GP|Solo Division member

GP|Solo Homepage

Columns

TechNotes
Tony Vittal tells you about the continuing evolution toward seamless and universal wireless connectivity.

MacNotes
Jeffrey Allen talks about the Mac's vulnerability to virus attacks.

SurvivingEmail
jennifer rose discusses what happens when email goes missing.

ProductNotes
Harmon-Kardon's Drive + Play to wire your car for your iPod and the Parrot 3200 LS-Color for Bluetooth.

DivisionNotes
Bylaws, Cool Tools, Solosez, and MilitarySez.

Feedback

[Tell us what's on your mind!]

[Want to write an article?]

[Contacts and Legal Stuff]
Who is responsible for all this.

Technology eReport

[Download the complete issue in PDF]

GP|Solo
ABA General Practice, Solo & Small Firm Division

Technology eReport

Volume 5, Number 2
May 2006
Table of Contents
Past Issues

The New Federal Procedural Rules on Electronic Discovery: Writing Technology Into the Litigation Process

By Adam I. Cohen

The new millennium has witnessed a plethora of judicial opinions and regulatory actions severely sanctioning sophisticated corporations and their prestigious law firms for botching electronic discovery, and the carnage does not appear to be on the decline. Moreover, as the proverbial "tip of the iceberg," these high-profile punishments do not reveal the cases where the handling of e-discovery helped determine the outcome in other ways. Although front-page news about e-discovery roadkill has been spreading a vague awareness as to the importance of e-discovery among litigators and their clients, the extent to which this recognition is accompanied by an understanding of what to do about it is questionable. Litigators, who choose not to arm themselves with such understanding personally or resort to tech-savvy colleagues, will find themselves rudely awakened by the changes to the Federal Rules of Civil Procedure projected to take effect in December 2006. These new rules elevate electronic discovery to the forefront of the litigation process in federal court, and will require federal court litigators to deal with technical, computer-related issues in a way that their law school instruction probably did not prepare them for.

Mandatory Early Discussion of Electronic Discovery Issues

Some of the best supporting examples for this proposition come from the least controversial, but most revolutionary, of the rules changes in terms of practical impact on the practice of litigation in

federal court: the related changes to Rules 16 and 26(f). The new rules require that as part of the parties' initial "meet and confer" to plan discovery, they must specifically address electronic discovery issues—including, for example, what steps they and their clients will employ to preserve dynamic electronic information and what format they will utilize for electronic production. The Rules Committee suggests that the precise subissues addressed will "depend on the nature and extent of the contemplated discovery and of the parties' information systems." Accordingly, it will be "important for counsel to become familiar with those systems before the conference."

This comment is reminiscent of Judge Scheindlin's exhortation that counsel must become familiar with their client's "data retention architecture." How many lawyers went into law school expecting that they would be required to have cozy familiarity with such intimidating-sounding aspects of computer information technology? Indeed, one might go so far as to say that for many lawyers, the avoidance of such matters led them to law school.

For their part, judges are invited to consider incorporating provisions for electronic discovery into their initial scheduling orders. In other words, your initial conference with your adversary at which you discuss and agree or disagree on a broad range of key electronic discovery issues assumes critical importance, as it will define the obligations your client will have to live by in implementing the notoriously expensive process of e-discovery. Woe to the lawyer who wades into such a conference with an incomplete or erroneous understanding of how the resolution of computer technology issues will affect the client. A court order setting into stone the results of an ill-conceived meet and confer position could prove extremely expensive to your client in terms of fees and expenses, to say nothing of how it might substantively impact the outcome of the case.

New Rules on Top of Changing Technology

Other changes in the rules write computer technology into the bedrock procedures of discovery in significant ways. (Remember, we are talking about the Federal Rules of Civil Procedure here, not some cases that are "nice to know" but can be "distinguished" by skilled advocates or that come up only sometimes.) For example, Rule 26(b)(2) establishes a procedure whereby parties need not provide electronic discovery from sources identified as "not reasonably accessible" (for burden or cost reasons) unless the requesting party makes a showing of good cause. Just think of the technical expertise required to deal with this rule—in identifying each potential source of electronically stored information within the menagerie of electronic media and systems in any modern business enterprise, in determining the requirements of procedures to access those sources, in assessing the burden or cost of such access, and in explaining the foregoing with enough specificity, but at the same time with sufficient clarity, to satisfy a judge who probably lacks IT expertise. Given that, as a gross understatement, computer storage, search, and retrieval technology is changing rapidly—what today we may consider not reasonably accessible may prove easily accessible tomorrow. Therefore, at a minimum, we should expect to see the development of a rich jurisprudence of "reasonable accessibility" as parties litigate over what this phrase means in particular contexts.

Other significant changes in the rules provide additional examples of how the new rules write computer technology into the law in ways that will require litigators to have greater resort to technical expertise as a routine part of litigating in federal court. Amendments to Rule 34 set forth procedures governing the format of production of electronically stored information. These rules establish as a default standard production in "a form or forms in which [electronically stored information] is ordinarily maintained or in a form or forms that are reasonably usable." Getting into the particulars of the pros and cons of making electronic productions in particular file formats requires venturing into relatively highly technical territory for lawyers. The rule does not address some of the elephants in the room that case law will have to flesh out—for example, under what circumstances must a party produce metadata? Under what circumstances should a party have to produce documents in native file format? As with the "two-tier" approach described in Rule 26(b)(2), the format rule uses the R word, requiring production in "reasonably usable" format. Again, as computer technology advances and such advances dictate new standards of "reasonable usability," we can expect to see parallel litigation activity and development in the jurisprudence of what is "reasonably usable."

Finally, consider the highly qualified "safe harbor" of Rule 37's protection from (at least certain) sanctions for spoliation where electronically stored information is lost through "routine, good-faith operation" of computer systems (at least where "exceptional circumstances" are absent). Identifying the manner of operating a computer system treated as routine and in good faith, particularly in the context of a duty to preserve, will likely change with advances in computer technology. When we perfect the magical big red "litigation hold" button that some courts seem to think has already been invented, the tolerance for any loss of data may disappear. In any event, lawyers will need to understand, argue, and explain what constitutes "routine, good-faith operation" of a particular computer system in the context of a particular preservation duty; and they will have to do so in a way that laypeople can grasp. Undoubtedly, we will see a new line of cases interpreting the rather dangerous-looking safe harbor.

The good news: "e-discovery challenged" litigators still have time to educate themselves or at least identify the right intellectual resources to add to their arsenal in marching to victory in the new age of electronic discovery. As litigators head to federal court after December 1, 2006, they will find a new aura of respect for the role of electronically stored information in litigation. Repent, Luddites, for your day of e-reckoning is upon you.

Adam Cohen is a senior managing director with the electronic evidence group at FTI Consulting, Inc. Before joining FTI, Mr. Cohen was a litigation partner at Weil, Gotshal & Manges LLP. He is the coauthor (with Weil partner David J. Lender) of the annually updated treatise* Electronic Discovery: Law and Practice *(Aspen Publishers) cited in three of the* Zubulake *opinions.

GP|Solo
ABA General Practice, Solo & Small Firm Division

Technology eReport

Volume 5, Number 2
May 2006
Table of Contents
Past Issues

Metadata Management in Microsoft Office: How Firms Can Protect Themselves against Unintentional Disclosure and Misuse of Metadata

By Randy Farrar and Susan McClellan

The steady growth of electronic document exchange has intensified awareness that Microsoft Office files include metadata beyond their printable content. Unintentional disclosure can be awkward or even raise malpractice concerns. Although metadata has been used to identify, classify, and manage documents in the legal environment for many years, most lawyers still lack a good understanding of metadata management. Although this article's intention is not to provide a comprehensive "how to" guide on metadata, you will come away with a better sense of what metadata is, how it can be misused and overlooked, and what you can do to proactively control and manage it.

Metadata Defined

As we all know, Microsoft Word includes many automated features to aid in document production and collaboration. Unfortunately, these automated features can embed electronic information used to reveal the identity of those who edited the document (revision authors); and track the time, date, and frequency of edits (track changes and revisions), commentary (inserted comments), the document template (a unique firm identifier), and other data employed to control the document's text and format. There's even an option in Microsoft Word called "Fast Save" that, if selected, allows deleted text to remain as part of a document's electronic file history (new text is appended). These are just a few of the hidden elements and document information found in a Microsoft Office document that make up the document's metadata.

Metadata Scenarios

Many users often dupe-and-revise (using save as) to save time. When this occurs, the original author information, document properties, document variables, hidden text (forgotten), and last print date stay with the document. Much of this metadata can be seen by looking at the document properties or by opening the document using a text editor. If the document is being prepared for a client who is paying for its creation, then it is even more important that all the metadata is removed before it is shared with the client.

Tracked changes being left in a document are a common occurrence, which alerts many people to the dangers of metadata. When a document has been edited using a powerful collaboration feature in Microsoft Word called track changes, the changes stay with the document—even if they are not visible to the eye—unless those changes have been accepted. Turning off the track changes feature does not eliminate the changes tracked by the program. If you send the document to another user, whether a cooperator or an adversary, the recipient simply has to turn track changes on to see all the revisions of that document.

Comments, as with track changes, remain with a document, if not deleted. When the "Reviewing" choice is set to "Final" and not "Final Showing Markup", then comments are invisible to the eye. If this document is shared outside the firm, the recipient can view the comments, which may contain embarrassing or even damaging information.

Metadata referred to here as "identifier metadata" can reveal the originator based on the metadata's uniqueness to both the user and firm. Identifier metadata includes uniquely named styles, bookmarks, hidden document variables, and custom document properties. Identifier metadata, although not necessarily considered high risk, should to be managed if the originator needs to remain anonymous or if document creation strategy is revealed by the metadata trail.

Metadata "mismanagement" stories abound. Case in point: in 2004, a Microsoft Word document, produced as part of a lawsuit filed by SCO against DaimlerChrysler and AutoZone, revealed that SCO's lawyers had also prepared a complaint against Bank of America. The document identified Bank of America as the defendant instead of the automaker. This revision and others in the document could clearly be seen through tracked changes. In another metadata disclosure blunder, the British government published a dossier on Iraq's security and intelligence services without removing the related metadata. Upon further review, it was discovered that much of the text was plagiarized directly from a U.S researcher whose work was published on the Internet. To add insult to injury, the report also revealed a list of the dossier's last ten authors and their edits and commentary.

Key Strategies for Metadata Control

As the legal community becomes more aware of metadata and the damage unintentional disclosure of document information can cause, the need to establish metadata control strategies and parameters becomes increasingly evident. Here are three recommended approaches worth considering:

1. **Educate your staff about metadata concerns**. Understand features that embed metadata (i.e., track changes) as well as the control and ramifications of these features. You can eliminate much of the metadata inherited from the "dupe and revise" practice by using firm templates to create new clean documents that have minimal metadata. You can also find powerful template and automation

packages on the market now that, in many instances, work better and faster than the standard dupe-revise approach. These packages also provide tools the help you copy text from one document into another without the inclusion of hidden metadata in the "copied" text.

2. **Control and manage metadata via third-party metadata scrubbing and management software**. Microsoft provides a metadata removal tool for Microsoft Word. Unfortunately, its rudimentary approach doesn't catch outgoing email attachments, and scrubs only a limited number of metadata elements. A more powerful third-party metadata application not only scrubs metadata but also allows a firm to manage the metadata at a very detailed level. For instance, you may want to keep track changes in a document, but eliminate the author and editing time information. Or a firm may want to ensure the user's name is never left in a document, but rather the firm's name is used instead. Always use a metadata removal application that publishes a clean copy of the document before it is shared electronically outside the firm.

3. Establish a firm-wide metadata scrubbing and management standard. Establishing metadata-related policies and procedures eliminates the need for individual users at your firm to decide what metadata gets scrubbed and makes the scrubbing process more efficient. This step is very important and should involve key users, especially lawyers. The firm metadata standard can be set up in levels that reflect what metadata gets scrubbed or changed (managed). For instance, a cooperator level might include most document properties but leave author information for collaboration purposes. An adversary level scrub might remove all metadata including turning all field codes to text and then converting the scrubbed document into a PDF for added metadata protection.

In conclusion, metadata in Microsoft Office documents can pose serious business and ethical risks if left unmanaged or ignored. It is important to educate law firm users about metadata elements and risks and articulate a metadata strategy by considering the establishment of metadata standards or best practices.

As president/CEO and chief software architect at Esquire Innovations, Inc., Randall Farrar has pioneered the development and marketing of several software applications geared toward the legal market. His training background has given him a thorough working knowledge of the specific problems faced by the legal industry when it comes to document production. He has extensive knowledge of many Microsoft products and has been the project lead and developer on more than 100 legal migrations and upgrades.

Susan McClellan, Esquire Innovations' director of marketing and operations, has been working in legal technology for seven years. She is responsible for marketing strategy, marketing execution, as well as Esquire's sales efforts, new business initiatives, and oversight of the day-to-day office operations.

GP|Solo
ABA General Practice, Solo & Small Firm Division

Technology eReport

Volume 5, Number 2
May 2006
Table of Contents
Past Issues

TechNotes

Trends in Technology

J. Anthony Vittal

Imagineering Comes True

When Steven Spielberg first conceived the screenplay for *Minority Report*, the film starring Tom Cruise, he convened a group of futurist technologists to develop a likely scenario for the technology to be commonly available in 2054. One of the concepts they developed, which was incorporated into the film, was the transparent display panels used ubiquitously throughout the film to display images and information in the workplace and the marketplace. That concept has been realized.

At the end of May 2006, researchers at the Technical University of Braunschweig in Düsseldorf, Germany, announced the development of entirely transparent organic light-emitting diode (OLED) pixels. Instead of using silicon transistors, commonly used in the liquid crystal displays found in today's thin-panel monitors and screens, they use transparent thin-film transistors (TFTs) manufactured from a 100-nanometer-thick layer of zinc-tin oxide. Unlike silicon-based LCDs, which absorb most visible light, these TFTs transmit more than 90% of visible light, making them virtually transparent.

In the transparent displays, the OLED pixels are placed on top of the TFTs, which are deposited on inexpensive flexible plastic substrates using conventional techniques. By varying the voltage in the driving TFTs, the OLEDs can emit anywhere from 0 to 700 candelas[1] of light per square meter. By comparison, today's typical flat-panel computer screens reach a brightness of approximately 300

candelas per square meter. Thus, these transparent OLED displays, as developed in the research laboratory, already are generating brightness levels more than twice those of contemporary monitors.

What will these transparent display panels be used for? Any application where one needs information displayed in the field of view. Imagine having driving directions and critical instrument readings displayed in your windshield. A surgeon having vital signs and other information displayed in his or her field of view while operating, instead of having to look away from the surgical field. What about seeing a witness through your display panel while you are examining the witness about a document in that panel? On a more prosaic note, consider having a television screen or computer monitor you can place in front of a window without obstructing the view. The potential uses are as varied as our imaginations.

When will you be able to buy one? According to the head of the responsible team from the High-Frequency Institute at the T.U. of Braunschweig, prototype displays should be available within two years. In the ordinary course, we should expect to see the first generation of these devices on dealers' shelves by the end of the decade.

High-Speed Wireless Computing

WiFi wireless networking is becoming ubiquitous. Cities across the country are rolling out free basic (relatively slow) WiFi connectivity in partnership with various providers. For those of us who are road warriors, we can get online in city halls, airports, courthouses, hotels, and any Starbucks coffeehouse. Windows® and Macintosh® notebooks have built-in WiFi capability. WiFi also is proposed for inclusion in the Linux kernel.

But what happens when you aren't within range of a wireless access point? Cellular providers are offering alternative wireless solutions involving a wireless PC card modem accessing their third-generation (3G) networks using either UMTS (Universal Mobile Telecommunications Service) or EVDO. High-speed download packet access (HSDPA) is another alternative. These protocols offer download speeds of between 400 and 700 kbps (kilobits per second). Compared to 802.11b WiFi (at up to 11 megabits per second) or 802.11g (at up to 54 mbps) or 802.11g+ "SuperG" (at up to 108 mbps), these wireless solutions are as slow as molasses in Minnesota in December.

Telecommunications equipment manufacturer Nortel and wireless chip manufacturer Qualcomm have teamed up to develop a new 3.5G technology known as the UMTS-HSDPA (universal mobile telecommunications system- high-speed download packet access) standard. Demonstrated at the CTIA Wireless 2006 trade show in Las Vegas, the venture has achieved download speeds of up to 7.2 mbps—more than an order of magnitude faster than 3G protocols—all over a cellular network. Using test terminals based on Qualcomm's MSM6280 mobile station modem and HSDPA network equipment from Nortel, the 3.5G technology demonstrated significant benefits in addition to the vastly improved speed. Not only does the technology quadruple network capacity for data

transmissions, it doubles the number of users per cell site when compared to current 3G technology.

This improvement in the performance of HSDPA makes the technology competitive with other wireless technologies such as WiMax, which boasts peak data speeds of up to 20 mbps, and average data rates between 1 and 4 mpbs.

For us, it means that we can be connected to the Internet (and therefore to our offices, our legal research services, and everything else we need to access) without any wires. If we can place a cellular telephone call, we can be connected at speeds close to those we experience in our own offices. In places where there is no high-speed wired connectivity to the Internet (no DSL, no digital cable), and therefore no WiFi, this new 3.5G technology will level the playing field by offering truly universal high-speed access.

Now all we need are operating systems that will switch off seamlessly between WiFi, WiMax (when it arrives), and the new 3.5G technology, and we truly will have universal wireless computing. The new technology will create the demand for them, and they will develop. In the meantime, enjoy the improvements.

Happy computing!

[1] A candela is the standard definition of luminous intensity under the International System of Units.

***Tony Vittal, the former general counsel of Credit.com, Inc., has returned to private practice in California. He writes and speaks frequently on technology-related topics and is a member of the Editorial Board of, and a regular contributor to, the* Technology eReport *and the* Technology & Practice Guide *issues of* GPSolo.**

GP | Solo
ABA General Practice, Solo & Small Firm Division

Technology eReport

Volume 5, Number 2
May 2006
Table of Contents
Past Issues

MacNotes

“There Be Dragons Here” (Even for the Mac Users)

By Jeffrey Allen

For some time, we Mac people have smugly sat back and watched the Windows world suffer through one virus outbreak after another. We used to make jokes about the vulnerability of the Windows Operating System and, of course, the biggest of all targets, Internet Explorer. I suspect that for many of us those jokes do not seem quite so funny these days as we have learned that the Mac lacks the invulnerability to virus attacks that many attributed to it over the years.

To some of us, the Mac’s vulnerability to virus attacks came as no surprise. I have long felt that the Mac OS and Safari had weaknesses that would enable those who designed computer viruses to knock out a few that would affect the Mac. Some note that we had no problem with this until Apple started to use the Intel chips, and suggest that there is a causal relationship between the conversion to Intel chips and the Mac’s newly discovered vulnerability to virus attacks. There may be a causal relationship, but it is not likely the fact that Apple has shifted towards what some refer to as the “dark side” with the adoption of the Intel chips.

Apple really had little choice about switching over. After several years they could not get a G5 to work in a laptop. Apple really was forced to adopt another chip. Available Intel chips power both desktops and laptops nicely. By making the switch, Apple could upgrade its laptop line, juice up the power and the speed, and continue to hold a competitive position in the market.

Yes, the simple fact of the matter is that the Intel Macs can run Windows too. Moreover, they can do a better job of running Windows than older Macs with emulator programs, such as Virtual PC. That fact has helped remove barriers for those Windows users seriously contemplating a switch to the Mac. The additional power in combination with the style advantage the Mac already possessed has helped make the Mac more popular than ever. From my perspective, the increase in popularity, caused in part by the shift to Intel processors, has served as the impetus for invasion.

Windows security issues, particularly those associated with Internet Explorer, are legendary. I believe that the number of virus attacks on Windows resulted from the security flaws inherent to the system, acted upon by the mass adoption of that software. Simply put, Windows and Internet Explorer offered a major target due, in large part, to the vast number of users. The virus-maker wishing to get the greatest bang for the effort would create a virus for the Windows environment. Why bother to even mess with the Mac world when it was such a small piece of the pie?

As the Mac became more popular and more widely accepted, it became a more viable target for the virus makers. The more people who used the Mac, the more it made sense to make a virus for the Mac.

So, where does that leave us? Microsoft continues to patch holes in its software. Apple has responded to the successful virus attacks by patching its software. For the time being, Apple's Macintosh OS and Safari remain safer from viral invasion than Windows and Internet Explorer. Microsoft has a new operating system on the horizon (although it keeps moving its anticipated release date back). Apple will also have a new iteration of its system in the not too distant future. Hopefully both systems and the associated browsers will provide better security than the current versions.

For those of you who have shifted to other browsers, such as Firefox or Mozilla, rest assured that they probably have their vulnerabilities as well. It just takes someone with the interest to exploit them.

In the mean time, you should take some actions to protect yourself and your computer. Going unprotected on the Internet begs for infection. It compares to having unprotected sex with the next several thousand people you see. Practice safe browsing online, just as you would practice safe sex.

As with sex, the most complete protection comes from abstinence. Just like sex, however, most of us would be loath to give up our Internet access, email, and so forth. You might, however, consider disconnecting your computer from the Internet when you have no need for the connection. That

means losing the convenience of automatically checking email, so you will want to weigh the trade-offs.

No matter what you decide about leaving the computer connected all the time or only when you use the Internet, you still need protection. The first thing you need to do is get and install a good antivirus program. Because most people consider the Mac safer than Windows, most antivirus programs protect Windows, not the Mac. Antivirus software makers have focused on Windows, just as did the virus makers. Although that may change in the near future, the leaders of the limited universe of Mac antivirus systems are Intego and Symantec (Norton).

After you have installed antivirus software, remember to regularly check for upgrades to virus definitions. The software can check for you automatically. It normally does that as a part of the boot-up sequence. Because many of us leave our computers on 24-7, the computer does not run that sequence very often. Accordingly, you must either set the program to check for updates on a regular basis (no less than weekly) or you must do that yourself on a manual basis.

Set the program so that it checks out all things that come onto the computer, by download or from email attachments. You might consider including an automatic search of files transferred from other media sources (CDs, DVDs, or other hard disks). That can be somewhat time consuming, and it is a bit of a hassle to wait sometimes. As a result, you might want to make that choice manually, skipping the process for media that has remained under your control and that you know will not infest your computer with malware.

As an extra precaution, you should run a virus scan over your entire disk when you first install the program and every so often afterward (once a month at least, better yet, once a week).

Even though you use antivirus software, you still need to take further precautions. For a variety of reasons, you need to have and use a viable back-up plan. The possible infestation of your system by a virus offers just one of the problems that can bring your system down. By regularly and properly backing up your system, you reduce the risk that you will suffer significant hardship due to a virus attack.

You can find many programs to assist you in backing up your software. Retrospect and Bounce Back Professional (CMS Products) are two of the best known. Synchronize! Pro X also has worked quite well. Ideally you will use a program that backs up (clones) your entire hard disk in the initial use and thereafter updates the backup by synchronizing it to the hard disk in your computer. Be sure to check your backup to ensure that it works. It should be able to replace the entire disk or a single file or group of files. In creating your backup plan, remember to make multiple backups and to rotate the backup media. That way you protect against the problem of backing up the virus. If some of the media in your rotation have the virus, you can simply use one that does not. If that happens to be a day or two behind, you may be able to safely update the files from one of the more recent, but contaminated, backups by using your antivirus software to clean the virus off. This

solution works if you use hard disks for back up. If you back up to other media, you will first have to restore to a hard disk (preferably an external hard disk) and then clean the virus off.

When surfing the net, remember to always practice safe browsing. Remember, **“There be dragons here!”**

GP|Solo
ABA General Practice, Solo & Small Firm Division

Technology eReport

Volume 5, Number 2
May 2006
Table of Contents
Past Issues

Surviving Email

Lost in Space: When Email Goes Missing

By jennifer j. rose

Over the decade past, we've become addicted to email. Its ubiquity, ease of transmission, cost savings, and speed have made most of us forget the era when it took days for a uniformed agent of the United States government to personally deliver the missive we'd written on Crane's Crest, personally autographed, inserted into a paper receptacle onto which we'd affixed a tiny colorful square and frequently sealed with a kiss. Along the way, we also managed to forget that the United States Postal Service occasionally failed to deliver. It's all too easy to assume that the email sent from your computer is always delivered seconds later to its intended recipient. However, sometimes the email postman not only doesn't ring twice, he fails to deliver at all.

Let's look at some of the reasons for missing and lost email. Starting with the most obvious, let's place the blame squarely on the shoulders of others.

Spam filters intended to protect us from unsolicited offers from VmtAGRA news, Highest qualities Replika Watches, Refinance and pay less!, and word salads have become overly aggressive, blocking wanted mail for no good reason. Just as a mailman may decide to quit delivering mail to an entire block just because an angry dog guards one house, a spam filter can block all IP addresses, servers, or an entire domain. Mail that sails through perfectly well may be blocked tomorrow, unblocked a week from now, or permanently blocked, all depending upon traffic levels and the whim of the ISP, because some spam filters only work sporadically. Spam control can exist on several levels—at the user's very own desktop, at the server, or at the network. And sometimes a user can be completely powerless when it comes to asking that an ISP stop protecting him or her

from unwanted mail.

Even though it appears transparent, transmission of email is hardly so. Each email message must traverse a series of "hops" from one system through another and finally to the intended recipient. Too many hops, too many timeouts, and too many disconnections can cause the system to simply give up, often with a kind reminder to the sender that the message could not be delivered. And sometimes the sender never even learns that much.

Absent a message that the email has bounced, the sender blithely assumes that the message was successfully transmitting and resides in the recipient's inbox. And when we do receive the notice of undelivered mail, sometimes simply taking the reasonable step of resending that email just isn't enough. How many times have you resent that email, only to have it bounced right back as undeliverable or rejected as spam? It's enough to make a grown lawyer scream.

This spring Verizon Communications settled a class-action lawsuit over blocking email from certain Asian and European providers by offering its customers up to a whopping $28. See http://www.emailblockingsettlement.com/. That's small consolation to email customers with clients in those countries.

What steps should you take when email is blocked or undelivered? Beyond simply resending it and hoping for the best, determine whether the recipient has an alternate address to which email can be sent. Try sending the message from one of your own alternate email addresses, which may even mean sending it off from a Yahoo (http://www.yahoo.com) or Gmail (http://www.gmail.com) account. Asking that the recipient unblock email from your address is one option, although many recipients are unable or unwilling to take those steps. And sometimes even doing so is about as easy or effective as calling someone whose telephone has been disconnected to reconnect the phone!

Now let's look at some of human reasons why email does not reach its intended recipient.

At the recipient end, because it's still easier to blame someone else, consider how the recipient may treat his or her incoming mail. Is your mail residing in the recipient's own junk mail filter, which the recipient only cleans out during blue moons? Does the recipient have too many of the wrong rules and filters set up, relegating your mail to the "Jokes and Other Silly Stuff" folder? Maybe the recipient simply deleted it, either inadvertently or intentionally? And then there's always the odd chance that the recipient is simply hiding out and ignoring your e-mail—like I've done with eReport editor Jeff Allen's mail asking me where this column is.

And, finally, does some of the blame rest on your very own shoulders? Yes, here's where the "duh" factor comes in. Check to see if you actually did send that email. Perhaps you only thought you did, planning to do so later, setting it for a delayed send, or otherwise doing something really, really stupid. Did you send it to the right person — jallenlawtek@aol.com instead of some other

address starting with “Ja” on your autocomplete recipient field? Did you address it correctly? It’s easy to confuse an “l” with a “1,” forget a hyphen or period, or even type the name or domain name extension wrong. Did you create a subject line which that direct the recipient’s attention to your email? Subject lines that are completely blank or contain only something like “important information” can end up ignored or directed to the junk pile more easily than those subject lines that read “ Stanley real estate contract.”

When all else fails, consider the quaint solutions we used before the advent of email. Fax your message. Have it personally delivered in a plain manila wrapper. Pick up the telephone and call. And be thankful for all the email that does find its way quickly and efficiently to the right person.

jennifer j. rose, editor-in-chief of* GPSolo*, receives her email at jjrose@jjrose.com in Morelia, Michoacán, Mexico.

GP|Solo
ABA General Practice, Solo & Small Firm Division

Technology eReport

Volume 5, Number 2
May 2006
Table of Contents
Past Issues

ProductNotes

Harmon Kardon Drive + Play

By Jeffrey Allen

Some car manufacturers, recognizing the iPod phenomenon, have started building iPod-docking stations into their vehicles. If you just bought a new car that did not include an iPod docking station (or if you have an older car), you no longer need to feel left out. For only $199 (plus installation), Harmon Kardon's Drive + Play will retrofit your car for your iPod. It will provide you with a large enough screen that you can see it easily and a set of controls you can have mounted near the driver's seat for easy access. It will cause your iPod to play back through your car's stereo system using an FM modulation process. More significantly, it does all of those things smoothly, simply, and without spoiling the sound with extraneous noises often present in frequency modulation devices. You can use the Drive + Play portably or permanently mount it in your vehicle.

My 2005 Jeep Grand Cherokee came with all kinds of gadgetry built into it. It did not, however, include an iPod dock. I solved that problem myself with the Drive + Play. I chose to have mine permanently mounted. It cost about $100 for the work, which I chose to have done professionally rather than do myself to ensure that I got an aesthetically pleasing installation. The car came with a very nice sounding stereo system, so the iPod sounded great when played through it. I have had it installed for more than three months and have been extremely pleased with it.

Harman Kardon's Drive + Play lets you hardwire your iPod into your automobile. It includes an illuminated navigation wheel, a backlit LCD display that lets you view the contents of your iPod, and the "Brain," an interface box that connects the iPod to the vehicle and charges it while you're driving through a dock connector interface.

A 3.5mm output connects to any car with an auxiliary input jack, and it can send your songs to an FM receiver if your car can't accept an auxiliary input. It can also route other audio signals like satellite radio to the car's audio system.

The Drive + Play works with all docking iPods 3G, 4G, HP, Mini, nano, and 5G video. The device is designed so that you can arrange to put the iPod almost anywhere in the car; presumably to allow for easy removal, under the assumption you will not want to completely give your iPod over to the vehicle. As I had recently upgraded to a 5G video iPod, I found myself with two iPods. Rather than get rid of the older iPod, I simply gave my iPod 3G to my car. I found a nice niche for it in the car, attached the docking cable to it, and I now leave the iPod in the car all the time. When I travel I take either the 5G or my nano.

I am delighted with my Drive + Play. It has a cleaner transmitted sound than any other FM modulator I have used.

Parrot 3200 LS-Color

By Jeffrey Allen

Would you like an installed Bluetooth hands-free kit for your car? Parrot's 3200 LS-Color may just satisfy your needs. The 3200 LS gives you a sophisticated, convenient, well-functioning kit that should work with most Bluetooth phones. (I tried it with several and had no problem pairing with it or using it.)

The 3200 LS-Color has extremely impressive features. For starters, it comes with a very good color display (TFT 160 x 128 pixels with 262,144 colors). The 3200 LS-Color stores up to 150 of your phone contacts in its own memory. It has voice recognition for up to 150 names, allowing you to dial numbers by saying the contact's name. If you choose, you may also store a photo with a contact; if you do, the device displays the picture when you call that person. You can keep up to five phones registered to the 3200 LS-Color at a time. The 3200 LS-Color provides full duplex audio, echo cancellation, and selectable hi-fi polyphonic ring tones. With some vehicles, the radio

will automatically mute while you talk on the phone. I found the sound quality on both sides of the conversation quite good. Overall, the kit worked very well and proved easy to use.

The 3200 LS-Color lists for $320, but you can get it online for about $205. It should cost around $120 to have it installed (price varies depending on installer and vehicle). For more information, see the Parrot website, www.parrot.biz.

GP|Solo
ABA General Practice, Solo & Small Firm Division

Technology eReport

Volume 5, Number 2
May 2006
Table of Contents
Past Issues

DivisionNotes

Bylaws

Attention all members, the Bylaws Committee is recommending that the Division Bylaws be changed. Please download and review the revisions to the Bylaws (MS Word) and email genpractice@abanet.org with your comments, questions, and suggestions. The Bylaw revisions were approved by Council on May 6, 2006, and will be up for approval at the Annual Meeting of the Membership on August 5, 2006 at the Annual Meeting.

Cool Tools

GP|Solo's Resources Section continues to expand. The latest addition is Cool Tools a page that gathers the latest and greatest free tools are available online. From simple ideas like being able to transfer files too big for email to heady concepts like Social Bookmarking, stop by to see what is available to make your life easier.

Solosez

Solosez is an email discussion list for solo and small firm lawyers. Now celebrating its 10th anniversary, Solosez has grown to be the ABA's busiest list. Solosez has now even earned a place in Wikipedia.

For a taste of what Solosez has to offer, check out the popular threads on Solosez's website. Last month's threads were:

- (Off Topic) Dating . . . Who Pays?
- Lawyer's Obligations As An Employer?
- Giving Away PC - How Best to Clean
- Any Patent Attorneys Here?

MilitarySez

MilitarySez is an email forum for lawyers who are in the military, either on active or reserve duty, contemplating a career in the military, or who have questions about legal issues involving the military. Recently formed, it is modeled on Solosez, the ABA's busiest discussion list. As a cyber-water cooler, MilitarySez offers an opportunity for practitioners to pose questions, offer advice, and share information. Discussion group participants determine the topics for discussion. You need not be a member of GP|Solo or even the ABA to join the list, just go to GP|Solo's Military home page to sign up. http://www.abanet.org/genpractice/military/index.html

GP|Solo
ABA General Practice, Solo & Small Firm Division

Technology eReport

Volume 5, Number 2
May 2006
Table of Contents
Past Issues

Contacts and Legal Stuff

Dwight L. Smith
GPSolo Division Chair
Ste. 1030
1800 S. Baltimore
Tulsa, OK 74119
918.585.1446

Jeffrey Allen
***Technology eReport* Editor**
Graves & Allen
436 14th St.
Oakland, CA 94612-2716
510.839.8777
jallenlawtek@aol.com

jennifer j. rose
Editor-in-Chief, *GPSolo*
JR de Alarcon 28
Col. Santa Maria de Guido
58090 Morelia
MEXICO
52.443.323.5283
jenniferrose@abanet.org

Technology eReport Editorial Board

Wells Anderson
Active Practice LLC
5200 Willson Rd. #150
612.791.0471

Daniel Coolidge
Coolidge & Graves
108 Bible Hill Rd.
Warner, NH 03278
603.456.2532

Bruce Dorner
Dorner Law Office
80 Nashua Rd.
Londonderry, NH 03053-3426
603.434.2230
callmylawyer@attGLOBAL.NET

Patricica Joyce
Law Office of Patricia M. Joyce
230 Chestnut Dr.
East Greenwich, RI 02818
401.885.7200

Ross Kodner
Microlaw Inc.
2320 West Camden Road
Milwaukee, WI 53209
414-476-8433
rkodner@microlaw.com

Alan Pearlman
Alan Pearlman, LTD
707 Skokie Blvd, Ste. 600
Northbrook, IL 60062
847.205.4383

Natalie Thornwell
State Bar of Georgia
104 Marietta St. NW

Atlanta, GA 30303
404.572.8770

J. Anthony Vittal
Credit.Com Inc.
550 15th St., Ste. 37
San Francisco, CA 94103
415.901.1561
tony.vittal@abanet.org

ABA Staff

Alexa Giacomini
General Practice, Solo and Small Firm Division Director
321 N. Clark St.
Chicago, IL 60610
312-988-5636
giacomia@staff.abanet.org

Tom Campbell
ABA Publishing
***Technology eReport* Editor**

Douglas Knapp
***Technology eReport* Design and Production**