SEIZE THE ADVANTAGE

GETTING HIGH-VALUE ELECTRONIC INFORMATION EARLY AND MINIMIZING YOUR TIME AND EXPENSE

Sonal Bhatia
Keenan Law Firm, LLC
524 Walnut St., Ste. 200
Kansas City, MO 64106
(816) 809-2100
sonal@kclaborlaw.com

#NELA16
National Employment Lawyers Association
2016 Annual Convention
June 22-25, 2016
Westin Bonaventure Hotel & Suites, Los Angeles, California

The last thing you need is more stuff to read! So the purpose of this paper will be to offer you some succinct ideas to take home and use. I'm going to focus on three areas: exploring **instant messaging**, mining your **client's technology knowledge**, and nailing down the defendant's **search and production methods** with early depositions and demands for native format.

In Texto Veritas: How to Use Texts and IMs to Get to the Truth

Ninety percent of companies use instant messaging for communication between employees in the workplace. If you're not discovering the often candid messages employees write (usually in the moment), you're likely not capturing the true dynamics of the workplace. Also very prominent: text messaging and chat systems utilized on mobile phones.

An *amuse bouche*: this is an excerpt from interoffice Skype messaging (very commonly used by sales teams) in a sex discrimination case. These are two managers casually chatting about a new, young, female employee who has just been hired. You would likely not find this in email.

Chat Message	7/5/2016 8:30	live:sboss	Suzie Boss	she starts in 2 weeks.	#live:jmanager/$live:sboss;379ea5693mmf1m93
Chat Message	7/5/2016 8:32	live:jmanager	Jim Manager	Would I approve?	live:jmanager
Chat Message	7/5/2016 8:32	live:sboss	Suzie Boss	She's got a boyfriend.	#live:jmanager/$live:sboss;379ea5693mmf1m93
Chat Message	7/5/2016 8:32	live:jmanager	Jim Manager	That's not what I asked.	#live:jmanager/$live:sboss;379ea5693mmf1m93
Chat Message	7/5/2016 8:33	live:sboss	Suzie Boss	https://www.facebook.com/	#live:jmanager/$live:sboss;379ea5693mmf1m93
Chat Message	7/5/2016 8:34	live:jmanager	Jim Manager	Her boyfriend is more handsome than me (and probably 15 years younger), but she'll do.	live:jmanager
Chat Message	7/5/2016 8:35	live:sboss	Suzie Boss	I think the last one was way over your age range.	#live:jmanager/$live:sboss;379ea5693mmf1m93

Bottom line: **ask for instant messages and texts.** One shenanigan that defendants sometimes play is to claim that you did not ask for the right messaging platform. For instance, they'll say "Oh, you didn't ask for messages sent by Skype," or "Oh, you didn't ask specifically for WhatsApp." The best way to deal with this is to start your document requests with a very broad and exhaustive definition of "document" that they cannot wriggle out of.

Here is an example from our requests:

> "Document(s)" means all materials within the scope of Fed. R. Civ. P. 34, including but not limited to: all writings and recordings, including the originals and all non-identical copies, whether different from the original by reason of any notation made on such copies or otherwise (including but not limited to: email and attachments, correspondence, memoranda, notes, diaries, minutes, statistics, letters, minutes, contracts, reports, studies, checks, statements, tags, labels, invoices, brochures, periodicals, receipts, returns, summaries, pamphlets, books, interoffice and intraoffice communications, offers, notations of any sort of conversations, instant messages, social media messages (including but not limited to posts, messages, and status updates on Facebook, Skype, Twitter, WhatsApp, Instagram, MySpace, Slack, and LinkedIn), posts/responses/comments on any message boards, chat rooms, blogs, or review sites, working papers, applications, permits, file wrappers, indices, telephone calls, telephone logs and/or telephone bills documenting calls, text messages, meetings invites or printouts, Outlook calendar entries, "To Do" lists, , invoices, worksheets, and all drafts, alterations, modifications, changes and amendments to any of the foregoing, graphic or audio representations of any kind (including without limitation, photographs, charts, microfiche, microfilm, videotape, recordings, motion pictures, plans, drawings, surveys), and electronic, mechanical, magnetic, or optical records or representations of any kind (including without limitation, computer files and programs, tapes, discs, recordings). As used here, the term "document(s)" specifically includes any and all metadata. **All electronic documents are to be produced in native format.**

Defendants always attempt to produce documents in non-native format. You should require that they produce all documents, particularly emails, texts, and IMs, in native format. Do not let them give you scanned PDFs. With native format, you can look at embedded links, search Internet headers, see the email in an unedited format, and discover who each email was sent to. You can also see which documents were sent as attachments, and learn IP addresses (including locations of people when they sent certain

emails). There's a handy website called "ip2location.com," which will allow you to cut and paste Internet headers to analyze the route an email took to get from sender to recipient. Finally, native format can be much easier to use when you search using keywords. PDFs give you virtually none of this. Courts increasingly support requests for native format. Don't accept PDFs—demand native format!

Questions to Ask the Potential Client

When do you start with technology? From the first potential client meeting—while it's fresh in the client's mind, you have the opportunity to develop an understanding of the employer's technology usage and infrastructure. Being able to "talk the talk" of the employer, with its internal lingo, can provide an edge in discovery. Instead of asking about IT architecture late in discovery – probably too late to do anything about the defendant's discovery games – why not ask about the specific software and technology that your client recalls from the onset? Here is a list of questions to ask your client or potential client during the very first meeting:

(1) Does/Did your employer pay for your cellphone? What's your cell phone number? Do they pay for the cellphones of others in the workplace? Do you have their work phone numbers?
    a. If yes, does your employer, or do your coworkers communicate using cell phones?
        i. Does your employer/coworker(s) call you?
        ii. Does your employer/coworkers(s) text you?
        iii. Does your employer/coworker(s) use any mobile apps to communicate with you?
    b. If no, does your employer still contact you on your cell phone?
        i. Does your employer/coworker(s) call you?
        ii. Does your employer/coworkers(s) text you?
        iii. Does your employer/coworker(s) use any mobile apps to communicate with you?
(2) Tell me all the ways your employer and/or co-workers communicate with you.
(3) What programs/application/software do you log-in to every day at work? Tell me the names of all software and/or applications? How do you access each one? (On a phone, computer, tablet, other devices?)
(4) What other software do you use at work?
(5) Do you use any software to communicate with your coworkers inter-office or intra-office? Any chat rooms or messaging systems?
(6) Do you use any video software to communicate with coworkers or clients? What is it?
(7) Which social media applications do you use at home: Twitter, Facebook, Instagram, others?
    a. Are you friends with any of your coworkers on Facebook?
        i. If so, have you engaged in any "Facebook chat" with them?
    b. Do you interact with any of your coworkers using any other software or mobile app? Which ones? Who do you interact with?
(8) Do you ever work remotely or work from home, and if so, what technology has been set up for you to do that? Do you work from a work laptop at home, or do you use your own equipment?
(9) Do you use any cloud-based sharing systems at work? (Google Docs, Dropbox, etc.)
(10) What was the make and model of the computer assigned to you? Were you provided with any additional devices to use? What were they and how did you use them?

In addition to questions like these, ask new clients to create a thorough chart of software they used. Here is an example:

XYZ, Inc.'s Software Systems Chart

Name of Technology/Tools	Description	Hardware	User Name & Password	User ID	Password
DOTI	XYZ's CICS online facility. Accessed by users to see XYZ's data. Used for processing XYZ's data and manage their accounts. I accessed the "test" and "production" DOTI system. I had full-access to the test system because I couldn't cause problems with processing. I had very limited access to the production system - only "view" access to specific limited processing.	My Desktop	Yes	Unknown	Unknown
TSO	Access to all of the tools to perform my duties, like accessing files, running reports, managing data, accessing programs and jobs, etc.	My Desktop	Yes	Unknown	Unknown
SmartFile	Tool used to access data stored in files on XYZ's system	My Desktop	No	N/A	N/A
Xpeditor	Tool used to interactively run CICS online programs to view processing, data and files as they process through the program	My Desktop	Yes	Unknown	Unknown
TempAgency's time Entry	TempAgency's Time Entry facility used to enter all of my time every week. Internet facility to enter time.	My Desktop	Yes	tclient	Password1
TempAgency's Benefits	Benefit information from TempAgency through the internet	My Desktop or Home Laptop	Yes	tclient41	Password1
TempAgency Knowledge Spring	Training information from TempAgency through the internet	My Desktop or Home Laptop	Yes	tclient	Password1
TempAgency Payroll	Payroll system via the internet so I can review my pay stubs, tax information, etc.	My Desktop or Home Laptop	Yes	tclient	Password1

IT Time Entry via Web Portal	XYZ's Time Entry facility used to enter all of my time on every project/support ticket I worked on at XYZ. Tickets and work requests are tools used to track all work done by the IT group. This was an internal time entry system written by XYZ. There was no real name except "IT Time Entry"	My Desktop	Yes	Unknown	Unknown
Microsoft Office Tools	Microsoft WORD, Excel and PowerPoint	My Desktop	No	N/A	N/A
Windows	All tools, processes and programs that are part of Windows	My Desktop	Yes	Unknown	Unknown
DocuTech	XYZ's internal documentation repository. Contained information about XYZ's business, processes, procedures, etc.	My Desktop	No	N/A	N/A
Footprints	XYZ's facility/tool to track all work requests and support tickets for all work that is being performed by the IT department.	My Desktop	Yes	Unknown	Unknown
SQL Server Report System	Tool used to write queries to produce ad-hoc reports of data based on requirements from users, IT department, etc.	My Desktop	Yes	Unknown	Unknown
SQL Server Management Studio	System used to access data stored on XYZ's system. Similar to the SQL Server Report System, but it doesn't produce reports.	My Desktop	Yes	Unknown	Unknown
Request For Change	Project Management System	My Desktop	Yes	Unknown	Unknown

Having seen this chart, we know to ask for all documents from the "Docutech" system as part of our first requests for production. We also know to ask for all of the tickets from "Footprints" to build a comparator model of our client's performance vis-à-vis people with different demographic characteristics. Our fluency with the workplace lingo has the effect of showing defendants that we do our homework and literally know the ins and outs of their workplaces.

The Discovery Process: How to Know What They Have and Cut Out the Nonsense

The client can be a great source of technological knowledge, and tech-savvy clients may be able to tell you most of where to look. But sometimes clients don't know, understand, or recall the technology used in the workplace. One valuable way to understand the defendant's technology is to notice up a corporate representative deposition on technology issues. (This is an idea from Amanda Farahany – thank you Amanda!) Serve this notice with the initial summons and pleading if you are in a jurisdiction that allows

it; if not, serve it at the earliest possible opportunity. Here's a sample corporate rep deposition notice, and feel free to email me at sonal@kclaborlaw.com if you want me to send you one that you can use.

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NELA

SHANTI PLAINTIFF,	)	
	)	
Plaintiff,	)	
	)	Case No. 2:17-cv-0473
v.	)	
	)	
XYZ CORPORATION, et al.,	)	
	)	
Defendants.	)	

NOTICE OF DEPOSITION

Please take notice that on date(s)/time(s)/place(s) as may be agreed to by the parties, or otherwise commencing at 10:00 am, on Wednesday, July 13, 2017, at the offices of the Keenan Law Firm, LLC, 524 Walnut Street, Suite 200, Kansas City, Missouri, 64106, Plaintiff shall take the oral deposition of XYZ Corporation, address known to Defendant, through such representatives as shall be designated and properly prepared to testify pursuant to Fed. R. Civ. P. 30(b)(6). The deposition shall be transcribed by a qualified reporter and shall be videorecorded.

The topics for the deposition(s) are as follows; Plaintiff reserves the right to amend and/or supplement the topic(s) as may be needed. **The deponent is directed to bring with her/him any and all documents relied upon or consulted in preparation for her/his testimony under these topics.**

1. Defendant's methods, policies, and practices for keeping, organizing, and searching personnel-related records, including the content and organization of personnel files and/or human resources files; this topic refers to any personnel or human resources documents, regardless of the technical name used for them (for instance, if Defendant maintains separate confidential personnel records apart from a main personnel file, this topic includes the identity and manner in which those confidential personnel records are maintained).
2. Defendant's policies and procedures regarding information technology including: litigation holds, procedures for retaining, organizing, or deleting/destroying information; backup or cloud-based systems; the hardware and software in use in Plaintiff's workplace and any supporting systems (specifically including instant message systems, intranets, and chat systems); and search and production of electronically stored information in this case, from January 1, 2010, to present.
3. Defendant's process for searching for, retrieving, preserving, and producing information relevant to Plaintiff, Plaintiff's charge of discrimination and this litigation.

All parties and their counsel are invited to attend and ask questions.

Pay special attention to **search terms**. Make sure you ask the defendants to name all computers and devices they've searched both by serial number and by the names of the users during the time period you designate. Ask them to detail all of the search terms they have used and each application they have deployed those search terms in. Ask them who has performed the searches—including the exact dates, times, and the witnesses to those searches. Also ask about software and hardware preservation protocols and ask the defendants to produce all policies and procedures relating to these protocols.

An early corporate representative deposition on technology and preservation issues has at least three advantages: (1) it takes little time or money investment on your part, as you can use the same topics almost verbatim from case to case; (2) it shows the defendant that they will be face a strong offense by having to prepare for and present testimony at an early stage; and (3) it shows the defendant that they must play above-board on e-discovery, and cannot use inadequate search terms or fail to search in the right places.

Conclusion

Electronic discovery can seem daunting in terms of time and money. But you can save your time, save your money, and keep the defendant's feet to the fire if you ask the right questions early. As a parting tip, here's a tech resource you may want to explore: **Sidekick** (http://www.hubspot.com/products/sales/sales-tools), which allows you to find out the exact second someone is reading your emails so you can follow up with a phone call or other contact. E-discovery is in large part about knowing the details and knowing what the Defendant is thinking and what their next moves will be. You can stay ahead of the game by seizing the momentum early, with little time and little money invested. Feel free to email me any time at sonal@kclaborlaw.com.

DIY E-Discovery: How to Take Control of eDiscovery in your Cases

Jeff Kerr
CaseFleet
655 Highland Ave NE, Suite 8
Atlanta, Georgia 30312
jeff@casefleet.com
404-576-6648

#NELA16
National Employment Lawyers Association
2016 Annual Convention
June 22-25, 2016
Westin Bonaventure Hotel & Suites, Los Angeles, California

One of the reasons I decided to learn e-discovery was to save money. Early in my career as a lawyer, I developed a strong aversion to spending money on experts and litigation vendors. After spending $5,000 out of my own pocket in my first year of practice on an expert who literally did *nothing*, I decided I would try to go without so-called experts as much as possible. Fortunately, in my employment law cases, experts were rarely needed. When I did use experts, it was generally for specialized technological issues: offering testimony on a smartphone's retention of text message data or collecting sensitive evidence from a smartphone. But, most of the time, I did all of the e-discovery work myself.

My do-it-yourself approach differed from the approach recommended by many in the field of e-discovery. For example, lawyer and e-discovery expert Ralph Losey states that an e-discovery team "should include scientists and engineers in some way." Blogger and consultant Joshua Gilliland recommends having "expert witnesses conduct data collection." There are two undercurrents supporting these assertions. The first is the consideration that many lawyers do not have the technical skill to collect, review, and produce electronic evidence. The second is that attorneys who participate in collecting electronic evidence could later be disqualified as counsel if they are required to testify about the steps taken in collection. Both are legitimate concerns, but neither forbids a competent and knowledgeable attorney from handling most (if not all) of the technology aspects of an e-discovery case.

Let's first consider the threshold question of disqualification based on collecting evidence. Not surprisingly, this concern is most often raised by vendors whose business model presupposes that counsel will not handle the majority of the technical tasks associated with e-discovery. But is there any truth to the assertion?

The argument is that an attorney who performs tasks like downloading client data from an email account, copying files from a hard drive, or exporting data from a social media site becomes an involuntary expert witness in her own case. But the same point, which wouldn't make any sense, could be made with regard to attorneys who accept paper files or tangible evidence from their clients. We clearly have a responsibility to keep our clients' papers in a safe condition and not to modify them, but handling them doesn't subject us to the risk of disqualification. Accepting evidence from one's client, whether in tangible or electronic form, is part of an attorney's ordinary work for a client and should never make counsel subject to disqualification. If it did, we would have to hire a vendor in *every* case because almost every case today involves electronic evidence.

Assuming, then, that lawyers can do e-discovery without hiring a bevy of vendors, what are the keys to success? I submit that they are threefold: competence, transparency, and access to the proper tools.

I. Competence

I put competence first in the list because handling electronic evidence truly does require some skill and knowledge. For example, it's possible to collect emails from a webmail service such as Gmail or Yahoo! using Outlook, but it requires patience and willingness to read some documentation. It's unlikely that you'll inadvertently destroy the email account or alter its contents, but you won't be able to download the emails unless you're willing to fiddle with the Outlook configuration for the account. Following blogs and websites dedicated to e-discovery is an important aspect of competence - you need to stay up-to-date on the topic. You also must dedicate the time to become a competent and confident user of whichever tools you decide to use. Safely copying files from an external drive is something most of us can do, but this is a task that counsel should approach with caution, and it ties in with my next point on transparency.

II. Transparency

By transparency, I mean telling the other side what you plan to do and what you plan not to do. This is a good idea for a variety of reasons. First, it's often the best way to immunize yourself from charges by the other side that you mishandled electronic evidence. If you write to your opposing counsel, notify them of your intention to collect and preserve evidence by taking simple steps A, B, and C, but not by taking expensive steps X, Y, and Z, and opposing counsel either agrees with your approach or fails to object in a timely manner, then the chances are very slim you'll face problems down the road. Second, you

benefit from the "I'll show you mine if you show me yours" approach—that is, if you are transparent, there's a much better chance the other side will follow suit. Sharing some information about your e-discovery methods could lead the other side to share extremely valuable information with you at an early stage.

III. Tools

The third factor is having the proper tools. You can't do e-discovery if you don't have some basic tools for reviewing, tagging, collecting, and producing electronic evidence. I've used Navicat for dealing with databases, iExplorer for pulling data from an iPhone, Nuix Proof Finder for review and tagging, Outlook for collecting webmail, Adobe Acrobat DC for redacting and applying Bates-labels, and Bulk Rename Utility for numbering files by their file names. For an extra degree of safety when collecting data, I also own a USB write-blocker and a Forensic UltraDock fromWiebeTech. These tools are sufficient for most cases and, if you know how to use them, you can be an e-discovery ninja. Better yet, you can acquire *all* of them for a total price of less than $1,000. (We'll be discussing each of these tools in detail in upcoming blog posts - follow CaseFleet on twitter for updates!)

The primary cost of e-discovery when you take the DIY approach is the time it takes to learn the concepts and technology. After the upfront cost of the tools and the time spent learning them, the benefits pay permanent dividends and empower you take the reins in your cases without involving expensive vendors. Using these tools, discovery became another opportunity to get a good result for my client, instead of a costly burden.

Reprinted from the CaseFleet blog: https://www.casefleet.com/blog/

Original Article at https://www.casefleet.com/blog/diy-e-discovery-how-to-eliminate-vendors-and-take-the-reins-of-e-discovery/

eDiscovery Dictionary

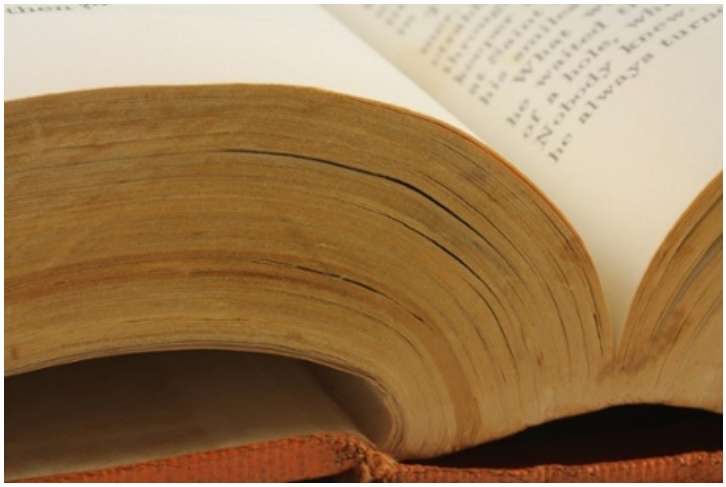
Jeff Kerr
CaseFleet
655 Highland Ave NE, Suite 8
Atlanta, Georgia 30312
jeff@casefleet.com
404-576-6648

#NELA16
National Employment Lawyers Association
2016 Annual Convention
June 22-25, 2016
Westin Bonaventure Hotel & Suites, Los Angeles, California

Carving: the process of searching through the unused parts of a disk for files that haven't been overwritten and recovering those files. Word do the wise: "deleted" does not mean gone--deleting a file usually just unlinks it from your computer's file system. With the right software, the deleted files can usually be recovered.

Clawback Agreement: a very handy agreement which states that if you accidentally give the other side your privileged documents, they have to give them back and can't use them against you or claim they aren't privileged anymore. There are no known reasons for *not* having a clawback agreement, but there are very good reasons to have one in place. A serviceable clawback agreement can be written in one paragraph. Go download one, and use it in every case. Like, right now. I'm not kidding.

Checksum: a sequence of numbers and letters that is essentially unique for each and every file in the world. Comes in several different flavors, including MD5 and SHA1. Extremely useful for finding duplicates, determining if someone has files they shouldn't have, and identifying evidence.



Cost Shifting: when the responding party forces the requesting party to pay for the costs of responding to certain discovery. Often a Solomonic remedy imposed by the Judge when one party is asking for too much but maybe shouldn't be

prevented outright from getting it. Under so-called American rules of discovery, cost shifting is unlikely to be applied to well-drafted and reasonable discovery requests.

Culling: processing a large set of data and removing the junk data so that it's easier to search and less expensive to host or transfer. It's best for the parties to agree on the criteria that will be used to cull the data.

Custodian: a person who cleans … just kidding. A *person*... Full stop. Seriously, a custodian is just a person. Why do we need a word that just means "person" in the context of e-discovery?

Deduplication: a process that removes multiple copies of the same file from a set of files, leaving you with only one of the copies. This is super helpful when you have to review a large number of files and you don't want to waste your time going line-by-line through to files to see if they are the same. **Horizontal deduplication** means removing *all* the duplicates across the board. **Vertical deduplication** means keeping a copy of a duplicate if it belongs to a different **custodian** (see above). With vertical deduplication and 9 custodians what is the maximum number of copies of the same file you might have after deduplication? If you answered 9, you are smart. Have a cookie.

DeNISTing: one way of **culling** data (see above). One takes a huge list of **checksums** (see above) for known junk files and removes any matching files from the data set. The NIST part derives from the National Institute for Standards and Technology, who, among other things, maintains the list of junk files.

eDiscovery: a process where the parties to litigation exchange electronic evidence. eDiscovery has been the subject of much teeth-gnashing and hair-pulling, with many lawyers and commentators complaining about its cost and difficulty, but eDiscovery is inescapable unless the parties live in caves and do not use computers. If a lawyer wants to prove that certain facts did or did not occur, then eDiscovery is strongly recommended.

Fielded: a form of production (usually **native**, or nearly native -- see below) wherein the *fields* that hold discrete bits of information remain in place. For example, an email when converted to a PDF file is no longer fielded because the "to:" and "from:" fields of the email in a PDF document have the same status as any of the other text on the page. In contrast, when email is produced in a native or near-native format, the "to:" and "from:" fields retain their special status, and it is possible to construct searches like 'from:hook@bidness.com to:crook@bidness.org subject:conspir!' using a **review platform**. This can be very effective.

Forms of Production: electronic evidence can be "produced" (i.e., exchanged) in multiple forms. For example, if there is a Word file on your client's laptop, and you need to produce it to another party, you have several choices: (1) you can copy the file to some sort of transfer media (e.g., a thumb drive) to produce an exact copy; (2) you can convert the file to PDF and produce the PDF file; (3) you can print the file to **TIFF** (see below) also produce

a **load file** (also see below) that contains searchable text; or (4) you can literally print the file out on a piece of paper using a printer and deliver a copy of the paper to the other party. There are pros and cons to each form of production. If you are billing hourly, the only known "pro" of option 4 (printing) is that it wastes a lot of time and paper, and often results in motion practice. For reasons that we do not comprehend, some attorneys are flustered by native production and instead choose to have files produced PDF. *Recommendation*: talk about about forms of production with your opposing counsel *before* discovery starts; if you are requesting evidence, tell the other party (in writing) the form of production that you want.

Hash: see **Checksum**

Linear Review: assume that your client has 1TB of data that *could* be responsive to discovery requests. Assume that you agree on some keywords with the other party. Assume that those keywords are "hits" for 500,000 documents. Linear review is the process of having a human--usually a *lawyer*--set eyes on each of the documents before any of them are produced to the other side. On average, human reviewers can review 55 documents per hour, and the average hourly cost for a reviewer is $70 per hour. That means you'll spend, ahem, ***more than $600,000 on document review!*** The process will also take several months, even for a large review team. But the legal system ain't got time for this. Discovery is supposed to finish … it can't drag on and on for years while reviewers strain their eyes and wonder if this is what they went to law school for. In short, linear review is a bad idea, and it's prohibitively expensive and time-consuming. Alternatives include technology-assisted review and creative use of keyword searches, selective review, and clawback agreements.

Litigation Hold: a document provided to a custodian when litigation is on the horizon or already happening that instructs him or her how to avoid deleting or corrupting evidence. Sometimes litigation hold letters confuse ordinary people by telling them things like "cease rotating backup tapes." Ideally, a litigation hold should be readable and comprehensible by its target audience, and compliance with the hold should be monitored. Watch out for company-sponsored paper shredding or hard-drive dumping events!

Load File: a special file that you get (or give) with other files that provides additional information about those files, such as the directories they came from, metadata not contained in the files themselves, Bates numbers corresponding to the files, and information about the requests to which the files are supposed to responsive. Even though load files are essentially "flat"--i.e., non-relational databases (like Excel files)--they appear in any number of bizarre proprietary formats. There is no agreed-upon standard for formatting load files, and unless one happens to own the same software that was used to generate the load file, viewing one can be a serious pain in the hindquarters. If you don't own the software that generated the load file, you may want to ask for a comma-delimited (CSV) file instead, which at least you can open in Excel.

MD5: see **Checksum**

Meet & Confer: a meeting (or phone call) at the beginning of a case for lawyers to talk about discovery and try to reach agreement on preliminary matters like forms of production and dates for depositions. Required in federal court. Most often the meet & confer session is "phoned-in" both literally and figuratively, to the detriment of everyone involved. Best if counsel prepare beforehand, talk with their clients about eDiscovery and the evidence that's likely to be sought, and come with a game plan.

Metadata: least helpful definition: "data about data." More helpful definition: contextual information about computer files that helps explain how/when/where/why they were created. Metadata can also prove that a piece of a evidence "is what it purports to be"--e.g., "even though he denies it ladies and gentlemen, this email is in fact an email written by Mr. X on [insert date] from his home computer." Metadata comes in two main categories, embedded metadata and system metadata. The handy thing about embedded metadata is that it travels with the file, so that if you copy the file to transfer media and give it to your opponent, it will still be there. In contrast, system metadata does not travel, and is therefore difficult to produce in discovery. Examples of system metadata are: directory paths, last-modified dates, and created dates. System metadata is often produced in **load file** (see above) that accompanies the discovery response.

Native: A file that is in the form in which it was originally created. If the file started its life by someone opening Microsoft Word, typing something, and then hitting "save," then the native file will have a ".doc" or ".docx" extension. The opposite of a native file is printing a ".doc" file to paper or to "virtual" paper--e.g., TIFF (see below) or PDF.

Near Native: functionally the same as native. Because some things can't really be produced in the application that created them, then we call the next best thing near-native. An example is an email generated in Gmail.

Review Platform: software for examining electronic evidence--either your own or the other side's. Can be hosted in a "cloud" environment--in which case expect to pay by GB, and don't say I didn't warn you. Alternatively, software that runs on one's desktop. Ranges from inexpensive to insanely expensive. More often the latter. We're trying to change this.

Preservation Demand: a letter or email to your adversary demanding that he or she keep evidence safe and prevent it from being destroyed. Sometimes critical to point to when seeking sanctions at a later date if the other side "lost" some evidence. Preservation demands are often wildly overbroad, but hey, how is the sender supposed to know what the receiver has and doesn't have?

PST: a super handy file format for wrapping up huge numbers of emails and attachments in a way that preserves their ability to be searched. We like PSTs. Ask for them, often.

Quick Peek Agreement: whoever came up with this term should be shot. It just means an agreement that you can sit with your opponent and look at certain documents in the same room to facilitate coming to some sort of agreement about what to do with them next. There could be some other provision like that you can't tell the judge what you say. Frankly, I've never had occasion to use one of these, but I'm sure I wouldn't call it a "quick peek" if I did! Inane terminology overload.

Redaction: taking the secret parts of a document and crossing them out with a black Sharpie.

Relational Database: the thing that runs your bank account, your email account, your smartphone app, your Facebook account, your doctor's medical records system, and generally everything else in the world, including many of the things that are valuable in eDiscovery. Learning a bit about them and their lingo--*highly recommended*.

Rule 502(d): see Clawback

Sources: the places where electronic evidence lives--computer disks, smart phones, thumb drives, Dropbox. Custodians (see above) have been known to have them.

TIFF: a mild form of disagreement among opposing counsel, usually caused by bickering about forms of production. Ok, sorry for the pun. A TIFF is an image file, like a JPEG, PNG, or GIF, except that it has almost no legitimate purpose for existing. (At least one can make hilarious cat videos with GIFs!) In very backward, retrograde forms of eDiscovery, native files (see above) are converted to TIFF images and produced as such, with a load file (see above) provided to make up for the fact that *the TIFF conversion process strips out almost every useful piece of information contained in the original file!* Responding parties: please stop giving us TIFFs. Producing parties: don't accept TIFFs.

Vendor: people who firmly believe that you cannot survive without them. Sometimes, but not always, they are right. If you are about to try **carving** (see above) and are not yourself trained in this field, please call a vendor.

Reprinted from the CaseFleet blog: https://www.casefleet.com/blog/

Original Article at https://www.casefleet.com/blog/dictionary-of-ediscovery/

Going Native: The Importance of Native Files in eDiscovery

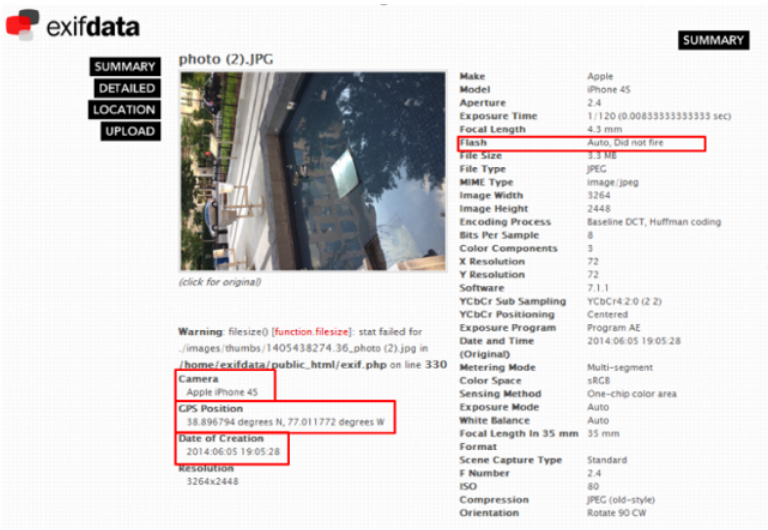
Jeff Kerr
CaseFleet
655 Highland Ave NE, Suite 8
Atlanta, Georgia 30312
jeff@casefleet.com
404-576-6648

#NELA16
National Employment Lawyers Association
2016 Annual Convention
June 22-25, 2016
Westin Bonaventure Hotel & Suites, Los Angeles, California

Other than witness testimony, nearly all the evidence worth discovering in litigation is electronic. More often than not, it's emails, text messages, database records, digital images, metadata, and Microsoft Office files that tell us the truth about what really happened. But there are several obstacles on the eDiscovery road to obtaining this valuable electronic evidence. One of the worst is the widespread practice of converting electronic evidence from its original, "native" form into some other form—and, in the process, degrading its ability to reveal the truth.

The typical alternative to producing native files consists of converting those files to TIFF images or PDF files, but sometimes producing parties will actually print out native files and deliver them in paper form. The upshot is that the requesting party receives a *different* file from what was requested and a *different* file from what was originally created by the requesting party or its agents. These differences are often profound: the converted files (or, worse, pages) are stripped of embedded data that frequently sheds light on the history and origin of the files (when they were created, who last edited them, etc.). Sometimes essential parts of the contents of the files will be truncated. I have seen printouts of spreadsheets where more than half of the columns were simply gone. Word documents often contain comment bubbles and records of tracked changes, and these can disappear entirely during the conversion process. Converting electronic files to a different form also provides a convenient way to hide key documents in an avalanche of unsearchable irrelevance. While native electronic files are generally text-searchable, conversion frequently strips out searchable text.

An example of the type of metadata held within a .jpg image that would be lost if the image was converted to PDF.



It gets worse than just losing metadata. Native files are often searchable by their parts or "fields." If you have to search through millions of emails, your job will be nearly impossible if you can't perform searches that target certain senders and recipients. Native files include this functionality by default, but not so with converted files. And native files are cheaper to exchange because they are more compact than converted files. Take a Word file, print it out, and scan it to PDF at 250 DPI—you'll see that the converted version is many times bigger than the original native file.

Procedurally, there's a simple trick for getting native files—*ask for them!* It's best to explain why you need native files at the earliest possible meeting with your adversary, to document your request for native files, and to include detailed instructions for producing native files in your document requests. If your opponent refuses to comply, it's often worth your time to take the issue to the court. Discovery is about revealing the truth, and native documents serve this goal much better than degraded pseudo-copies in TIFF, PDF, or paper form.

When an opponent refuses to supply documents in native format, it's very helpful to be able to make a strong case to the court on the evidentiary superiority of native files. To this end, I like to provide examples as part of my arguments.

- Your Honor, the documents produced by my opponent include a PDF version of what appears to be an image taken with a digital camera. My opponent has confirmed that this image was in fact taken with her client's iPhone. By converting the image file to a PDF file, my opponent has stripped out and failed to produce important evidence. In native form, JPG files often contain embedded data showing when an image was taken, the device used to take the image, and the GPS coordinates of the location where the image was taken. This evidence has high

probative value, and it essential for determining whether the image is authentic. Requiring my opponent to produce the native file is essential for revealing the truth during the discovery process.

- Your Honor, my opponent produced several PDF copies of files that were originally Excel spreadsheets. These converted files are not only more difficult to search, but they also do not include key evidence that the native Excel files contain. For example, native Excel files almost always include formulas, and those formulas contain key information about the assumptions and logic underlying the data. A PDF "printout" of a spreadsheet strips out *all* of the formulas and also makes it impossible to tell where formulas were used. The native Excel file is the best evidence in this case, and my opponent's PDF printout represent an incomplete and inadequate production that only obscures the truth. We ask, therefore, that the Court order production of the original native file.

Arguments like these are much more effective than generic assertions about the benefits of native files. Although many parties resist producing native files, when dealing with eDiscovery, it is often worth the time required to take a stand and to require an one's adversary to produce in native format.

To learn more about the benefits (and nuances) of native production in eDiscovery, check out the following articles and blog posts from Craig Ball:

- What is Native Production for E-mail?
- The Case for Native Production (PDF)
- Blind as a Cat: Lawyers vs. Native Production
- Lawyer's Guide to Forms of Production (PDF)

Reprinted from the CaseFleet blog: https://www.casefleet.com/blog/

Original Article at https://www.casefleet.com/blog/going-native-the-importance-of-native-files-in-e-discovery/

"ESI on the Offense: Holding Defendants Feet to the Fire"

Best Practices for ESI Discovery
NELA 2016 –Los Angelas
By Trang Tran

Federal Rules 34 and the new amendment to Rule 26 are good tools obtain electronically stored information (ESI) in it's native electronic format. Below are several best practices and supporting authorities to get you started.

1. You should ask for ESI.

Under Fed. R. Civ. P. 34, a requesting party "may specify the form or forms in which electronically stored information is to be produced." Fed. R. Civ. P. 34(b)(1)(C). The 2006 Advisory Committee on Rule 34 explains:

> "Using current technology, for example, a party might be called upon to produce word processing documents, e-mail messages, electronic spreadsheets, different image or sound files [voice mail], and material from databases. […] The rule therefore provides that the requesting party may ask for different forms of production for different types of electronically stored information."

Fed. R. Civ. P. 34, 2006 Amendment to Advisory Committee Notes.
In a typical employment case, emails and MS Word documents involved in the disciplinary action or termination would be responsive to discovery requests. Instead of relying on the paper versions of key documents in the case, the plaintiff can requests that the emails and documents be produced in native format,the form in which the document was created. "[E]lectronic information produced in the form in which the file was created (or'native format') will contain application metadata . . . . An electronic document or file produced in native format may also be accompanied by system metadata, such as the date the file was created or the identity of the computer on which it was created." The Sedona Conference Working Group on Electronic Document Production, The Sedona Principles: Best Practices Recommendations & Principles for Addressing Electronic Document production, p. 62 (Sedona Conference Working

Group Series 2007). When a judge appears reluctant to impose on a company to respond to ESI discovery, reference to the 14 Sedona Principles, can reassure the court that Discovery requests for electronically stored information is very reasonable and there are clear industry norms for ESI preservation and production. In order to take advantage of the metadata[1] found in ESI, one simply must ask for it. See Fed. R. Civ. P. 34, 2006 Amendment to Advisory Committee Notes (explaining that "[Rule 34] therefore provides that the requesting party may ask for different forms of production for different types of electronically stored information").

2. The Producing Party Has An Obligation To Produce ESI.

As the producing Party, Defendants have an duty on a Producing party to produce ESI as it is kept in "the usual course of business," in the "form or forms in which it is ordinarily maintained," or—when not possible to do the former—to produce ESI in "a reasonably usable form or forms." Fed. R. Civ. P 34(b)(2)(E).

> **(E) Producing the Documents or Electronically Stored Information.**
> Unless otherwise stipulated or ordered by the court**,** these procedures apply to [...] electronically stored information:
> **(i) A party must produce documents as they are kept in the usual course of business [...];**
> **(ii) If a request does not specify a form for producing electronically stored information, a party must produce it in a form or forms in which it is ordinarily maintained or in a reasonably usable form or forms; [...]**
> **Fed. R. Civ. P. 34(b)(2)(E),(i),(ii).**

As a result, the producing party must respond to discovery by providing the responsive information in their native format: spreadsheet in Microsoft Excel; PST files and email as they are maintained in Microsoft Outlook; a word processing document is kept in a native format such as Word or Pages; etc., Human Resource files as they are maintained in PeopleSoft; or attendance records as they are kept in Oracle Time and Labor software.

[1] For more information about Metadata and how to use it, refer to the materials from my co-presenter Jeff Kerr

3. Don't Settle for Paper, TIFF OR PDF files.

Many Defendants' knee jerk reaction to ESI discovery]are to convert the information from their electronic format such as emails into a paper print out, a PDF or worse individual files called TIFF. This process often involves 3-4 steps, where each document is converted to paper, scanned, bates numbered, screened individually for privileged information. By the time emails are produced as paper, PDF, or TIFF files, the context of the communications along with the attachments related to the emails are disjointed and difficult to comprehend. This is backwards from the way things should go.

When a requesting party does not specify the form in which ESI is to be produced, the default rule for production of ESI is for producing party to produce in native file formats because that is the way it is ordinarily maintained or, when not possible to do the former , the rule is to produce in "a reasonably usable form". Fed. R. Civ. P. 34(b)(2)(E)(ii).

Converting ESI such as emails and spreadsheets to printouts or TIFF and PDF should be the last resort.

> "[b]ut the option to produce in a reasonably usable form does not mean that a responding party is free to convert electronically stored information from the form in which it is ordinarily maintained to a different form that makes it more difficult or burdensome for the requesting party to use the information efficiently in the litigation. If the responding party ordinarily maintains the information it is producing in a way that makes it searchable by electronic means, the information should not be produced in a form that removes or significantly degrades this feature." Fed. R. Civ. P. 34, 2006 Amendment to Advisory Committee Notes **(emphasis added).**

Despite this, many defendants insist that TIFF image files of electronic documents is the most common choice. The reason for this is many companies, law firms, and legal treatises have failed to keep up with new technological innovation. Many common discovery practices involving ESI are found based on dated recommendations found in *Effective Use of Courtroom*

Technology: A Judge's Guide to Pretrial and Trial 73 (Federal Judicial Center 2001).

When a Defendant insist it has met its obligations by converting electronic files into paper, TIFF, or PDF FILES, remind the court that the rule says that the requesting party may specify the "form..in which [ESI] is to be produced," Fed. R. Civ. P. 34(b)(1)(C), and the defendant has not shown compelling reasons why it cannot produce the information in the format requested by the plaintiff. See, e.g., In re P*orsche Cars North America, Inc. Plastic Coolant Tubes Products Liability Litigation*, 279 F.R.D. 447, 450 (S.D. Ohio 2012) (court granted plaintiffs' request for native format "absent a showing by [defendant] that such a production would be unduly burdensome); *Romero v. Allstate Ins*. *Co*., 271 F.R.D. 96, 107 (E.D. Pa. 2010) ("the Court finds that Plaintiffs are entitled to have documents produced in native format with their associated metadata" where defendants do not allege that they will be financially burdened or prejudicially harmed by the production of metadata); C*amesi v. Univ. of Pittsburgh Med. Ctr*.,No. CIV.A.09–85J, 2010 WL 2104639, at *7 (W.D.Pa. May 24, 2010)(ordering defendants to produce ESI in its native format "absent a clear showing of substantial hardship and/or expense"); *In re Netbank, Inc. Secs. Litig*., 259 F.R.D. 656, 681–82 (N.D. Ga. 2009)("Although the Defendants have listed a number of hypothetical problems with providing documents in native format, they have not asserted these to be actual problems arising in the present case. . . . [T]he court is confident that the precision of record citations can be appropriately dealt with should [plaintiff] desire to use any of the documents at issue as exhibits or evidence. . .. The Defendants having given no good reason why they should not produce [plaintiff's] requested documents in native format, the Motion to Compel production of ESI information in native format is granted.")

4. Overcoming Defendants' Objections to ESI Discovery

A common strategy in opposing ESI discovery is to employ a blanket conclusory general objections. The rules frown upon the use of general objections to frustrate a plaintiff's effort to obtain the legitimate ESI discovery from the Defendant pursuant to Fed.R.Civ.P. 26 and 34. "Rule 1 of the Federal Rules of Civil Procedure mandates that the Rules are to be 'construed and administered to secure the just, speedy, and inexpensive determination of every action.'" Armstrong v. Hussmann Corp., 163 F.R.D. 299 (E.D.Mo.1995). The above rule "has been construed broadly to encompass any matter that bears on, or that reasonably could lead to other matter that could bear on, any issue that is or may be in the case." *Oppenheimer Fund, Inc. v. Sanders*, 437 U.S. 340, 351, 98 S.Ct. 2380, 2389, 57 L.Ed.2d 253 (1978). Rule 26(b)(1) of the Federal Rules of Civil Procedure provides that,"[p]arties may obtain discovery regarding any matter, not privileged, that is relevant to the claim or defense of any party, including the existence, description, nature, custody, condition, and location of any books, documents, or other tangible things and the identity and location of persons having knowledge of any discoverable matter. For good cause, the court may order discovery of any matter relevant to the subject matter involved in the action. Relevant information need not be admissible at the trial if the discovery appears reasonably calculated to lead to the discovery of admissible evidence." Fed.R.Civ.P. 26(b)(1). Information that is reasonably calculated to lead to the discovery of admissible evidence is considered relevant for the purposes of discovery. See *Daval Steel Prods. V. M/V Fakredine*, 951 F.2d 1357, 1367(2d Cir.1991); *Morsel Diesel, Inc. v. Fidelity & Deposit Co*., 122 F.R.D. 447, 449 (S.D.N.Y.1988).

If a party resists or objects to discovery, Rule 37(a) of the Federal Rules of Civil Procedure provides that the other party, "upon reasonable notice to other parties and all persons

affected thereby, may apply for an order compelling disclosure or discovery....” Fed.R.Civ.P. 37(a). The defendant, as the objecting party, bears the burden of showing why discovery should be denied. *Blakenship v. Hearst Corp.,* 519 F.2d 418, 429 (9th Cir.1975). The burden of proof lies with the party opposing discovery to show good cause to deny the discovery sought. *Chamberlain v. Farmington Sav. Bank*, 247 F.R.D. 288, 290 (D.Conn.2007). The Defendants can not resist discovery of ESI by asserting general objections. “[G]eneral and conclusoryobjections as to …burden are unsufficient to exclude discovery of requested information.” *Melendez v. Greiner*, No.01Civ.7888, 2003 WL 22434101, at *1 (S.D.N.Y.Oct.23, 2003). The Defendant must support its position with a “particular and specific demonstration of fact.” 452 U.S. 89, 201, 101 S.Ct. 2193, 68 L.Ed.2d 693 (1981) (emphasis added).

It is not enough for Defendant to merely make conclusory statements. Id. Moreover, the court is afforded broad discretion in deciding discovery issues. See *Willis v. Amerada Hess Corp*., 379 F.3d 32, 41 (2d Cir.2004). Under the Federal Rules, a party is required to provide discovery of electronically stored information unless that party shows that the source of such information is ‘not reasonably accessible because of undue burden or cost.’ Fed.R.Civ.P. 26(b)(2)(B). Once it is shown that a source of electronically stored information is not reasonably accessible, the requesting party may still obtain discovery by showing good cause, considering the limitations of Rule 26(b)(2)(C) which balance the costs and potential benefits of discovery. ‘The decision whether to require a responding party to search for and produce information that is not reasonably accessible depends not only on the burdens and costs of doing so, but also on whether those burdens and costs can be justified in the circumstances of the case.’ Fed.R.Civ.P. 26, Advisory Committee Note to the 2006 amendments to Rule 26(b)(2).” *Barrera v. Boughton*, 3:07cv1436 (RNC) (DFM), 2010 WL 3926070 *3, (D.Conn.Sept.30, 2010).

A Defendant must bring forward adequate evidence that it would be too costly to produce the requested ESI discovery and cannot merely asserted broad objections.

A party resisting discovery must show how the requested discovery was overly broad, burdensome, or oppressive by submitting affidavits or offering evidence revealing the nature of the burden. See *Merrill v. Waffle House, Inc.,* 227 F.R.D. 475,477 (N.D. Tex. 2005); see also S.E.C. v. Brady, 238 F.R.D. 429, 437 (N.D. Tex. 2006) ("A party asserting undue burden typically must present an affidavit or other evidentiary proof of the time or expense involved in responding to the discovery request."). Federal Rules of Civil Procedure Rules 26(b), 26(c), and 34(b) have been amended, effective December 1, 2015. Rule 26(b)(1) now provides that,"[u]nless otherwise limited by court order, the scope of discovery is as follows: Parties may obtain discovery regarding any nonprivileged matter that is relevant to any party's claim or defense and proportional to the needs of the case, considering the importance of the issues at stake in the action, the amount in controversy, the parties' relative access to relevant information, the parties' resources, the importance of the discovery in resolving the issues, and whether the burden or expense of the proposed discovery outweighs its likely benefit. Information within this scope of discovery need not be admissible in evidence to be discoverable." FED. R. CIV. P. 26(b)(1). The defendant, as the objecting party, bears a difficult burden when they resist discovery of ESI.

5. Take Charge Of ESI Discovery Before Defendants Respond To Discovery.

To put this all to work, you need to start early in the lawsuit. If you wait until after a Defendant has responded to discovery and cherry picked documents they want to pick out, print, and produce before you request the ESI in their native electronic format, the company may use it

against you because what you are asking them to do is to go through the production process twice. The cost of duplicating their efforts and drain on time and resources is a consideration under Rule 26. You can avoid this by sending a letter early in the case or in conjunction with service of discovery.

"Please provide written answers to the following questions concerning the electronic discovery in the Defendant's possession. Once we receive Defendant's written responses we can schedule a conference call between the parties to discuss the same. Please do not send us any ESI discovery until the following concerns and questions are resolved:

I. System Configuration Questions

1) What custodians and devices have been identified as the items to target for collecting of ESI (electronically stored information)? Be sure to specify the type of device and associated custodian (i.e. servers, workstations, laptops, tablets, PDAs, cell phones, external drives, external media, etc.)
2) What has been done with the above identified devices since the January 30, 2012 Plaintiff's litigation hold letter was sent via email. Have they been moved out of production to a secure location with controlled access? Have any of the above devices been provided to other staff for use and if so, in what capacity are they being utilized? Be as specific as possible.
3) Is one or more file server(s) utilized to house files, documents, databases, etc. that all or some staff members can access and modify? If so, provide any general information on these servers (i.e. HP ProLiant) and the type of files that they house.
4) Provide information on the configuration any file server(s.) Specifically, is there a single internal drive or multiple internal drives? If multiple drives, are the internal media configured in a RAID array or multiple RAID arrays and if so, what RAID level or levels are configured (i.e. RAID 0, 1, 5, etc.)?
5) Are any external devices attached to the servers and used as either additional storage or backup devices? If so, please describe.

II. Acquisition Questions

1) Provide the acquisition method or methods to be utilized when creating images of the devices. Also, specifically include all of the hardware and/or software utilized in the acquisition process and the format of the acquisition. Be as descriptive as possible.
2) Will the internal clocks of each device that are being imaged, be checked and recorded to confirm that they are accurate? Can reports of all the device BIOS clocks be provided to Plaintiff?
3) If any server contains one or more RAID array, be sure to provide addition information how the RAID server will be imaged and which tools will be utilized. Since the process to image a RAID server is different and more complex than imaging a device with a single drive, be as specific as possible. By example, will the drives be imaged individually and the RAID reconstructed, will a live-acquisition be done on the full array

using the internal RAID controller, or will a targeted acquisition be done?
4) Will the acquisition methods for all devices generate and validate hash values? If so, which value or values will be utilized (i.e. MD5, SHA-1, SHA-256?) Will the acquisition methods generate log files of all imaging processes showing time/date of acquisition, serial numbers of source and destination drives, error count (bad sectors), and validated HASH values and can those log files be provided to Plaintiff?

III. Data Extraction Questions

1) Provide the search parameters that will be utilized in order to generate the data "hits." Be as specific as possible and include file types, "to and from" dates, and keywords utilized. If utilizing "to and from" dates as part of the search criteria, please provide if those "to and from" dates are specifically targeted for the modified date, the accessed date, the created date, else some combination of two or more of these date parameters.
2) Provide the names of all software applications that will be utilized to extract the data from the images. Explain how these applications handle metadata once the data is extracted. By this, specifically:

a) Does the metadata remain intact and complete?
b) Does the application strip out portions of the metadata and if so, what remains?
c) Does the application export the metadata to a separate file? If so, what is the format
of that file?

3) Explain how the software examination/extraction tool Defendant is utilizing handles deleted data, data that resides in unallocated space, and data that resides in file slack (file fragments.) Will any data carving be performed to recover files from unallocated space?
4) If data carved files are recovered, what naming convention is utilized for these files?
5) Most data carved files are without MAC time stamps and also often times, files extracted from an archive file (i.e. email container) can be without MAC times. Therefore knowing this, if a timeline is utilized as one of the search parameters for this data extraction (to and from dates), how will files without MAC (modified, access, created) times be handled? Will they also be included in the data export or will they be ignored?
6) What type of measures will be taken to ensure that the extracted data is without duplicates (de-dupped)? Will HASH values be used to determine and eliminate duplicates?

IV. eMail Configuration Questions

1) Explain the process the Defendant utilizes for managing email. Including the following:
a) Is an email server utilized (i.e. MS Exchange)? If so, what is the server application?
b) Does each or any user manage their email separately on their desktop computer and if so, what application is utilized (i.e. MS Outlook, Mozilla Thunderbird, etc.) for each identified custodian?
c) Do any of the users utilize both a work and personal account on their work computer?
d) Does any or each user utilize a web-based email that requires logging into a web portal to manage their emails? If so, how do you intend to collect this data if it's not downloaded to a local computer with an email desktop application?

> e) Provide a listing of all custodians relative to this case and their email addresses both work and personal.

It is best to notify the Defendant early in the case to discuss the ESI production protocol, including source data, software and document formats, which was exactly what Plaintiff (and Plaintiff's ESI expert) are requesting through discovery. This approach is preferable to leaving it up to Defendants to unilaterally served discovery production as itdeems relevant and completely ignored the valid ESI production protocol and format issues. This deliberative and lock step process by the requesting party is recognized by The Sedona Conference. "Indeed, because knowledge of the producing party's data is usually asymmetrical, it is possible that refusing to 'aid' opposing counsel in designing an appropriate search protocol that the party holding the data knows will produce responsive documents could be tantamount to concealing relevant evidence." *The Case for Cooperation*, 10 SEDONA CONF.J., 339, 344 (2009). (Courtesy Copy Attached at Appendix 1)

The Sedona Conference advised:

> "Cooperation …requires…that counsel adequately prepare prior to conferring with opposing counsel to identify custodians and likely sources of relevant ESI, and the steps and costs required to access that information. It requires disclosure and dialogue on the parameters of preservation. It also requires forgoing the short tactical advantages afforded one party to the information asymmetry so that, rather than evading their production obligations, parties communicate candidly enough to identify the appropriate boundaries of discovery. …In place of gamesmanship, cooperation substitutes transparency and communication about the nature and reasons for discovery requests and objections and the means of resolving disputes about them.

Id. at 344-45. (footnote omitted) (emphasis added).

This approach is a cost saving measure for all parties. The Sedona Conference in 2009 recognized that cooperation between counsel regarding the production of electronically stored information "allows the parties to save money, maintain greater control over the dispersal of information, maintain goodwill with courts, and generally get to the litigation's merits at the earliest practical time." *The Case for Cooperation*, 10 SEDONA CONF.J., 339, 339 (2009).

> "Although d]iscovery disputes have existed since discovery began[,]…ESI has vastly increased the quantities of available information and the way it can be accessed. With almost all information electronically created and stored, there has been an exponential increase in the amount of information litigants must preserve, search, review, and produce. ESI is often stored in multiple locations, and in forms difficult and expensive to retrieve. These reasons compel increased transparency, communication, and collaborativediscovery…[I]n order to preserve our legal system, cooperation has become imperative.
> Id. at 340. (emphasis added) (emphasis added).

"The Federal Rules of Civil Procedure, case law, and the Sedona Principles all emphasize that electronically stored information ('ESI') should be a party-driven process." *Aguilar v.Immigration and Customs Enforcement Div. of U.S. Dept. of Homeland Sec*., 255 F.R.D. 350, 358 (S.D.N.Y. 2008). Discussions about ESI should begin early in the case. Rule 26(f) requires that the parties meet and confer to develop a discovery plan that discusses "any issues about disclosure or discovery of [ESI], including the form or forms in which it should be produced." Fed. R. Civ. P. 26(f)(3)(C). "Of course, the best solution in the entire area of electronic discovery is cooperation among counsel." *William A. Gross Const. Associates, Inc. v. American Mfrs. Mut. Ins. Co*., 256 F.R.D. 134, 136 (S.D.N.Y. 2009). "As the Sedona Conference recognized . . ., cooperation between counsel regarding the production of electronically stored information 'allows the parties to save money, maintain greater control over the dispersal of information, maintain goodwill with courts, and generally get to the litigation's merits at the earliest practicable time.' The Case for Cooperation, 10 Sedona Conf. J. 339, 339 (2009)." *Trusz v. UBS Realty Investors LLC,* No. 3:09CV268(JBA)(JGM), 2010 WL 3583064, at *4 (D. Conn. Sept. 7, 2010). "[C]ourts have emphasized the need for the parties to confer and reach agreements regarding the form of electronic document production before seeking to involve the court." *Aguilar, 255 F.R.D. at 358.* By conferring early, you are able to better target your ESI discovery

and position yourself in a better position for a motion to compel. Below are sample language for a ESI conference letter. Good hunting.

10 Sedona Conf. J. 339

Sedona Conference Journal
Fall, 2009

Supplement
Article

THE CASE FOR COOPERATION

Author: **The Sedona Conference®**

Editor-in-Chief: **William P. Butterfield, Hausfeld LLP**

Executive Editors: **Richard G. Braman, The Sedona Conference® Kenneth J. Withers, The Sedona Conference®**

Contributing Editors[a1]***:*** **John D. Luken, Dinsmore & Shohl LLP Charles R. Ragan, Huron Consulting Group Christopher M. Schultz, Perkins Coie LLP Gregory B. Wood, Fulbright & Jaworski L.L.P.**

EXECUTIVE SUMMARY

The Sedona Conference® issued its *Cooperation Proclamation* in 2008. The *Proclamation* initiated a comprehensive nationwide effort to promote the concept of cooperation in pretrial discovery. The *Proclamation* calls for information sharing, dialogue, training, and the development of tools to facilitate cooperative, collaborative, and efficient discovery. The *Proclamation* has been well received, especially by those judges who regularly confront discovery disputes that could be avoided by cooperative conduct among counsel. Indeed, nearly one hundred state and federal judges have already endorsed the *Proclamation* and the number continues to grow.

Cooperation in this context is best understood as a two-tiered concept. First, there is a level of cooperation as defined by the Federal Rules, ethical considerations and common law. At this level, cooperation requires honesty and good faith by the opposing parties. Parties must refrain from engaging in abusive discovery practices. The parties need not agree on issues, but must make a good faith effort to resolve their disagreements. If they cannot resolve their differences, they must take defensible positions.

Then, there is the second level. While not required, this enhanced cooperative level offers advantages to the parties. At this level, the parties work together to develop, test and agree upon the nature of the information being sought. They will jointly explore the best method of solving discovery problems, especially those involving electronically stored information ("ESI"). The parties jointly address questions of burden and proportionality, seeking to narrow discovery requests and preservation requirements as much as reasonable. At this level, cooperation allows the parties to save money, maintain greater control over the dispersal of information, maintain goodwill with courts, and generally get to the litigation's merits at the earliest practicable time.

***340** The line between the first and second level cooperation is, of necessity, difficult to draw. There is no precise definition of "cooperation," as there are no precise definitions of good faith or reasonableness. However, absent a more cooperative posture in the discovery process, the cost of litigation and the burden imposed as courts are forced to attempt to resolve more and more discovery disputes, will ultimately bring the system to a halt.

Discovery disputes have existed since discovery began. But ESI has vastly increased the quantities of available information and the way it can be accessed. With almost all information electronically created and stored, there has been an exponential increase in the amount of information litigants must preserve, search, review, and produce. ESI is often stored in multiple locations, and in forms difficult and expensive to retrieve. These reasons compel increased transparency, communication, and collaborative discovery. The alternative is that litigation will become too expensive and protracted in a way that denies the parties an opportunity to resolve their disputes on the merits. As a result, in order to preserve our legal system, cooperation has become imperative.

Such cooperation is not in conflict with the concept of zealous advocacy. Cooperation is not capitulation. Cooperation simply involves maintaining a certain level of candor and transparency in communications between counsel so that information flows as intended by the Rules. It allows the parties to identify those issues that truly require court intervention. The parties may not always agree, but with cooperation their real disputes can be addressed sooner and at lower cost. As discussed in this paper, the concept of discovery cooperation is not new. It finds support in the Federal Rules of Civil Procedure, ethical standards, court decisions, economic considerations, and common sense. In a survey of 2,690 attorneys recently involved in federal litigation, more than 90% of respondents, representing both plaintiffs and defendants, "agreed" or "strongly agreed" with the statement, "[a]ttorneys can cooperate in discovery while still being zealous advocates for their clients."

This Cooperation initiative is being implemented in stages. First came The Sedona Conference's® *Proclamation*, which alerted stakeholders to the need for cooperation and its advantages. The announcement was an expression of support for the concept. Now, in this paper, we offer arguments supporting cooperation. The final stage will provide practical examples to train and support lawyers, judges, and others in cooperative discovery techniques. Using these steps, The Sedona Conference® will offer solutions to many of the problems associated with contemporary discovery, and allow litigants to devote their resources toward a resolution of their disputes on the merits.

***341 TABLE OF CONTENTS**

*342 I. OVERVIEW

"If there is a hell to which disputatious, uncivil, vituperative lawyers go, let it be one in which the damned are eternally locked in discovery disputes with other lawyers of equally repugnant attributes." -- Judge Wayne E. Alley in Krueger v. Pelican Products Corp.[1]

Although lawyers may be relieved that Judge Alley's authority does not extend beyond the mortal confines of the courtroom, his comments signal a shared and growing distaste, if not disdain, by judges for the cost, delay, and disruption resulting from unnecessary or abusive discovery disputes.[2] That *Krueger* was decided twenty years ago, prior to the explosion of routine electronic communications, demonstrates that the problem is not new. However, the advent of electronically stored information ("ESI") has dramatically exacerbated the problem, increasing the volume of potentially discoverable material, the complexity and cost of the discovery process, and the opportunities for not only unduly burdensome and overly broad discovery requests, but also responses and production that obfuscate and evade. "Hide the ball" has become "hide the byte."

As this paper argues, the growth in ESI has not changed the obligation of cooperation in discovery that attorneys owe to the court and opposing counsel under both the Federal Rules of Civil Procedure and the rules of professional conduct.[3] Those obligations have long existed and were reinforced with respect to electronic discovery by the 2006 Amendments to the Rules.[4] However, the explosion of ESI has made the development of parameters to guide cooperation in discovery more essential than ever. The complexity of ESI has created uncertainty over what constitutes cooperation and good faith regarding preservation, search, review, and production. Additionally, the magnitude of the ESI has dramatically increased costs to the judicial system generally, and clients, specifically. Cooperation can help mitigate both difficulties.

Cooperation in this context is best understood as a two-tiered concept. First, there is a level of cooperation as defined by the Federal Rules, ethical considerations, and common law. At this level, cooperation requires honesty and good faith by the opposing parties. Parties must refrain from engaging in abusive discovery practices. The parties need not agree on issues, but they must make a good faith effort to resolve their disagreements. If they cannot resolve their differences, they must take defensible positions.

Then, there is the second level of cooperation. While not required, this enhanced cooperative level offers advantages to the parties. At this level, the parties work together to develop, test, and agree upon the nature of the information being sought. They will jointly explore the best method of solving discovery problems, especially those involving ESI. The parties jointly address questions of burden and proportionality, in order to narrow discovery requests and preservation requirements as much as reasonable. At this level, cooperation allows the parties to save money, maintain greater control over the dispersal of information, maintain goodwill with courts, and address the litigation's merits at the earliest practicable time.

The line between first and second level cooperation is, of necessity, difficult to draw. There is no precise definition of "cooperation," as there are no precise definitions of good faith or reasonableness. However, counsel understand that absent a more cooperative posture in the discovery process, the cost of litigation and the burden imposed as courts are forced to attempt to resolve disputes, will ultimately bring the system to a halt.

***343** One commentator has visualized these tiers of cooperation as concentric circles forming a target with a "bull's eye" in the center. An outer ring is what the rules clearly require. An inner ring goes beyond the requirements to the level of cooperation that can be achieved with creative energy applied to mutual self-interest. The rules require that attorneys hit the

target somewhere, but make it clear that attorneys should aim for the center.[5]

A. The Costs of Unnecessary Discovery Disputes

Unnecessary discovery battles affect not just judicial tempers, increasing the likelihood of sanctions, but also impair the functioning of the judicial system by overburdening already stretched courts,[6] preventing adjudication of meritorious claims or forcing settlement of meritless ones due to excessive costs,[7] and undermining the very purpose for which discovery obligations exist -- to allow adjudication on the merits.[8] Clients ultimately bear the costs of responding to lengthy and often repetitive or overly broad interrogatories and document requests -- and boilerplate objections to them -- or of sifting through reams of unresponsive electronic and physical documents, followed, in many cases, by time-consuming motion practice and hearings.[9] Substantively, the client may be no better off upon resolution of the dispute by the court since parties often find themselves in the same position they would have been in had they cooperated at the outset.[10]

But client costs may extend beyond financial outlays from drawn-out disputes. For example, failure of counsel to evaluate whether a discovery request is reasonable and not unduly burdensome before making it, or objecting to requests with boilerplate rather than fact-based objections, can warrant sanctions that impair adjudication on the merits, such as deeming facts admitted or objections waived.[11] Where counsel has not cooperated to identify appropriate parameters for electronic discovery, courts may reject later claims that discovery is overbroad, forcing unnecessary discovery costs on the client.[12]

B. The Benefits of Cooperation for E-Discovery

The appropriate level of transparency and communication with opposing counsel on the thorny issues involved in e-discovery can provide some degree of protection from the costs and potential sanctions that may result from lack of cooperation. For example, transparency and cooperation in initial phases of discovery may help identify both what must be preserved and the routine destruction policies in place that may help establish good faith if destruction is later challenged,[13] avoiding costly delays and possible spoliation sanctions. Good faith efforts to identify the sources and custodians of relevant ESI early in discovery and communication of that information to opposing counsel may help to not only avoid subsequent duplicative and costly searches, but also may rebut inferences of bad faith in discovery planning or intentional suppression of information if additional relevant sources are later identified. Early, transparent discussions on data storage systems ***344** employed by the parties puts each on notice as to what information may not be reasonably accessible, possibly avoiding the need for later motions to compel and post hoc explanations as to why documents were not produced.[14] Additionally, consultation about technical issues that arise in discovery can avoid later inferences of bad faith.[15] Further, transparency may establish the form in which a party normally maintains ESI, potentially avoiding disputes over whether data should have been produced in native format.[16]

Courts increasingly recognize that “electronic discovery requires cooperation between opposing counsel and transparency in all aspects of preservation and production of ESI.”[17] For instance, working cooperatively with opposing counsel to identify a reasonable search protocol, rather than making boilerplate objections to the breadth of a requested protocol or unilaterally selecting the keywords used without disclosure to opposing counsel,[18] may help avoid sanctions or allegations of intentional suppression. Indeed, because knowledge of the producing party’s data is usually asymmetrical, it is possible that refusing to “aid” opposing counsel in designing an appropriate search protocol that the party holding the data knows will produce responsive documents could be tantamount to concealing relevant evidence.[19]

C. Cooperation in Discovery and Zealous Advocacy Are Not Conflicting Concepts

Still, from the perspective of many practitioners, abandoning a purely adversarial stance during discovery in favor of cooperation appears antithetical to the concept of zealous advocacy.[20] This paper demonstrates that cooperation -- in the sense intended by the *Proclamation* -- and zealous advocacy are not conflicting concepts under professional conduct rules. Cooperation requires neither conceding nor compromising the client’s interests. Nor does it require foregoing court resolution of *legitimate* discovery disputes. Court criticism has centered on *unnecessary* disputes -- those that could have been avoided by cooperating and communicating according to procedural and ethical obligations -- rather than those arising from good faith disagreements about the parameters and progress of discovery that may require court intervention. Cooperation avoids

unnecessary disputes and violation of ethical rules while preserving for court resolution of those disputes that cannot be resolved through good faith cooperation.

Cooperation, as envisioned by the *Proclamation*, requires, for example, that counsel adequately prepare *prior* to conferring with opposing counsel to identify custodians and likely sources of relevant ESI, and the steps and costs required to access that information. It requires disclosure and dialogue on the parameters of preservation. It also requires forgoing the short term tactical advantages afforded one party by information asymmetry so that, rather than evading their production obligations, parties communicate candidly enough to identify the appropriate boundaries of discovery. Last, it requires that opposing parties evaluate discovery demands relative to the amount in controversy. In short, it forbids making overbroad discovery requests for purely oppressive, tactical reasons, discovery objections for evasive rather than legitimate reasons, and "document dumps" for obstructionist reasons. In place of gamesmanship, cooperation substitutes transparency and communication about the nature and reasons for discovery requests and objections and the means of ***345** resolving disputes about them. In at least twelve recent decisions, jurists have recognized the need for discovery cooperation and cited with approval the *Cooperation Proclamation*.[21]

As noted in the Overview section of this paper, to understand what is meant by the word "cooperation" in this context, it is useful to think of a two-tiered approach. First, there is a level of cooperation required by the Federal Rules, ethical considerations and common law. This limited level of cooperation requires communication and good faith by parties.[22] It requires that parties refrain from engaging in abusive discovery practices. It does not require agreement on issues, but it requires that parties take defensible positions if agreement cannot be reached.[23] But there is also a second level of cooperation. While not specifically required, this enhanced level of cooperation is usually advantageous for parties. As noted by one commentator, this enhanced level of cooperation "urges [parties] to seek out new ways to work together, and it urges them to do so not in spite of their interests but in furtherance of them."[24] Thus, parties engaging in this level of cooperation will work together to develop and test search criteria. They will jointly explore the best method of solving difficult problems like data discovery. They will address burden and proportionality by seeking to narrow discovery requests and preservation requirements as much as is reasonable. Through such cooperation, parties save money, maintain more control over what information is disseminated, engender good will with courts, and generally get to the merits of litigation much sooner.

This paper lays out the legal and ethical foundations for the duty to cooperate in discovery and the economic case for cooperation independent of those foundations. It begins with a discussion of cooperation required, either expressly or impliedly, by the Federal Rules of Civil Procedure. Second, it presents professional conduct rules that embody the duty to cooperate and discusses illusory conflicts with other professional conduct rules. It argues that the concept of zealous advocacy, properly understood as bounded by an attorney's duties as an officer of the court and to follow the law, does not conflict with the duty to cooperate in discovery. Third, evolving legal authority for the duty to cooperate is presented through a discussion of recent case law that addresses, in particular, cooperation in electronic discovery and growing court frustration with bad faith litigation conduct. A discussion of the practical reasons for cooperation -- economic and strategic benefits -- concludes the analysis.

II. THE FEDERAL RULES OF CIVIL PROCEDURE ASSUME COOPERATION IN DISCOVERY

A. The Evolution of American Discovery Procedures

The Federal Rules of Civil Procedure do not explicitly require counsel to cooperate in discovery, but the duty is implicit in the structure and spirit of the Rules. Indeed, the liberalization of discovery beginning in 1938 with the adoption of the Rules was designed to promote the resolution of disputes. Such resolution was intended to be based on facts underlying the claims and defenses with a minimum of court intervention, rather than on gamesmanship that prevented those facts from coming to light entirely or at least far too late in the process to serve the fair and efficient administration of justice. A brief look at the history of the modern Federal Rules makes clear that cooperation has been an essential element of the logic underlying them.

The modern Federal Rules were adopted in reaction to the pre-1938 system. Prior to 1938, lawyers prepared for trial principally through a process of formal pleadings, with complex rules for ***346** replies and responses that put a premium on gamesmanship at the expense of concealing critical facts until trial.[25] Attorneys relied primarily on an opponent's pleadings for discovery, without much disclosure.[26] By contrast, the new Rules allowed counsel to discover information about the

opponent's case before trial through the devices outlined in the Rules. As the Supreme Court has recognized, the more liberal approach to discovery made "trial less a game of blind man's buff and more a fair contest with the basic issues and facts disclosed to the fullest practicable extent."[27]

The Court has also noted that these new instruments of discovery were designed to serve
(1) as a device, along with the pre-trial hearing under Rule 16, to narrow and clarify the basic issues between the parties, and (2) as a device for ascertaining the facts, or information as to the existence or whereabouts of facts, relative to those issues. Thus civil trials in the federal courts no longer need be carried on in the dark.[28]

In the first set of amendments to Rule 26 in 1946, the Advisory Committee sought to clarify that the "purpose of discovery is to allow a broad *search* for facts, the names of witnesses, or any other matters which may aid a party in the preparation or presentation of his case."[29]

In *Hickman v. Taylor*, the Supreme Court identified the value of pre-trial discovery:

> The way is now clear, consistent with recognized privileges, for the parties to obtain the fullest possible knowledge of the issues and facts before trial .... Mutual knowledge of all the relevant facts gathered by both parties is essential to proper litigation. To that end, either party may compel the other to disgorge whatever facts he has in his possession. The deposition-discovery procedure simply advances the stage at which the disclosure can be compelled from the time of trial to the period preceding it, thus reducing the possibility of surprise.[30]

The Court further cautioned that counsel may not hide "any material, non-privileged facts" from the opposing party.[31] Reflecting a core principle underlying the *Cooperation Proclamation*, the Court recognized that the inherent role of "a lawyer [as] an officer of the court" requires attorneys to "work for the advancement of justice while faithfully protecting the rightful interests of his clients."[32] By permitting disclosure of even privileged information in some circumstances, the Court struck a balance between the ostensibly competing duties of attorneys to the court and to their clients. It noted that a chief objection to liberal discovery -- that it promotes a fishing expedition -- had been rejected because of the mutual benefits of discovery.[33]

Discovery was further liberalized in 1970 when the requirement to show "good cause" to obtain discovery under Rule 34 was eliminated.[34] Other 1970 changes in the mechanics of discovery were designed "to encourage extrajudicial discovery with a minimum of court intervention,"[35] preserving, of course, the ultimate authority of the courts to "limit discovery in accordance with [the] rules" even as to matters within the scope of Rule 26(b).[36] The rules thus contemplated that while discovery was to be managed largely by the parties, courts may intervene to limit or otherwise manage discovery when necessary.

***347** In 1980, the Rules were amended to address growing concerns with discovery abuse. Despite the intent that liberalized discovery rules would advance the interests of fair administration of disputes, concern mounted that adversarial, rather than cooperative, conduct drove the process. In a landmark 1978 law review article, Magistrate Judge Wayne Brazil of California made an impassioned plea for substantial changes to both procedural and ethical standards. Such changes, he argued, were necessary and appropriate because:

> The adversary character of civil discovery, with substantial reinforcement from the economic structure of our legal system, promotes practices that systematically impede the attainment of the principal purposes for which discovery was designed. The adversary structure of the discovery machinery creates significant functional difficulties for, and imposes costly economic burdens on, our system of dispute resolution.[37]

Specifically, along with more far-reaching recommendations, Brazil proposed, "shifting counsel's principal obligation during the investigation and discovery stage away from partisan pursuit of clients' interests and toward the court [and] expanding the role of the court in monitoring the execution of discovery."[38]

Beginning in 1980, a series of amendments to Rule 26 addressed discovery abuses. The amendments encouraged cooperation by suggesting -- and later requiring -- parties to "meet and confer" to, *inter alia*, develop a discovery plan.[39] By 1993, parties were made *jointly* responsible for development of the discovery plan and "for attempting in good faith" to agree to one.[40]

When good faith discussions failed to produce an agreement, the Rule contemplated that parties may seek court assistance.[41] However, court intervention should be invoked only after "counsel ... has attempted without success to effect with opposing counsel a reasonable program or plan for discovery."[42] Narrow disputes were not to be resolved by resorting to requests for protective orders or conferences with the court.[43] The Advisory Committee observed that parties' discovery obligations are intertwined with the underlying goal of the Federal Rules to promote the administration of justice:

> Given our adversary tradition and the current discovery rules, it is not surprising that there are many opportunities, if not incentives, for attorneys to engage in discovery that, although authorized by the broad, permissive terms of the rules, nevertheless results in delay. As a result ... the rules have not infrequently been exploited to the disadvantage of justice. These practices impose costs on an already overburdened system and impede the fundamental goal of the just, speedy, and inexpensive determination of every action.[44]

The amendments also provided courts with explicit authority to sanction parties who failed to meet their obligations to engage in "good faith" discovery planning.[45]

Acknowledging the reality that the discovery process "cannot always operate on a self-regulating basis," Rule 26(b)(1) was amended to address overbroad and unnecessary discovery, and introduce the notion of proportionality, intending "to encourage judges to be more aggressive in identifying and discouraging discovery overuse."[46] The amendments also recognized the duties of counsel to "reduce repetitiveness and *oblige lawyers to think through their discovery activities in advance* ***348** so that full utilization is made of each deposition, document request, or set of interrogatories."[47] Recognizing again that discovery is not to be used as an adversarial tool, but instead to ensure the administration of justice, the Advisory Committee noted that discovery was not to be used to "wage a war of attrition or as a device to coerce a party."[48] Finally, by imposing on counsel the duty to sign each discovery request, response, or objection and, thus certify the reasonableness of each, Rule 26(g) imposed "an affirmative duty to engage in pretrial discovery in a responsible manner that is consistent with the spirit and purposes" of the Rule.[49] With false certification subject to sanctions and a determination of reasonableness ultimately in the hands of the court, the amended Rule reflected the role of the courts as a backstop when parties failed to meet their obligations rather than to diminish those obligations: "If primary responsibility for conducting discovery is to continue to rest with the litigants, they must be obliged to act responsibly and avoid abuse."[50]

In 1993, Rule 26(f) was amended to omit provisions requiring a court scheduling conference after the parties met and conferred, reserving judicial supervision of the timing, scope, and extent of discovery until after the parties had conferred.[51] Former subdivision (f) "envisioned the development of proposed discovery plans as an optional procedure,"[52] whereas the new Rule directed, with few exceptions, "in all cases ... litigants must meet ... and plan for discovery" prior to submitting proposals to the court.[53] The Rule requires parties to "attempt in good faith to agree on the contents of the proposed discovery plan."[54]

In 2000, the scope of Rule 26(a) disclosures was narrowed to information the party intended to use to support its claims or defenses.[55] While courts retained ultimate authority over the scope of discovery, the Advisory Committee Note makes clear that cooperation prior to court intervention was the expectation of the rule:

> The rule change signals to the court that it has the authority to confine discovery to the claims and defenses asserted in the pleadings, and signals to the parties that they have no entitlement to discovery to develop new claims or defenses that are not already identified in the pleadings. *In general, it is hoped that reasonable lawyers can cooperate to manage discovery without the need for judicial intervention.* When judicial intervention is invoked, the actual scope of discovery should be determined according to the reasonable needs of the action.[56]

Principles of party cooperation were carried forward in the 2006 amendments to Rule 26(f), directing parties to discuss issues relating to ESI, including the form in which it should be produced.[57]

It can hardly be questioned that the amendments subsequent to Judge Brazil's 1978 critique did not fully mitigate adversarial, rather than cooperative, discovery conduct.[58] However, a failure of the parties to comply with their obligations to cooperate, and of courts to enforce those obligations, does not negate the inherent obligation to cooperate embodied in the Rules. As

discussed below, courts faced with complex and confrontational e-discovery disputes have increasingly recognized that obligation. The following section discusses in more detail the specific Rules that impliedly assume cooperation.

B. The Federal Rules of Civil Procedure Assume Cooperation

Consistent with the history just described, a careful analysis of the Federal Rules of Civil Procedure demonstrates that the Rules both promote and assume cooperation in discovery between ***349** litigating parties throughout the litigation. While the Rules do not always precisely define how and when cooperation is expected in the context of discovery, their framework identifies both how and why cooperation is assumed. The specific Federal Rules of Civil Procedure that provide a framework for the expectation of cooperation during discovery include Rules 1, 26, and 37.[59]

Rule 1 directs that all of the Rules be "construed and administered to secure the just, speedy, and inexpensive determination of every action and proceeding."[60] Thus, because cooperation in discovery can reduce both the duration of the discovery period and its costs, specific Rules governing discovery that require good faith discussions and conduct should be construed to promote cooperation. Moreover, Rule 1 reinforces the primacy of attorneys' obligations to ensure the objectives of the Rules are achieved -- the Advisory Committee Note directs that attorneys, "as officers of the court," share responsibility with the court to ensure that "civil litigation is resolved not only fairly, but also without undue cost or delay."[61] Cooperation by counsel to conduct discovery, particularly electronic discovery, efficiently and in good faith to ensure information sought and produced is consistent with fair administration of the litigation is thus implicit in Rule 1's command. Conduct that uses discovery for illegitimate adversarial purposes -- to oppress, coerce, delay or evade -- contravenes attorneys' obligations under Rule 1.

More specifically, several subsections included in Rule 26 assume a certain level of cooperation regarding discovery in the earliest stages of a case. Rule 26(a) imposes obligations on parties and counsel to disclose certain information at the outset of litigation, including the categories of relevant ESI.[62] Pursuant to Rule 26(f), the parties must confer at an initial conference about the nature of the claims involved and certain other specifics relating to the scope of discovery.[63] These obligations extend to conferences regarding the production of ESI.[64] In both instances of early discussion, the opportunity exists for counsel to cooperate beyond simply disclosing plainly required information. Though cooperation is not explicitly mandated under Rule 26(f), Rule 26's command that counsel engage in "good faith" efforts to develop a joint discovery plan suggests that counsel must do more than meet to announce their absolute positions on contested discovery issues, without any attempt to resolve those disputes based on the *legitimate* needs of the parties. The requirement to "confer" mandates, at a minimum, a good faith basis for disagreements. If cooperation were not an element of the required conference, the requirement that parties "confer" would be surplusage.

The Rules also require that parties must have a legitimate basis for their discovery demands and disputes, based on some prior, reasonable factual inquiry. This type of augmented duty to cooperate, beyond the mandated initial disclosures and conferences, may under certain circumstances be imposed by the obligations contained in Rule 26(g). That rule requires that parties sign discovery requests, responses and objections certifying, *inter alia*, that each is "not interposed for any improper purpose, such as to harass, cause unnecessary delay, or needlessly increase the cost of litigation" and is not "unreasonable nor unduly burdensome or expensive, considering the needs of the case, prior discovery in the case, the amount in controversy, and the importance of the issues at stake in the action."[65] Whether parties can so certify without good faith communication and transparency with the opposing party to identify needs, costs, and other issues seems unlikely. Thus, the type of cooperation The Sedona Conference® advocates in this context goes beyond the mere disclosure of certain mandated facts, requiring, in addition, assistance and joint effort to achieve the very best discovery protocol. In *Mancia v. Mayflower Textile Services Co.*, the court held that Rule 26(g)'s obligation of certification, following a "reasonable inquiry," was "intended to impose an 'affirmative duty' on counsel to behave responsibly during discovery" -- which requires cooperation and communication, ***350** particularly in the realm of e-discovery.[66] This construction of Rule 26(g) is supported by Rule 1 and the Advisory Committee Note to Rule 26(g), which provides in part:

> Rule 26(g) imposes an affirmative duty to engage in pretrial discovery in a responsible manner that is consistent with the spirit and purposes of Rules 26 through 37. In addition, Rule 26(g) is designed to curb discovery abuse by explicitly encouraging the imposition of sanctions. The subdivision provides a deterrent to both excessive discovery and evasion by imposing a certification requirement that obligates each attorney to stop and think about the legitimacy of a discovery request, a response thereto, or an objection. The term "response" includes answers to interrogatories and to requests to admit as well as

> responses to production requests.[67]

Any certification of discovery requests or responses that violates the requirements of Rule 26(g) is subject to sanction, absent "substantial justification."[68]

Finally, Rule 37 is entitled "Failure to Make Disclosures or to Cooperate in Discovery; Sanctions." Specifically, Rule 37(f) provides for sanctions for failure to "participate in good faith in developing and submitting a proposed discovery plan." The requirement of "good faith" requires an honesty of intent in discovery planning. That standard cannot be met by a party who has failed to confer with the opposing side about the scope of the claim and likely defenses in order to determine the appropriate scope of discovery; to conduct pre-meeting and ongoing due diligence regarding the availability, location and costs of discovering information and sharing that information with the opposing party; to seek agreement on the form of production and the means of searching and retrieving information; and to develop a reasonable discovery budget consistent with the nature of the claim.

In addition to the Federal Rules of Civil Procedure, 28 U.S.C. Section 1927 allows the imposition of costs and attorneys' fees when attorneys engage in dilatory conduct not justified by *legitimate* needs of the client, providing that:

> Any attorney or other person admitted to conduct cases in any court of the United States or any Territory thereof who so multiplies the proceedings in any case unreasonably and vexatiously may be required by the court to satisfy personally the excess costs, expenses, and attorneys' fees reasonably incurred because of such conduct.[69]

Consistent with the approach of the *Cooperation Proclamation*, sanctions envisioned by the statute focus on unjustified delay -- delay legitimately based on a client's needs is not sanctionable under the statute.[70] The *Proclamation* requires cooperation to identify and flesh out legitimate disputes and to provide courts with a factual foundation on which to make a decision should the parties be unable to reach a resolution absent court intervention.

These mechanisms give the courts the broad discretionary authority to issue an array of sanctions against parties who fail to cooperate during discovery. Considered *in toto*, the Federal Rules impose on attorneys an obligation not to engage in conduct that delays, burdens or renders litigation unfair. The means by which parties can fulfill their obligations under Rule 1 can be found in the specific rules governing discovery conduct. The goal of the *Cooperation Proclamation* and associated resource materials is to provide parameters for what good faith, cooperative conduct in electronic discovery entails and what it does not.

*351 III. COMPLIANCE WITH PROFESSIONAL CONDUCT RULES REQUIRES COOPERATION IN DISCOVERY[71]

The duty to cooperate is likewise embodied in the professional conduct rules to which attorneys are bound. Though ethical rules discuss an attorney's obligation to act with zeal in asserting the client's interests,[72] that duty is not unqualified.[73] It is bounded by an attorney's ethical duties to opposing counsel, opposing parties, third parties, and importantly, the tribunal and the judicial system as a whole.[74] As the *Mancia* court recently noted:

A lawyer who seeks excessive discovery given what is at stake in the litigation, or who makes boilerplate objections to discovery requests without particularizing their basis, or who is evasive or incomplete in responding to discovery, or pursues discovery in order to make the cost for his or her adversary so great that the case settles to avoid the transaction costs, or who delays the completion of discovery to prolong the litigation in order to achieve a tactical advantage, or who engages in any of the myriad forms of discovery abuse that are so commonplace is ... hindering the adjudication process, and making the task of the "deciding tribunal not easier, but more difficult," and violating his or her duty of loyalty to the "procedures and institutions" the adversary system is intended to serve. Thus, rules of procedure, ethics and even statutes make clear that there are limits to how the adversary system may operate during discovery.[75]

Professional conduct rules require attorneys to simultaneously meet ethical duties to their clients and the tribunal and to conform their conduct to the requirements of the law.[76] Indeed the Preamble to the Model Rules of Professional Conduct ("MRPC") upon identifying zealous advocacy as the attorney's role immediately confines that duty -- it is subject to the

"rules of the adversary system."[77] Other limitations on zealous advocacy are replete throughout the Preamble,[78] and are reflected in specific rules.

The need for litigators to balance simultaneous ethical duties is nothing new.[79] Apart from the ethical duties implicated by discovery conduct, discussed below, the list of ethical obligations to ensure the fairness and integrity of the justice system that trump attorneys' duties to their client is lengthy and familiar. For example, counsel has a duty to inform unrepresented persons with interests potentially adverse to the client of that adversity and must refrain from giving them any legal advice, ***352** though doing so may be beneficial to the client.[80] To fulfill their duties as officers of the court, attorneys must report adverse controlling authority to the court, even where opposing counsel has not done so, and correct even inadvertent misstatements of material fact or law, though doing so is contrary to the client's interest.[81] Moreover, counsel is bound by these duties to the tribunal even where compliance requires disclosure of confidential information.[82] Similarly, counsel must withdraw from representation, regardless of the impact on the client (subject, of course, to court approval) when continued representation would require a violation of ethical rules or other law.[83] The list of mandatory ethical obligations that may be contrary to the client's interest goes on.

Thus, lawyers' obligation of zealous advocacy is confined by, rather than in conflict with, their obligations to the court.[84] As discussed below, while there is a place for zealous advocacy in discovery, an attorney's ethical and procedural obligations to cooperate with opposing counsel are not subjugated to the concept of zealous advocacy. Meeting one's duty to a client does not excuse failure to identify sources of and produce basic evidence sought in discovery,[85] frivolous discovery requests, unfounded objections in discovery,[86] false representations or certifications to the court,[87] or discovery delay for delay's sake.[88]

A. The Duty to Expedite Litigation Requires Cooperation

First and fundamentally, an attorney's ethical duty to conform his or her conduct to the requirement of the law unquestionably requires, in the context of discovery, compliance with procedural rules of the court.[89] As discussed *supra* Part II.B, those rules include Rule 1 of the Federal Rules of Civil Procedure, noting an attorney has an obligation, as an officer of the court, to avoid undue delay and cost;[90] Rule 26(f), which assumes a certain degree of cooperation in discovery planning; and Rule 26(g), requiring an attorney to certify that discovery requests and responses are not made for an improper purpose. Consistent with those rules, Rule 3.2 of the MRPC requires attorneys to make reasonable efforts to expedite litigation. Refusal to cooperate in discovery by making overly broad or unnecessarily costly discovery requests or objecting to requests without legitimate foundation is inconsistent with the duty to expedite litigation. Cooperation in discovery planning is thus assumed not only by the Civil Rules, it is among the obligations of Rule 3.2 of the MRPC.

Cooperating to expedite discovery does not conflict with any notion of zealous advocacy. First, the duty to expedite must be "*consistent with the interests of the client*."[91] Thus, neither Rule 3.2 nor the cooperation envisioned by the *Proclamation* would require counsel to forego pursuing even time-consuming resolution of discovery disputes necessary to serve the legitimate interests of the client. For example, cooperation does not foreclose objections to expansive discovery requests after a thorough inquiry about the nature and sources of responsive information. Cooperation *does*, however, require communicating with opposing counsel about the basis for the objection and making a good faith effort to narrow discovery and achieve a mutually agreeable solution. Second, failure to make reasonable efforts to expedite can only be founded on the *legitimate* interests of the client. What Rule 3.2 and the procedural rules, as emphasized here and advanced in the *Proclamation*, *do* forbid is discovery delay for the purpose of delay only. Though delay for delay's sake ***353** may benefit the client, the rules do not recognize that benefit as a *legitimate* interest.[92] Consequently, good faith cooperation in discovery to meet the obligations of Rule 3.2 works in tandem with, not in opposition to, the concept of zealous advocacy.

B. The Duties of Candor to the Tribunal and Fairness to the Opposing Party Require Cooperation

The duty to cooperate in discovery is also embodied in Model Rule 3.4 which prohibits a party from obstructing another party's access to evidence or unlawfully altering, destroying, or concealing a document or other material having potential evidentiary value. When failure to cooperate in preservation, discovery planning, and production results in obstruction or destruction, attorneys violate not only procedural rules that risk court-imposed sanctions, they risk discipline by the state ethics enforcement authorities.[93] Where ESI is involved, obstruction or destruction does not require affirmative acts -- it can result when counsel simply does nothing. For example, failure to engage opposing counsel in a meaningful dialogue about

preservation obligations can result in destruction of relevant evidence from routine operation of document destruction and retention systems. Additionally, failure to cooperate in discussions regarding a meaningful electronic discovery plan based on information about each party's custodians and electronic storage systems may in itself be obstruction. As discussed more fully *supra* Part II, the Federal Rules require participation in a Rule 26(f) conference to discuss ESI issues. In addition to Model Rule 3.4's candor and fairness requirements, Model Rule 1.1 requires that counsel provide "competent representation," which is defined as requiring "legal knowledge, skill, thoroughness and preparation reasonably necessary to the representation." To fulfill these corollary obligations to meet and confer in candor and with competence, counsel must be sufficiently informed and knowledgeable about the client's existing sources of ESI and data management and storage systems, and prepared to discuss them, at the Rule 26(f) conference. That is because, as one commentator noted, in an age of electronic information, "it is, as a practical matter, impossible to get meaningful discovery if one side refuses to discuss the parameters of what constitutes a reasonable search, leading to unfair and oppressive results."[94] Likewise, a responding party engages in obstructionist conduct forbidden by ethical rules when it refuses to discuss means of narrowing the opposing side's proposed search protocol, though it has superior information about what methodology is likely to produce responsive documents, and then dumps a clearly unmanageable number of documents on the requesting party.[95]

A knowing failure to comply with civil discovery rules that assume cooperation could likewise violate Rule 3.4(d)'s admonition that an attorney may not knowingly disobey the rules of a tribunal except when based on a non-frivolous assertion that no valid obligation exists. Thus, attorneys who sign discovery requests, disclosures, or objections that were made with an improper purpose or that are unreasonable or unduly burdensome violate not only Rule 26(g), they also violate Model Rule 3.3 by making a false statement of fact to the tribunal. Rule 26(g) was intended to impose on counsel an affirmative duty to behave responsibly in discovery. That obligation, as the *Mancia* court noted, "requires cooperation by counsel to identify and fulfill legitimate discovery needs" while avoiding unduly costly and burdensome discovery.[96] In the context of electronic discovery, it will nearly always be preferable for counsel to certify the propriety of their discovery requests or objections after engaging in extensive cooperation prior to the commencement of discovery. For example, producing parties can, with more certainty, conclude requests are overly broad or unduly burdensome or that sources requested to be searched are unlikely to yield documents admissible in evidence after meeting with opposing counsel to discuss the opposing side's needs, investigating and evaluating the client's existing sources of ESI and the client's data ***354** management and storage systems, and communicating with the opposing side about those systems. Similarly, parties requesting discovery can more accurately certify that the request is neither "unreasonable nor unduly burdensome" -- that it is narrowly tailored -- after conferring with the opposing side to understand potential sources of information, the means by which that information will be retrieved, the costs of doing so, and potentially less burdensome sources of information.[97]

While neither Rule 3.2 nor Rule 3.4 explicitly require cooperation, attorneys will be hard pressed to meet their obligations under these provisions without cooperating on the scope, nature, and means of discovery both prior to discovery's initiation and throughout the litigation.

C. Ethical Rules Do Not Subordinate the Duty to Cooperate to the Duty of Confidentiality

The duty of confidentiality has long co-existed with discovery obligations and other ethical duties to the court. Though some have argued that seeking an informational advantage by minimizing documents provided to the opposing party is firmly grounded in the duty to preserve client secrets and protect privileged information,[98] that assertion does not answer whether an attorney violates his ethical duties to the court, not to mention his obligation to follow federal and local rules, when he withholds information requested by opposing counsel that is *not privileged*. At least one court has firmly rejected the argument that zealous advocacy obligates counsel to construe discovery requests narrowly to withhold documents harmful to the client.[99] The duty of attorneys to conform their conduct to the law prohibits them from withholding information that the Federal Rules require be produced upon good faith discovery requests or that would be produced if the parties engaged in good faith discussion about the nature and scope of discovery sought. While cooperation does not require attorneys to *volunteer* smoking gun documents that opposing counsel has not requested, it does require good faith efforts to produce information that the attorney reasonably understands is being sought.

In the context of electronic discovery, the duties of confidentiality, loyalty and zealous advocacy do not excuse failure to cooperate with opposing counsel in identifying likely sources of responsive ESI and developing appropriate search protocols that are likely to produce documents counsel knows the client possesses and the opposing party seeks. This does not mean that counsel must steer the opposing side to harmful documents. However, counsel may not use his superior information as to

the location or nature of responsive documents to thwart good faith discovery requests by refusing to engage cooperatively to identify the sources likely to contain relevant information and the search terms likely to produce responsive documents.[100]

Thus, where the Federal Rules assume cooperation, the ethical duties discussed above will likewise require attorneys to adhere to the cooperation expected under the Federal Rules. Moreover, even under circumstances where the Federal Rules do not explicitly address discovery cooperation, an attorney's ethical obligations under Rules 3.3 and 3.4 might nonetheless require cooperation.

IV. COURTS RECOGNIZE BOTH THE NEED FOR COOPERATION AND THE OBLIGATION TO COOPERATE

Courts have long recognized the need for attorneys to work cooperatively to conduct discovery, a need that has grown with the volume of ESI now typically involved in litigation. More recently, this recognition is often expressed as frustration over having to decide an avoidable dispute or simply an exasperated call for cooperation among counsel. For example, faced with overreaching ***355** discovery demands by one side and obstinate resistance to production by the other, one court observed that "the gravest error committed by the Magistrate was thinking that the parties could meet and confer to discuss any outstanding discovery requests" and concluded simply that "[t]his Court demands the mutual cooperation of the parties."[101] Courts further recognize that counsel's role as advocate in an adversarial system is not inconsistent with cooperating "to achieve orderly and cost effective discovery of the competing facts on which the system depends" and that the "rules of procedure, ethics, and even statutes make clear that there are limits to how the adversary system may operate during discovery."[102] As noted by the court in *In re Seroquel Products Liability Litigation*:

> [T]he posturing and petulance displayed by both sides on this issue shows a disturbing departure from the expected professionalism necessary to get this case ready for appropriate disposition. Identifying relevant records and working out technical methods for their production is a cooperative undertaking, not part of the adversarial give and take. This is not to say that the parties cannot have reasonable disputes regarding the scope of discovery. But such disputes should not entail endless wrangling about simply identifying what records exist and determining their format. This case includes a myriad of significant legal issues and complexities engendered by the number of plaintiffs. Dealing as effective advocates representing adverse interests on those matters is challenge enough. It is not appropriate to seek an advantage in the litigation by failing to cooperate in the identification of basic evidence.[103]

As discussed in Part II above, courts also recognize that the Federal Rules of Civil Procedure encourage and in many respects assume cooperation during discovery. "The overriding theme of [the 2006] amendments to the discovery rules has been open and forthright sharing of information by all parties to a case with the aim of expediting case progress, minimizing burden and expense, and removing contentiousness as much as practicable."[104] Thus, courts have held that counsel must confer and engage in good faith, meaningful discussions with the opposing party on discovery issues;[105] refrain from making discovery requests that are overly burdensome, costly, or disproportionate to the issue at stake;[106] make a reasonable inquiry into the factual basis for discovery objections and avoid boilerplate objections;[107] refrain from substantially unjustified discovery arguments;[108] perform a reasonable search for documents on a timely basis;[109] negotiate reasonable and workable search protocols;[110] provide accurate information to the court about steps taken in discovery;[111] provide a knowledgeable 30(b)(6) witness on IT issues;[112] and, in appropriate situations, either introduce expert testimony to support the suitability of search and review protocols, or avoid the need for expert testimony by cooperating with opposing counsel to create a mutually agreeable protocol.[113]

Even where courts decide discovery disputes without determining that the conduct of either side has violated procedural or ethical rules, courts are increasingly urging parties, often in frustrated or blunt language, to attempt to resolve or avoid such disputes by discussion and cooperation. Faced with a discovery dispute caused by the failure of the parties and a nonparty to provide "careful thought, quality control, testing, and cooperation with opposing counsel in designing search terms" for the production of ESI, one court found itself "in the uncomfortable position of having to craft a keyword search methodology for the parties," and concluded simply that "the best solution in the entire area of electronic discovery is cooperation among counsel."[114] After a detailed but restrained ***356** discussion of a series of unnecessary disputes over the scope of document requests and interrogatories, the adequacy of responses to such, and claims of privilege, another court noted that "the costs associated with adversarial conduct in discovery have become a serious burden not only on the parties but on this Court as

well."[115] The court went on to comment that "counsel's obligations to act as advocates for their clients and to use the discovery process for the fullest benefit of their clients ... must be balanced against counsel's duty not to abuse legal procedure." and "reiterate[] its advice to counsel to communicate and cooperate in the discovery process."[116] Indeed, courts faced with protracted discovery disputes often lament the conduct of both sides and initially decline to make a decision, instead instructing the parties to confer and attempt to resolve the issues.[117] Other courts, having decided some or all pending discovery disputes, urge (if not plead with) the parties to meet and confer as to future disputes rather than repeat the process.[118]

V. THE BENEFITS OF COOPERATION

As these cases suggest, attorneys can expect courts to increasingly enforce cooperation obligations imposed by procedural and ethical rules and to urge parties in increasingly strong terms to cooperate in ways that may go beyond what such rules and ethical requirements require.[119] Given this pressure from the bench, the unrelenting growth in the volume of electronic data, the economics of modern litigation, the financial and strategic benefits of cooperation, and the costs and risks of obstructionist conduct, cooperation in discovery is no longer merely desirable or laudatory, but rather is imperative to advance a client's interests.

A. The Economic Imperative to Cooperate in Discovery

The most straightforward reason for parties to cooperate throughout the discovery process is simple economics -- unnecessarily combative discovery wastes time and money. While this has always been the case, the increased volume and complexity of discoverable ESI in modern litigation has increased the costs of combative approaches to discovery as well as the potential savings of a more cooperative approach. While a 1983 study found "relatively little discovery occurs in the ordinary lawsuit" and "no evidence of discovery in over half our cases,"[120] a lawsuit between corporations may now involve "more than one hundred million pages of discovery documents, requiring over twenty terabytes of server storage space."[121] Obviously, this increase in the volume of documents and other information potentially responsive to discovery requests directly increases discovery costs. Moreover, the inherent complexity of ESI (such as multiple storage locations, varying formats, obsolete technology, metadata, and dynamic information) further increases the costs of preservation, review, and production. As a result, an adversarial approach to discovery, which might once have resulted in a minor but tolerable increase in litigation costs, could today substantially multiply such costs, potentially changing litigant behavior and often making discovery costs case-determinative.

Evidence increasingly indicates "that the sheer volume and complexity of electronically stored information (ESI) can increase litigation costs, impose new risks on lawyers and their clients, and alter expectations about likely court outcomes."[122] Where such expansive discovery may once have been the exception to the rule,[123] it can now account for as much as ninety percent of total litigation expenses.[124] Increased volume is a primary culprit, as modern discovery "may encompass hundreds of thousands, if not millions, of electronic records."[125] For example, the amount of ESI is estimated to have increased thirty ***357** percent annually from 1999 through 2002 alone.[126] Businesses in North America alone send and store an estimated 2.5 trillion new e-mails per year.[127] Consequently, larger corporate parties have expansive amounts of discoverable ESI,[128] while even individuals and small businesses often have quantities of data "substantially out of proportion to their ability to bear" the resulting costs of discovery.[129]

The inherent complexity of ESI also creates new and potentially costly issues in discovery. Deleted information is often not actually destroyed.[130] ESI often changes dynamically and can even change merely by being accessed.[131] Hidden metadata can include responsive information but can be difficult for the unprepared to preserve and produce.[132] Difficult to manage backup data may be responsive and need to be preserved, even if not searched and produced.[133] In addition, ESI typically resides in many locations, including hard drives, network servers, floppy disks, backup tapes, PDAs, thumb drives, smart cards, and cell phones.[134] It includes voice recordings as well as text documents, and instant messaging. And, emerging social media promise to increase the complexity and cost of e-discovery.[135] These complications magnify the cost issues raised by the sheer quantity of electronic documents. In addition, they can expose unprepared parties to spoliation claims for failure to preserve and produce.[136]

This increase in the volume and complexity of documents in today's digital world has not, however, altered the basic rules of

discovery.[137] Documents must still be preserved, collected and produced, often at great cost. In one case, restoration of data from two hundred backup tapes was estimated to cost $9.75 million even before the recovered documents were reviewed.[138] Beyond the cost of preservation and collection, ESI is still generally reviewed by attorneys for relevance and privilege -- an activity that some now estimate may account for as much as 75-90 percent of the costs of e-discovery.[139] Production and review, even in smaller cases, can cost hundreds of thousands of dollars.[140] Businesses now frequently spend more money to prepare for electronic discovery through technology upgrades and revised IT processes -- an expenditure that smaller companies may be ***358** unable to make.[141] Ultimately, these discovery cost increases "could dominate the underlying stakes in dispute" and even lead parties to decide against litigating meritorious claims or defenses.[142]

Against this backdrop of increasing volume and complexity of ESI magnifying the costs of discovery, antagonistic discovery strategies can be even more expensive and problematic than in the past. Such strategies "lead to delay as well as expenditures of much time and money on repetitive scope-of-discovery issues."[143] With the smaller scope and complexity of paper-based document discovery in litigation in prior years, these delays and cost increases could be minimal, or at least more tolerable. However, given the already substantially increased cost of discovery in light of the increased volume and complexity of ESI, the incremental costs imposed by combative approaches to discovery and unnecessary discovery disputes can be even more problematic.

This additional burden on parties and the judicial system is, in large part, avoidable. Commentators note that electronic discovery's complications and expense can be most problematic when the information is "not managed properly."[144] While the proliferation of ESI and its particular attributes have increased discovery costs in many ways, ESI by its very nature is particularly susceptible of being properly managed so as to limit costs. For example, ESI can be more accessible than paper records. Once identified and collected, ESI is generally easier to de-duplicate, sort, search and otherwise process in bulk. It can also be easier to actually handle and produce.[145]

Agreement between parties on key parameters such as the identity of custodians whose data will be preserved and/or collected; the date ranges, search terms, and methodologies to be employed by the parties to identify responsive data; and the format(s) in which document production will occur has the potential to unlock ESI's more useful attributes to reduce discovery expenditures for all parties. Early agreement on such key parameters makes it much less likely that a party will be ordered to supplement its production (and thus incur the expense of repeating searches, reviews, and production) because its opponent convinces a court that the producing party's unilateral choices were too narrow or otherwise inappropriate. In a survey of 2,690 attorneys recently involved in federal litigation, more than 60% of respondents, representing both plaintiffs and defendants, "agreed" or :strongly agreed" with the statement, "[t]he parties ... were able to reduce the cost and burden of the ... case by cooperating in discovery." Lee ET AL., *supra* note 19, at 30-31.

In this regard, cooperation does not mean simply volunteering data or information. Rather, cooperation suggests early, candid, and ongoing exchanges between counsel. For each side, these exchanges must address both the potentially discoverable information which that side possesses and its needs for information in the possession of the other side. Such dialogue can facilitate reciprocal agreements regarding preservation and production obligations that can enable each party to fulfill its own discovery obligations at lower cost and with less risk and to obtain the information it needs from the other side without undue expense or tribulation.

Indeed, cooperation in discovery is not an "all or nothing" matter. The parties can mutually reduce costs and risks by agreeing on many or most issues even if they cannot resolve all potential discovery disputes. Even in cases where both parties follow a good faith, cooperative approach, there may still be issues on which the parties legitimately disagree. Nonetheless, when that occurs, both sides should consider whether a cooperative, negotiated approach may be preferable to a judicial determination. Most cases settle because the parties elect not to face the expense of litigating to a conclusion on the merits and the risk of an unfavorable result. Similarly, parties who follow a cooperative approach to discovery can often resolve quite legitimate differences regarding discovery through negotiated resolutions by, for example, finding a livable middle ground between two fully defensible positions, or trading "wins" on multiple issues to create an overall resolution. Indeed, early cooperation on basic discovery parameters not only directly prevents or limits the additional litigation expense which might otherwise be imposed by discovery disputes on those matters, but it may also ***359** foster a less confrontational approach in which the parties are able to resolve downstream differences without involving the court.

Overreaching discovery demands, obstructionist responses to legitimate discovery and unproductive discovery disputes all

unnecessarily drain the resources of litigants and slow, or even prevent, adjudication on the merits. In contrast, when parties conduct discovery in a diligent but cooperative and candid manner, each can obtain the discovery it needs to adjudicate the dispute on the merits (or to reach a mutually agreeable settlement) while minimizing discovery expense. In any given case, it is thus in the interest of both sides to embrace a mutually cooperative approach to the exchange of discoverable documents and data. While either party could upset this balance by pursuing overreaching discovery, responding to legitimate discovery in an obstructionist manner, or forcing unnecessary discovery disputes, courts may use the rules of civil procedure and professional conduct to encourage compliance with a cooperative approach.[146] Aware of the already large cost of discovery of ESI and of the significant but unnecessary cost of discovery disputes, encouraged or pushed toward cooperation rather than gamesmanship by the courts and the rules of procedural and professional responsibility, and armed with better tools to effectuate such cooperation, it is in the self-interest of all parties to pursue a cooperative approach to discovery.

B. The Strategic Benefits of Cooperation

One potential difficulty in attempting to follow such a cooperative approach is that, particularly at the outset of a dispute, tensions are high, clients are unhappy if not angry, and the suggestion by counsel that a case may be resolved more efficiently and effectively by taking a cooperative approach to discovery may be interpreted by the client as weakness. Model Rule 2.1 states that "a lawyer shall abide by a client's decisions concerning the objectives of representation and, as required by Rule 1.4, shall consult with the client as to the means by which they are to be pursued." At the same time, as discussed in Part III, other professional responsibility rules, guidelines for civility and professionalism, and court rules instruct lawyers that civility, professional integrity, personal dignity, candor, diligence, respect, courtesy, and cooperation are essential to the fair administration of justice and conflict resolution. When a client understands these professional responsibilities of an attorney, the mandate of Rule 2.1 is consistent with a cooperative, reasonable approach to discovery. However, a client driven by distrust, fear, or a desire for retribution or to win at any cost may perceive discovery as just another opportunity to penalize the opponent and cooperation as a weakness. Such client motivations and perceptions can put the attorney in the middle and create a fundamental impediment to the reasonable cooperation in discovery so essential in the age of ESI.

Cooperation, however, is in the interest of even an aggressive client, and an attorney who persuasively explains this to the client serves both the client and his or her own professional obligations. Such a client must first understand what cooperation is and is not. Cooperation in the discovery context does not mean giving up vigorous advocacy; it does not mean volunteering legal theories or suggesting paths along which discovery might take place; and it does not mean forgoing meritorious procedural or substantive issues. Cooperation does mean working with the opposing party and counsel in defining and focusing discovery requests and in selecting and implementing electronic searching protocols. It includes facilitating rather than obstructing the production and review of information being exchanged, interpreting and responding to discovery requests reasonably and in good faith, and being responsive to communications from the opposing party and counsel regarding discovery issues. It is characterized by communication rather than stonewalling, reciprocal candor rather than "hiding the ball," and responsiveness rather than obscuration and delay.

Cooperation defined in this manner is not only largely compelled by the attorney's obligation to comply with legal rules, ethical obligations and the professional rules of conduct, but it also offers the client the benefits of creating and maintaining credibility with the court and the opposition, enhancing the effectiveness of advocacy, and minimizing client costs and risks. A client ***360** should be informed and understand that the attorney's duties to the client[147] are not unlimited[148] but are circumscribed both by court rules[149] and obligations of civility and professionalism.[150] Statements of civility and professionalism published by many courts and bar associations are particularly informative in explaining to a client the limits of representation and the obligations of an attorney to the administration of justice. These statements discuss conduct that may not be unethical but would be considered unprofessional and hence unacceptable.[151] The California Guidelines provide, for example, that an attorney has obligations of "civility, professional integrity, personal dignity, candor, diligence, respect, courtesy, and *cooperation*, all of which are essential to the fair administration of justice and conflict resolution."[152] Statements of professionalism and civility such as these provide important foundational justifications that can be brought to bear when persuading clients bent on being overly aggressive and resistant to take a more cooperative approach to dispute resolution.

Moreover, both counsel and clients should recognize that an obstructionist, overreaching, or simply non-cooperative approach to discovery invites adverse consequences for the non-cooperative party itself. This can take the form of non-cooperative conduct in return from the other side, leading the parties to conduct discovery "the hard way," with each party incurring unnecessary expense as a result of the other side's non-cooperative approach, but neither gaining a strategic or

tactical upper hand. It can also take the form of an adverse decision or even sanctions on the discovery dispute in question. Non-cooperative conduct early in the discovery process can lead a court to view that party's position less favorably when discovery disputes ripen and come before the court.

In addition, a cooperative approach that actively engages the other side on search methodologies and other e-discovery parameters and which incorporates the opposing party's legitimate needs into the production process makes it more likely that the court will accept the producing party's efforts as reasonable when a dispute later arises. That reduces the likelihood that the court will require the client to engage in costly repeat searches, reviews, and other discovery tasks.[153]

Similarly, non-cooperative conduct by a requesting party early in discovery can make the court reluctant to require further discovery from an opponent that has tried to cooperate. Thus, one court has recently recognized that, where the producing party asked opposing counsel "repeatedly to suggest search terms" but was rebuffed, "it is unfair to allow [the requesting party] to fail to participate in the process and then argue that the search terms were inadequate. This is not the kind of collaboration and cooperation that underlies the hope that the courts can, with the sincere assistance of the parties, manage e-discovery efficiently and with the least expense possible."[154]

Moreover, both counsel and the client should understand the desirability if not necessity of creating and maintaining credibility with the court, court staff, and opposing counsel. The most effective advocate is one who is believed and one who can be trusted. Indeed, the credibility of the attorney transcends a particular case or a particular client. A client must understand that an attorney's obligations to other clients mandates candor with both the court and with opposing counsel. The attorney's word must be trusted and that attorney's professional credibility cannot be compromised for one case or one client. The benefits of being represented by an attorney with a reputation of trustworthiness and candor is that the court and opposing parties will be more willing to accept representations and the need to prepare and present "proof" (and thus briefing, hearings and other formal proceedings) may be lessened. Furthermore, an attorney who has a reputation for being ***361** credible will likely have the adversarial advantage over the course of the dispute resolution process, particularly over an attorney who has below par credibility. Success in advocacy and persuasiveness on substantive issues is enhanced by the cooperative approach to discovery. Cooperatively working through procedural issues can have the effect of building a reservoir of goodwill and trust that can be drawn upon in advocating for the client's position on important substantive issues. Likewise, reasonableness, civility and flexibility begets a like response.

In short, a cooperative approach is more likely to speed up the time for reaching a resolution, to enhance the possibility of settlement, enhance the likelihood of an optimum result and lower the overall cost of the dispute resolution process.

C. Avoiding the Prisoner's Dilemma

When both sides to litigation pursue a cooperative approach to discovery, each party benefits by reducing its discovery expense while it still obtaining necessary information to which it is entitled. However, the phenomenon which game theory refers to as the "Prisoner's Dilemma" suggests that the fear of being disadvantaged if the other side were to take a non-cooperative approach to discovery could lead both sides to reject cooperation, thus raising litigation expenses for both sides while giving neither any advantage as a result of this additional cost. Either party in a particular case may perceive that one could gain an advantage over the other by employing obstructionist, overreaching or combative tactics, potentially preventing its opponent from obtaining needed and discoverable data, but itself reaping the benefits of receiving full discovery from its more cooperative opponent. In the classic Prisoner's Dilemma, the prospect that an opponent might seek such an advantage could lead both sides to defensively pursue a non-cooperative approach, so that, in the end, neither gains a unilateral advantage over the other and both are actually worse off than if both had cooperated.[155] In discovery, this would result in each spending more on discovery than would have been the case if both sides had taken a cooperative approach, but with neither party gaining the benefits of mutual cooperation much less an upper hand over the other side.

However, the Prisoner's Dilemma phenomenon breaks down where the actors involved must repeatedly face the same or similar decisions with the same or similar costs, benefits and risks. Under these circumstances, a party considering taking a non-cooperative approach in an attempt to gain an advantage over the other side must evaluate the risk of the other side responding with similar conduct during a subsequent "round."[156] In the discovery setting, for example, an obstructionist approach regarding e-discovery parameters during a Rule 26(f) conference may lead to non-cooperative conduct by the other side in subsequent meet-and-confer situations where the first party would itself benefit from mutually cooperative

resolutions. Indeed, even in a single Rule 26(f) conference or other individual meet-and-confer situation, there are often multiple issues to address, each of which can be viewed as a "round" in which non-cooperative conduct by one side could induce non-cooperative conduct by the other side in subsequent rounds.

Thus, a party's non-cooperative conduct in each round potentially has later adverse consequences for that very party, and the threat of such can lead both sides to a cooperative approach.[157] This leads the parties, each following its own self-interest, to pursue a cooperative approach that leads both to the mutually beneficial result -- here, lowering discovery expenses. The opportunity (indeed, the requirement) imposed by the civil rules and many local rules to address and attempt to agree upon key discovery parameters early in each case, coupled with the high likelihood that there will be many additional downstream steps in each case can induce both sides to behave in a cooperative manner.

The Prisoner's Dilemma phenomenon further breaks down where the actors involved can communicate with each other to develop and exchange enforceable, reciprocal commitments; where each actor can learn about the other's reputation for trustworthiness as to such commitments from the ***362** other's prior interactions with third parties; and where each actor must be concerned with the impact of its own present conduct on its reputation and thus its ability to elicit conduct that it may seek from others in the future.[158] Unlike the two isolated hypothetical individuals in the Prisoner's Dilemma who *cannot* communicate with each other, attorneys and parties in litigation can cooperatively bargain for interdependent commitments on specific issues before actually performing and conveying benefits on the other side. They can also enforce such commitments through court involvement, consider the reputation of the opposing counsel and party in deciding whether to enter such agreements, and consider the consequences of their actions on their own reputation, all of which permits and encourages cooperative solutions.[159]

Finally, the circumstances of litigation introduce a variable not present in the classic Prisoner's Dilemma: the possibility of an intervening enforcement authority. In litigation, the attorneys and parties conducting discovery must also consider how a court will view and potentially reward or penalize their actions. As discussed in Section B above, an obstructionist or overreaching approach by a party in discovery may lead to unfavorable decisions by the court as to that very issue or as to other discovery disputes in the same case. Moreover, forcing the court to address an unnecessary discovery dispute or taking an inappropriately aggressive or unsupported position may undermine the credibility of counsel and the party on subsequent procedural or substantive issues. This threat can provide incentives for each party to pursue a cooperative approach. Of course, judicial willingness to support reasonable discovery approaches and to penalize overreaching and obstructionist positioning will increase the effectiveness of this incentive. Indeed, that attorneys will again appear before the courts, and their clients may as well, creates a dynamic in which the threat of future obstructionist conduct by opponents, or risk of gaining a reputation among the judiciary as unduly combative during discovery, encourages cooperative behavior.

Thus, while there may remain cases in which a party opts for a contentious, non-cooperative approach to discovery, potentially forcing onto the opponent disputes not of its choosing and their attendant costs, in most cases, mutual self-interest should lead both sides to a cooperative approach. Indeed, as the explosion in electronic data and the economics of litigation, and pressure from the courts induce more attorneys and parties to conduct discovery in a cooperative manner, those who continue to pursue unduly combative approaches may find that their conduct increasingly stands out as inappropriate to both courts and other counsel, rendering such conduct increasingly counter-productive.

VI. CONCLUSION

If parties are expected to continue to manage discovery in the manner envisioned by the Federal Rules of Civil Procedure, cooperation will be necessary. Without such cooperation, discovery will become too expensive and time consuming for parties to effectively litigate their disputes.

Footnotes

a1 The *Case for Cooperation* was the subject of robust dialogue at two meetings of The Sedona Conference® Working Group on Electronic Document Retention and Production (WG1), and we thank all of the WG1 members who contributed to the dialogue vastly improving this paper. In addition, we wish to acknowledge editorial contributions from The Hon. Shira A. Scheindlin (SD

NY), Hon. James M. Rosenbaum (D MN), and Prof. Steve Gensler (U of OK School of Law). We also want to thank Jeannine Kenney, an associate who works with William Butterfield, for her research and assistance in preparing this paper. Finally, we wish to acknowledge our Working Group Series Sustaining and Annual Sponsors, whose generous support enables us to pursue our Working Group Series activities (see www.thesedonaconference.org/content/sponsorship for a listing of our WGS Sponsors).

1 *Krueger v. Pelican Products. Corp*., C/A No. 87-2385-A (W.D. Okla. 1989).

2 Judge Alley's opprobrium has been quoted in *Dahl v. City of Huntington Beach*, 84 F.3d 363, 364 (9th Cir. 1996), *Mancia v. Mayflower Textile Servs. Co*., 253 F.R.D. 354, 361 n.3 (D. Md. 2008) and *Network Computing Servs. v. Cisco Sys., Inc*., 223 F.R.D. 392, 395 (D.S.C. 2004). *See also* W. Bradley Wendel, *Rediscovering Discovery Ethics*, 79 MARQ. L. REV. 895, 895, 906 (1996) (noting courts are "imposing public duties upon lawyers in discovery that ... have content and carry severe sanctions for their violation" and noting that discovery conduct is provoking judicial backlash).

3 As discussed more fully *infra* Part II, the Federal Rules presume cooperation in discovery. *See, e.g*., Fed. R. Civ. P. 1, 1993 Advisory Committee Note (noting that Rule 1 imposes on attorneys a shared responsibility to ensure that civil litigation is resolved without undue cost or delay).

4 For example, Rule 26(f)(3) was amended to include in the 26(f) conference any issues relating to preservation, disclosure, or discovery of ESI and the form in which it should be produced. *See* Fed. R. Civ. P. 26 (f), 2006 Advisory Committee Note.

5 *See* Steven 5. Gensler, *A Bull's-Eye View of Cooperation in Discovery*, 10 Sedona Conf. Journal at 370-372 (2009 Supp.).

6 *See* John 5. Beckerman, *Confronting Civil Discovery's Fatal Flaws*, 84 MINN. L. REV. 505, 508 (2000) (noting the number of opinions in which courts have addressed discovery disputes has risen significantly compared with the prior decade).

7 *See* Final Report, Joint Project of the American College of Trial Lawyers Task Force on Discovery and The Institute for the Advancement of the American Legal System (2009), *available at* http://www.actl.com/AM/Template.cfm?Section=Advanced_Search&section=PR_2009&template=/ CM/ContentDisplay.cfm&ContentFileID=889.

8 *See* Wendel, *supra* note 2, at 906 n.41.

9 *See, e.g*., Gary E. Hood, *Refuse to Play the Game: An Alternative Document Production Strategy in Intellectual Property Litigation*, 16 INTELL. PROP. & TECH. L. J. 1+, 1-2 (2004) (discussing the routine nature of lengthy discovery disputes in intellectual property litigation).

10 For example, in *Mancia v. Mayflower Textile Servs. Co*., after several sets of interrogatory and document requests, four months of motions practice, and a court hearing on discovery violations, the court ordered parties to develop a discovery budget, determine whether additional discovery sought could be provided from less duplicative and expensive sources, attempt to reach agreement on additional discovery, including phased discovery, provide a status report to the court on any disputes, and if necessary return to the court for resolution. *See* 253 F.R.D. 354, 364-65 (D. Md. 2008). The outcome -- an order for cooperation and communication -- put the parties in nearly the same positions they would have been in had the disputes not ensued. *See id*.

11 *Id*. at 357 (noting Fed. R. Civ. P. 26 (g) requires counsel to certify that a discovery request, response, or objection is consistent with the rules of procedure, is not made to delay or increase the costs of litigation, is not unreasonably burdensome or expensive, and that violation is subject to sanction). The *Mancia* court noted that making boilerplate objections without identifying the specific basis for the objections is prima facie evidence of a Rule 26(g) violation and grounds for finding the objection waived. *Id*. at 358-59. *See also* Wendel, *supra* note 2, at 912-13 (discussing *Asea, Inc. v. S. Pac. Transp. Co*., 669 F.2d 1242, 1246 (9th Cir. 1981) in which the court upheld the sanction of finding a fact admitted when defendants submitted a boilerplate response to admission requests and found such responses abused discovery and were not consistent with the requirement of good faith).

[12] *See Kipperman v. Onex Corp.*, 2008 WL 4372005, at *8 (N.D. Ga. Sept. 19, 2008) (rejecting defendants objections that plaintiffs' requested e-mail search was burdensome where the court had previously offered defendants the opportunity to narrow the search terms).

[13] Fed. R. Civ. P. 26(f) (parties must discuss issues regarding preserving discoverable information). *See also id.* 37(e) (absent exceptional circumstances, sanctions may not be imposed for failing to provide ESI lost due to routine, *good faith*, operation of an ESI system) (emphasis added).

[14] Fed. R. Civ. P. 26 (b)(2)(B) provides that parties need not provide discovery of ESI that is not reasonably accessible due to undue burden or cost.

[15] *See In re Serequel Prods. Liab. Litig.*, 244 F.R.D. 650, 662 (M.D. Fla. 2007) (shielding technical staff from opposing party rather than cooperating by fostering consultation "is not an indicum of good faith").

[16] Fed. R. Civ. P. 34 (b)(2)(E) (party must produce ESI in the form in which it is ordinarily maintained).

[17] *William A. Gross Constr. Assets. v. Am. Mfrs. Mut. Ins. Co.*, 256 F.R.D. 134, 136 (S.D.N.Y. 2009). *Accord Residential Funding Corp. v. DeGeorge Fin. Corp.*, 306 F.3d 99, 112 (2d Cir. 2002) ("as a discovery deadline or trial date draws near, discovery conduct that might have been considered 'merely' discourteous at an earlier point in the litigation may well breach a party's duties to its opponent and to the court"); *In re Seroquel*, 244 F.R.D. at 662 (party was obligated to cooperate with opposing counsel to identify key word protocol rather than unilaterally selecting limited terms); *Bush Ranch v. Du Pont*, 918 F. Supp. 1524, 1543 (M.D. Ga. 1995) ("It is the obligation of counsel under the rules, as officers of the court, to cooperate with one another so that in pursuit of truth, the judicial system operates as intended."); *Marion v. State Farm Fire and Cas. Co.*, 2008 WL 723976, at *3-4 (S.D. Miss. Mar. 17, 2008) ("This Court demands the mutual cooperation of the parties. It hopes that some agreement can be reached ... this Court will [not] hesitate to impose sanctions on any one-party or counsel or both - who engages in any conduct that causes unnecessary delay or needless increase in the costs of litigation.").

[18] *See In re Seroquel*, 244 F.R.D. at 662.

[19] In a survey of 2,690 attorneys recently involved in federal litigation, more than 90% of respondents, representing both plaintiffs and defendants, "agreed" or "strongly agreed" with the statement, "[a]ttorneys can cooperate in discovery while still being zealous advocates for their clients." Emory G. Lee III & Thomas E. Willging, Federal Judicial Center National, Case-Based Civil Rules Survey, 62-63 (Federal Judicial Center October 2009), *available at* http://www.fjc.gov/library/fjc_catalog nsf/autoframepage! openform&url=/library/fjc_catalog nsf/DPublication! openform&parentunid=363B0DBDB772C35D85257648007A18B7. At least one commentator, Jason R. Baron, has argued that in circumstances where a party is certain that opposing counsel's proposed search protocol would not capture documents it knows would be responsive violates Rule 3.4 of the Model Rules of Professional Responsibility by failing to suggest or use additional search terms that would result in production; such conduct is tantamount to suppression. *See* Symposium, *Ethics and Professionalism in the Digital Age: Ninth Annual Georgia Symposium on Ethics and Professionalism*, 60 Mercer L. Rev. 863, 877 (2009).

[20] Model R. Prof'l Conduct Preamble Paragraph 2 (2006).

[21] *See Capital Records, Inc. v. MP3tunes, LLC*, 2009 WL 2568431, at *2 (S.D.N.Y. Aug. 13, 2009); *In re Direct Sw. Inc., Fair Labor Standards Act (FLSA) Litig.*, 2009 WL 2461716, at *1, 2 (E.D. La. Aug. 7, 2009); *Wells Fargo Bank. N.A. v. LaSalle Bank Nat'l Ass'n*, No. 3:07-cv-449, 2009 WL 2243854, at *2 (S.D. Ohio July 24, 2009); *Dunkin' Donuts Franchised Rests. LLC v. Grand Cen. Donuts, Inc.*, 2009 WL 1750348, at *4 (E.D.N.Y. June 19, 2009); *Ford Motor Co. v. Edgewood Props., Inc.*, 257 F.R.D. 418, 424-25, 427 (D.N.J. May 19, 2009); *Newman v. Borders, Inc.*, 257 F.R.D. 1, 3 (D.D.C. Apr. 6, 2009); *William A. Gross Const. Associates, Inc. v. American Mfrs. Mut. Ins. Co.*, 256 F.R.D. 134, 136 (S.D.N.Y. March 19, 2009); *S.E.C. v. Collins & Aikman Corp.*, 256 F.R.D. 403, 415 (S.D.N.Y. Jan. 13, 2009); *Covad Commc'ns. Co. v. Revonet. Inc.*, 254 F.R.D. 147, 148-49 (D.D.C.

Dec. 24 2008); *Gipson v. Sw. Bell Tel. Co.*, Civ. No. 08-2017, 2008 U.S. Dist. LEXIS 103822, at *4 (D. Kan. Dec. 23, 2008); *Aguilar v. Immigration and Customs Enforcement Div. of U.S. Dept. of Homeland Sec.*, 255 F.R.D. 350, 353-56, 358-59, 362 (S.D.N.Y. Nov. 21, 2008); *Mancia v. Mayflower Textile Servs. Co.*, 253 F.R.D. 354, 359, 363 (D. Md. 2008).; *Mancia v. Mayflower Textile Servs. Co.*, 253 F.R.D. 354, 363 (D. Md. 2008).

22 See discussion *infra* Parts II, III, and IV. *See also* Steven S. Gensler, *Some Thoughts on the Lawyer's E-volving Duties in Discovery*, 36 N. KY. L. REV. 521, 550 (2009).

23 *See* Gensler, *supra* note 22, at 552.

24 *Id*. at 556.

25 *See Moore's Federal Practice*, Paragraph 26.02 at 26-31 (3d. ed. 2008).

26 *See* George L. Paul & Jason R. Baron, *Information Inflation: Can the Legal System Adapt?*, 13 RICH. J.L. & TECH. 10, 28 (2007), *available at* http://law.richmond.edu/jolt/v13i3/article10.pdf.

27 *United States v. Procter & Gamble Co.*, 356 U.S. 677, 682 (1958).

28 *Hickman v. Taylor*, 329 U.S. 495, 501 (1947).

29 Fed. R. Civ. P. 26, 1946 Advisory Committee Note (emphasis added) (citing case law for the proposition that the Rules "permit 'fishing' for evidence as they should").

30 329 U.S. at 507.

31 *Id*. at 513.

32 *Id*. at 510.

33 *See id*. at 508 n.8.

34 *See* Fed. R. Civ. P. 34, 1970 Advisory Committee Note.

35 *Margel v. E.G.L. Gam Lab Ltd*., 2008 U.S. Dist. LEXIS 41754, at *10 (S.D.N.Y. May. 29 2008) (citing Charles A. Wright, Arthur R. Miller & Richard L. Marcus, *Federal Practice & Procedure* § 2288 at 655-56 (2d ed. 1994)).

36 Fed. R. Civ. P. 26, 1970 Advisory Committee Note.

37 Wayne Brazil, *The Adversary Character of Civil Discovery: A Critique and Proposals for Change*, 31 VAND. L. REV. 1295, 1296 (1978).

38 *Id*. at 1349.

39 Rule 26(f) was added to the Federal Rules in 1980 to provide parties with a means for judicial intervention when facing abusive discovery tactics. *See* Fed. R. Civ. P. 26(f), 1993 Advisory Committee Note. The Rule was initially designed as an elective procedure used only in special cases upon a party's request. *See id*. In 1993, the Rule was amended to require all parties to meet as soon as practicable and formulate a discovery plan for submission to the court. *See id*. A 2006 amendment explicitly required the Rule 26(f) conference to include discussion regarding discovery of ESI and assertion of privileges in cases where those topics apply. *See id*., 2006 Advisory Committee Note.

40 Fed. R. Civ. P. 26 (f)(2).

41 *See id*., 1993 Advisory Committee Note.

42 *Id*., 1980 Advisory Committee Note.

43 *See id*.

44 *Id*. 1983 Advisory Committee Note (citations and quotations omitted).

45 *Id*. 37(f).

46 *Id*. 26(b), 1983 Advisory Committee Note.

47 *Id*. (emphasis added).

48 *Id*.

49 *Id*. 26(g), 1983 Advisory Committee Note.

50 *Id*.

51 *See id*. 26(f), 1993 Advisory Committee Note.

52 *Id*.

53 *Id*.

54 *Id*.

55 *See id*. 26(a)(1), (b)(1), 2000 Advisory Committee Note.

56 *Id*. 26(b)(1) (emphasis added).

57 *See id*. 26(f), 2006 Advisory Committee Note.

58 *See, e.g*., Beckerman, *supra* note 6, at 513 (arguing that "civil discovery suffers from conceptual inconsistencies and structural flaws" requiring far-reaching changes to the rules).

59 In a companion paper discussing how the Federal Rules address cooperation, Professor Steven Gensler organizes the Rules into clusters. *See* Gensler, *supra* note 5, at 366-368. First, he notes that several provisions of the Rules impose duties on parties to communicate and give consideration to positions held by opposing parties as they engage in discovery planning. *See id*. (citing Fed. R. Civ. P. 26(f)(1), 26(f)(2), 26(f)(3) and 37(f)). Next, Professor Gensler concludes that a second cluster of rules require communication and good faith conduct by parties after discovery disputes arise. *See id*. (citing Fed. R. Civ. P. 26(c), 37(a)(1), 26(c)(3) and 37(a)(5). Finally, Professor Gensler recognizes a third cluster of rules that demand good faith regarding the content and purpose of discovery requests and responses. *See id*. (citing Fed. R. Civ. P. 26(g)(1), 26(g)(1(B)(i), 26(g)(1)(B)(ii) and 26(g)(1)(B)(iii)).

60 Fed. R. Civ. P. 1.

61 *Id*., 1993 Advisory Committee Note.

62 *See id*. 26(a)(1)(A)(ii).

63 *See id*. 26(f).

64 *See id*. 26(f)(3)(c).

65 *Id*. 26(g)(1)(B).

66 253 F.R.D. 354, 357-58 (D. Md. 2008).

67 Fed. R. Civ. P. 26 (g), 1983 Advisory Committee Note.

68 *Id*. 26(g)(3).

69 28 U.S.C. § 1927 (2000).

70 *See* H. CONF. REP. NO. 96-1234 (1980), as reprinted in 1980 U.S.C.C.A.N. 2781, 2782.

71 While professional conduct is governed by state-adopted ethical rules, the discussion in this section necessarily focuses on Model Rules. The Model Rules, and much of their commentary, however, have been adopted, in large part, by nearly every state. *See* Model Rules of Professional Conduct, Dates of Adoption, Am. Bar Ass'n, *available at* http://www.abanet.org/cpr/mrpc/alpha_ states html; State Adoption of Comments To Model Rules of Professional Conduct as of February 2009, Am. Bar Ass'n, *available at* http:// www.abanet.org/cpr/jclr/comments.pdf. In addition to state conduct rules, other relevant state-issued guidelines, apart from ethical rules, may apply. *See, e.g*., California Attorney Guidelines of Civility and Professionalism, Sec. 9, *available at*

www.calbar.ca.gov/calbar/pdfs/reports/Atty-Civility-Guide.pdf; The Texas Lawyer's Creed, Sec. 3, Paragraphs 14-19, *available at* http:// www.texasbar.com/Content/ContentGroups/Bar_Groups/Foundations1/Texas_Bar_ Foundation/TX_Lawyers_Creed htm.

72 *See* Model R. Prof'l Conduct Preamble Paragraph 2 ("As advocate, a lawyer zealously asserts the client's position under the rules of the adversary system."); *Id*. 1.3 cmt. 1 (The obligation to serve a client diligently requires the attorney to "act with commitment and dedication to the interests of the client and with zeal in advocacy upon the client's behalf").

73 See Sylvia Stevens, *Whither Zeal? Defining "Zealous Representation,"* Oregon State Bar Bulletin, July 2005, *available at* http:// www.osbar.org/publications/bulletin/05jul/barcounsel.html; Allen K. Harris, *Zealous Advocacy: Duty or Dicta: Have the 'Z' Words Become a Disservice to Lawyers?*, OKLAHOMA BAR JOURNAL, *available at* http://www.okbat.org/obj/atticles_ 03/121303harris htm. Both commentators note that when the ABA Model Rules replaced the Code of Professional Responsibility, the term "zeal" was not included in Rule 1.3. While the word "zeal" remains in the Preamble and Comment to Rule 1.3, the duty imposed by the Rule is "reasonable diligence and promptness." Model R. Prof'l Conduct, 1.3. This conclusion is consistent with the Restatement (Third) of the Law Governing Lawyers, which notes that a lawyer's obligation to act "zealously" on behalf of the client is not unlimited: "The Preamble to the ABA Model Rules of Professional Conduct (1983) and EC 7-1 of the ABA Model Code of Professional Responsibility (1969) refer to a lawyer's duty to act 'zealously' for a client. The term sets forth a traditional aspiration, but it should not be misunderstood to suggest that lawyers are legally required to function with a certain emotion or style of litigating, negotiating, or counseling. For legal purposes, the term encompasses the duties of competence and diligence." *See* RESTATEMENT (THIRD) OF THE LAW GOVERNING LAWYERS Section 16 cmt. d.

74 Commentary to Model Rule 1.3 confines the obligation to act with zeal to "whatever lawful and ethical measures are required to vindicate a client's cause." Model R. Prof'l Conduct 1.3, cmt. 1.

75 *Mancia v. Mayflower Textile Servs. Co.*, 253 F.R.D. 354, 362-63 (D. Md. 2008).

76 *See* Model R. Prof'l Conduct Preamble Paragraph 1 (lawyer is both representative of clients and officer of the court); *id*. Paragraph 5 ("A lawyer's conduct should conform to the requirements of the law, both in professional service to clients and in the lawyer's business and personal affairs. A lawyer should use the law's procedures only for legitimate purposes and not to harass or intimidate others .... While it is a lawyer's duty, when necessary, to challenge the rectitude of official action, it is also a lawyer's duty to uphold legal process.").

77 *Id*. Paragraph 2.

78 *See id*. Paragraph 4 ("lawyer should keep in confidence information relating to representation of a client except so far as disclosure is required or permitted by the Rules of Professional Conduct or other law"); *id*. Paragraph 9 (lawyer has an "obligation zealously to protect and pursue a client's legitimate interests, within the bounds of the law, while maintaining a professional, courteous and civil attitude toward all persons involved in the legal system.").

79 *See* Wendel, *supra* note 2, at 895.

80 *See* Model R. Prof'l Conduct 4.3, cmt. 1.

81 *See id*. 3.3(a), cmt. 11 (noting that the truth-seeking judicial process takes precedence over the client's interest in such cases).

82 *See id*. 3.3(c).

83 *See id*. 1.16(a)(1).

84 For an actual conflict to exist between rules regarding zealous advocacy and duties to the court, it must be impossible for an attorney to comply with both obligations. However, the MRPC, by making clear which rules are mandatory and which are aspirational, establishes that some duties will take precedence over others.

85 *See In re Seroquel Prods. Liab. Litig.*, 244 F.R.D. 650, 665 (M.D. Fla. 2007) (failure to produce usable and reasonably accessible documents resulting from failure to cooperate was sanctionable conduct).

86 *See* Model R. Prof'l Conduct 3.1, 3.4(d).

87 *See id*. 3.3.

88 *See id*. 3.2, cmt. 1 ("The question is whether a competent lawyer acting in good faith would regard the course of action as having some substantial purpose other than delay.").

89 *See id*. 3.4(c) (an attorney may not "knowingly disobey an obligation under the rules of a tribunal except for an open refusal based on an assertion that no valid obligation exists"); *id*. Preamble Paragraph 5 ("lawyer's conduct should conform to the requirements of the law"); *see also* Wendel, *supra* note 2, at 919 (Rules 3.4 (c) and 3.4(d) require attorneys to make good faith efforts to abide by civil discovery rules).

90 *See* Fed. R. Civ. P. 1, 1993 Advisory Committee Note.

91 Model R. Prof'l Conduct 3.2 (emphasis added).

92 Commentary to Rule 3.2 recognizes that the benefits of "improper delay" -- one without a "substantial purpose other than delay" or for the "purpose of "frustrating an opposing party's attempt to obtain rightful redress or repose" -- are "not a legitimate interest of the client". Model R. Prof'l Conduct 3.2 cmt. 1.

93 *See Qualcomm Inc. v. Broadcomm Corp.*, 539 F. Supp. 2d 1214 (S.D. Cal. 2007). In a patent infringement action, the defendant alleged that the plaintiff had intentionally hidden the existence of certain patents from an international standard-setting consortium until the consortium had set standards and, to comply with those standards, the industry had developed products that necessarily infringed on the plaintiff's patents. The court found for the defendants on the merits and following trial entered an order detailing the plaintiff's actions to obstruct discovery and instructing plaintiff's counsel to show cause why they should not be sanctioned and face professional discipline. The court characterized plaintiff's counsel's actions as "gross litigation misconduct," the court detailed "constant stonewalling, concealment, and repeated misrepresentations," including the withholding of over 200,000 pages of relevant emails and electronic documents.

94 *Ethics and Professionalism in the Digital Age: Ninth Annual Georgia Symposium on Ethics and Professionalism*, *supra* note 19, at 874.

95 *See id*. at 875-877 (discussing *Kipperman*, *supra* note 12*)*.

96 *Mancia v. Mayflower Textile Servs. Co.*, 253 F.R.D. 354, 357-58 (D. Md. 2008).

97 *See id*. at 358 (noting that although overbroad discovery requests are served in part because parties do not have enough information to narrowly tailor them, that difficulty is avoided by cooperating prior to serving the request).

98 *See* Beckerman, *supra* note 6, at 526.

99 *See* Wendel, *supra* note 2, at 914-18 (discussing *Wash. State Physicians Ins. Exch. & Ass'n v. Fisons Corp.*, 858 P.2d 1054 (Wash. 1993)). In *Washington State Physicians*, defendant objected to plaintiff's request for documents for any drug other than the specific product at issue in the litigation where defendant knew documents relating to other drugs contained information about the toxicity of the active ingredient in the product in suit. The court rejected defendant's argument that its ethical duties to the client required it to both construe discovery requests narrowly and avoid turning over damaging documents, concluding that defendant's objections "did not comply with either the spirit or the letter of the discovery rules and thus were signed in violation of the certification requirement." 858 P.2d at 1083.

100 *See Ethics and Professionalism in the Digital Age: Ninth Annual Georgia Symposium on Ethics and Professionalism*, *supra* note 19, at 874-877.

101 *Marion v. State Farm Fire and Cas. Co.*, 2008 WL 723976, at *3-4 (S.D. Miss. Mar. 17, 2008) (internal quotations omitted). *See also In re Seroquel*, 244 F.R.D. 650, 660 (M.D. Fla. 2007).

102 *Mancia*, 253 F.R.D. at 361-62 (citing the *Cooperation Proclamation*).

103 244 F.R.D. at 660.

104 *Board of Regents of the Univ. of Nebraska v. BASF Corp*, 2007 WL 3342423, at *5 (D. Neb. Nov. 5, 2007).

105 *See Mancia*, 253 F.R.D. at 364-65. *See also CBT Flint Partners, LLC v. Return Path. Inc.*, 2008 WL 4441920, at *3 (N.D. Ga. Aug. 7, 2008); *Mikron Indus., Inc. v. Hurd Windows & Doors*, 2008 WL 1805727, at *1 (W.D. Wash. Apr. 21, 2008).

106 *See Mancia*, 253 F.R.D. at 358; *Marion*, 2008 WL 723976, at *2, *4.

107 *See Mancia*, 253 F.R.D. at 358-59, 364.

108 *See CBT Flint Partners*, 2008 WL 4441920, at *2-3.

109 *See Keithley v. The Home Store.com, Inc.*, 2008 WL 3833384, at *8, *12, *14-15 (N.D. Cal. Aug. 12, 2008).

110 *See SEC v. Collins & Aikman Corp.*, 256 F.R.D. at 414, 418 (S.D.N.Y. 2009) (citing the *Cooperation Proclamation*). *See also In re Seroquel Prods. Liab. Litig.*, 244 F.R.D. 650, 662, 664 (M.D. Fla. 2007).

111 *See Keithley*, 2008 WL 3833384, at *1, 10, 13, 15-16.

112 *See Ideal Aerosmith v. Acutronic USA, Inc.*, 2008 WL 4693374, at *2-3 (W.D. Pa. Oct. 23, 2008).

113 *See Victor Stanley, Inc. v. Creative Pipe, Inc.*, 250 F.R.D. 251, 260 n.10 (D. Md. 2008).

114 *Gross Constr. Assocs. v. Am. Mfers. Mut. Ins. Co.*, 256 F.R.D. 134, 136 (S.D.N.Y. 2009) (citing the *Cooperation Proclamation*).

115 *Gipson v. Sw. Bell Tel. Co.*, 2009 WL 790203, at *21 (D. Kan. Mar. 24, 2009) (citing Rule 26(g) and *Mancia v. Mayflower Textile Servs. Co.*, 253 F.R.D. 354, 359 (D. Md. 2008)).

116 *Id*.

117 *See, e.g.*, *Dunkin' Donuts Franchised Rests. LLC v. Grand Cent. Donuts, Inc.*, 2009 WL 1750348, at *4 (E.D.N.Y. June 19, 2009) (citing the *Cooperation Proclamation*).

118 *See, e.g.*, *Marion v. State Farm Fire and Cas. Co.*, 2008 WL 723976, at *4 (S.D. Miss. Mar. 17, 2008).

119 *See Newman v. Borders, Inc.*, 257 F.R.D. 1, 3 n.3 (D.D.C. 2009) (noting "the perceptible trend in the case law that insists that counsel genuinely attempt to resolve discovery disputes" and citing the *Cooperation Proclamation*).

120 David M. Trubek, et al., *The Costs of Ordinary Litigation*, 31 UCLA L. REV. 72, 89-90 (Oct. 1983).

121 Robert Douglas Brownstone, *Collaborative Navigation of the Stormy E-Discovery Seas*, 10 RICH. J.L. & TECH. 53, at *21 (2004).

122 James N. Dertouzos, Nicholas M. Pace & Robert H. Anderson, *The Legal and Economic Implications of Electronic Discovery: Options for Future Research*, RAND Institute for Civil Justice, 2008, at ix, *available at* http://rand.org/pubs/occasional_papers/2008/RAND_OP183.pdf (hereinafter "Dertouzos, et al.").

123 *See, e.g.*, Trubek, *supra* note 120, at 91.

124 *See* Mike Dolan & John Thickett, *Unbundling and Offshoring*, 71 TEX. B. J. 730, 730 (Oct. 2008).

125 *Hopson v. City of Baltimore*, 232 F.R.D. 228, 244 (D. Md. 2005).

126 *See* Dertouzos, et al., *supra* note 122, at 1 (citing School of Information, University of California at Berkeley, *How Much Information?* (2003)).

127 Daniel Hodgman, *A Port in the Storm?: The Problematic and Shallow Safe Harbor for Electronic Discovery*, 101 NW. U. L. REV. 259, 276 (2007) (citing David Narkiewicz, *Electronic Discovery and Evidence*, 25 PENNSYLVANIA LAWYER 57 (2003)).

128 *See* Brownstone, *supra* note 121, at 53.

129 Hon. Shira A. Scheindlin & Jeffrey Rabkin, *Electronic Discovery in Federal Civil Litigation: Is Rule 34 Up to the Task?*, 41 B.C. L. REV. 327, 349 (2000).

130 *See, e.g.*, *United States v. Crim. Triumph Capital Group, Inc.*, 211 F.R.D. 31, 46 n.8 (D. Conn. 2002) ("When a user deletes a file, the data in the file is not erased, but remains intact ... where it was stored until the operating system places other data over it.").

131 *See* Hodgman, *supra* note 127, at 275 (citing THE SEDONA PRINCIPLES: BEST PRACTICES RECOMMENDATIONS & PRINCIPLES FOR ADDRESSING ELECTRONIC DOCUMENT PRODUCTION (2007)).

132 "Courts generally have ordered the production of metadata when it is sought in the initial document request and the producing party has not yet produced the documents in any form." *Aguilar v. Immigration and Customs Enforcement Div. of the U.S. Dept. of Homeland Sec.*, 255 F.R.D. 350, 357 (S.D.N.Y. 2008); *In re Priceline.com Inc. Sec. Litig.*, 233 F.R.D. 88, 91 (D. Conn. 2005) (production ordered in TIFF format with corresponding searchable metadata databases); *Williams v. Sprint/United Mgmt. Co.*, 230 F.R.D. 640, 654 (D. Kan. 2005) (ordering production of Excel spreadsheets with metadata even though no request had been made initially because producing party should reasonably have known that metadata was relevant). *But see Wyeth v. Impax Lab., Inc.*, 248 F.R.D. 169, 171 (D. Del. 2006) ("reviewing [metadata] can waste litigation resources"); *Williarms*, 230 F.R.D. at 651 ("Emerging standards of electronic discovery appear to articulate a general presumption against the production of metadata"); *Michigan First Credit Union v. Cumis Ins. Soc., Inc.*, 2007 WL 4098213 (E.D. Mich. Nov. 16, 2007) (declining to require production of documents in native format due to burden concerns).

133 *See, e.g.*, *Wells v. Xpedx*, 2007 WL 1200955 (M.D. Fla. Apr. 23, 2007) (producing party has duty to search hard drives, servers, and backup tapes for responsive deleted emails and files); *Zubulake v. UBS Warburg LLC*, 217 F.R.D. 309 (S.D.N.Y. 2003) (requiring recovery and production of all deleted emails relevant to discrimination and retaliation claims); *Renda Marine, Inc. v. United States*, 58 Fed. Cl. 57 (2003) (requiring production of backup tapes after finding that numerous relevant emails were deleted); *Samide v. Roman Catholic Diocese of Brooklyn*, 5 A.D.3d 463 (N.Y. App. Div. 2d Dep't 2004) (requiring recovery and production of all relevant deleted emails). *See also* Thomas Y. Allman, et al., *Preservation, Management and Identification of Sources of Information that are Not Reasonably Accessible*, The Sedona Conference Working Group on Electronic Document Retaliation & Production (2008) *available at* http://www.thesedonaconference.org. *But see Scotts Co. LLC v. Liberty Mut. Ins. Co.*, 2007 WL 1723509 (S.D. Ohio June 12, 2007) (upon objection, requesting party may have to establish that requested deleted information is both relevant and retrievable); *Oxford House, Inc. v. City of Topeka*, 2007 WL 1246200 (D. Kan. Apr. 27, 2007) (deleted files not required to be produced due to undue burden).

134 *See* Dertouzos, et al., *supra* note 122, at 2; THE SEDONA PRINCIPLES: BEST PRACTICES RECOMMENDATIONS & PRINCIPLES FOR ADDRESSING ELECTRONIC DOCUMENT PRODUCTION (2007).

135 *See Covad Commc'ns Co. v. Revonet, Inc.*, 258 F.R.D. 5, 16 (D.D.C. 2009) ("[T]he universe of items to be considered for production is ever expanding with the ubiquity of e-mail and other forms of electronic communication, such as instant messaging and the recording of voice messages. Electronic data is difficult to destroy and storage capacity is increasing exponentially, leading to an unfortunate tendency to keep ESI even when any need for it has long since disappeared. This phenomenon - the antithesis of a sound records management policy - leads to ever increasing expenses in finding the data and reviewing it for relevance or privilege.").

136 *See, e.g.*, *Coleman (Parent) Holdings, Inc. v. Morgan Stanley & Co.*, 2005 WL 674885, at *1 (Fla. Cir. Ct. Mar. 23, 2005) (failure to use good faith in production and preservation of e-mails exposed company to liability for spoliation); *In re Telxon Corp. Sec. Litig.*, 2004 WL 3192729, at *23 (N.D. Ohio July 16, 2004) (sanctions imposed for bad faith modification of electronic records, loss of electronic files, and failure to produce relevant e-mails).

137 *See* Gensler, *supra* n. 22, at 581.

138 *See* Richard Van Duizend. *Guidelines for State Trial Courts Regarding Discovery of Electronically-Stored Information*, Conference of Chief Justices, at vi (2006) *available at* http:// www ncsconline.org/images/EDiscCCJGuidelinesFinal.pdf.

139 *See* Dertouzos, et al., *supra* note 122, at 3. *See also Covad Commc'ns*, 258 F.R.D. at 14 ("Experience shows" that review for relevance and privilege "may dwarf the cost of the search").

140 *See, e.g.*, *Oxford House, Inc. v. City of Topeka*, 2007 WL 1246200, at *4 (D. Kan. Apr. 27, 2007) (production of deleted files estimated to cost more than $100,000); *Ex parte Cooper Tire & Rubber Co.*, 987 So. 2d 1090, 1104 (Ala. 2007) (acknowledging producing party's evidence that discovery burden would "entail thousands of hours and will cost hundreds of thousands of

dollars").

141 *See* Dertouzos, et al., *supra* note 122, at ix.

142 *Id*. at 3 (noting, however, a lack of empirical research on "[t]he extent to which costs have increased"). *See also id*. at 13 ("[S]everal interviewees claimed that the significant burdens of e-discovery outweighed the benefits of going to trial, especially in low-stakes cases.").

143 Brownstone, *supra* note 121, at 53.

144 Dertouzos, et al., *supra* note 122, at ix.

145 *See id*. at 15.

146 *See* discussion *supra* at Parts II and III.

147 *See* Model. R. Prof. Conduct 1.2 ("a lawyer shall abide by a client's decisions concerning the objectives of representation and, as required by Rule 1.4, shall consult with the client as to the means by which they are to be pursued").

148 For example, abiding by the client's decisions does not extend to counseling or assisting in criminal or fraudulent conduct, asserting frivolous positions, making false statements or presenting false evidence to a court or other tribunal, or unlawfully obstructing access to evidence or concealing or destroying evidence. *See id*. 2.1(d), 3.1, 3.3, 3.4.

149 The Federal Rules of Civil Procedure and analogous state rules define the substantive duties with which attorneys must comply. For example, Rule 26(a) mandates that the parties make certain initial disclosures; Rule 26(b) limits the scope of permitted discovery; and Rule 26(f) requires meeting for the exchange of initial information.

150 *See* Van Duizend, *supra* note 138.

151 *See id*.

152 California Attorney Guidelines, *supra* note 71, at 3 (emphasis added).

153 *See, e.g., Kipperman*, *supra* note 12, at *8 (defendant's failure to cooperate as to search terms led to rejection of argument that plaintiff's requested search was overbroad).

154 *Covad Commo'ns. Co. v. Revonet. Inc*., 254 F.R.D. 5, 14 (D.D.C. 2009) (citing the *Cooperation Proclamation*). *Accord Wells Fargo Bank v. LaSalle Bank Nat'l Ass'n*, 2009 WL 2243854, at *2-3 (S.D. Ohio July 24, 2009) (refusing to require defendant to restore and search back-up tapes after close of discovery where the parties could have avoided the dispute "by conferring appropriately early in the case about ESI," citing the *Cooperation Proclamation*, describing parties' conduct as filing "one paragraph boilerplate statements about ESI" in the Rule 26(f) report and "waiting for the explosion later" rather than "deal[ing] systematically with ESI problems at the outset of the litigation").

155 *See* Robert Axelrod, THE EVOLUTION OF COOPERATION, at 7-10, 125 (Rev. Ed., Perseus Books Group 2006); Ronald J. Gilson & Robert H. Mnookin, *Disputing Through Agents: Cooperation and Conflict Between Lawyers in Litigation*, 94 COLUM.

L. REV. 509, 514-15 (1994).

156 *See* Axelrod, *id*. at 12, 20-21, 125; *see also* G. Paul & J. Baron, *supra* note 26, at 56 note. 134.

157 *See* Axelrod, *id*. at 131-32.

158 *See id*. at 11-12.

159 *See* Gilson & Mnookin, *supra* note 155, at 564 (counsel's concern about reputation may facilitate cooperative solutions).

THE SEDONA CONFERENCE® WORKING GROUP SERIES

WGS℠

THE SEDONA PRINCIPLES:
SECOND EDITION
Best Practices Recommendations & Principles for Addressing Electronic Document Production

A Project of The Sedona Conference®
Working Group on Electronic Document
Retention & Production (WG1)

JUNE 2007

The Sedona Conference®

The Sedona Principles
(Second Edition)
Addressing Electronic Document Production

Editor in Chief: Jonathan M. Redgrave

Executive Editors:
Richard G. Braman
Kenneth J. Withers

Senior Editors:
Thomas Y. Allman
Conor R. Crowley
Ted S. Hiser

Technology Advisor: John H. Jessen

REPRINT REQUESTS:
Requests for reprints or reprint information should be directed to
Richard Braman, Executive Director of The Sedona Conference,
at tsc@sedona.net or 1-866-860-6600.

The editors wish to thank Jessica Buffenstein and David Degnan
for their tireless efforts cite-checking and proofreading.

Foreword

Welcome to the Second Edition of *The Sedona Principles: Best Practices Recommendations and Principles for Addressing Electronic Document Production*, a project of The Sedona Conference® Working Group on Best Practices for Electronic Document Retention and Production (WG1). The Sedona Conference® Working Group Series℠ is designed to bring together some of the nation's finest lawyers, consultants, academics and jurists to address current problems in the areas of antitrust law, complex litigation and intellectual property rights that are either ripe for solution or in need of a "boost" to advance law and policy. (See Appendix D for further information about The Sedona Conference® in general, and the WGS℠ in particular).

Since the first publication of *The Sedona Principles* in January 2004, the *2004 Annotated Version of The Sedona Principles* in the Spring of 2004, and the July 2005 version of *The Sedona Principles,* there have been many developments in the case law as well as significant amendments to the Federal Rules of Civil Procedure and several state civil procedure rules. The Principles, however, have maintained their vitality.

The Second Edition includes updates throughout the Principles and Comments reflecting the new language found in the amended Federal Rules and advances in both jurisprudence and technology. The Introduction has been expanded to include a comparison of *The Sedona Principles* with the amended Federal Rules. Particular attention has been given to updating the language and commentary on Principle 12 (metadata) and Principle 14 (the imposition of sanctions).

The Second Edition has also been rearranged for ease of reference. The 14 Principles themselves are found in the front of this publication, together with a chart cross-referencing each Principle to corresponding sections of the amended Federal Rules of Civil Procedure. In the body of this publication, each rule is followed by one or more Comments, most of which include a "Resources and Authorities" section pointing the reader to selected leading case law, exemplar court rules, and leading legal scholarship for further study.

This version also includes other clerical, minor stylistic, and grammatical edits, as well as updates of the appendices. Since The Sedona Conference® has now published *The Sedona Conference Glossary: E-Discovery and Digital Information Management,* we have eliminated the separate glossary that previously appeared as Appendix A to *The Sedona Principles.*

I want to thank the entire Working Group for all their hard work and contributions, and especially the Editorial Committee and Steering Committee for leading this effort to arrive at the new milestone of a Second Edition! Finally, but certainly not least, the Working Groups of The Sedona Conference could not accomplish their goals without the financial support of the sustaining and annual sponsors of the Working Group Series listed at www.thesedonaconference.org/sponsorship.

Richard G. Braman
Executive Director
The Sedona Conference®
June 2007

The Sedona Principles for Electronic Document Production
Second Edition

1. Electronically stored information is potentially discoverable under Fed. R. Civ. P. 34 or its state equivalents. Organizations must properly preserve electronically stored information that can reasonably be anticipated to be relevant to litigation.

2. When balancing the cost, burden, and need for electronically stored information, courts and parties should apply the proportionality standard embodied in Fed. R. Civ. P. 26(b)(2)(C) and its state equivalents, which require consideration of the technological feasibility and realistic costs of preserving, retrieving, reviewing, and producing electronically stored information, as well as the nature of the litigation and the amount in controversy.

3. Parties should confer early in discovery regarding the preservation and production of electronically stored information when these matters are at issue in the litigation and seek to agree on the scope of each party's rights and responsibilities.

4. Discovery requests for electronically stored information should be as clear as possible, while responses and objections to discovery should disclose the scope and limits of the production.

5. The obligation to preserve electronically stored information requires reasonable and good faith efforts to retain information that may be relevant to pending or threatened litigation. However, it is unreasonable to expect parties to take every conceivable step to preserve all potentially relevant electronically stored information.

6. Responding parties are best situated to evaluate the procedures, methodologies, and technologies appropriate for preserving and producing their own electronically stored information.

7. The requesting party has the burden on a motion to compel to show that the responding party's steps to preserve and produce relevant electronically stored information were inadequate.

8. The primary source of electronically stored information for production should be active data and information. Resort to disaster recovery backup tapes and other sources of electronically stored information that are not reasonably accessible requires the requesting party to demonstrate need and relevance that outweigh the costs and burdens of retrieving and processing the electronically stored information from such sources, including the disruption of business and information management activities.

9. Absent a showing of special need and relevance, a responding party should not be required to preserve, review, or produce deleted, shadowed, fragmented, or residual electronically stored information.

10. A responding party should follow reasonable procedures to protect privileges and objections in connection with the production of electronically stored information.

11. A responding party may satisfy its good faith obligation to preserve and produce relevant electronically stored information by using electronic tools and processes, such as data sampling, searching, or the use of selection criteria, to identify data reasonably likely to contain relevant information.

12. Absent party agreement or court order specifying the form or forms of production, production should be made in the form or forms in which the information is ordinarily maintained or in a reasonably usable form, taking into account the need to produce reasonably accessible metadata that will enable the receiving party to have the same ability to access, search, and display the information as the producing party where appropriate or necessary in light of the nature of the information and the needs of the case.

13. Absent a specific objection, party agreement or court order, the reasonable costs of retrieving and reviewing electronically stored information should be borne by the responding party, unless the information sought is not reasonably available to the responding party in the ordinary course of business. If the information sought is not reasonably available to the responding party in the ordinary course of business, then, absent special circumstances, the costs of retrieving and reviewing such electronic information may be shared by or shifted to the requesting party.

14. Sanctions, including spoliation findings, should be considered by the court only if it finds that there was a clear duty to preserve, a culpable failure to preserve and produce relevant electronically stored information, and a reasonable probability that the loss of the evidence has materially prejudiced the adverse party.

The Sedona Principles & the Federal Rules

Topic of Discussion	Sedona Principle	Federal Rule(s) (amended 2006)	Relevant Sedona Comment(s)
Discovery Scope	Principles 1, 2, 5, 6, 8, 9, 11	Rule 34(a)	Comments 1a, 2a, 2b, 2c, 3a, 5a, 6c, 8a, 9a, 9b, 11a, 11b
Preservation Obligations	Principles 1, 3, 5, 6, 8, 9, 12	n.a.	Comments 1c, 2c, 3a, 3d, 5a, 5b, 5c, 5d, 5e, 5g, 5h, 5i, 6a, 6b, 6d, 6e, 6f, 8c, 9b, 12a, 12b, 14a
Form of Preservation	Principle 12	n.a.	Comments 12a, 12b
Metadata	Principle 12	n.a.	Comments 6f, 12a, 12b, 12c, 12d
Form of Production	Principles 4, 12	Rule 34(b)	Comments 3b, 4a, 12a, 12b, 12d
Meet and Confer	Principle 3	Rule 26(f)	Comments 1d, 2e, 3a, 3b, 3c, 3d, 4a, 4c, 5a, 7a, 9a, 10a, 12c
Initial Disclosure	Principle 3	Rule 26(a)(1)	Comment 3d
Preservation Orders	Principle 5	n.a.	Comment 5f
Discovery Requests	Principle 4	Rule 34(a)	Comment 3b, 4a, 4b
Tiered Production	Principle 8	Rule 26(b)(2)(B)	Comments 2c, 8a, 8b, 9a
Cost-Shifting	Principle 13	Rule 26(b)(2)(B)	Comments 2c, 13a, 13b, 13c
Proportionality Limits	Principle 2	Rule 26(b)(2)(C) (was Rule 26(b)(2)(b)	Comments 2a, 2b, 13b
ID of Unsearched Sources	Principle 4	Rule 26(b)(2)(B)	Comments 2c, 3a, 4b, 8b
Inadvertent Privilege Production	Principle 10	Rule 26(b)(2)(5)	Comments 10a, 10d
Spoliation Sanctions	Principle 14	n.a.	Comments 14a, 14b, 14c, 14d 14e, 14f
Safe Harbor	Principle 14	Rule 37(f)	Comments 14b, 14d, 14f
Nonparty Discovery	Principle 13	Rule 45	Comments 7b, 13c

Preface

On December 1, 2006, new rules took effect in federal courts governing the discovery of "electronically stored information" in civil litigation. The adoption of these rules represented a watershed in a process begun several years before, a process in which *The Sedona Principles* played a pivotal role. As judges and practitioners are being introduced to these new rules across the country, questions naturally arise as to the continued role of *The Sedona Principles* in e-discovery. Do the Federal Rules of Civil Procedure supplant *The Sedona Principles* as the primary source of guidance for judges, counsel, and clients facing electronic discovery? As important as the Federal Rules of Civil Procedure are, we believe the answer to that question is "no." The rules do not answer many of the most vexing questions judges and litigants face. They do not govern a litigant's conduct before suit is filed, nor do they provide substantive rules of law in such important areas as the duty of preservation or the waiver of attorney-client privilege. While the amended rules and the accompanying Committee Notes will be very influential references, they do not govern procedure in state court or in alternative dispute resolution forums. Far from supplanting *The Sedona Principles*, the new Federal Rules have highlighted the many areas of electronic discovery in which there is continued and growing need for guidance.

We have come a long way in five years. In the Spring of 2002, many of us who would later form the Sedona Conference® Working Group on Electronic Document Production began discussing ways to develop "best practices" for lawyers to follow in addressing electronic information in litigation and investigations. Litigants, particularly entities that generated large volumes of electronic information, did not know what obligations might apply to the preservation and production of electronic information. Clearly, the world was changing, and both the costs of discovery and risks of claims of evidence spoliation or discovery abuse threatened to rise. A cottage industry of electronic discovery consultants and continuing legal education providers was beginning to develop. Courts handled e-discovery disputes, but few decisions were reported and yet fewer provided meaningful guidance outside the context of particular facts. It seemed doubtful to us that the normal development of case law would yield, in a timely manner, the best practices for organizations to follow in producing electronic information.

In October 2002, The Sedona Conference® Working Group on Electronic Document Retention and Production, a group of attorneys and others experienced in electronic discovery matters, met to address the production of electronic information in discovery. The group was concerned about whether rules and concepts developed largely for paper discovery would be adequate to address issues of electronic discovery. After vigorous debate, a set of core principles emerged for addressing the production of electronic information. These principles became known as *The Sedona Principles*.

The initial draft was published in March of 2003 and widely disseminated by members of the Working Group and through the Internet and other channels. Between March and November of 2003, participants in the Working Group presented the draft *Sedona Principles* as part of more than twenty presentations to the bench and bar across the country. At these presentations, and in informal meetings and communications, participants solicited commentary and edits that could assist in revising the initial draft. Working Group participants also sought views from across the spectrum of the bar and consultants who are involved in this area.

The Working Group met again in October of 2003 to discuss and evaluate comments and possible revisions and to seek further input from Working Group members. The document was finalized in January 2004 and reflected the considered review of the initial draft and changes that were believed to enhance the document as a guide to courts, parties and counsel. A first "Annotated Version" was published in June 2004, the purpose being to show how the decisions of courts dovetailed or varied with *The Sedona Principles*. A 2005 Annotated Version was published in July 2005. By then, the case law on electronic discovery was burgeoning, as the references demonstrated. We now find that *The Sedona Principles* are at the center of a major evolution in how both federal and state courts treat electronic discovery, as is detailed in the Introduction. Accordingly, the commentary in this edition has been revised to include citations to other best practice guidelines and, in particular, to address the best practice guidelines in the context of the 2006 amendments to the Federal Rules of Civil Procedure concerning electronic discovery, effective December 1, 2006.

When the Working Group began its deliberations, the starting point was that under Rule 34 and many of its state counterparts, all "data compilations" were deemed documents just like traditional paper documents and subject to discovery. This equal treatment suggested that electronic information should be searched for, processed and produced like paper. However, the Working Group recognized that there are significant differences between paper and electronic

information in terms of structure, content and volume. Simply put, the way in which information is created, stored and managed in electronic environments is inherently different from the paper world. For example, the simple act of typing a letter on a computer involves multiple (and ever-changing) hidden steps, databases, tags, codes, loops, and algorithms that have no paper analogue. The interpretation and application of the discovery rules had not accommodated these differences consistently and predictably so that litigants could efficiently and cost-effectively meet discovery obligations. The Working Group was conceived to help guide organizational practices and legal doctrine. In drafting the principles and commentary, we tried to keep in mind the "rule of reasonableness." That rule is embodied in Rule 1 of the Federal Rules of Civil Procedure (courts should secure the just, speedy and inexpensive determination of all matters) and is applied through former Rule 26(b)(2) (now renumbered as Rule 26(b)(2)(C) – proportionality test of burden, cost and need) and in many state counterparts. The rule of reasonableness means that litigants should seek – and the courts should permit – discovery that is reasonable and appropriate to the dispute at hand while not imposing excessive burdens and costs on litigants and the court. In addition, the Working Group operated on the premise that electronic information production standards could bring needed predictability to litigants and guidance to courts.

The Working Group unanimously concluded that dialogue between and among litigants was a prerequisite to resolving (or avoiding) potentially costly and disruptive electronic discovery disputes. We recognized that adversarial litigation, at times aggressively pursued, may make reasonable dialogue counter-intuitive. Nevertheless, the Working Group urged that parties were well-served by an early discussion about the issues in dispute, the types of information sought, the likely sources and locations of such information, and the realistic costs of identifying, locating, retrieving, reviewing, and producing such information. Electronic discovery is a tool to help resolve a dispute and should not be viewed as a strategic weapon to coerce unjust, delayed, or expensive results. The need to act in good faith also extends to the efforts taken to reasonably preserve relevant electronic information, to the form of the production, and to the allocation of the costs of the preservation and production. All discovery issues should be considered in light of the nature of the litigation and the amount in controversy, as well as the cost, burden, and disruption to the parties' operations.

The principles set forth herein were intended to be concrete enough to provide direction, but flexible enough to allow courts to fashion solutions for the inevitable exceptions. Indeed, the accompanying commentary reflects numerous circumstances and illustrations where the presumptive rule must be adapted to the particular facts. Importantly, the absence of qualifiers and caveats from the stated principles should not be interpreted as a disregard for such circumstances or the need for careful application of the principles by courts, parties and counsel.

The Sedona Principles were intended originally to complement the Federal Rules of Civil Procedure, as they provided only broad standards, by establishing guidelines specifically tailored to address the unique challenges posed by production of electronically stored information. The hope was that, by encouraging before-the-fact and consistent guidance, parties would prepare for meaningful electronic discovery and avoid costly and uncertain discovery disputes. In addition, the Working Group believed it was essential to provide an analytical framework of the substantive law so that courts and counsel could better grapple with the application of the principles in the real world. The Working Group went so far as to suggest in the Preface to the original publication that the principles might also serve as the basis for new federal rules, state rules, or local court rules regarding electronic information production. The original editors wrote: "Our earnest hope is that the efforts of the Working Group will stimulate productive discussion and promote the formulation of legal doctrine consistent with principles of fairness, equity and efficiency."

The Advisory Committee on the Federal Rules of Civil Procedure met and published for public comment a set of draft amendments to the Federal Rules, specifically addressing electronic information, in August 2004. In the following six months, the Committee held three public hearings, heard oral testimony from 74 witnesses, and received 180 written submissions. In May 2005, revised proposals were sent to the Standing Committee on Rules of Practice and Procedure, and in September 2005 the Judicial Conference of the United States recommended that the U.S. Supreme Court adopt amendments to the Federal Rules of Civil Procedure specifically and substantially dealing with issues of what the Advisory Committee now dubbed "electronically stored information." In April 2006, the U.S. Supreme Court adopted the proposals, which ultimately became effective on December 1, 2006.

The Rules amendments adopt the concept that economies will be achieved if parties are required to meet as early as practicable to discuss issues surrounding discovery of electronically stored information. For the first time ever, the new Rules mention the duty to preserve information potentially relevant to litigation. The Rules also recognize that some electronically stored information may be difficult to access and produce, and establish a framework for identifying and evaluating whether the costs and burdens of producing some information outweigh the potential benefit to the resolution

of the dispute. Other amendments are also made with respect to the form of production, interrogatories, third party subpoenas, inadvertent production of privileged documents, and, to a limited extent, grounds for imposing sanctions.

Meanwhile, the Working Group has continued to meet, and publish, on topics relevant to how to handle electronic information in the context of litigation or investigations. The small group of twenty-four that first met in October 2002 has now grown to more than 400, with participation from the bench, academia, government, and all segments of the civil bar.

This publication, like the original *Sedona Principles*, has three major components. It starts by setting forth the 14 Sedona Principles, followed by a chart cross-referencing *The Sedona Principles* with the amended Federal Rules of Civil Procedure. An Introduction sets forth the basic concepts of electronic discovery and summarizes the role of *The Sedona Principles* in both federal and state courts. The following section sets forth the 14 Sedona Principles. These principles embody the consensus views of the Working Group participants and represent what we believe is a reasonable and balanced approach to the treatment of electronic data. The third component, detailed commentary, expands the basic formulations of the principles into a more comprehensive analysis to address the presumptions, legal doctrines, and certain notable exceptions to the application of the principles. These detailed Comments, divided into logical groupings, are supported by select citations to leading cases and references to key secondary sources and authorities, including the Conference of Chief Justices' Guidelines and other recent scholarship. Throughout, the document has been updated to take into account the 2006 Amendments to the Federal Rules, and also to discuss the numerous important court decisions that are influencing the development of the law in this area. Particular attention has been paid to updating Principle 12 on the preservation and production of metadata and Principle 14 on the imposition of sanctions.

Working Group 1 Steering Committee:

Thomas Y. Allman
Conor R. Crowley
Sherry B. Harris
John H. Jessen
Timothy L. Moorehead
Ashish S. Prasad
Jonathan M. Redgrave
Ariana J. Tadler
Lori Ann Wagner[1]

June 2007

[1] Readers should note that this effort represents the collective view of The Sedona Conference® Working Group on Electronic Document Production and does not necessarily reflect or represent the views of The Sedona Conference®, any one participant (or observer) or law firm/company employing a participant or any of their clients. A list of all participants and members of the Working Group (as well as observers to the process) is set forth in Appendix C.

Table of Contents

Table of Contents, cont.

Table of Contents, cont.

Table of Contents, cont.

Table of Contents, cont.

Introduction

Discovery in a World of Electronically Stored Information

Discovery, and document production in particular, is a familiar aspect of litigation practice for many lawyers. The explosive growth and diversification of electronic methods for recording, communicating, and managing information has transformed the meaning of the term "document." While twenty years ago PCs were a novelty and email was virtually nonexistent, today more than ninety percent of all information is created in an electronic format.

For courts and lawyers, whose practices are steeped in tradition and precedent, the pace of technological and business change presents a particular challenge.[2] As electronically stored information (often referred to as "ESI") has become more prevalent, courts, litigants, and rule-makers have attempted to meet this challenge, sometimes by applying traditional approaches to discovery, sometimes by turning to treatises (including earlier editions of *The Sedona Principles*), and sometimes by innovating.

Civil litigation in the federal courts is governed by the Federal Rules of Civil Procedure, which were amended in 2006 to include explicit, and in some cases, unique provisions to govern the discovery of electronically stored information.[3] In the main, the Federal Rules are consistent with and reflect the same approach as *The Sedona Principles*. However, there are differences that are discussed in more detail below.

This revised edition of *The Sedona Principles* seeks to synthesize the current and best thinking from the case law and the amended Federal Rules to provide practical standards for modern discovery.[4]

1. What Is Electronic Discovery?

Electronic discovery refers to the discovery of electronically stored information. Electronically stored information includes email, web pages, word processing files, audio and video files, images, computer databases, and virtually anything that is stored on a computing device – including but not limited to servers, desktops, laptops, cell phones, hard drives, flash drives, PDAs and MP3 players. Technically, information is "electronic" if it exists in a medium that can only be read through the use of computers. Such media include cache memory, magnetic disks (such as computer hard drives or floppy disks), optical disks (such as DVDs or CDs), and magnetic tapes. Electronic discovery is often distinguished from "conventional" discovery, which refers to the discovery of information recorded on paper, film, or other media, which can be read without the aid of a computer. Of course, there is also the discovery of tangible "things" which usually refers to physical objects and property.

For readers less familiar with technical terms relevant to electronic discovery, a glossary of terms is provided in *The Sedona Conference Glossary: E-Discovery & Digital Information Management,* which is *available at* http://www.thesedonaconference.org.

---

2 "[I]t has become evident that computers are central to modern life and consequently also to much civil litigation. As one district court put it in 1985, '[c]omputers have become so commonplace that most court battles now involve discovery of some computer-stored information.'" Charles Alan Wright, Arthur R. Miller, & Richard L. Marcus, *Federal Practice & Procedure,* § 2218 at 449 (2d ed. 2006) (quoting *Bills v. Kennecott Corp.,* 108 F.R.D. 459, 462 (D. Utah 1985)). Similarly, the *Manual for Complex Litigation* recognizes that the benefits and problems associated with computerized data are substantial in the discovery process. *Manual for Complex Litigation (Fourth)*, § 21.446 (Fed. Jud. Ctr. 2004).

3 The 2006 amendments to the Federal Rules of Civil Procedure addressing the discovery of electronically stored information became effective December 1, 2006. *See* http://www.uscourts.gov/rules.gov/rules/EDiscovery_w_Notes.pdf. The amendments impact rules 16, 26, 33, 34, 37, 45 and Form 35. For a summary of the new rules and competing viewpoints on their efficacy, see Thomas Y. Allman, *The Impact of the Proposed Federal E-Discovery Rules,* 12 Rich. L. J. & Tech. 13 (2006); Richard L. Marcus, *E-Discovery & Beyond: Toward Brave New World or 1984?* 236 F.R.D. 598, 618 (2006) and Kenneth J. Withers, *Electronically Stored Information: The December 2006 Amendments to the Federal Rules of Civil Procedure,* 4 Nw. J. Tech. & Intell. Prop. 171 (2006), *available at* http://www.northwestern.edu/journals/njtip/v4/n2/3. Unless otherwise indicated, all references to the Federal Rules of Civil Procedure and accompanying Committee Notes are to the language in force December 1, 2006. Shortly after completion of the amendments addressing electronic discovery, the entire Federal Rules of Civil Procedure underwent "restyling," a process intended to clarify and simplify the language and presentation of the rules without affecting their substantive meaning. *See* http://www.uscourts.gov/rules/supct1106/CV_CLEAN_FINAL5-30-07.pdf. The restyled rules are anticipated to go into effect December 1, 2007. While a full analysis of any effect the restyling may have on the interpretation or application of the rules remains for a future date, the Editors wish to point out that the restyling likely will result in one significant nonsubstantive change – Fed. R. Civ. P. 37 (f) addressing sanctions for the failure to produce electronically stored information will be renumbered Fed. R. Civ. P. 37(e). See Principle 14, *infra*.

4 *See Zubulake v. UBS Warburg*, 229 F.R.D. 422, 440 (S.D.N.Y. 2004) (*"Zubulake V"*) (citing the ABA Standards and *The Sedona Principles,* in addition to the evolving revisions to the Federal Rules and local District Rules).

2. How is Discovery of Electronically Stored Information Different?

The answer to the question –"why and how is electronic discovery different?" – lies in the subtle, but sometimes profound, ways in which electronically stored information presents unique opportunities and problems for document production. Magistrate Judge Nan Nolan noted some of these differences in *Byers v. Illinois State Police*, 53 Fed. R. Serv. 3d 740, No. 99 C 8105, 2002 WL 1264004 (N.D. Ill. May 31, 2002):

> Computer files, including emails, are discoverable…However, the Court is not persuaded by the plaintiffs' attempt to equate traditional paper-based discovery with the discovery of email files…Chief among these differences is the sheer volume of electronic information. Emails have replaced other forms of communication besides just paper-based communication. Many informal messages that were previously relayed by telephone or at the water cooler are now sent via email. Additionally, computers have the ability to capture several copies (or drafts) of the same email, thus multiplying the volume of documents. All of these emails must be scanned for both relevance and privilege. Also, unlike most paper-based discovery, archived emails typically lack a coherent filing system. Moreover, dated archival systems commonly store information on magnetic tapes which have become obsolete. Thus, parties incur additional costs in translating the data from the tapes into useable form.

Id. at *31-33.

The qualitative and quantitative differences between producing paper documents and electronic information can be grouped into the following six broad catagories.

A. Volume and Duplicability

There is substantially more electronically stored information than paper documents, and electronically stored information is created and replicated at much greater rates than paper documents.

The dramatic increase in email usage and electronic file generation poses particular problems for large data producers, both public and private. A single large entity can generate and receive millions of emails and electronic files each day. A very high percentage of information essential to the operation of public and private enterprises is stored in electronic format and much is never printed to paper. Not surprisingly, the proliferation of the use of electronically stored information has resulted in vast information accumulations. While a few thousand paper documents are enough to fill a file cabinet, a single computer tape or disk drive the size of a small book can hold the equivalent of millions of printed pages. Organizations often accumulate thousands of such tapes as data is stored, transmitted, copied, replicated, backed up, and archived.

Electronic information is subject to rapid and large scale user-created and automated replication without degradation of the data. Email provides a good example. Email users frequently send the same email to many recipients. These recipients, in turn, often forward the message, and so on. At the same time, email software and the systems used to transmit the messages automatically create multiple copies as the messages are sent and resent. Similarly, other business applications are designed to periodically and automatically make copies of data. Examples of these include web pages that are automatically saved as cache files and file data that is routinely backed up to protect against inadvertent deletion or system failure.[5]

[5] Neither the users who created the data nor information technology personnel are necessarily aware of the existence and locations of the copies. For instance, a word processing file may reside concurrently on an individual's hard drive, in a network-shared folder, as an attachment to an email, on a backup tape, in an internet cache, and on portable media such as a CD or floppy disk. Furthermore, the location of particular electronic files typically is determined not by their substantive content, but by the software with which they were created, making organized retention and review of those documents difficult.

B. Persistence

Electronically stored information is more difficult to dispose of than paper documents. A shredded paper document is essentially irretrievable.[6] Likewise, a paper document that has been discarded and taken off the premises for disposal as trash is generally considered to be beyond recovery. Disposal of electronically stored information is another matter altogether. The term "deleted" is misleading in the context of electronic data, because it does not equate to "destroyed." Ordinarily, "deleting" a file does not actually erase the data from the computer's storage devices. Rather, it simply finds the data's entry in the disk directory and changes it to a "not used" status – thus permitting the computer to write over the "deleted" data. Until the computer writes over the "deleted" data, however, it may be recovered by searching the disk itself rather than the disk's directory. This persistence of electronic data compounds the rate at which electronic data accumulates and creates an entire subset of electronically stored information that exists unknown to most individuals with custody and ostensible control over it.

C. Dynamic, Changeable Content

Computer information, unlike paper, has content that is designed to change over time even without human intervention. Examples include: workflow systems that automatically update files and transfer data from one location to another; backup applications that move data from one storage area to another to function properly; web pages that are constantly updated with information fed from other applications; and email systems that reorganize and purge data automatically. As a result, unlike paper documents, much electronically stored information is not fixed in a final form.

More generally, electronically stored information is more easily and more thoroughly changeable than paper documents. Electronically stored information can be modified in numerous ways that are sometimes difficult to detect without computer forensic techniques. Moreover, the act of merely accessing or moving electronic data can change it. For example, booting up a computer may alter data contained on it. Simply moving a word processing file from one location to another may change creation or modification dates found in the metadata. In addition, earlier drafts of documents may be retained without the user's knowledge.

D. Metadata

A large amount of electronically stored information, unlike paper, is associated with or contains information that is not readily apparent on the screen view of the file. This additional information is usually known as "metadata." Metadata includes information about the document or file that is recorded by the computer to assist in storing and retrieving the document or file. The information may also be useful for system administration as it reflects data regarding the generation, handling, transfer, and storage of the document or file within the computer system. Much metadata is neither created by nor normally accessible to the computer user.

There are many examples of metadata. Such information includes file designation, create and edit dates, authorship, comments, and edit history. Indeed, electronic files may contain hundreds or even thousands of pieces of such information. For instance, email has its own metadata elements that include, among about 1,200 or more properties, such information as the dates that mail was sent, received, replied to or forwarded, blind carbon copy ("bcc") information, and sender address book information. Typical word processing documents not only include prior changes and edits but also hidden codes that determine such features as paragraphing, font, and line spacing. The ability to recall inadvertently deleted information is another familiar function, as is tracking of creation and modification dates.

---

[6] Modern technology, however, has made recovery at least a theoretical possibility. *See* Douglas Heingartner, *Back Together Again,* New York Times, July 17, 2003, at G1 (describing technology that can reconstruct cross-shredded paper documents).

Similarly, electronically created spreadsheets may contain calculations that are not visible in a printed version or hidden columns that can only be viewed by accessing the spreadsheet in its "native" application, that is, the software application used to create or record the information. Internet documents contain hidden data that allow for the transmission of information between an internet user's computer and the server on which the internet document is located. So-called "meta-tags" allow search engines to locate websites responsive to specified search criteria. "Cookies" are text files placed on a computer (sometimes without user knowledge) that can, among other things, track usage and transmit information back to the cookie's originator.[7]

Generally, the metadata associated with files used by most people today (such as Microsoft Office™ documents) is known as "application metadata." This metadata is embedded in the file it describes and moves with the file when it is moved or copied. On the other hand, "system metadata" is not embedded within the file it describes but stored externally. System metadata is used by the computer's file system to track file locations and store information about each file's name, size, creation, modification, and usage.

Understanding when metadata is relevant and needs to be preserved and produced represents one of the biggest challenges in electronic discovery. Sometimes metadata is needed to authenticate a disputed document or to establish facts material to a dispute, such as when a file was accessed in a suit involving theft of trade secrets. In most cases, however, the metadata will have no material evidentiary value – it does not matter when a document was printed, or who typed the revisions, or what edits were made before the document was circulated. There is also the real danger that information recorded by the computer as application metadata may be inaccurate. For example, when a new employee uses a word processing program to create a memorandum by using a memorandum template created by a former employee, the metadata for the new memorandum may incorrectly identify the former employee as the author. However, the proper use of metadata in litigation may be able to provide substantial benefit by facilitating more effective and efficient searching and retrieval of electronically stored information.

E. Environment-Dependence and Obsolescence

Electronic data, unlike paper data, may be incomprehensible when separated from its environment.[8] For example, the information in a database may be incomprehensible when removed from the structure in which it was created. If the raw data (without the underlying structure) in a database is produced, it will appear as merely a long list of undefined numbers. To make sense of the data, a viewer needs the context, including labels, columns, report formats, and similar information. Report formats, in particular, allow understandable, useable information to be produced without producing the entire database. Similarly, stripping metadata and embedded data from data files such as spreadsheets can substantially impair the functionality of the file and the accuracy of the production as a fair representation of the file as kept and used in the ordinary course of business.

Also, it is not unusual for an organization to undergo several migrations of data to different platforms within a few years. Because of rapid changes in computer technology, neither the personnel familiar with the obsolete systems nor the technological infrastructure necessary to restore the out-of-date systems may be available when this "legacy" data needs to be accessed. In a perfect world, electronically stored information that has continuing value for business purposes or litigation would be converted for use in successor systems, and all other data would be discarded. In reality, such migrations are rarely flawless.

---

[7] There is much confusion over the use of terms and distinctions between application and systems metadata can be confusing. *See* Craig Ball, *Understanding Metadata: Knowing Metadata's Different Forms and Evidentiary Significance Is Now an Essential Skill for Litigators,* 13 Law Tech. Prod. News 36 (Jan. 2006).

[8] In addition, passwords, encryption, and other security features can limit the ability of users to access electronic documents.

F. Dispersion and Searchability

While a user's paper documents will often be consolidated in a handful of boxes or filing cabinets, the user's electronically stored information may reside in numerous locations – desktop hard drives, laptop computers, network servers, floppy disks, flash drives, CD-ROMS, DVDs and backup tapes. Many of these electronic documents may be identical backup or archive copies. However, some documents may be earlier versions drafted by that user or by other users who can access those documents through a shared electronic environment.

Consequently, it may be more difficult to determine the provenance of electronically stored information than paper documents. The ease of transmitting electronic data and the routine modification and multi-user editing process may obscure the origin, completeness, or accuracy of a document. Electronic files are often stored in shared network folders that may have departmental or functional designations rather than author information. In addition, there is growing use of collaborative software that allows for group editing of electronic data, making authorship determination more difficult. Finally, while electronically stored information may be stored on a single location, such as a local hard drive, it is likely that such documents may also be found on high-capacity, undifferentiated backup tapes, or on network servers—not under the custodianship of an individual who may have "created" the document.

While the dispersed nature of electronically stored information complicates discovery, the fact that many forms of electronically stored information and media can be searched quickly and accurately by automated methods provides new efficiencies and economies. In many instances, software is able to search far greater volumes of these types of electronically stored information than human beings could review manually.

3. What Are *The Sedona Principles* and How Have They Influenced the Evolution of E-Discovery?

The reliance upon discovery of electronically stored information has increased markedly in the last decade, although indications of its growing importance to civil litigation have been apparent since the early 1980s.

The Sedona Principles are at the heart of two major parallel developments, one involving the identification and articulation of "best practices" and the other involving rulemaking. The *Principles* evolved from discussions involving wide segments of the parties affected by and deeply involved in the actual e-discovery practice and represent a consensus viewpoint. They evolved into "final" form by 2004. The focus on best-practice guidelines is also embodied in the American Bar Association's "Civil Discovery Standards" and the Conference of Chief Justices' "Guidelines for State Trial Courts." On the rulemaking front, early developments at the state level[9] were followed by the work of the Advisory Committee on Civil Rules of the Judicial Conference of the United States, beginning in 2000, to explore the need for targeted rulemaking. That effort resulted in the 2006 amendments to the Federal Rules of Civil Procedure (the "amended Federal Rules" or the "2006 amendments"). Since the adoption of the amended Federal Rules, a number of states have begun to consider whether to adopt some form of e-discovery rules or guidelines. Many appear to be awaiting the consequences of the federal amendments. Other states require or encourage early discussions of preservation issues and identification of key sources of electronically stored information.[10] An effort by the Uniform Law Commissioners to promote uniform rulemaking modeled on the amended Federal Rules is also underway.

The Sedona Principles have an impressive track record of providing useful assistance to individual federal and state courts facing novel e-discovery issues. They have been influential in providing intellectual support in a number of precedent-

[9] The State of Texas was the first state to enact formal e-discovery rules, having added Rules §§196.3 and 196.4 to its Rules of Civil Procedure in 1999. The State of Mississippi enacted a similar rule in 2003.

[10] *See* New York Rules for the Commercial Division of the Supreme Court, §202.70(g).

setting cases involving preservation obligations,[11] search methodology,[12] production of metadata[13] and the handling of privileged information,[14] to name only a few examples.

We anticipate that the role of providing guidance and best practices will continue to be the province of *The Sedona Principles* – a process illustrated by the changes in Principles 12 (metadata) and 14 (sanctions), as well as the expanded commentary under all fourteen principles. Indeed, there are efforts underway to adopt similar principles in Canada and other countries.[15]

4. What is the Relationship Between *The Sedona Principles* and Court Rules?

A. Federal Rules of Civil Procedure

The Sedona Principles helped shape the legal environment in which the amended Federal Rules were drafted and adopted. In turn, the 2007 revision of *The Sedona Principles* is heavily influenced by consideration of the amended Federal Rules. This interplay between *The Sedona Principles* and the amended Federal Rules will continue. However, *The Sedona Principles* address a number of key topics that the amendments do not. For example, civil procedure rules only apply once litigation commences, and are procedural and not substantive. Therefore the amended Federal Rules do not establish standards governing pre-litigation preservation.[16] *The Sedona Principles* cover the topic in several best practice standards which continue to play a major role in the developing national consensus on the topic.[17]

In many respects, the processes and procedures adopted in the amended Federal Rules and *The Sedona Principles* are consistent. A summary chart comparing *The Sedona Principles* and the amended Federal Rules, by key topics, is found in the front of this publication.

(i) Scope of Discovery of Electronically Stored Information. Amended Federal Rule 34 now provides for the discovery[18] of "electronically stored information" as well as documents and tangible things. This clarification of the scope of discovery parallels Sedona Principle 1 that electronic information of all forms and in all media is potentially subject to discovery. For consistency, the Working Group has adopted the phrase "electronically stored information" for use throughout *The Sedona Principles* in order to employ terminology that is consistent with the Rules.[19]

---

[11] *Consolidated Aluminum Corp. v. Alcoa, Inc.,* No. 03-1055-C-M2, 2006 WL 2583308, at *6 n. 18 (M.D. La. July 19, 2006) (relying on *The Sedona Principles* in determining scope of preservation obligation).

[12] *Treppel v. Biovail,* 233 F.R.D. 363 (S.D. N.Y. 2006) (relying on *The Sedona Principles* in determining appropriateness of defined search strategies required).

[13] *Williams v. Sprint/United Management Co.,* 230 F.R.D. 640 (D. Kan. 2005) (relying on *The Sedona Principles* in determining whether production of metadata was required).

[14] *Hopson v. The Mayor and City Council of Baltimore,* 232 F.R.D. 228, 234 (D. Md. 2005) (relying on *The Sedona Principles* in establishing protocol for privileged document clawback agreement).

[15] *See The Sedona Principles Addressing Electronic Document Production Canadian Edition* (A Project of The Sedona Conference Working Group 7 (WG7)) (February 2007 Public Comment Draft) *available at* http://www.thesedonaconference.org/content/miscFiles/2_13WG7Draft.pdf.

[16] Thomas Y. Allman, *Rule 37(f) Meets Its Critics: The Justification for A Limited Safe Harbor for ESI, 5* Nw. J. Tech. & Intell. Prop. 1 (2006).

[17] *See* Sedona Principle 5 (a party must act reasonably and in good faith in executing preservation obligations, but is not expected to take every conceivable step). Other principles dealing with preservation obligations are Principle 3 (early discussion); 6 (presumptions regarding responding parties); 8 (disaster recovery backup tapes); 9 (deleted, shadowed, fragments or residual data); 12 (metadata) and 14 (sanctions for failure to preserve).

[18] Fed. R. Civ. P. 26(a)(1), which requires "initial disclosures" independent of the Rule 34 discovery request process, also includes an obligation to disclose electronically stored information which a party intends to use to support its claims or defenses.

[19] Even before "electronically stored information" was explicitly added to Rule 34, it was "black-letter law that computerized data is discoverable if relevant." *Anti-Monopoly, Inc. v. Hasbro, Inc.,* No. 94 Civ. 2120, 1995 WL 649934, at *2 (S.D.N.Y. Nov. 3, 1995); *see also Bills v. Kennecott Corp.,* 108 F.R.D. 459, 463-64 (D. Utah 1985) ("[I]nformation stored in computers should be as freely discoverable as information not stored in computers.").

(ii) Limits on Required Production (General). All discovery – including discovery of electronically stored information – is subject to the proportionality limits set forth in Rule 26(b)(2)(C), which require a court to weigh the potential benefit or importance of requested information against the burden on the party that would have to produce the documents.[20] Rule 26(b)(2)(C)(iii) provides for limiting discovery when "the burden or expense of the proposed discovery outweighs its likely benefit, taking into account the needs of the case, the amount in controversy, the parties' resources, the importance of the issues at stake in the litigation, and the importance of the proposed discovery in resolving the issues." Rule 26(b)(2)(C)(i) provides that discovery may be limited if "the discovery sought is unreasonably cumulative or duplicative, or is obtainable from some other source that is more convenient, less burdensome, or less expensive." The Federal Rules are intended to protect parties from unduly burdensome, unnecessary, or inefficient discovery. Rule 26(b)(1) limits discovery to matters, not privileged, which are relevant to a claim or defense.

The Sedona Principles reflect these limits in Principle 2, which provides that "the technological feasibility and realistic costs of preserving, retrieving, reviewing, and producing electronically stored information" should be taken into account in achieving balance. Principle 6 acknowledges and expands the concept by noting that "responding parties are best situated" to evaluate the appropriate procedures, methodologies and technologies to preserve and produce their electronically stored information.

(iii) Limits on Discovery Based on Accessibility. Rule 26(b)(2)(B) establishes a two-tiered approach to discovery unique to the production of electronically stored information. Relevant electronically stored information that resides on sources that are identified as "not reasonably accessible because of undue burden or cost" may be withheld from production, without resort to a court order, provided there is an appropriate identification of the sources of electronically stored information that are not being produced. If the producing party can sustain the burden of demonstrating the undue burden or costs on a challenge, the requesting party then has the burden to show "good cause" for production from these sources.[21] Cost-shifting may be ordered as a condition of production.

Sedona Principle 8 also suggests an initial presumptive limit on discovery, but relates the limit on the initial scope of discovery for relevant evidence to the actual use of information in a business. Sedona Principle 8 states that the "primary source" for discovery should be "active data and information." The commentary to Principle 8 harmonizes the two approaches.

(iv) Protective Orders and Cost-Shifting. Rule 26(c) allows a court to enter a protective order against burdensome discovery and historically is the source of the authority to shift costs for all forms of discovery. The 2006 amendments reinforce this by adding a provision in Rule 26(b)(2)(B) that a producing party may seek a protective order to test its obligations to preserve or produce electronically stored information.

Unlike the Federal Rules, Sedona Principle 13 explicitly states that the costs of "retrieving and reviewing" electronically stored information that is not "reasonably available" may be shifted to the requesting party. The revised commentary under Principle 13 addresses the differences, as well as distinction, between cost shifting under Rule 26(b)(2)(B) and Rule 26(c).

---

[20] *See In re Microcrystalline Cellulose Antitrust Litig.*, 221 F.R.D. 428, 429 (E.D. Pa. 2004) (applying limits of Rule 26 (b)(2) (prior to renumbering) to limit unreasonable demand for sales data not needed in antitrust action).

[21] Ordinarily a requesting party should obtain and evaluate the information from accessible sources before insisting that the responding party search and produce from sources that are not reasonably accessible. *See* Fed. R. Civ. P. 26(b) Committee Note.

(v) Mandatory Early Discussions. The Rule 26(f) requirement for an early "meet and confer" prior to the Rule 16 scheduling conference has been substantially strengthened and expanded in a manner similar to that advocated by Sedona Principle 3.[22] Parties are now expected to have early and meaningful discussions of "any issues relating to preserving discoverable information" and to develop a proposed discovery plan that takes into account "disclosure or discovery" of electronically stored information including, but not limited to, both the form of production and the method of handling claims of privilege after production.

(vi) Form of Production and Metadata. Electronically stored information is created in a form "native" to that application and computer system, together with system and application metadata. This electronically stored information may be produced in a variety of forms other than its "native" form. Some forms of production replicate the view of the user and provide other capabilities such as searchability, but with limited or no metadata or embedded data. The Advisory Committee rejected proposals to mandate any particular form of production and did not take a position on the need to produce metadata. Rule 26(f) instead emphasizes the need to discuss this topic early to attempt to reach agreement, and Rule 34(b) provides a process for resolving disputes, while providing two alternative forms of production in the event the parties do not reach agreement or a court order is not entered: the form or forms "in which it is ordinarily maintained" or "in a form or forms that are reasonably usable."

The phrase "ordinarily maintained" is not synonymous with "native format." It is common for electronic information to be migrated to a number of different applications and formats in the ordinary course of business, particularly if the information is archived for long-term storage. Routine migration will likely result in the loss or alteration of some elements of metadata associated with the native application, and the addition of new elements. Given the variety of forms in which electronically stored information is found and the many options available in producing it, a difference may exist between the form in which electronically stored information is preserved and that in which it is produced for use, depending upon the issues involved and the preferences of the parties or any agreements or orders pending production.[23]

Sedona Principle 12, in contrast, deals directly with the issue of the need to preserve and produce metadata. It has been amended in this 2007 Version to provide more explicit guidance regarding issues relating to both the relevance and usability of metadata. Previously, Principle 12 only provided guidance on a narrow aspect of the metadata issue.[24]

(vii) Inadvertent Production of Privileged or Work Product Information. Because of the tremendous volume of electronically stored information that may need to be reviewed in response to a discovery request, and the complex nature of the information itself, which may contain metadata, embedded data, and non-obvious contextual links, reviewing electronically stored information for privilege is particularly difficult. Even the most diligent review is likely to result in some inadvertent production of privileged information. Serious practical and ethical issues exist when privileged information is inadvertently produced during discovery, not the least of which is the potential waiver under applicable law.[25] Because rules of procedure cannot enlarge or abridge substantive rights, including the substantive law of privilege and waiver, the amended Federal Rules only create a procedure by which parties are now required, by Rule 26(f), to conduct an early discussion of the possible

---

[22] *See* Sedona Principle 3, which states: "Parties should confer early in discovery regarding the preservation and production of electronic data and documents when these matters are at issue in the litigation, and seek to agree on the scope of each party's rights and responsibilities." Mandatory early discussion of contentious e-discovery issues was enthusiastically endorsed by many who testified at the Public Hearings in early 2005. The Testimony and filed Comments of almost 200 witnesses are accessible from the U.S. Courts website ("Comments"). *See* 2004 Civil Rules Committee Chart, including Request to Testify, *available at* http://www.uscourts.gov/rules/e-discovery.html. The Comments represent a valuable snapshot of e-discovery concerns and practices as of 2005 and contain many insightful observations.

[23] *See In re Priceline.Com Inc. Securities Litig.*, 233 F.R.D. 88, 89-91 (D. Conn. 2005) (resolving disputes over the form of preservation and production by ordering that production be in TIFF and PDF form but that the original data be maintained in its original native file format for the duration of the litigation).

[24] Sedona Principle 12 formerly focused on the need for the test of materiality in determining if preservation and production of metadata was needed. As implied in the *Priceline.Com* opinion, *supra*, it may be advisable to distinguish between the file format used in preservation and the form or forms used for production.

[25] Jonathan M. Redgrave and Kristin M. Nimsger, *Electronic Discovery and Inadvertent Productions of Privileged Documents,* 49 Fed. Law. 37 (July 2002).

need for voluntary agreements to govern the treatment of a post-production privilege claim. Any agreement on the topic may be included in the Rule 16(b) Scheduling Order, but the Committee Notes recognize that such agreements between the parties, even if embodied in a court order, may not bind non-parties, a controversial subject being addressed by the Advisory Committee on the Rules of Evidence.[26] Rule 26(b)(5)(C) provides a standard procedure by which parties can identify and retrieve inadvertently produced documents and electronically stored information. It also sets forth a procedure by which the receiving party can challenge the privilege assertion.

Sedona Principle 10 is consistent with this approach, emphasizing the need for reasonable, mutually agreed-upon procedures to protect privileges and objections to production. Importantly, revisions to comment 10.d help to define and distinguish two common categories of agreements, the "clawback" and the "quick peek."

(viii) Sanction Limitations. The 2006 amendments do not directly address the nature and extent of preservation obligations. Instead, new Rule 37(f) limits the availability of rule-based sanctions when electronically stored information has been "lost as a result of the routine, good faith operation of an electronic information system."

While Rule 37(f) does not purport to limit the power to issue sanctions under a court's inherent power, this provision represents a considered policy decision intended to prevent unreasonable and unnecessary interruption of routine information systems during discovery.[27] *The Sedona Principles* do not include a directly comparable provision to Rule 37(f). Instead, Sedona Principle 14 focuses on the underlying issue – the elements required to justify the imposition of sanctions. The nature and extent of preservation obligations are discussed in general respects in Principles 1 and 5, with specific examples of how they apply in Principles 6, 7, 8, 9, 11 and 12.

A slight change in Principle 14 has been made in the 2007 version to more closely conform the culpability element in Principle 14 to emerging case law and to reflect the influence of the policy decision underlying Rule 37(f).[28]

(ix) Third Party Discovery. The obligations and protections added by the 2006 amendments generally apply to discovery of third parties. *See* Fed. R. Civ. P. 45. *The Sedona Principles* do not expressly distinguish between discovery of parties and non-parties, although the commentary does reflect the different treatment of non-parties versus parties in terms of evaluating burdens.

B. State Rules

The volume of reported e-discovery decisions has been smaller in state courts, leading to the misperception that electronic discovery was more prevalent in the types of disputes brought into federal court. As recently as a few years ago, outside the hotly contested areas of divorce law and employment disputes, few reported state court decisions existed. This is quickly changing as electronic discovery becomes more commonplace in state court litigation. *The Sedona Principles* have played a major role in these early cases.[29]

---

[26] Proposed Evidence Rule 502, currently under consideration by the Advisory Committee Evidence Rules, addresses the impact on third parties of non-waiver agreements approved by the courts, among other topics. The proposed rule has been approved by the Advisory Committee on Evidence on April 13, 2007, *available at* http://www.uscourts.gov/rules/Excerpt_EV_Report_Pub.pdf#page=4 .

[27] *Turner v. Resort Condos. Int'l LLC*, No. 1:03-cv-2025, 2006 WL 1990379, at *8 (S.D. Ind. July 13, 2006) (refusing to issue sanctions for alleged failures in preservation where there was no bad faith alteration or destruction of evidence).

[28] The clarification has been made that "grossly negligent" conduct can support sanctions for inadequate conduct in searching for discoverable information. *See Phoenix Four, Inc. v. Strategic Resources Corp.*, No. 05 Civ. 4837(HB), 2006 WL 1409413, at *9 (S.D.N.Y. May 23, 2006) (sanctioning party and counsel for failure to adequately search former servers used by defendant).

[29] *See Bank of America Corp. v. SR Int'l Bus. Ins. Co.,* No. 05-CVS-5564, 2006 WL 3093174 (N.C. Super. Ct. Nov. 1, 2006).

It is by no means certain that the 2006 amendments to the Federal Rules will be adopted in the majority of the states. Rules of civil procedure are promulgated by the highest court in each state, based on input from committees or, in some cases, by action (or inaction) of legislative bodies.[30] Historically, while amendments to the Federal Rules of Civil Procedure have been highly influential on state procedural rulemaking, in recent years the benefits of uniformity have been questioned.[31] To some extent, this can be attributed to the frequency of changes in the rules and some unpopular experimentation, including the addition of mandatory disclosures in the 1993 rule amendments, modified in the 2000 amendments.

Two national initiatives are directed at promoting uniformity among the state trial courts. Both have been heavily influenced by *The Sedona Principles.* The first effort, which eschews formal rulemaking, is that of the Conference of Chief Justices ("CCJ") which has issued "Guidelines for State Trial Courts on Discovery of Electronically Stored Information" (August, 2006) (the "Guidelines").[32] The avowed purpose of the Guidelines is to provide "a reference document to assist state courts in considering issues related to electronic discovery," but not to supplant the rulemaking process of individual states ("[t]he Guidelines should not be treated as model rules that can simply be plugged into a state's procedural scheme"). The effort may be leading to some success at the state level.[33]

The second effort is that of the Electronic Discovery Committee of the National Conference of Commissioners on Uniform Laws ("NCCUSL") to develop uniform model discovery rules for adoption in the states.[34] Although still in draft form as of this writing, the effort to date has been closely modeled on the federal amendments.

5. Why Do Courts and Litigants Need Sedona Best Practice Standards Tailored to E-Discovery?

With the advent of the 2006 amendments to the Federal Rules, the dramatic growth in case law, and the increased number of best-practice guidelines such as those authored by the Conference of Chief Justices and the National Uniform Law Commissioners, it is fair to ask about the role remaining for best-practice standards like *The Sedona Principles*. The Federal Rules are necessarily procedural and cannot provide the level of detail found in *The Sedona Principles*.

Cases are necessarily fact specific. The Rules and Guidelines are not self-executing. A significant role likely remains for the evolution of current, authoritative best-practice standards and principles such as *The Sedona Principles* to provide guidance in the interpretation and application of electronic discovery rules and case law**.**

The Working Group began to examine the issue of electronic document production closely in 2002, focusing both on its similarities to and differences from paper document production. The principles and commentary that follow, as revised in 2007 Second Edition, reflect our continuing efforts to assist the reasoned and just evolution of the law as it relates to the preservation and production of electronically stored information.

---

30 *See* Linda S. Mullenix, *The Varieties of State Rulemaking Experience and the Consequences for Substantive Procedural Fairness* and *Table – State Rulemaking Authorities,* Roscoe Pound Institute 2005 Forum for State Appellate Court Judges, *available at* www.roscoepound.org/new/updates/2005Forum.htm.

31 *See* Stephen N. Subrin, *Federal Rules, Local Rules, and State Rules: Uniformity, Divergence, and Emerging Procedural Patterns,* 137 U. Pa. L. Rev. 1999 (1989) (movement leading to passage of Rules Enabling Act motivated in part by need for uniformity among courts prompted by the changes compelled by "the telephone, telegraph, train, and airplane").

32 The Conference of Chief Justices, *Guidelines for State Courts Regarding Discovery of Electronically Stored Information* (Aug. 2006), *available at* http://www.ncsconline.org/WC/Publications/CS_ElDiscCCJGuidelines.pdf.

33 *See Bank of America Corp., supra* note 37.

34 Information on the current status of the uniform model discovery rules is found at http://www.nccusl.org/Update/CommitteeSearchResults.aspx?committee=248.

Principles & Commentaries

1. Electronically stored information is potentially discoverable under Fed. R. Civ. P. 34 or its state equivalents. Organizations must properly preserve electronically stored information that can reasonably be anticipated to be relevant to litigation.

Comment 1.a. Discovery of electronically stored information under the 2006 Federal E-Discovery Amendments

Discovery in federal and state litigation extends to information relevant to the claims or defenses of a party or relevant to the subject matter of a dispute and likely to lead to the discovery of admissible evidence. This includes any machine-readable electronic information stored on physical media from which it can be retrieved, hereinafter referred to as "electronically stored information."

Before the 2006 amendments to Rule 34, there was some doubt in the federal courts about the full extent of discovery of some forms of electronic information due to Rule 34's focus on production of "documents." To some, the test of discoverability was synonymous with what was intentionally created or viewed by human users, and some doubt existed about other forms of electronic information, especially metadata and system information generated automatically by computers. Although Rule 34 was amended in 1970 to add "data compilations" to the list of discoverable documents, there was no suggestion that "data compilations" was intended to turn all forms of "data" into Rule 34 "documents."

Rule 34(a) has been clarified so that discovery extends to all stored information, including information that it is only readable by machine. Rule 34(a) states that discovery may be had of "electronically stored information (including writings, drawings, graphs, charts, photographs, sound recordings, images and other data or data compilations stored in any medium from which information can be obtained)." As with all discovery, of course, limits resting on the critical principle of proportionality are involved. *See* Principle 2, *infra.*

The form or forms in which the information should be produced, including the extent to which metadata should be produced, is a matter for early negotiation and discussion among parties. *See* Principle 12, *infra*. For cases governed by the Federal Rules, a procedure is set forth in Rule 34(b) to identify and discuss the form or forms of production of electronically stored information to be produced. Pending production, electronically stored information may be preserved in a variety of file formats, provided the relevant electronic content, and content searchability, are not degraded. *See also* Principles 9 and 12, *infra*. However, where special considerations are present, or the requesting party has so requested, consideration should be given to maintaining the information in its native format. *See* Principle 12, *infra*.

When electronically stored information is deleted, it is sometimes available as fragments, shadows, or residual portions of the original data set. This type of information is subject to discovery, but the evaluation of the need for and burdens of such discovery should be analyzed separately on a case-by-case basis. *See* Principle 9, *infra.*

The scope of discovery of electronically stored information does not depend on the internal designation or records classification that may or may not have been assigned to it. Any electronically stored information, whether or not it is internally viewed as of business, legal, regulatory, or personal value, is potentially discoverable.

RESOURCES AND AUTHORITIES

Fed. R. Civ. P. 34(a).

Report of the Civil Rules Advisory Committee, May 27, 2005 (rev. July 25, 2005), *available at* http://www.uscourts.gov/rules/reports/st09-2005.pdf ("Advisory Committee Report").

Thomas Y. Allman, *The Impact of the Proposed Federal E-Discovery Rules,* 12 Rich. J.L. & Tech. 13 (2006).

Richard L. Marcus, *E-Discovery & Beyond: Toward Brave New World or 1984?* 236 F.R.D. 598, 618 (2006).

Lee H. Rosenthal, *A Few Thoughts on Electronic Discovery After December 1, 2006,* 116 Yale L.J. Pocket Part 167 (2006).

Shira A. Scheindlin and Jeffrey Rabkin, *Electronic Discovery in Federal Civil Litigation: Is Rule 34 Up to the Task?,* 41 B.C. L. Rev. 327 (2000).

Shira A. Scheindlin and Jonathan M. Redgrave, *Discovery of Electronic Information, in 2 Bus. and Commercial Litig. in Fed. Court,* Ch 22, (Robert L. Haig ed., 2005 and Supp. 2006).

Kenneth J. Withers, *Electronically Stored Information: The December 2006 Amendments to the Federal Rules of Civil Procedure,* 4 Nw. J. of Tech. & Intell. Prop. 171 (2006), *available at* http://www.law.northwestern.edu/journals/njtip/v4/n2/3.

Comment, *Defining "Document" in the Digital Landscape of Electronic Discovery,* 38 Loy. L.A. L. Rev. 1541 (2005).

Panel Discussion, Advisory Committee Conference, Fordham University Law School, *Rule 33 and 34: Defining E-Documents and the Form of Production,* 73 Fordham L. Rev. 33 (2004).

Zubulake v. UBS Warburg LLC, 217 F.R.D. 309, 324 (S.D.N.Y. 2003) (*"Zubulake I"*) (finding that plaintiff entitled to all emails and electronic documents relevant to employment discrimination claim, including those only preserved on backup tapes; however, given burden and expense of restoring inaccessible backup tapes, a cost-shifting analysis is appropriate).

Comment 1.b. The importance of proper records and information management policies and programs

Organizations should adopt policies and programs that provide rational and defensible guidelines for managing electronically stored information. These guidelines should be created after considering the business, regulatory, tax, information management, and infrastructure needs of the organization, including the need to conserve electronic storage space on email and other servers. Thus, a company that determines it only needs to retain email with business record significance should set forth such a practice in its document retention policy. Employees would then be responsible for implementing the policy, neither destroying documents and electronically stored information prematurely, nor retaining them beyond their useful life. Any such program should include provisions for legal holds to preserve documents and electronically stored information related to ongoing or reasonably anticipated litigation, governmental investigations, or audits. The existence, reasonableness and effectiveness in practice of such a program should be a significant consideration in any spoliation analysis.[35]

[35] Of course, no organization can ensure 100 percent compliance with its records management program, but this limitation inheres in all document retention programs, whether paper or electronic.

The advantages of an effective records and information retention program are particularly pronounced with respect to distributed data and disaster recovery backup tapes. An effective retention program, combined with a preservation program triggered by the reasonable anticipation of litigation, would establish the principal source of discovery material, thus reducing the need to routinely access and review multiple sources of likely duplicative data, including backup tapes. An appropriate records and information management program would involve most or all of the following:

- establishing an appropriate and workable retention schedule for paper and electronically stored information
- helping business units establish practices and customs, tailored to the needs of their businesses, to identify the business records they need to retain
- addressing the retention of email and other communications, such as instant messaging and voicemail
- addressing other forms of electronically stored information that are created in the ordinary course of business
- developing communications policies that establish and promote the appropriate use of company systems. and
- training individuals to manage and retain business records created or received in the ordinary course of business.

Any records and information management program, regardless of its scope and provisions, should be accompanied by a "legal hold"[36] policy that applies once litigation or other investigatory demands are made known. *See* Principle 5, *infra*. These policies can assist in providing access to relevant material and help explain how the entity deals with preserving or collecting information subject to a hold.

Implementing policies with features such as those described above can provide a solid basis to plan for the treatment of electronic documents during discovery. By following an objective, preexisting policy, an organization can formulate its responses to electronic discovery not by expediency, but by reasoned consideration. Under such an approach, a responding party may be able to limit its discovery responses to producing only those materials that are reasonably available to it in the ordinary course of business.

A written records and information management policy can enable an organization to ensure that it is retaining all records necessary to the business, regulatory, and legal needs of the organization. A written policy can also provide guidance on how to properly dispose of documents, both written and electronic, that are without use to the organization. Such policies and programs allow an organization to demonstrate that it has legitimately destroyed documents and electronically stored information by following reasonable and objective standards. The United States Supreme Court noted that the existence of a reasonable records and information management policy, instituted and applied in good faith, should be considered in determining appropriate consequences for the destruction of evidence. *See Arthur Andersen LLP v. United States,* 544 U.S. 696 (2005).

Organizations should simultaneously address the retention and destruction of back-up media such that the storage and treatment of the information on such media are handled in a manner consistent with any records management or legal hold requirements. In some instances, an organization can address electronic and paper records and information with a single set of policies that require identical treatment. However, many entities find it necessary and appropriate to separate policies by functions and to employ technological resources for targeted and specific purposes.

---

[36] The nomenclature (e.g., "litigation hold") is not important; the important factor is that the organization has a means to comply with its legal obligations to preserve relevant information in the event of actual or reasonably anticipated litigation or investigation.

RESOURCES AND AUTHORITIES

The Sedona Guidelines: Best Practice Guidelines & Commentary for Managing Information and Records in the Electronic Age, A Project of the Sedona Conference Working Group on Best Practices for Electronic Document Retention & Production (2007).

ANSI/ARMA Standard 9-2004, *Requirements for Managing Electronic Messages as Records,* ARMA International (Oct. 7, 2004).

Christopher R. Chase, *To Shred or Not to Shred: Document Retention Policies and Federal Obstruction of Justice Statutes,* 8 Fordham J. Corp. & Fin. L. 721 (2003).

Arthur Andersen LLP v. United States, 544 U.S. 696, 704 (2005) ("'Document retention policies,' which are created in part to keep certain information from getting into the hands of others, including the Government, are common in business … It is, of course, not wrongful for a manager to instruct his employees to comply with a valid document retention policy under ordinary circumstances.").

Morris v. Union Pac. R.R. Co., 373 F.3d 896, 900 (8th Cir. 2004) (following Stevenson and distinguishing dicta in *Lewy v. Remington Arms Co.,* ruling that there must be a finding of intentional destruction indicating a desire to suppress the truth, and, in light of the trial court's conclusion that defendant did not intentionally destroy an audiotape of a collision, reversing and remanding for a new trial).

Stevenson v. Union Pac. R.R. Co., 354 F.3d 739, 751 (8th Cir. 2004) (defendant's routine document retention procecdure, which permitted it to destroy track maintenance records, was permissible before lawsuit commenced, but such records should have been preserved once litigation began).

Lewy v. Remington Arms Co., 836 F.2d 1104, 1112 (8th Cir. 1988) (establishing balancing test to determine appropriateness of adverse inference instruction and remanding for determination whether 1970 retention policy was reasonable considering the facts and circumstances of particular documents, and instituted in good faith; company may not blindly destroy documents).

Comment 1.c. Preservation in the context of litigation

An organization's document and information management policies and programs should focus on the business needs of the organization and the budgetary constraints on its use of technology. An organization also must retain documents and electronically stored information that may be relevant to current or reasonably anticipated litigation. *See* Principle 5 and associated commentary, *infra*. Further, most organizations are subject to statutory and regulatory constraints that require the preservation of particular documents and electronically stored information for specified time periods. For example, the Sarbanes Oxley Act of 2002, 116 Stat. 745 (2002), contains a number of document preservation requirements applicable to many publicly traded companies.

Preservation obligations resemble the "retention" obligations imposed by business necessity, statutes, or regulations. However, while the retention schedules often focus on the "records" of an organization, the preservation duty goes further. For example, one of the typical subjects of discovery is unstructured information in the form of emails, word processing documents, spreadsheets, and the like, which may not be subject to the same retention schedules as formal "records." The duty to preserve may also extend, under some circumstances, to electronically stored information which takes the form of shadowed or residual data, which is embedded in a file, or is in sources deemed neither reasonably accessible nor part of the "records" managed by the entity. For all these reasons, care must be taken in designing and implementing processes to give notice of preservation obligations to appropriate custodians.

The duty to preserve transcends any requirements of internal policy or schedule regarding retention and destruction. As part of a legal hold process, a party should be prepared to take good faith measures to suspend or modify any feature of information systems which might impede the ability to preserve discoverable information.

The Federal Rules do not include specific articulations of the obligation to preserve electronically stored information, either with respect to the onset of the obligation, which is case specific, or its scope, which is influenced by the nature of the case and the types of potential claims and defenses involved. The precise preservation obligations must be determined on a case-by-case basis and will vary depending upon the types of electronically stored information involved. However, the 2006 Amendments, for the first time, acknowledged the intersection of preservation and procedure by amending Rule 26(f) to require discussion of "preservation" issues at the early "meet and confer" before the meeting with the court pursuant to Rule 16. In addition, Rule 37(f) was added to emphasize the role of procedures and processes in managing information systems and the risks involved in their "routine, good faith" operation. The Committee Notes make it clear that while preservation obligations arise independent of the Federal Rules, the good-faith obligation recognized in Rule 37(f) may require a party to take affirmative steps to prevent information systems from causing a loss of discoverable information.

Beyond satisfying these legal duties, however, it is neither feasible nor reasonable for organizations to take extraordinary measures to preserve documents and electronically stored information if there is no business or regulatory need to retain such documents and electronically stored information and there is no reasonable anticipation of litigation to which those documents may be relevant. For example, some commentators have observed that organizations should consider routinely making mirror image copies of employee disk drives when an employee leaves an organization or when computer equipment is recycled or discarded. While there may be unusual circumstances when that is advisable, as a general rule it would be wasteful and wholly unnecessary to accumulate such massive quantities of unused data because it is technically possible to do so. Rather, in accordance with existing records and information management principles, it is more rational to establish a procedure by which selected items of value can be identified and retained as necessary to meet the organization's legal and business needs when changes in personnel or hardware occur.

For a more detailed discussion of the preservation obligation as it applies to electronically stored information, see generally *Principle 5,* infra *and also Principles 2 (proportionality), 5 (general responsibility), 8 (disaster recovery backup tapes), 9 (deleted, shadowed, fragmented or residual information) and 12 (metadata).*

RESOURCES AND AUTHORITIES

Shira A. Scheindlin and Jonathan M. Redgrave, *Discovery of Electronic Information, in 2 Bus. & Commerical Litig. in Fed. Courts,* §§ 22:37 to 22:39 and 22:44 to 22:47 (Robert L. Haig ed., 2005 & Supp. 2006) (addressing duty to preserve, when the duty is imposed, and litigation hold procedures).

Ronald J. Hedges, *Discovery of Electronically Stored Information: Surveying the Legal Landscape,* Ch. III at 91-97 (BNA Books 2007) (addressing preservation issues).

Arthur Andersen LLP v. United States, 544 U.S. 696, 704 (2005) ("'Document retention policies,' which are created in part to keep certain information from getting into the hands of others, including the Government, are common in business …. It is, of course, not wrongful for a manager to instruct his employees to comply with a valid document retention policy under ordinary circumstances.").

Morris v. Union Pac. R.R. Co., 373 F.3d 896, 900 (8th Cir. 2004) (following Stevenson and distinguishing dicta in *Lewy v. Remington Arms Co.,* ruling that there must be a finding of intentional destruction indicating a desire to suppress the truth, and, in light of the trial court's conclusion that defendant did not intentionally destroy an audiotape of a collision, reversing and remanding for a new trial).

Stevenson v. Union Pac. R.R. Co., 354 F.3d 739, 751 (8th Cir. 2004) (defendant's routine document retention procedure, which permitted it to destroy track maintenance records, was permissible before lawsuit commenced, but such records should have been preserved once litigation began).

Lewy v. Remington Arms Co., 836 F.2d 1104, 1112 (8th Cir. 1988) (establishing balancing test to determine appropriateness of adverse inference instruction and remanding for determination whether 1970 retention policy was reasonable considering the facts and circumstances of particular documents, and instituted in good faith; company may not blindly destroy documents).

Comment 1.d. Parties should be prepared to address records and information management policies and procedures at the initial meet and confer sessions

Amended Rule 26(f) requires early discussion of preservation issues and other disclosure and discovery issues involved in the production of electronically stored information. Because of the importance of existing records management policies and practices, it is likely that they will become the subject of discussion. Parties should be prepared to discuss, at least in general, their records management policies and practices, including the litigation hold process. In this regard, parties should consider when, and in what circumstances, a claim of privilege or attorney work product may be made with respect to litigation hold directives. In considering what information to discuss and what policies to produce, parties should consider the impact of production (or non-production) on any later need to demonstrate the good faith operation of records management programs and electronic information systems in the face of any claims of evidence spoliation. This and other topics relating to the early discussion at such conferences is supported by Principle 3. See discussion at Comments 3a and 3b, *infra*.

RESOURCES AND AUTHORITIES

Fed. R. Civ. P. 26(f)(3) (requiring that parties discuss the discovery of electronically stored information at the initial meet and confer).

2. When balancing the cost, burden, and need for electronically stored information, courts and parties should apply the proportionality standard embodied in Fed. R. Civ. P. 26(b)(2)(C) and its state equivalents, which require consideration of the technological feasibility and realistic costs of preserving, retrieving, reviewing, and producing electronically stored information, as well as the nature of the litigation and the amount in controversy.

Comment 2.a. Scope of reasonable inquiry

The traditional approach to preserving and producing paper documents has been to undertake a good faith effort to identify sources and locations that are reasonably likely to contain relevant information and to advise custodians to preserve potentially relevant information. This is followed by employing reasonable steps to gather and produce documents, after reviewing them for privilege, trade secrets, confidential information or other appropriate bases for non-production.

A similar approach applies to efforts to identify, preserve, and produce relevant information in electronic format. The fact that the information is in a different form does not alter the principle or place a new or greater discovery obligation upon litigants with relevant electronically stored information merely because of the increased volume of potential information involved. Instead, litigants should rely on these traditional foundations for good faith compliance with discovery obligations and employ the unique capabilities of computer tools to assist in identifying, preserving, retrieving, reviewing, and producing relevant electronically stored information and documents.

For further discussion of the requirements for the preservation of electronically stored information, see Principle 5, infra. See also *Principle 8, which suggests practical distinctions in regard to production of electronically stored information based on the methods and characteristics of its storage.*

RESOURCES AND AUTHORITIES

Lee H. Rosenthal, *A Few Thoughts on Electronic Discovery After December 1, 2006,* 116 Yale L.J. Pocket Part 167 (2006).

Shira A. Scheindlin and Jonathan M. Redgrave, *Discovery of Electronic Information, in 2 Bus. & Commercial Litig. in Fed. Courts,* Ch. 22, (Robert L. Haig ed., 2005 & Supp. 2006).

Comment 2.b. Balancing need for and cost of electronic discovery

The proportionality standard of Rule 26(b)(2)(C) requires a balancing of the need for discovery with the burdens imposed and is particularly applicable to electronic discovery. Among the factors pertinent to electronic discovery are: (a) large volumes of data; (b) data stored in multiple repositories; (c) complex internal structures of collections of data and the relationships of one file to another; (d) data in different formats and coding schemes that may need to be converted into text to be reviewed; and (e) frequent changes in information technology. Understanding and generally quantifying these often technical factors are necessary for parties and the court to make reasoned judgments regarding going forward with or limiting discovery.

Electronic discovery burdens should be proportional to the amount in controversy and the nature of the case. Otherwise, transaction costs due to electronic discovery will overwhelm the ability to resolve disputes fairly in litigation.

Costs cannot be calculated solely in terms of the expense of computer technicians to retrieve the data but must factor in other litigation costs, including the interruption and disruption of routine business processes and the costs of reviewing the information. Moreover, burdens on information technology personnel and the resources required to review documents for relevance, privilege, confidentiality, and privacy should be considered in any calculus of whether to allow discovery, and, if so, under what terms. In addition, the non-monetary costs (such as the invasion of privacy rights, risks to business and legal confidences, and risks to privileges) should be considered. Evaluating the need to produce electronically stored information often requires that a balance be struck between the burdens and need for electronically stored information, taking into account the technological feasibility and realistic costs involved.

The Advisory Committee emphasized the importance of the balancing process, quite apart from, and as the underpinning for, the other production limitations. Accordingly, a reference to Rule 26(b)(2)(C) was added to Rule 26(b)(2)(B), and the Committee Note was amended to state that "the limitations [of the rule] continue to apply to all discovery of electronically stored information, including that stored on reasonably accessible electronic sources." Many state courts apply equivalent concepts to reach similar results under existing state rules.

RESOURCES AND AUTHORITIES

Charles Alan Wright, Arthur R. Miller, & Richard L. Marcus, *Federal Practice and Procedure* § 2008.1 (2d ed. 2006).

McPeek v. Ashcroft, 212 F.R.D. 33, 36 (D.D.C. 2003) (declining to order searches of backup tapes where plaintiff had not demonstrated a likelihood of obtaining relevant information).

Comment 2.c. Limits on discovery of electronically stored information from sources that are not reasonably accessible

Rule 26(b)(2)(B) explicitly limits initial discovery of electronically stored information to information from reasonably accessible sources, the so-called "first tier" of discovery. Reasonably accessible sources generally include, but are not limited to, files available on or from a computer user's desktop, or on a company's network, in the ordinary course of operation.

The converse is information that is "not reasonably accessible" because of undue burden or cost. Examples of such sources may include, according to the Advisory Committee, backup tapes that are intended for disaster recovery purposes and are not indexed, organized, or susceptible to electronic searching; legacy data that remains from obsolete systems and is unintelligible on the successor systems; and data that was "deleted" but remains in fragmented form, requiring a modern version of forensics to restore and retrieve.

A party served with a request for production of electronically stored information from a source that it believes in good faith (a) may contain relevant information but (b) is not reasonably accessible, must identify that source but may object to searching or producing from it. The Rule requires an identification sufficiently detailed to allow the requesting party to evaluate the likelihood that such sources of electronically stored information contain non-duplicative, relevant information as well as the costs and burdens associated with searching or producing electronically stored information from those sources. Importantly, the Rules do not require the identification of all inaccessible sources of electronically stored information, but only those that the producing party believes in good faith may contain relevant, non-duplicative information.

If the parties are unable to reach agreement regarding discovery from such sources, a motion to compel may be brought. In the event of a dispute regarding accessibility, the responding party bears the burden of demonstrating undue burden or cost and may be required to show the specific costs and other elements of the burden. If the responding party meets its burden, the burden shifts to the requesting party to prove that the need for the discovery and the other factors of a "good cause" determination are present for part or all of the discovery requested. The court may permit sampling to assess potential relevance or allow discovery and require that electronically stored information from the data source at issue be produced under appropriate conditions, including the sharing or shifting of costs. The willingness of a requesting party to pay for the additional costs of access, while relevant, is not dispositive.

A producing party may also anticipate a request for production by affirmatively raising issues about its need to preserve or produce information by filing for a protective order that addresses those concerns. Rule 26(b)(2)(B) was revised to explicitly acknowledge that a producing party "may wish to determine its search and potential preservation obligations by moving for a protective order." *See* Report of the Civil Rules Advisory Committee, May 27, 2005 (rev. July 25, 2005) *available at* http://www.uscourts.gov/rules/reports/st07-2005.pdf.

For a discussion of the limits of preservation efforts, including those for electronically stored information that is not reasonably accessible, but is reasonably likely to contain potentially relevant information, see *Principle 5. For a discussion of backup tapes,* see *Principle 8. For a discussion of cost shifting in electronic discovery,* see *Principle 13.*

RESOURCES AND AUTHORITIES

Report of the Civil Rules Advisory Committee, May 27, 2005 (rev. July 25, 2005), *available at* http://www.uscourts.gov/rules/reports/st09-2005.pdf.

Charles Alan Wright, Arthur R. Miller, & Richard L. Marcus, *Federal Practice and Procedure* § 2008.2 (2nd ed. 2006).

Conference of Chief Justices, *Guidelines for State Trial Courts Regarding Discovery of Electronically-Stored Information, Guideline 1(B)* (August, 2006) (defining "accessible" information as "electronically-stored information that is easily retrievable in the ordinary course of business without undue cost and burden").

Tex. R. Civ. P. 196.4 (responding party must produce the electronic or magnetic data that is responsive to the request and is reasonably available to the responding party in its ordinary course of business).

Thomas Y. Allman, *The Impact of the Proposed Federal E-Discovery Rules,* 12 Rich. J.L. & Tech. 13 (2006).

Hon. Anthony J. Battaglia, *Dealing with Electronically Stored Information: Preservation, Production, and Privilege,* 53 Fed. Law. 26 (May 2006).

Kenneth J. Withers, *Electronically Stored Information: The December 2006 Amendments to the Federal Rules of Civil Procedure,* 4 Nw. J. Tech. & Intell. Prop. 171 (2006), *available at* http://www.law.northwestern.edu/hournals/njtip/v4/n2/3.

Zubulake v. UBS Warburg LLC, 217 F.R.D. 309, 319-320 n.61 (S.D.N.Y. 2003) (*"Zubulake I"*) (noting that consideration of cost-shifting is appropriate where stored data is not in a "readily useable" format, such as backup tapes) (noting that Sedona Principles 8 and 9 recognize the distinction between "active data" and backup tapes in a manner very similar to the test employed in the instant case).

Comment 2.d. Need to coordinate internal efforts

Decisions regarding the preservation of electronically stored information should be a team effort, often involving counsel (both inside and outside), information systems professionals, end-user representatives, records and information management personnel, and, potentially, other individuals with knowledge of the relevant electronic information systems and how data is used, such as information security personnel. Parties may also use outside consultants to assist with this process. Such consultants may be included in team activities to the extent consistent with the protection of privileged communications.

The team approach permits an organization to leverage available resources and expertise in ensuring that the organization addresses its preservation and production obligations thoroughly, efficiently and cost-effectively. Furthermore, maintaining a team allows the organization to build a knowledge base about its systems and how they are used. The organization may identify a person or persons who will act as the organization's spokesperson or witness on issues relating to the production of electronically stored information. Of course, the size of the team and the distribution of responsibilities among team members will vary depending upon the size of the organization and the scope of litigation. In short, coordination of information, resources and effort is essential.

For a discussion of the role and risks of counsel in regard to preservation and production of electronically stored information, see *Comment 6f.*

RESOURCES AND AUTHORITIES

Zubulake v. UBS Warburg LLC, 229 F.R.D. 422, 431-33 (S.D.N.Y. 2004) (*"Zubulake V"*) (faulting counsel for failing to take adequate steps to preserve data, including failure to interview key players in the litigation about the storage of their documents and failure to take steps beyond issuing the litigation hold to ensure documents were preserved).

Comment 2.e. Communications with opposing counsel and the court regarding electronically stored information

The efficacy of "meet and confers," or other types of communications, depends upon the parties' candor, diligence and reasonableness. A party should accurately represent the complexities and attendant costs and burdens of preservation and production as well as relevance and need for production. Overstated or excessive cost estimates will reduce the organization's credibility, as will vague statements regarding relevance. Further, a producing party should be prepared to present opposing counsel and the court with a reasonable plan for the preservation and production of relevant electronically stored information. When an organization does not present the court with a reasonable plan, the court may err on the side of protecting the integrity of the data collection process and require unnecessary preservation.

Often, neither counsel nor the court will have sufficient technical knowledge to understand the systems at issue. In preparing for court conferences or meet and confer conferences, counsel should consult with their clients' information technology departments and vendors regarding the technical issues involved in data preservation. In turn, organizations should devote sufficient resources to developing presentations that make complex technical issues comprehensible to counsel and the court. When providing affidavits or testimony to counsel or the court on these issues, the organization should be careful to ensure that the affidavits or testimony are not only accurate but also comprehensible to lay individuals with little technical knowledge.

RESOURCES AND AUTHORITIES

Residential Funding Corp. v. DeGeorge Fin. Corp., 306 F.3d 99, 113 (2d Cir. 2002) (ineffectiveness of plaintiff's vendor may suggest "purposeful sluggishness" on the part of plaintiff, potentially warranting sanctions on remand).

Coleman (Parent) Holdings, Inc. v. Morgan Stanley & Co., Inc., No. 502003CA005045XXOCAI, 2005 WL 679071, at *7 (Fla. Cir. Ct. Mar. 1, 2005) *rev'd on other grounds sub nom. Morgan Stanley & Co., Inc. v. Coleman (Parent) Holdings, Inc., ---* So.2d ----, 2007 WL 837221 (Fla. App. 4 Dist. March 21, 2007) (ordering adverse inference instruction against Morgan Stanley and shifting the burden of proof onto the company as sanctions for its destruction of email and non-compliance with the court's prior discovery order, including repeated representations by counsel that Morgan Stanley had thoroughly complied with the court's order); *see also Clare v. Coleman (Parent) Holdings, Inc.,* 928 So. 2d 1246 (Fla. Ct. App. 2006) (reversing lower court's revocation of individual lawyer's pro hac vice status because court's record indicated no misconduct on the part of counsel, who merely acted as messenger from client party in regard to allegations of misconduct regarding spoliation and who was denied due process rights).

3. Parties should confer early in discovery regarding the preservation and production of electronically stored information when these matters are at issue in the litigation and seek to agree on the scope of each party's rights and responsibilities.

Comment 3.a. Parties should attempt to resolve electronic discovery issues at the outset of discovery

Early discussion of issues relating to the preservation and production of electronically stored information may help reduce misunderstandings, disputes and unnecessary motions, including post-production sanction motions involving the failure to preserve relevant information. The Federal Rules and a number of local district court rules, as well as increasing numbers of state rules, require that parties engage in such discussions at the outset of any action. Indeed, the Advisory Committee observed that "alert[ing] the court to the possible need to address the handling of discovery of electronically stored information early in the litigation if such discovery is expected to occur" fosters resolution of issues before they cause unnecessary delay and expense on matters unrelated to the merits of the litigation.

An obligation to discuss the issues in good faith applies to both parties, and requesting parties must be prepared to be as precise as possible in regard to potential discovery. So-called "any and all" discovery requests that lack particularity in identifying the responsive time period, subject area, or people involved, should be discouraged, along with blanket objections of "overbreadth." *See* Principle 4, *infra*. Some of the issues that parties should seek to resolve early in an action include: (i) the identification of data sources which will be subject to preservation and discovery; (ii) the relevant time period; (iii) the identities of particular individuals likely to have relevant electronically stored information; (iv) the form or forms of preservation and production; (v) the types of metadata to be preserved and produced; (vi) the identification of any sources of information that are not reasonably accessible because of undue burden or cost, such as backup media and legacy data; (vii) use of search terms and other methods of reducing the volume of electronically stored information to be preserved or produced; and (viii) issues related to assertions of privilege and inadvertent production of privileged documents. The Advisory Committee Note to Rule 26(f) suggests that parties should pay particular attention to achieving a balance between competing needs to preserve relevant evidence and to continue critical routine operations in order to reach agreement on "reasonable preservation steps."

Best practices include the memorializing agreements in writing to guide the parties and, as necessary, informing the court.

> *Illustration i.* In the circumstance of an ongoing preservation obligation, the parties should discuss maintaining select data on a live server or other device and agree upon a process for later review and production.
>
> *Illustration ii.* Plaintiffs in a lawsuit involving allegations of securities fraud against multiple defendants seeking extensive damages request preservation of electronic documents by all defendants. The defendants, most of whom are large investment banks and other financial institutions, respond that preservation obligations need to be tailored so that they are defined, manageable, and cost-effective while also preserving evidence that is truly needed for the resolution of the dispute. The parties meet and confer upon a protocol for preserving existing data, including preserving select (not all) backup tapes, certain archived data, and select legacy systems; distributing retention notices (and updates); creating a limited number of mirror images of select computer hard drives; undertaking measures to collect potentially relevant data; and distributing a questionnaire regarding electronic data systems. The defendants assess the costs and burdens involved in the various proposed steps and reach agreement on the scope and limitations of the obligations. The protocol averts motion practice and provides certainty as to the expected preservation efforts.

RESOURCES AND AUTHORITIES

Fed. R. Civ. P. 16(b)(5), 26(f)(3) (requiring that electronically stored information be a topic of the initial meet and confer and discovery plan).

Conference of Chief Justices, *Guidelines for State Trial Courts Regarding Discovery of Electronically-Stored Information,* Guideline 3 (Aug. 2006).

Manual for Complex Litigation (*Fourth*), § 40.25(2) (Fed. Jud. Ctr. 2004) (providing a list of considerations for electronically stored information discovery conferences).

D. Kan. *Guidelines for Discovery of Electronically Stored Information* (parties have a duty to disclose, as part of the Fed. R. Civ. P. 26(f) conference, any electronically stored information that may be used to support a claim or defense; steps that will be taken to preserve electronically stored information; whether embedded data or metadata exist and, if so, the extent to which it will be produced and how the parties will address issues of privilege; whether restoration of backups is needed and who will bear the costs; the format and media of production; and how inadvertently disclosed privileged materials will be treated.).

D.N.J. L. R. 26.1(d) (counsel have a duty to investigate a client's information management systems and identify persons with knowledge of those systems and shall confer and attempt to agree on preservation and production of digital information and who will bear the costs of preservation, production, and restoration of any digital discovery).

Treppel v. Biovail Corp., 233 F.R.D. 363, 374 (S.D.N.Y. 2006) (stressing the importance of reaching early agreements, including use of preservation orders, on topics which could become contentious in post-production disputes and criticizing failure to discuss potential search terms).

In re Bristol-Myers Squibb Sec. Litig., 205 F.R.D. 437, 441, 444 (D.N.J. 2002) (holding that Fed. R. Civ. P. 26(a)(1) requires a party to disclose the existence of electronic information at the time it makes initial disclosures and that the Fed. R. Civ. P. 26(f) "meet and confer should include a discussion on whether each side possesses information in electronic form, whether they intend to produce such material, whether each other's software is compatible, whether there exists any privilege issue requiring redaction, and how to allocate costs involved with each of the foregoing.").

Comment 3.b. Procedural issues relating to form of production

Federal Rule of Civil Procedure 26(f) calls for an early discussion of form of production issues. Rule 34 sets forth a more detailed explanation of the ways in which parties should request and respond to requests seeking production or inspection of electronically stored information.

At the outset, parties seeking discovery should have sufficient technical knowledge of production options so that they can make an educated and reasonable request. These should be discussed at the Rule 26(f) conference and included in any Rule 34(a) requests. Likewise, responding parties should be prepared to address form of production issues at the Rule 26(f) conference.

With respect to requests and responses, the revised Rule 34(b) provides that a request may specify the form or forms in which electronically stored information is to be produced. If objection is made to the requested form or forms for producing electronically stored information, or if no form was specified in the request, the responding party must state the form or forms it intends to use.

If a request does not specify the form or forms for producing electronically stored information, and absent agreement of the parties, a responding party must produce the information in a form or forms in which it is ordinarily maintained or in a form or forms that are reasonably usable unless otherwise ordered by the court. A party need not produce the same electronically stored information in more than one form.

Significantly, the Committee Note to amended Rule 34 makes clear that the option to produce in a "reasonably usable form" does not mean that a responding party is free to convert electronically stored information from the form in which it is ordinarily maintained to a different form that makes it more difficult or burdensome for the requesting party to search and review the documents. Parties and counsel will need to carefully consider the ways in which they preserve and produce documents to ensure that they will be able to realize Rule 34's goal of a fair and reasonable approach to the form of production.

For a discussion of the metadata issue in the context of discovery, see *Principle 12,* infra.

RESOURCES AND AUTHORITIES

Fed. R. Civ. P. 34 (governing the form of production).

Conference of Chief Justices, *Guidelines for State Trial Courts Regarding Discovery of Electronically-Stored Information,* Guideline 6 (Aug. 2006).

ABA Civil Discovery Standards (1999) (rev. Aug. 2004), Standard 29(b)(ii)(A), *available at* http://www.abanet.litigation/discoverystandards/2004civildiscoverystandards.pdf.

Craig Ball, *Understanding Metadata: Knowing Metadata's Different Forms and Evidentiary Significance is Now an Essential Skill for Litigators,* 13 L. Tech. Prod. News 36 (Jan. 2006).

Sattar v. Motorola, Inc., 138 F.3d 1164, 1171 (7th Cir. 1998) (affirming district court's denial of plaintiff's motion to compel hard copies of over 200,000 emails even though plaintiff's system was unable to read defendant's electronic files, because a more reasonable accommodation was (i) some combination of downloading the data from the tapes to conventional computer disks, (ii) loaning plaintiff a copy of the necessary software, or (iii) offering plaintiff on-site access to its own system).

Williams v. Sprint/United Mgmt. Co., 230 F.R.D. 640, 652 (D. Kan. 2005) (*"Williams I"*)("When a party is ordered to produce electronic documents as they are maintained in the ordinary course of business, the producing party should produce the electronic documents with their metadata intact, unless that party timely objects to the production of metadata, the parties agree that the metadata should not be produced, or the producing party requests a protective order.").

Comment 3.c. Privilege logs for voluminous electronically stored information

In litigations with a large volume of relevant, non-duplicative paper documents and electronically stored information, the volume of privileged information may be correspondingly large. The applicable rule states the following:

> [w]hen a party withholds information otherwise discoverable under these rules by claiming that it is privileged or subject to protection as trial preparation material, the party shall make the claim expressly and shall describe the nature of the documents, communications, or things not produced or disclosed in a manner that, without revealing information itself privileged or protected, will enable other parties to assess the applicability of the privilege or protection.

Fed. R. Civ. P. 26 (b)(5)(A).

Traditionally, parties have complied with this rule by producing a privilege log with separate entries for each document that contain objective information about the document (such as author, addressee and Bates number) as well as a field that describes the basis for the privilege claim. Even if there are few documents, preparing a privilege log is often extremely time-consuming. Even with the best efforts of counsel, it often results in a privilege log that is of marginal utility at best. The immense volume of electronic documents now subject to discovery exacerbates the problem.

One solution that parties may consider at the outset is to agree to accept privilege logs that will initially classify categories or groups of withheld documents, while providing that any ultimate adjudication of privilege claims, if challenged, will be made on the basis of a document-by-document review. The basis for this approach is the 1993 rules amendment comment to Rule 26(b)(5), which states the following:

> The rule does not attempt to define for each case what information must be provided when a party asserts a claim of privilege or work product protection. Details concerning time, persons, general subject matter, etc., may be appropriate if only a few items are withheld, but may be unduly burdensome when voluminous documents are claimed to be privileged or protected, particularly if the items can be described by categories.

Fed. R. Civ. P. 26 Committee Note (1993).

An agreement of this nature at the outset of litigation to log privileged documents by category that provides for a fair and full defense of individual privilege claims if challenged, will reduce motion practice regarding log deficiencies and other procedural challenges that are becoming more common given the huge volume of documents at issue.

Comment 3.d. Preservation of expert witness drafts and materials

The obligation to preserve and produce electronically stored information may apply to expert witness materials. The 1993 amendments to Rule 26(a)(2)(B) require the disclosure of all "information considered by the [expert] in forming the [expert's] opinion." Under this standard, courts have held that the failure to preserve information could lead to sanctions and the exclusion of testimony. It is not hard to imagine that litigants will quickly adapt the electronic spoliation disputes of document discovery to the realm of expert witness disclosures (for example, requests for all of the electronic copies of expert witness reports, for access to the expert's hard drive to search for deleted data, or requests for access to all email accounts of the expert).

Because of this potential for dispute, and recognizing that the issue will almost always affect both parties, the best course for the parties is to discuss, early in the case, the issue of which expert witness materials need to be preserved and exchanged in accordance with Rule 26(a)(2)(B). If an agreement cannot be reached, it is preferable to propose a sensible solution to the court early in a disputed motion rather than to face accusations of evidence spoliation later.

RESOURCES AND AUTHORITIES

The Sedona Conference Commentary on the Role of Economics in Antitrust Law (June 2006), Principle II-2 ("The process by which an economic opinion is reached can and should be shielded from discovery.").

Gabrielle R. Wolohojian & David A. Giangrasso, *Expert Discovery and the Work Product Doctrine – Is Anything Protected?* 48-APR B. B.J. 10 (Mar./Apr. 2004).

Trigon Ins. Co. v. United States, 204 F.R.D. 277, 282-84, 289-91 (E.D. Va. 2001) (finding that government had duty to preserve correspondence between experts and consultants, including drafts of expert reports; that the destruction of such evidence was intentional, warranting sanctions for spoliation of evidence; and that an adverse inference instruction regarding the experts' testimony and their credibility in general was warranted).

4. Discovery requests for electronically stored information should be as clear as possible, while responses and objections to discovery should disclose the scope and limits of the production.

Comment 4.a. Requests for production should clearly specify what electronically stored information is being sought

A requesting party that seeks production of electronically stored information should, to the greatest extent practicable, clearly and specifically indicate the types of electronic information it seeks. Such discovery requests should go beyond boilerplate definitions seeking all email, databases, word processing files, or whatever other electronically stored information the requesting party can generally describe. Instead, the request should target particular electronically stored information that the requesting party contends is important to resolve the case. By identifying relevant individuals and topics, parties can avoid the sort of blanket, burdensome requests for electronically stored information that invite blanket objections and judicial intervention.

The requesting party should also identify the form or forms in which it wishes the electronically stored information to be produced, and, if it deems it important or useful, any particular fields or types of metadata sought. A request for production of electronically stored information in the form in which it is maintained should be interpreted as seeking production in native format, with all relevant metadata, and a producing party should object or otherwise raise its concerns if it is not prepared to make production in that form. An early discussion of the potential form or forms of production is advisable in order to permit planning for preservation steps and to identify any disputes that may have to be resolved. *See* Principles 3 *infra* and Principle 12, *supra*.

In federal cases, the subject of form of production must be discussed at the Rule 26(f) conference. If agreement is reached, it may be embodied in a Rule 16(b) Scheduling Order. If the parties do not reach agreement or the court is not asked to resolve the matter, the producing party may use one of two "default forms," either the form "in which it is ordinarily maintained," or a form that is "reasonably usable." Fed. R. Civ. P. 34(b)(2).

For a more detailed discussion of the process and advantages related to a particular form of production, including a discussion of the role of metadata, see *Comment 3.c and Comment 12.a.*

RESOURCES AND AUTHORITIES

Fed. R. Civ. P. 34 Committee Note (2006) (Rule 34 applies to electronic data compilations from which information can be obtained only with the use of detection devices, and when the data can as a practical matter be made usable by the discovering party only through respondent's devices, respondent may be required to use his devices to translate the data into usable form.).

Tex. R. Civ. P. 196.4 ("To obtain discovery of data or information that exists in electronic or magnetic form, the requesting party must specifically request production of electronic or magnetic data and specify the form in which the requesting party wants it produced.").

Wright v. AmSouth Bancorp., 320 F.3d 1198, 1205 (11th Cir. 2003) (holding that trial court did not abuse its discretion by finding plaintiff's request for "computer diskette or tape copy of all word processing files created, modified and/or accessed by, or on behalf" of five employees of the defendant over a two-and-one-half-year period as overly broad in scope, unduly burdensome, and not reasonably related to the plaintiff's age discrimination claims).

Zubulake v. UBS Warburg LLC, 217 F.R.D. 309, 321-22 (S.D.N.Y. 2003) ("*Zubulake I*") (noting that specificity is the touchstone of any good discovery request and holding that one factor to consider when deciding whether to shift costs of production of electronic evidence is "the extent to which the request is specifically tailored to discover relevant information").

Comment 4.b. Responses and objections

Responses and objections should clearly and specifically state all objections and should also indicate the extent to which production of relevant electronically stored information will be limited, based on undue burden or cost of production efforts, not restricted to those sources of information identified as "not reasonably accessible."

It is neither reasonable nor feasible for a party to search or produce information from every electronic file that might potentially contain information relevant to every issue in the litigation, nor is a party required to do so. It should be reasonable, for example, to limit searches for email messages to the accounts of key witnesses in the litigation, for the same reasons that it has been regarded as reasonable to limit searches for paper documents to the files of key individuals. Likewise, it should be appropriate, absent unusual circumstances, to limit review for production to those sources most likely to contain nonduplicative relevant information (such as active files or removable media used by key employees). The use of search terms may assist in reducing the volume of information that must be further reviewed for relevance and privilege.

In cases governed by the Federal Rules, a producing party that does not intend to produce relevant electronically stored information from sources identified as not reasonably accessible because of undue burden or cost must identify those sources to the requesting party. *See* Fed. R. Civ. P. 26(b)(2)(B). Absent local rule or a court order, this Rule does not require the specificity of a traditional privilege log, nor does it require the listing of electronic information systems or storage devices that have not been identified as a source of nonduplicative, relevant information.

If the requesting party did not specify a form or forms for the requested production, or the responding party objects the form or forms requested, the responding party must identify the form or forms it intends to use. If the requesting party specified a form or forms for the requested production, the responding party should either note agreement or include an objection and then identify the form or forms it intends to use. *See* Fed. R. Civ. P. 34(b).

The better practice is to discuss and attempt to agree upon such practical limitations in responses so that any disputes can be addressed and resolved early.

RESOURCES AND AUTHORITIES

Fed. R. Civ. P. 34 (specifying that requester may designate form in which production is to occur).

Tex. R. Civ. P. 193.2(a) (to object to a discovery request, the responding party must make a timely objection in writing and state specifically the legal or factual basis for the objection and the extent to which the party is refusing to comply with the request).

In re Ford Motor Co., 345 F.3d 1315, 1317 (11th Cir. 2003) (stating that the producing party's choice to review database and only produce those relevant portions was adequate discovery response absent specific evidence to the contrary).

Thompson v. U.S. Dep't of Hous. & Urban Dev., 219 F.R.D. 93, 98-99 (D. Md. 2003) (stating that "[c]onclusory or factually unsupported assertions by counsel that the discovery of electronic materials should be denied because of burden or expense can be expected to fail" and noting that the producing party was previously cautioned that its objections to producing electronic records would have to be "particularized" with an affidavit that "identifies evidentiary facts to support the claims of unfair burden or expenses").

Comment 4.c. Meet and confer obligations relating to search and production parameters

It is usually not feasible, and may not even be possible, for most business litigants to collect and review all data from their computer systems in connection with discovery. The extraordinary effort that would be required to do so could cripple many businesses. Yet, without appropriate guidelines, if any data is omitted from a production, an organization may be accused of withholding data that should have been produced, and if that data is not preserved, of spoliation. Unnecessary controversy over peripheral discovery issues can often be avoided at the outset by discussion by the parties of the potential scope and related costs of collecting relevant data. Accordingly, and consistent with the amended Federal Rules and best practices, parties should be prepared to discuss the sources of electronically stored information that have been identified as containing relevant information, as well as the steps that have been taken to search for, retrieve, and produce such information.

RESOURCES AND AUTHORITIES

Fed. R. Civ. P. 26(f) (requiring parties to address issues associated with electronic production at an early stage in litigation).

Fed. R. Civ. P. 16(b)(5), 16(b)(6) (adapting scheduling order to include provisions relating to electronically stored information).

5. The obligation to preserve electronically stored information requires reasonable and good faith efforts to retain information that may be relevant to pending or threatened litigation. However, it is unreasonable to expect parties to take every conceivable step to preserve all potentially relevant electronically stored information.

Comment 5.a. Scope of preservation obligation

The common law duty to preserve evidence clearly extends to electronically stored information. Indeed, the vast majority of information upon which businesses operate today is generated electronically, and much of this information is never printed to paper. Therefore, organizations must take reasonable steps to preserve electronically stored information when litigation is pending or reasonably anticipated.

The preservation obligation necessarily involves two related questions: (1) when does the duty to preserve attach, and (2) what evidence, including potentially discoverable electronically stored information, must be preserved. The first inquiry remains unchanged from prior practice. In the world of electronically stored information, the need to recognize when the duty has been triggered may be more important with respect to those electronic information systems that quickly delete or overwrite data in the ordinary course of operations.

The second inquiry presents a much greater challenge with respect to electronically stored information than with paper. The obligation to preserve relevant evidence is generally understood to require that the producing party make reasonable and good faith efforts to identify and manage the information that it has identified as reasonably likely to be relevant. Satisfaction of this obligation must be balanced against the right of a party to continue to manage its electronic information in the best interest of the enterprise, even though some electronic information is necessarily overwritten on a routine basis by various computer systems. If such overwriting is incidental to the operation of the systems – as opposed to a deliberate attempt to destroy evidence in anticipation of or in connection with an investigation or litigation – it should generally be permitted to continue after the commencement of litigation, unless the overwriting destroys potentially discoverable electronic information that is not available from other sources.

Just as organizations need not preserve every shred of paper, they also need not preserve every email or electronic document, and every backup tape. To require such broad preservation would cripple entities which are almost always involved in litigation and make discovery even more costly and time-consuming. A reasonable balance must be struck between (1) an organization's duty to preserve relevant evidence, and (2) an organization's need, in good faith, to continue operations. *See* Fed. R. Civ. P. 37(f).

> *Illustration i.* L Corporation ("L Corp.") routinely backs up its email system every day and recycles the backup tapes after two weeks. Discovery is served relating to a product liability claim brought against L Corp. arising out of the design of products sold one year ago. L Corp. promptly and appropriately notifies all employees involved in the design, manufacture, and sale of the product to save all documents, including emails relating to the issues in the litigation, and the legal department takes reasonable steps to ensure that all relevant evidence has, in fact, been preserved. L Corp. continues its policy of recycling backup tapes while the litigation is pending. Absent awareness of a reasonable likelihood that specific unique and relevant information is contained only on a backup tape, there is no violation of preservation obligations, because the corporation has an appropriate policy in place and the backup tapes are reasonably considered to be redundant of the data saved by other means.

For a discussion of the duty to preserve information which is found on sources identified as not reasonably accessible because of undue burden or cost, see *Comment 5.b. ("Organizations must prepare for electronic discovery to reduce cost and risk") and Comment 5.h. ("Disaster recovery backup tapes").*

RESOURCES AND AUTHORITIES

Fed. R. Civ. P. 37(f).

Report of the Civil Rules Advisory Committee, May 27, 2005 (rev. July 25, 2005), *available at* http://www.uscourt.gov/rules/reports/st09-2005.pdf.

Ronald J. Hedges, *Discovery of Electronically Stored Information: Surveying the Legal Landscape,* 86-91 (BNA Books 2007) (discussing circumstances in which preservation obligations may arise).

Thomas Y. Allman, *Defining Culpability: The Search for A Limited Safe Harbor in Electronic Discovery,* 2006 Fed. Cts. L. Rev. 7 (2006).

Maria Perez Crist, *Preserving the Duty to Preserve: The Increasing Vulnerability of Electronic Information,* 58 S.C. L. Rev. 7 (2006).

Richard L. Marcus, *Confronting the Future: Coping with Discovery of Electronic Material,* 64-SUM L. & Contemp. Probs. 253, 267-68 (2001).

Martin H. Redish, *Electronic Discovery and the Litigation Matrix,* 51 Duke L.J. 561, 621 (2001).

7 Moore's Federal Practice Section 37A.12[5][e] (3d ed. 2006) ("The routine recycling of magnetic tapes that may contain relevant evidence should be immediately halted on commencement of litigation.").

When Duty to Preserve Arises:

Stevenson v. Union Pac. R.R. Co., 354 F.3d 739, 748 (8th Cir. 2004) (spoliation found when train company failed to produce cab voice tapes following a fatal crash because the railroad knew that fatal crashes frequently lead to litigation and the voice tapes were particularly crucial pieces of evidence).

Kronisch v. United States, 150 F.3d 112, 126 (2d Cir. 1998) (The "obligation to preserve evidence arises when the party has notice that the evidence is relevant to litigation – most commonly when suit has already been filed, providing the party responsible for the destruction with express notice, but also on occasion in other circumstances, as for example when a party should have known that the evidence may be relevant to future litigation.").

Testa v. Wal-Mart Stores, Inc., 144 F.3d 173, 177-178 (1st Cir. 1998) (duty to preserve arises at a time measured by the "institutional notice – the aggregate knowledge possessed by a party and its agents, servants and employees").

Silvestri v. General Motors Corp., 271 F.3d 583, 591 (4th Cir. 2001) (holding that the duty to preserve evidence arises when the party knows or reasonably should know that the evidence may be relevant to pending or anticipated future litigation).

Fujitsu Ltd. v. Federal Express Corp., 247 F.3d 423, 436 (2d Cir. 2001) (holding that "[t]he obligation to preserve evidence arises when the party has notice that the evidence is relevant to litigation or when a party should have known that the evidence may be relevant to future litigation").

Zubulake v. UBS Warburg LLC, 220 F.R.D. 212, 216-17 (S.D.N.Y. 2003) (*"Zubulake IV"*) (in employment discrimination case, duty to preserve attached as soon as plaintiff's supervisors became reasonably aware of the possibility of litigation, rather than when EEOC complaint was filed several months later).

Rambus, Inc. v. Infineon Techs. AG, 220 F.R.D. 264 (E.D. Va. Mar. 17, 2004), subsequent determination, 222 F.R.D. 280 (May 18, 2004) (the duty to preserve evidence arises before litigation when a party reasonably should know that the evidence may be relevant to anticipated litigation; thus, once a party reasonably anticipates litigation, it must suspend any routine document purging system, and put in place a litigation hold to ensure the preservation of relevant documents; concomitantly, there is a duty not to initiate a document destruction regime that may result in the destruction of potentially relevant information if a party reasonably anticipates litigation); *see also Samsung Elecs. Co. v. Rambus, Inc.,* 439 F. Supp. 2d 524 (E.D. Va. 2006) (finding that Rambus' destruction of evidence at a time when it anticipated litigation could form the basis of a finding of exceptionality within the meaning of the patent statute authorizing attorney's fees in exceptional cases); *Hynix Semiconductor Inc. v. Rambus, Inc.,* No. C-00-20905 RMW, 2006 WL 565893 (N.D. Cal. Jan. 5, 2006) (finding no spoliation or bad faith in implementation of document management and destruction policy because litigation was not "probable" at the time the party introduced the policy, as the "path to litigation was neither clear nor immediate" at that time).

Scope of Duty to Preserve:
Mosaid Techs. Inc. v. Samsung Elecs. Co., 348 F. Supp. 2d 332, 336 (D.N.J. 2004) (while a litigant is under no duty to keep or retain every document in its possession, even in advance of litigation, it is under a duty to preserve what it knows, or reasonably should know, will likely be requested in reasonably foreseeable litigation).

Zubulake v. UBS Warburg LLC, 217 F.R.D. 309, 324 (S.D.N.Y. 2003) (*"Zubulake I"*) (plaintiff entitled to all emails and electronic documents relevant to employment discrimination claim, including those only preserved on backup tapes; however, given burden and expense of restoring inaccessible backup tapes, a cost-shifting analysis is appropriate).

Concord Boat Corp. v. Brunswick Corp., No. LR-C-95-781, 1997 WL 33352759, at *4 (E.D. Ark. Aug. 29, 1997) (corporation fulfilled duty to preserve by retaining all relevant emails subsequent to the filing of the complaint and the preservation order, but not all emails prior to litigation: "to hold that a corporation is under a duty to preserve all email potentially relevant to any future litigation would be tantamount to holding that the corporation must preserve all email;" such a holding, the court found, would be crippling to large corporations, which are often involved in litigation).

Comment 5.b. Organizations must prepare for electronic discovery to reduce cost and risk

The main purpose of computer systems is to assist the organization in its business activities. Nonetheless, the need to respond to discovery in litigation is a fact of life for many organizations. Preparing in advance for electronic discovery demands can greatly ease the burdens and risk of inaccuracy inherent in efforts to prepare for initial disclosures and meet and confer sessions once litigation begins. In addition, the accessibility of information and the costs of responding to requests for discovery of information contained in computer systems can be best controlled if the organization takes steps ahead of time to coordinate with and prepare IT staff, records management personnel, managers, and users of these systems for the potential demands of litigation. Preparing for electronic discovery can also help the organization reasonably calculate the cost and burden of discovery requests, control production costs, and minimize the risk of failing to preserve or produce relevant information from computer systems.

Such steps include instituting defined policies and procedures for preserving and producing potentially relevant information, and establishing processes to identify, locate, preserve, retrieve, and produce information that may be relevant or required for initial mandatory disclosures. Organizations should provide training regarding these policies and procedures.

> *Illustration i.* Med Corporation ("Med") is a manufacturer of pharmaceutical products. Med has established a three-week rotation for system backups. One of Med's products, LIT, is observed to cause serious adverse reactions in a number of patients, and the FDA orders it withdrawn from the market. Anticipating the potential for claims relating to LIT, Med's litigation department collects all potentially relevant information from employees. The litigation response system helps Med identify and quickly move to preserve all potentially relevant data, including email, user files, corporate databases, shared network areas, public folders, and other repositories. The process results in relevant data being collected on a special litigation database server that is independent of normal system operations and backups.

Eight months later, a class action is filed against Med for LIT injuries. Plaintiffs' counsel obtains an *ex parte* order requiring Med to save all of its backup tapes, to refrain from using any auto-deletion functions on email and other data, pending discovery, or to reformat or reassign hard drives from employees involved in any way with LIT. Med's Information Systems department estimates that complying with the order will cost at least $150,000 per month, including the cost of new tapes, reconfiguration of backup procedures and tape storage, purchase and installation of additional hard drive space for accumulating email and file data, and special processing of hard drives when computers are upgraded or employees leave the company or are transferred.

Med promptly moves for relief from the order, demonstrating through its documented data collection process that the relevant data has been preserved, and that the requested modifications of its systems are unnecessary due to the preservation efforts already in place. The court withdraws its order and Med is able to defend the litigation without impact on normal operations of its computer systems or excessive electronic discovery costs.

RESOURCES AND AUTHORITIES

Fed. R. Civ. P. 26(b)(2)(B).

Fed. R. Civ. P. 37(f) Committee Note (2006) ("Whether good faith would call for steps to prevent the loss of information on sources that the party believes are not reasonably accessible under Rule 26(b)(2)(B) depends upon the circumstances of each case. One factor is whether the party reasonably believes that the information on such sources is likely to be discoverable and not available from reasonably accessible sources.").

Zubulake v. UBS Warburg LLC, 220 F.R.D. 212, 217 (S.D.N.Y. 2003) *("Zubulake IV")*, (parties must retain all relevant documents in existence or created after the duty to preserve attaches, but organizations need not preserve "every shred of paper, every email or electronic document, and every back-up tape").

Comment 5.c. Corporate response regarding litigation preservation

Organizations should define the scope of their preservation obligations as soon as practicable after the duty to preserve arises. Failure to initiate reasonable preservation protocols as soon as practicable may increase the risk of disputes that relevant information was not preserved. In so doing, the execution of what has come to be known as a "litigation hold" is advisable, to provide a repeatable, documented process to assist in meeting preservation obligations.

The duty to comply with a preservation obligation is an affirmative duty. The scope of what is necessary will, of course, vary widely between and even within organizations depending upon the nature of the claims and defenses, and the information at issue. That said, organizations addressing preservation issues should carefully consider likely future discovery demands for relevant electronically stored information to avoid needless repetitive steps to capture data again in the future. Ideally, an effective process to identify and retain documents and electronically stored information reasonably subject to the preservation obligation should be established as soon as practicable. An appropriate notice should be effectively communicated to those employees and others likely to have or know of such information. Senior management and legal advisors should be involved in the retention decisions and processes.

RESOURCES AND AUTHORITIES

Gregory G. Wrobel, *et al., Counsel Beware: Preventing Spoliation of Electronic Evidence in Antitrust Litigation,* 20-SUM Antitrust 79 (2006).

Mafe Rajul, *"I Didn't Know My Client Wasn't Complying!" The Heightened Obligation Lawyers Have to Ensure Clients Follow Court Orders in Litigation Matters,* 2 Shidler J.L. Com. & Tech. 9 (2005).

Zubulake v. UBS Warburg LLC, 229 F.R.D. 422, 432 (S.D.N.Y. 2004) (*"Zubulake V"*) (faulting counsel for failing to interview key players in litigation or do keyword search of databases in course of creating and enforcing litigation hold).

Rambus, Inc. v. Infineon Tech. AG, 220 F.R.D. 264 (E.D. Va. Mar. 17, 2004), *subsequent determination*, 222 F.R.D. 280 (May 18, 2004) (duty not to initiate a document destruction regime if a party reasonably anticipates litigation).

Comment 5.d. Preservation notice to affected persons ("legal holds")

Upon determining that litigation or an investigation is threatened or pending and has triggered a preservation obligation, the organization should take reasonable steps to communicate the need to preserve information to appropriate persons, except when particular circumstances make hold notices unnecessary or inadvisable.

The recipient list will include persons responsible for maintaining information potentially relevant to that litigation or investigation. The list may also include the person or persons responsible for maintaining and operating computer systems or files, including back-up and archiving systems, which may fall within the scope of the preservation obligation. The notice does not need to reach all employees, only those reasonably likely to maintain documents relevant to the litigation or investigation. In many cases, the notice should be sent to a person or persons responsible for maintaining and operating computer systems or files that have no particular custodian or owner but may fall within the scope of the preservation obligation.

While the form and content of the notice may vary widely depending upon the circumstances, the notice need not provide a detailed list of all information to retain. Instead, it should describe the types of information that must be preserved, with enough detail to allow the recipient to implement the hold. The notice should state that electronically stored information, as well as paper, are subject to the need for preservation. Additionally, the notice should: (i) describe the subject matter of the litigation and the subject matter, dates, and other criteria defining the information to be preserved; (ii) include a statement that relevant electronically stored information and paper documents must be preserved; (iii) identify likely locations of relevant information (e.g., network, workstation, laptop or other devices); (iv) provide steps that can be followed for preserving the information as may be appropriate; and (v) convey the significance of the obligation to the recipients.

The notice need not demand preservation of all documents, only those affected by the preservation obligation. Additionally, the preservation obligation, except in extreme circumstances, should not require the complete suspension of normal document management policies, including the routine destruction and deletion of records.

Communications should be accomplished in a manner reasonably designed to provide prominent notice to the recipients. Depending on the scope and duration of the litigation, it may be advisable to repeat such notice. When preservation obligations apply to documents and data spanning a significant or continuing time period, organizations should analyze whether special steps are needed to preserve unique, relevant electronic information stored on outdated or retired systems.

> *Illustration i.* Pursuant to its procedures for litigation response, upon receipt of notice of the claim, the organization identifies the departments and employees involved in the dispute. Those individuals whose files are reasonably likely to contain relevant documents and information are notified via email of the dispute and are asked to take steps to retain documents (including electronic communications, data and records) that may be relevant to the litigation described in the notice. The notice identifies a contact person who can address questions regarding preservation duties. The notice is also distributed to the identified Information Technology liaison, who works with management and legal counsel to identify any systems files or data that may be subject to the preservation obligation.

Parties also should consider whether notice must be sent to third parties, such as contractors and vendors, including those that provide information technology services. This concern arises out of Rule 34, which frames a party's obligation in terms of its possession, custody, or control of documents.

It must be recognized that in some circumstances, a legal hold notice may be unnecessary (e.g., the relevant information is already secured) or inadvisable (e.g., the notice itself may trigger evidence destruction efforts by the employee under investigation).

Comment 5.e. Preservation obligation not ordinarily heroic or unduly burdensome

The preservation obligation does not ordinarily impose heroic or unduly burdensome requirements on organizations with respect to electronically stored information, although a party may request, and a court can compel, the exercise of extraordinary efforts to preserve electronically stored information even if it is not reasonably accessible in the ordinary course of business, or is particularly transitory and costly and burdensome to preserve. The obligation to preserve normally requires reasonable and good faith efforts. The obligation to undertake extraordinary efforts should be exercised only when there is a substantial likelihood that the information exists; that it would not remain in existence absent intervention; that the information (or its substantial equivalent) cannot be found in another, more accessible data source; and that its preservation is likely to materially advance the resolution of the litigation in a just, efficient, and relatively inexpensive manner.

> *Illustration i.* A requesting party seeks an order, over objection, that backup tapes created during a relevant period should be preserved and restored. It develops sufficient proof to raise the likelihood that substantial amounts of deleted but relevant information existed in the time frame covered by the backup tapes. Before ruling on the merits of the request, the court should consider having the producing party restore and search a sample of the tapes to determine the likelihood that relevant and discoverable material, not otherwise available, can be recovered and that it is worthwhile to do so. If recovery of information from the backup tapes is ordered, the court should consider whether further use of sampling techniques would minimize the burdens on the producing party.

RESOURCES AND AUTHORITIES

Fed. R. Civ. P. 26(b)(2) ("The frequency or extent of use of the discovery methods otherwise permitted under these rules and by any local rule shall be limited by the court if it determines that … the burden or expense of the proposed discovery outweighs its likely benefit, taking into account the needs of the case, the amount in controversy, the parties' resources, the importance of the issues at stake in the litigation, and the importance of the proposed discovery in resolving the issues.").

Charles Alan Wright, Arthur R. Miller, & Richard L. Marcus, *Federal Practice and Procedure* § 2008.1 (2d ed. 2006).

Convolve, Inc. v. Compaq Computer Corp., 223 F.R.D. 162, 177 (S.D.N.Y. 2004) (relying on proposed amendment to Fed. R. Civ. P. 37(f) in holding preservation efforts would have required "heroic efforts far beyond those consistent with [defendants] regular course of business," since the data in question were "ephemeral," existing only until the tuning engineer made the next adjustment).

Comment 5.f. Preservation orders

In general, courts should not issue a preservation order over objection unless the party requesting such an order demonstrates its necessity, which may require an evidentiary hearing in some circumstances. Because all litigants are obligated to preserve relevant evidence in their possession, custody, or control, a party seeking a preservation order must first demonstrate a real danger of evidence destruction, the lack of any other available remedy, and that a preservation order is an appropriate exercise of the court's discretion.

That said, jointly stipulated preservation orders may aid the discovery process by defining the specific contours of the parties' preservation obligations. Before any preservation order is issued, the parties should meet and confer to discuss the scope and parameters of the preservation obligation. Whether agreed to or ordered over objection, preservation orders should be narrowly tailored to require preservation of documents and electronically stored information that are nonduplicative and relevant to the case, without unduly interfering with the normal functioning of the affected party's operations and activities, including the operation of electronic information systems.

Ex parte preservation orders should rarely be entered. Such orders violate the principle that responding parties are responsible for preserving and producing their own electronically stored information. More generally, preservation orders rarely should be issued over objection, and only after a full and fair opportunity to present evidence and argument. This is particularly important when dealing with electronically stored information that may be transitory, not reasonably accessible, or not susceptible to reasonable preservation measures.

Usually, neither the party seeking a preservation order nor the court will have a thorough understanding of the other parties' computer systems, the electronic data that is available, or the mechanisms in place to preserve that electronic data. For example, courts sometimes believe that backup tapes are inexpensive and that preservation of tapes is not burdensome. However, backup systems and technologies vary greatly. Without information about the specifics of the backup system in use, it is difficult to tell what steps are reasonable to meet the needs of the case.

The 2006 amendments to the Federal Rules carefully balance the need to discourage unnecessary, premature and/or overbroad preservation orders with the need to prevent the loss of information important to the litigation and to help parties who sought to memorialize agreements on the scope of their preservation obligations. As set forth in the Committee Note to Rule 26(f), "the requirement that the parties discuss preservation does not imply that courts should routinely enter preservation orders. A preservation order entered over objections should be narrowly tailored. *Ex parte* preservation orders should issue only in exceptional circumstances." Rule 26(b)(2)(B) was also amended to make it clear that either party may seek immediate relief in connection with preservation obligations.

RESOURCES AND AUTHORITIES

Report of the Civil Rules Advisory Committee, May 27, 2005 (rev. July 25, 2005), *available at* http://www.uscourts.gov/rules/reports/st09-2005.pdf (Fed. R. Civ. P. 26(b)(2)(B) text has been changed to recognize that the responding party may wish to determine its search and potential preservation obligations by moving for a protective order (C-50) and Fed. R. Civ. P. 37(f) "exemption [for violation of protective orders] was deleted for fear that it would invite routine applications for protective orders, and often over broad orders" (C-88-89.).

Manual for Complex Litigation (*Fourth*), § 11.442 (Fed. Jud. Ctr. 2004).

Capricorn Power Co. v. Siemens Westinghouse Power Corp., 220 F.R.D. 429, 433-34 (W.D. PA. 2004) (discussing new balancing test to be used to evaluate necessity of preservation order, which looks at: "1) the level of concern the court has for the continuing existence and maintenance of the integrity of the evidence in question in the absence of an order directing preservation of the evidence; 2) any irreparable harm likely to result to the party seeking the preservation of evidence absent an order directing preservation; and 3) the capability of an individual, entity, or party to maintain the evidence sought to be preserved, not only as to the evidence's original form, condition or contents, but also the physical, spatial and financial burdens created by ordering evidence preservation").

Comment 5.g. All data does not need to be "frozen"

A party's preservation obligation does not require "freezing" of all electronically stored information, including all email. Organizations need not preserve "every shred of paper, every email or electronic document, and every back-up tape," nor do they have to go to extraordinary measures to preserve "all" potentially relevant evidence.

Civil litigation should not be approached as if information systems were crime scenes that justify forensic investigation at every opportunity to identify and preserve every detail. Theoretically, a party could preserve the contents of waste baskets and trash bins for evidence of statements or conduct. Yet, the burdens and costs of those acts are apparent and no one would typically argue that this is required. There should be a similar application of reasonableness to preservation of electronic documents and data.

Even though it may be technically possible to capture vast amounts of data during preservation efforts, this usually can be done only at great cost. Data is maintained in a wide variety of formats, locations and structures. Many copies of the same data may exist in active storage, backup, or archives. Computer systems manage data dynamically, meaning that the

data is constantly being cached, rewritten, moved and copied. For example, a word processing program will usually save a backup copy of an open document into a temporary file every few minutes, overwriting the previous backup copy. In this context, imposing an absolute requirement to preserve all information would require shutting down computer systems and making copies of data on each fixed disk drive, as well as other media that are normally used by the system. Costs of litigation would routinely approach or exceed the amount in controversy. In the ordinary course, therefore, the preservation obligation should be limited to those steps reasonably necessary to secure evidence for the fair and just resolution of the matter in dispute.

> *Illustration i.* In a Freedom of Information Act ("FOIA") action, the district court enters a preliminary injunction that the agency believes requires it to freeze all computers that could potentially contain documents subject to the FOIA dispute. In implementing the order, the agency determines that the categorical freeze on all agency hard drives requires the purchase of new equipment with each personnel change and wherever there are certain types of equipment malfunctions. The agency should approach the court for implementation of a more limited order so that only those computers that contain responsive records will be preserved and all others can be released for reuse.

RESOURCES AND AUTHORITIES

Thomas Y. Allman, *Defining Culpability: The Search for A Limited Safe Harbor in Electronic Discovery,* 2006 Fed. Cts. L. Rev. 7 (2006).

Zubulake v. UBS Warburg LLC, 220 F.R.D. 212, 217 (S.D.N.Y. 2003) (*"Zubulake IV"*) (parties must retain all relevant documents in existence or created after the duty to preserve attaches, but organizations need not preserve "every shred of paper, every email or electronic document and every back-up tape").

Manual for Complex Litigation (Fourth), Sample Order 40-25 (Fed. Jud. Ctr. 2004) (broad interim protective order intended to encourage the parties to negotiate a more permanent stipulated order).

Comment 5.h. Disaster recovery backup tapes

Absent specific circumstances, preservation obligations should not extend to disaster recovery backup tapes created in the ordinary course of business. When backup tapes exist to restore electronic files that are lost due to system failures or through disasters such as fires or tornadoes, their contents are, by definition, duplicative of the contents of active computer systems at a specific point in time. Thus, employing proper preservation procedures with respect to the active system should render preservation of backup tapes on a going-forward basis redundant. Further, because information on backup tapes is generally not retained for substantial periods of time, but instead is periodically overwritten when new backups are made, preserving information on backup tapes would require the time-consuming and costly process of altering backup systems, exchanging backup tapes, purchasing new tapes or hardware, and storing the tapes removed from rotation.

In some organizations, however, the concepts of backup and archive are not clearly separated, and backup tapes are retained for a relatively long time period to retain files that may need to be accessed in the future. Backup tapes may also be retained for long periods out of concern for compliance with record retention laws. Under these circumstances, the stored backup tapes may contain the only remaining copy of relevant data or documents. Organizations that use backup tapes for archival purposes should be aware that this practice is likely to cause substantially higher costs for evidence preservation and production in connection with litigation. Organizations seeking to preserve data for business purposes or litigation should, if possible, consider employing means other than traditional disaster recovery backup tapes. They should not be used for recordkeeping.

> *Illustration i.* Pursuant to an information technology management plan, once each day a producing party routinely copies all electronic information on its systems and retains, for a short period of time, the resulting backup tape for the purpose of reconstruction in the event of an accidental erasure, disaster or system malfunction. A requesting party seeks an order requiring the producing party to preserve, and to cease reuse of, all existing backup tapes pending discovery in the case. Complying with the requested order would impose significant expenses and burdens on the producing party, which are documented in factual submissions. No credible evidence is shown establishing the likelihood that, absent the requested order, the producing party will not produce all relevant information during discovery. The producing party should be permitted to continue the routine recycling of backup tapes in light of the expense, burden and potential complexity of restoration and search of the backup tapes.

Finally, if it is unclear whether there is a reasonable likelihood that nonduplicative, relevant information is contained on backup tapes, the parties and/or the court may consider the use of sampling to better understand the nature and relevance of the information at issue. Depending on the circumstances of the case, sampling may establish that there is very little, if any, unique, relevant information on the tapes, and that there is no need for the tapes to be retained or restored. Similarly, sampling may establish that it is reasonable to retain and restore only certain intervals of available tapes to satisfy the party's good faith compliance with its preservation and production obligations.

> *Illustration i.* A requesting party seeks an order, over objection, that backup tapes created during a relevant period should be preserved and restored. It develops sufficient proof to raise the likelihood that substantial amounts of deleted but relevant information existed in the time frame covered by the backup tapes. Before ruling on the merits of the request, the court should consider having the producing party restore and search a sample of the tapes to determine the likelihood that relevant and discoverable material, not otherwise available, can be recovered and that it is worthwhile to do so. If recovery of information from the backup tapes is ordered, the court should consider whether further use of sampling techniques would minimize the burdens on the producing party.

According to the Report of the Civil Rules Advisory Committee presenting the proposed amendments to the Federal Rules, disaster recovery tapes which are "intended for disaster recovery purposes that are often not indexed, organized, or susceptible to electronic searching" are identified as sources that may not reasonably be accessible and therefore are not subject to initial production absent a court order. However, a party will need to disclose backup tapes that it determines are not reasonably accessible if it has a reasonable, good faith belief that relevant, non-duplicative data reside on those tapes; and, therefore, the Rule assumes the preservation of such backup tapes.

RESOURCES AND AUTHORITIES

Report of the Civil Rules Advisory Committee, May 27, 2005 (rev. July 25, 2005), C-42 *available at:* http://www.uscourts.gov/rules/reports/st09-2005.pdf (giving examples from "current technology").

Fed. R. Civ. P. 26 (b)(2)(B) Committee Note, ("A party's identification of sources of electronically stored information as not reasonably accessible does not relieve the party of its common-law or statutory duties to preserve evidence. Whether a responding party is required to preserve unsearched sources of potentially responsive information that it believes are not reasonably accessible depends on the circumstances of each case.").

Report of the Civil Rules Advisory Committee, May 27, 2005 (rev. July 25, 2005), C-83 *available at* http://www.uscourts.gov/rules/reports/st90-2005.pdf. ("Examples of [routine operations] include programs that recycle storage media kept for brief periods against the possibility of a disaster that broadly affects computer operations").

Fed. R. Civ. P. 37(f) Committee Note (2006) ("One factor [in deciding whether to interrupt programs] is whether the party reasonably believes that the information on such sources is likely to be discoverable and not available from reasonably accessible sources.").

7 Moore's Federal Practice § 37A.12[5][e] (3d ed. 2006) ("The routine recycling of magnetic tapes that may contain relevant evidence should be immediately halted on commencement of litigation.").

36 C.F.R. 1234.24(c)(2006) ("[B]ackup tapes should not be used for recordkeeping purposes.").

McPeek v. Ashcroft, 202 F.R.D. 31, 33 (D.D.C. 2001) ("There is certainly no controlling authority for the proposition that restoring all backup tapes is necessary in every case. The Federal Rules do not require such a search, and the handful of cases is idiosyncratic and provides little guidance.").

Zubulake v. UBS Warburg LLC, 220 F.R.D. 212, 217-18 (S.D.N.Y. 2004) (*"Zubulake IV"*) (concluding that "'as a general rule, then, a party need not preserve all backup tapes even when it reasonably anticipates litigation. … However, it does make sense to create one exception to this general rule. If a company can identify where particular employee documents are stored on backup tapes, then the tapes storing the documents of 'key players' to the existing or threatened litigation should be preserved if the information contained on those tapes is not otherwise available.").

Comment 5.i. Preservation of shared and orphaned data

An organization's networks or intranet may contain shared areas (such as public folders, discussion databases and shared network folders) that are not regarded as belonging to any specific employee. There are also collaborative work space areas (such as blogs, wikis, and intranet sites) where there is no one "owner" of the data within the organization. Such areas should be considered in the preservation and analysis to determine if they contain potentially relevant information and, if so, appropriate steps should be taken to preserve the relevant information.

If an organization maintains archival data on tapes or other offline media not accessible to end users of computer systems, steps should promptly be taken to preserve those archival media that are reasonably likely to contain relevant information not also present as active data on the organization's systems. These steps may include notifying persons responsible for managing archival systems to retain tapes or other media as appropriate.

6. Responding parties are best situated to evaluate the procedures, methodologies, and technologies appropriate for preserving and producing their own electronically stored information.

Comment 6.a. The producing party should determine the best and most reasonable way to locate and produce relevant information in discovery

It is the responsibility of the producing party to determine what is responsive to discovery demands and to make adequate arrangements to preserve and produce relevant information. There are various ways to manage electronic documents, and thus many ways in which a party may comply with its obligations. The failure to do so in an organized and methodical fashion, however, has led some courts to impose penalties upon both the party and the responsible employee.

Typically, the producing party identifies and informs the key individuals likely to have relevant information of the specific need to preserve all available relevant information – this instruction is sometimes referred to as a "litigation hold notice." Thereafter, the lawyers supervise the collection of the relevant information from custodians and other sources. The party then conducts a review for privilege, trade secrets, or other appropriate bases for nonproduction and takes reasonable steps to facilitate production A producing party should not be required to undertake more heroic efforts merely because the party seeking discovery is suspicious of the efforts undertaken by the producing party.

RESOURCES AND AUTHORITIES

In re Ford Motor Co., 345 F.3d 1315, 1317 (11th Cir. 2003) (stating that the producing party's choice to review database and only produce those relevant portions was adequate discovery response absent specific evidence to the contrary).

Comment 6.b. Scope of collection of electronically stored information

When responding to discovery requests, organizations should define the scope of the electronically stored information needed to appropriately and fairly address the issues in the case and to avoid unreasonable overbreadth, burden, and cost. Important steps in achieving the goal of reasonably limiting discovery may include: (1) collecting electronically stored information from repositories used by key individuals rather than generally searching through the entire organization's electronic information systems; (2) defining the information to be collected by applying reasonable selection criteria, including search terms, date restrictions, or folder designations; or (3) avoiding collection efforts that are disproportionate to, or are inappropriate in, the context of a particular litigation.

Discovery should not be permitted to continue indefinitely merely because a requesting party can point to undiscovered documents and electronically stored information when there is no indication that the documents or information are relevant to the case, or further discovery is disproportionate to the needs of the case.

> *Illustration i.* A party seeking access to email relevant to the case demands that it be permitted to copy and inspect the active email accounts of all users. The request should be denied. The producing party is in the best position to determine how to comply with its discovery obligations. Electronic information that is not deemed relevant should not be subject to inspection by the requesting party. The Rules do not create the right to a fishing expedition merely because the information sought is in electronic form. The concept of relevance is no broader or narrower in the electronic context than in the paper context.

RESOURCES AND AUTHORITIES

Fennell v. First Step Designs, Ltd., 83 F.3d 526, 532-33 (1st Cir. 1996) (affirming order denying electronic discovery where that discovery would be a "fishing expedition").

Comment 6.c. Rule 34 inspections

Inspection of an opposing party's computer system under Rule 34 and state equivalents should be the exception and not the rule for discovery of electronically stored information. Usually, the issues in litigation relate to the informational content of the data stored on computer systems, not the actual operations of the systems. Therefore, in most cases, if the producing party provides the informational content of the data, there is no need or justification for direct inspection of the respondent's computer systems. A Rule 34 inspection presents possible concerns such as:

a) revealing trade secrets
b) revealing other highly confidential or private information, such as personnel evaluations and payroll information, properly private to individual employees
c) revealing confidential attorney-client or work-product communications
d) unreasonably disrupting the ongoing business; and
e) endangering the stability of operating systems, software applications, and electronic files if certain procedures or software are used inappropriately.

Further, Rule 34 inspections of electronically stored information are likely to be particularly ineffective. The standard form of production, in which the producing party identifies and produces responsive information, allows the party with the greatest knowledge of the computer systems to search and utilize the systems to produce responsive information. A Rule 34 inspection, in contrast, requires persons unfamiliar with the party's recordkeeping systems, hardware, and software to attempt to manipulate the systems. Not only is such a process disruptive, it is less likely to be fruitful. In most cases, producing parties will be able to argue persuasively that their production of relevant electronically stored information from computer systems and databases was sufficient to discharge their discovery obligations.

To justify the onsite inspection of respondent's computer systems, a party should be required to demonstrate that there is a substantial need to discover information about the computer system and programs used (as opposed to the data stored on that system) and that there is no reasonable alternative to an onsite inspection. Any inspection procedure should: (1) be documented in an agreed-upon (and/or court-ordered) protocol; (2) recognize the rights of nonparties, such as employees, patients, and other entities; and (3) be narrowly restricted to protect confidential and personally identifiable information and system integrity as well as to avoid giving the discovering party access to information unrelated to the litigation. Further, no inspection should be permitted to proceed until the producing party has had a fair opportunity to review the information subject to inspection. Where the requesting party makes the required showing to justify inspection of the other party's systems, the information subject to inspection should be dealt with in such a manner as to preserve the producing party's rights and obligations, for example, through the use of "neutral" court-appointed consultants.

RESOURCES AND AUTHORITIES

In re Ford Motor Co., 345 F.3d 1315, 1317 (11th Cir. 2003) (district court abused discretion in granting *ex parte* motion to compel access to defendant's databases; noting that granting a motion to inspect the databases requires a discussion of whether the defendant failed to comply with the original discovery requests, the validity of defendant's objections to the request, and any protocols or limits needed to narrow the scope of the search).

Comment 6.d. Use and role of consultants and vendors

Responding parties may consider retaining consultants and vendors to assist them in preserving and producing their electronically stored information. Due to the complexity of electronic discovery, many organizations rely on consultants to provide a variety of services, including discovery planning, data collection, specialized data processing, and forensic analysis. Such consultants can be of great assistance to parties and courts in providing technical expertise and experience with the collection, review, and production of electronically stored information. However, parties should carefully consider the experience and expertise of a potential consultant before his or her selection, as standards for experts and consultants in this field have not been fully developed. Vendors offer a variety of software and services to assist with the electronic discovery process and a party's evaluation of vendor software and services should include the defensibility of the process in the litigation context, the cost, and the experience of the vendor. Ultimate responsibility for ensuring the preservation, collection, processing, and production of electronically stored information rests with the party and its counsel, not with the nonparty consultant or vendor.

At all times, counsel, clients, and vendors must understand everyone's role in the discovery process. Thus, even if a vendor is retained to serve in a non-testifying capacity, everyone should be aware of the potential need for testimony if forensic or other technical expertise is required to prepare electronically stored information for review or production. Additionally, care should be taken to ensure that the vendor does not assume the role of a legal advisor, and that all persons involved understand what communications are protected under the attorney-client privilege and what information may be protected as attorney work product.

For an additional discussion of this issue, see *Comment 10.c. (Use of special masters and court-appointed experts to preserve privilege).*

RESOURCES AND AUTHORITIES

N.Y. Bar Ass'n Formal Op. 2006-3 (concluding that where an outsourcing assignment requires a lawyer to disclose client confidences or secrets to an overseas non-lawyer, the lawyer must secure the client's informed consent in advance and must be mindful of different laws and traditions regarding the confidentiality of client information that exist overseas).

Gates Rubber Co. v. Bando Chem. Indus., Ltd., 167 F.R.D. 90, 100 (D. Colo. 1996) (appointing special master to secure materials from alleged destruction and simultaneously protect the rights of producing party to object to the production of certain materials under the usual rules of discovery).

Comment 6.e. Documentation and validation of collection procedures for electronically stored information

In developing collection procedures for electronically stored information, organizations should consider the appropriate scope of the collection, the cost of the collection, the burden on and disruption of normal business activities, and the defensibility of the process itself. All collection processes should be accompanied by documentation and validation appropriate to the needs of the particular case. Well-documented collection and production procedures enable an organization to respond to challenges – even those made years later – to the collection process, to avoid overlooking electronically stored information that should be collected, and to avoid collecting electronically stored information that is neither relevant nor responsive to the matter at issue. The documentation of the collection process should describe what is being collected, the procedures employed and steps taken to ensure the integrity of the information collected. Finally, this documentation should be revised as the organization introduces new or different technology.

Comment 6.f. Role of and risks to counsel regarding the preservation and production of electronically stored information

Generally speaking, the obligation to preserve and produce discoverable electronically stored information runs to and must be executed by parties to an action. However, counsel (both inside and outside) have very practical ethical and other responsibilities to ensure that the efforts to preserve and produce electronically stored information comply with the applicable requirements. While it is generally sufficient for counsel to furnish advice to clients and rely upon them to meet their obligations, courts have suggested that counsel has independent duties of supervision and, in some cases, of participation in the preservation and production process. Under the reasoning of those decisions, counsel must supervise the implementation of preservation or collection efforts of clients.

The volume and dynamic nature of electronic information make discovery more complex and difficult. The increased risks created by these complexities require both inside and retained counsel to meet a high standard of care in regard to discovery of electronically stored information. For cases pending in the federal courts, Rule 26(f)'s early meet and confer obligations and the affirmative disclosure obligations of Rule 26(b)(2)(B) ("identification" of sources not reasonably accessible because of undue burden and cost) imply that counsel must undertake early preparation sufficiently diligent to adequately represent the parties' positions. This position is reinforced by the Committee Notes to Rule 26(f), district court local rules, and court decisions.

Similar requirements exist in state courts. For example, the Guidelines for State Trial Courts Regarding Discovery of Electronically Stored Information (Guideline 2) recommend that a judge should "encourage" counsel to become familiar with the operation of the relevant information management systems, including how information is stored and retrieved.

The enhanced possibility of inadvertent production of privileged or work product information, the stakes in the management of privilege reviews, and careless handling of client communications raise serious ethical issues. Similarly, the disparate views on how lawyers should treat metadata (e.g., when to delete, when to send, when to review) create additional risks for lawyers, especially in cases across different jurisdictions.

RESOURCES AND AUTHORITIES

D. Kan. *Guidelines for Discovery of Electronically Stored Information* (parties have a duty to discuss the preservation of electronically stored information during the Fed. R. Civ. P. 26(f) conference).

D.N.J. L. R. 26.1(d) (parties have a duty to discuss the preservation of electronically stored information during the Fed. R. Civ. P. 26(f) conference).

Gregory G. Wrobel, *et al., Counsel Beware: Preventing Spoliation of Electronic Evidence in Antitrust Litigation,* 20-SUM Antitrust 79, 80 (2006).

ABA Civil Discovery Standards (1999) (rev. Aug. 2004) *available at* http://www.abanet.org/litigation/decisionstandard/2004civildiscoverystandards.pdf (discussion of duty of counsel).

Model Rules of Prof'l Conduct R. 3.4.("A lawyer shall not unlawfully obstruct another party's access to evidence or unlawfully alter, destroy or conceal a document or other material having potential evidentiary value.").

Compare, e.g., Maryland Bar Assoc. Comm. on Ethics Op. 2007-09 (Maryland lawyers who produce electronic materials in discovery have the professional duty to take reasonable measures to avoid the disclosure of confidential information embedded in metadata within the document; lawyers who receive electronic discovery materials have no ethical duty to refrain from viewing or using metadata; recent amendments to the Federal Rules of Civil Procedure regarding electronic discovery will impact the obligations of lawyers) *with* Florida Bar Opinion 06-02, ABA Comm. on Eth. & Prof'l Resp., Formal Op. 06-422 (2006), and NYSB Opinion 749 (a lawyer has both a duty to refrain from reviewing or using metadata and a duty to notify an adversary of inadvertent production).

In re Grand Jury Investigation, 445 F.3d 266, 275 (3rd Cir. 2006), *cert. denied, Doe v. United States,* 127 S.Ct. 538 (2006) (contents of discussions not privileged when the client may be committing crime of obstruction of justice by participating in a scheme to delete emails after receiving information from counsel about scope of pending subpoena).

Metro. Opera Ass'n, Inc. v. Local 100 Hotel Employees & Rest. Employees Int'l Union, 212 F.R.D. 178, 230 (S.D.N.Y. 2003) (finding that "the combination of outrages perpetrated by the [defendant] and its counsel, by both omission and commission" warranted the most severe sanction, and entered a judgment of liability against the defendant based on, inter alia, Rule 26(g) and inherent power of the court.), adhered to in *Metro. Opera Ass'n, Inc. v. Local 100 Hotel Employees & Rest. Employees Int'l Union, No. 00 Civ. 3613*(LAP), 2004 WL 1943099, at *8-9 (S.D.N.Y. Aug. 27, 2004) (affirming that sanctions under Rule 26(g) are imposed when a competent attorney could not have believed a filing was well grounded in fact and warranted in law).

Zubulake v. UBS Warburg LLC, 229 F.R.D. 422, 432-34 (S.D.N.Y. 2004) (*"Zubulake V"*) (counsel has obligation to work with client to identify all potential sources of relevant information; party sanctioned for, destruction of documents after being told repeatedly by counsel not to do so, and counsel's failure to identify key witnesses).

7. The requesting party has the burden on a motion to compel to show that the responding party's steps to preserve and produce relevant electronically stored information were inadequate.

Comment 7.a. Resolving discovery disputes

A party that receives a request for production of electronically stored information may object to some or all of the request, or may produce information that the requesting party deems inadequate or nonresponsive. This may prompt the requesting party to consider filing a motion to compel production. In cases governed by the Federal Rules, such a motion would be filed under Rule 37(a), which requires the moving party to certify that good-faith efforts have been made to resolve the dispute before resorting to the court. Fed R. Civ. P. 37 (a)(2)(A).

On a motion to compel, the moving party must demonstrate that the producing party's response to the discovery request, including its steps to preserve and produce electronically stored information, was inadequate, and that additional efforts are warranted. In so doing, a court should consider the balancing principles of Sedona Principle 2 and the proportionality limits of Rule 26(b)(2)(C), especially with respect to the technological feasibility and realistic costs of preserving, retrieving, producing, and reviewing electronically stored information.

Rule 26(b)(2)(B) establishes a procedure to resolve disputes regarding discovery from sources the responding party has identified as "not reasonably accessible" because of "undue burden or cost." This is discussed at Comment 2.c. Rule 26(c) establishes a procedure for obtaining a protective order to relieve a responding party from "undue burden or expense." Under either rule, the burden is on the responding party to establish the grounds for limiting discovery.

RESOURCES AND AUTHORITIES

Report of the Civil Rules Advisory Committee, May 27, 2005 (rev. July 25, 2005), *available at* http://www.uscourts.gov/rules/reports/st90-2005.pdf.

Comment 7.b. Discovery from non-parties

Electronically stored information may also be secured from nonparties by service of a subpoena or other process authorized by the relevant court procedures. Requesting parties must be sensitive to the burdens that such discovery places on nonparties.

In cases governed by the Federal Rules, Rule 45 has been explicitly extended to include electronically stored information within the scope of the types of information the inspection or production of which may be demanded. A party issuing the subpoena may indicate the form or forms in which production is to be made and the nonparty subject to the subpoena has the same rights and obligations in regard to production as parties. One major exception, of course, is that there is no mandatory discussion, prior to discovery, of a discovery plan or the opportunity to meet and discuss preservation or other key topics. The intent of the Advisory Committee was that parties issuing and responding to subpoenas would avail themselves of such an opportunity informally, a best practice that should be followed in most cases.

Under a 1991 amendment to the Federal Rules of Civil Procedure, Rule 45(c)(1) added a requirement not generally available to party litigants to the effect that the issuing party must "take reasonable steps to avoid imposing undue burden or expense on a person subject to the subpoena." Equally important, Rule 45(c)(2)(B) provides that, if objection is made to a subpoena, "an order to compel production *shall protect* any person who is not a party or an officer of a party from significant expense resulting from the inspection and copying commanded." (Emphasis supplied).

Courts balance the cost, burden, and need for discovery from nonparties when considering whether to quash or modify the discovery sought, or to shift some or all of the costs associated with requests for production of electronically stored information. (For cost-shifting standards on non-party subpoenas, *see* Comment 13.c.).

Excessively broad electronic document production requests directed to third parties can also lead to sanctions under Rule 45 and to liability under federal statutes protecting the privacy of electronic communications. As a result, requesting parties must carefully tailor requests directed to nonparties and should undertake efforts to negotiate with them the scope of the electronically stored information requested and the manner of production.

RESOURCES AND AUTHORITIES

Kenneth J. Withers, *Electronically Stored Information: The December 2006 Amendments to the Federal Rules of Civil Procedure,* 4 Nw. J.Tech. & Intell. Prop. 171, 205 (2006) *available at* http://www.law.northwestern.edu/journals/njtip/v4/n2/3.

Nicholas v. Wyndham Int'l., Inc., 373 F.3d 537, 543 (4th Cir. 2004). ("District court's denial of discovery from nonparty [corporation owned by plaintiffs], which was sought in ancillary proceeding by defendant in underlying proceeding pending in district outside the instant circuit, was immediately appealable, under collateral order doctrine, since review of denial would not be available via either appeal or contempt proceedings." However, court denied the defendant's request for discovery from non-party corporation owned by plaintiffs where plaintiffs had already been deposed and produced more than 400 pages of emails, including some from their corporation's account, and defendant's counsel conceded to the district court that non-party corporation "could have no more information about the facts of liability and damages than Plaintiffs themselves had.").

Theofel v. Farey-Jones, 341 F.3d 978 (9th Cir. 2003), amended, 359 F.3d 1066, 1073-74 (9th Cir. 2004) (holding that service of an overbroad, "patently unlawful" subpoena on a party's ISP, which led to the disclosure of private and privileged communications, violated the Stored Communications Act 18 U.S.C. § 2701(a) (2004), which provides a cause of action against anyone who intentionally accesses without authorization a facility through which an electronic communication service is provided or intentionally exceeds an authorization to access that facility and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage. 18 U.S.C. § 1030(a)(2)(C) (2004) provides a cause of action against one who intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains information from any protected computer if the conduct involved any interstate or foreign communication, 18 U.S.C. § 2701 *et seq.,* and the Computer Fraud and Abuse Act, U.S.C. § 1030 (2004).

8. The primary source of electronically stored information for production should be active data and information. Resort to disaster recovery backup tapes and other sources of electronically stored information that are not reasonably accessible requires the requesting party to demonstrate need and relevance that outweigh the costs and burdens of retrieving and processing the electronically stored information from such sources, including the disruption of business and information management activities.

Comment 8.a. Scope of search for active and purposely stored data

The scope of a search for relevant electronically stored information must be reasonable. For example, potentially relevant information may be located or reside on local and network computers, laptop computers, servers, handheld or portable storage devices (such as PDAs and flash memory drives), archive and backup data tapes, cellular phones, voicemail systems, or closed-circuit television monitoring systems.

However, it is neither feasible nor reasonable to require that litigants immediately or always canvas all potential reservoirs of electronically stored information in responding to preservation obligations and discovery requests. Many locations or sources will contain duplicative or redundant information, and many others may contain massive amounts of information not relevant to the claims and defenses in the case.

Accordingly, litigants and courts must exercise judgment, made upon reasonable inquiry and in good faith, about the active and purposely stored data locations that should be subject to preservation efforts. If the producing party is aware (or reasonably should be aware) that specific relevant information can only be obtained from a particular source, that information or the source on which it is located should be preserved for possible production absent agreement of the parties or order of the court. The mere suspicion that a source may contain potentially relevant information is not sufficient to demand the preservation of that source "just in case." Rather, the appropriate standard should be to preserve information on and search sources where the producing party is reasonably likely to locate potentially relevant information not available from other available, searched sources.

Resorting to sources that are not reasonably accessible, while certainly possible under some circumstances, should be required only on a showing of good cause, with the requesting party bearing the burden to show good cause on a motion to compel or in a hearing on a protective order. Production from such less accessible sources is subject to meeting the balancing or proportionality standards set forth in Principle 2, *supra*.

> *Illustration i.* A party seeking relevant emails demands a search of backup tapes and hard drives for deleted materials. No showing of special need or justification is made for the search. The request should be denied. Parties are not typically required to sequester and search the trash bin outside an office building after commencement of litigation; neither should they be required to preserve and produce deleted electronic information in the normal case. Production should primarily be from sources of active information which is arranged in a manner conducive to retrieval and storage.
>
> *Illustration ii.* After a key employee leaves X Company ("X Co.") to work for a competitor, a suspiciously similar competitive product suddenly emerges from the new company. X Co. produces credible testimony that the former employee bragged about sending confidential design specifications to his new company computer, copying the data to a CD, and deleting the data so that the evidence would never be found. The court properly orders that, given the circumstances of the case, the requesting party has demonstrated the need for the computer to be produced for mirror image copying of its hard drive. If the defendant is not willing to undertake the expense of hiring its own reputable data recovery expert to produce all available relevant data, inspection of the computer's contents by an expert working on behalf of X Co. may be justified, subject to appropriate orders to preserve privacy, to protect data, and to prevent production of unrelated or privileged material. Under a showing of special need, with appropriate orders of protection, extraordinary efforts to restore electronic information could also be ordered.

For a discussion of the limitations under the 2006 Amendments on initial discovery from sources that are not reasonably accessible because of undue burden or cost, see *Comment 8.b.*

RESOURCES AND AUTHORITIES

Conference of Chief Justices, *Guidelines for State Trial Courts Regarding Discovery of Electronically Stored Information,* Guideline 5 (Aug. 2006) (judges should first assess if the electronically stored information is discoverable and then balance the benefits and burdens of requiring discovery based on a multi-factor analysis rather than presumptions regarding accessible or active data).

ABA Civil Discovery Standards (1999) (rev. Aug. 2004) Standard 29(b)(iv) *available at* http://www.abanet.org/litigation/discoverystandards/2004civildiscoverystandards.pdf (listing factors for a court to consider in deciding whether to limit discovery of Electronically Stored Information and allocate costs).

Comment 8.b. Production from sources that are not reasonably accessible

The 2006 Amendments to the Federal Rules limits the obligation to search and produce from sources of relevant electronically stored information that is not reasonably accessible due to undue burden or cost. This limitation in Fed. R. Civ. P. 26(b)(2)(B) is a specific invocation of the proportionality rules embodied in Rule 26(b)(2)(C).

Whether a source is "reasonably accessible" does not solely depend on the technology required to access that information, but is more closely related to the costs and burdens involved in accessing and retrieving the information. The Advisory Committee gives, as examples from current technology, "backup tapes" intended for disaster recovery purposes that are often not indexed, organized, or susceptible to electronic searching; legacy data that remains from obsolete systems and is unintelligible on the successor systems; data that was "deleted" but remains in fragmented form requiring a modern version of forensics to restore and retrieve; and databases that were designed to create certain information in certain ways and that cannot readily create very different kinds or forms of information.

The "accessibility" limitation is similar to but different from the production limitation found in Principle 8, which also addresses the technical accessibility and the purpose of the storage, rather than simply the burdens and costs associated with access.

Rule 26(b)(2)(B) of the amended Federal Rules requires the producing party to identify by category or type any sources of relevant electronically stored information that it has identified as "not reasonably accessible." Specifically, this requires that if a party has determined that the only source of some relevant electronically stored information is one that is not reasonably accessible, then it must preserve that source, disclose it (with enough information so the other side can understand what is at issue), be ready to demonstrate why production of information is unduly burdensome or expensive, and, if possible, discuss these issues at the initial Rule 26(f) meet and confer sessions. This requirement should not be read as a mandate to list all sources of electronically stored information that are not searched, nor does it require a listing of such sources if a party has reasonably determined, in good faith, that the inaccessible source does not contain nonduplicative relevant information. However, a party may not deliberately make information inaccessible for the sole purpose of avoiding litigation discovery requests specific to a known case.

If the parties are unable to reach agreement as to the accessibility of specific sources of electronically stored information or the need to restore those sources for purposes of the dispute at issue, a motion to compel or for a protective order may be brought. This procedure is discussed in Comment 2.c.

For discussion of the use of cost-shifting in electronic discovery, see *Principle 13,* infra.

RESOURCES AND AUTHORITIES

Report of the Civil Rules Advisory Committee May 27, 2005 (rev. July 25, 2005), C. 42, *available at* http://www.uscourts.gov/rules/reports/st09-2005.pdf. ("[t]he rule requires that the information identified as not reasonably accessible must be difficult to access by the producing party for all purposes, not for a particular litigation. A party that makes information 'inaccessible' because it is likely to be discoverable in litigation is subject to sanctions now and would still be subject to sanctions under the proposed rule changes.").

Charles Alan Wright, Arthur R. Miller, & Richard L. Marcus, *Federal Practice and Procedure* § 2008.2 (2d ed. 2006).

Conference of Chief Justices, *Guidelines for State Trial Courts Regarding Discovery of Electronically-Stored Information, Guideline 1(a)* (Aug. 2006) (defining "accessible" information as "electronically-stored information that is easily retrievable in the ordinary course of business without undue cost and burden").

Thomas Y. Allman, *The Impact of the Proposed Federal E-Discovery Rules,* 12 Rich. J.L. & Tech. 13 (2006).

Hon. Anthony J. Battaglia, *Dealing with Electronically Stored Information: Preservation, Production, and Privilege,* 53 Fed. Law. 26 (May 2006).

Kenneth J. Withers, *Electronically Stored Information: The December 2006 Amendments to the Federal Rules of Civil Procedure,* 4 Nw. J. Tech. & Intell. Prop. 171 (2006), *available at* http://www..law.northwestern.edu/journals/njtip/v4/n2/3.

Tex. R. Civ. P. 194.6 ("[T]he requesting party must specifically request production of electronic or magnetic data and specify the form in which the requesting party wants it produced. The responding party must produce the electronic or magnetic data that is responsive to the request and is reasonably available to the responding party in its ordinary course of business.").

Zubulake v. UBS Warburg LLC, 217 F.R.D. 309, 319-20 n.61 (S.D.N.Y. 2003) (*"Zubulake I"*) (noting that consideration of cost-shifting is appropriate where stored data is not in a "readily usable" format, such as backup tapes; noting that Sedona Principles 8 and 9 recognize the distinction between "active data" and backup tapes in a manner very similar to the test employed in the instant case).

Comment 8.c. Forensic data collection

Intrusive access to desktop, server, laptop or other hard drives or media storage devices is sometimes ordered when key employees leave employment under suspicious circumstances, or if theft or misappropriation of trade secrets or confidential information may be involved. However, making forensic image backups of computers is only the first step of an expensive, complex, and difficult process of data analysis that can divert litigation into side issues and satellite disputes involving the interpretation of potentially ambiguous forensic evidence. While such an approach is clearly appropriate in some circumstances, it should not be required unless exceptional circumstances warrant the extraordinary cost and burden. When ordered, it should be accompanied by an appropriate protocol or other protective measures that take into account privacy rights, attorney-client privilege, and the need to separate out and ignore nonrelevant information. In some cases, it may be necessary, as an anticipatory matter, to meet certain preservation obligations by making or retaining copies of backup tapes or taking such steps as imaging the computer hard drives of departing employees, if appropriate. Such copies may best preserve all possibly relevant data. If the parties anticipate such a need, the topic of forensic-level preservation and review should be addressed at the initial meet and confer sessions.

The 2006 amendments to the Federal Rules clarify that the right to test, sample or inspect electronically stored information or gain access to computer systems or hard drives is within the scope of a discovery request, but is subject to protection from undue intrusiveness and with due respect for burdens and issues of confidentiality and privacy.

RESOURCES AND AUTHORITIES

Report of the Civil Rules Advisory Committee, May 27, 2005 (rev. July 25, 2005), *available at* http://www.uscourts.gov/rules/reports/st09-2005.pdf.

In re Ford Motor Co., 345 F.3d 1315, 1317 (11th Cir. 2003) (granting mandamus to prevent implementation of district court order allowing inspection of databases as an abuse of discretion).

McPeek v. Ashcroft, 212 F.R.D., 33, 36 (D.D.C. 2003) (declining to order searches of backup tapes where plaintiff had not demonstrated a likelihood of obtaining relevant information).

Comment 8.d. Outsourcing vendors and non-party custodians of data

The scope of discovery and the duty to preserve and produce information extend to relevant electronically stored information under the custody and control of a party, including information that a nonparty such as an information technology service provider or data processing contractor may possess. Many organizations outsource all or part of their information technology systems or share data with third parties for processing or for other business purposes. In contracting for such services, organizations should consider how they will comply with their obligations to preserve and collect electronic data for litigation. If such provisions are not within the scope of contractual agreements, costs may escalate and necessary services, including access to relevant data, may be unavailable when needed. Organizations also need to consider whether notice should be sent to nonparties, such as contractors and vendors, when litigation commences, particularly because such nonparties may not otherwise be aware of litigation or attendant preservation obligations.

RESOURCES AND AUTHORITIES

Keir v. UnumProvident Corp., No. 02 Civ. 8781, 2003 WL 21997747, at *12-13 (S.D.N.Y. Aug. 22, 2003) (finding that defendant's failure to timely notify its IT vendor of preservation order contributed to loss of responsive data).

9. Absent a showing of special need and relevance, a responding party should not be required to preserve, review, or produce deleted, shadowed, fragmented, or residual electronically stored information.

Comment 9.a. The scope of discovery of electronically stored information

At the outset of litigation parties should consider the potential need for preservation and production of electronically stored information that is not readily apparent to ordinary employees and records custodians and be prepared to discuss the matter at the initial meet and confer session. Such information includes system data as well as deleted, shadowed, fragmented, or residual information. A party seeking such information should articulate good cause for such preservation and production. The producing party should have a good understanding of the available electronically stored information and be able to argue the costs and burdens in the context of the case, including the relevance (and lack thereof) of the information to the claims and defenses in the case. In framing these positions, both sides should also consider the potential value of such information to the usability of any production separate and apart from the substantive relevance of the contents to the merits.

> *Illustration i.* Plaintiff claims that she is entitled to a commission on a transaction, based upon an email allegedly sent by the president of defendant corporation agreeing to the commission. Defendant asserts that there is no record of the email being sent in its email system or the logs of its Internet activity, and that the email is not authentic. In these circumstances, it is appropriate to require production of not only the content of the questioned email, but also of the email header information and metadata, which can play a crucial role in determining whether the questioned message is authentic.
>
> *Illustration ii.* Plaintiff alleges that the defendant engaged in billing fraud by overcharging for hourly work done for another client. The plaintiff presents two copies of an invoice indicating material differences. In this case, discovery of overwritten drafts, edits and deleted versions of the invoices may be appropriate.

RESOURCES AND AUTHORITIES

Concord Boat Corp. v. Brunswick Corp., No. LR-C-95-781, 1997 WL 33352759, at *9 (E.D. Ark. Aug. 29, 1997) ("Fourteen days worth of email, which might contain a few deleted emails, seems to hardly justify the expense necessary to obtain it. Similarly, even if earlier back up tapes containing 'snapshots' of the system were in existence, the potential limited gains from a search of such tapes would be outweighed by the substantial burden and expense of conducting the search. Accordingly, the Court finds that Defendant will not be required to restore and search any available back up tapes which might contain deleted [ ] email.").

McPeek v. Ashcroft, 202 F.R.D. 31, 33 (D.D.C. 2001) (rejecting notion that there is an absolute obligation to pursue potentially relevant data on backup tapes absent specific reason to do so).

Comment 9.b. Deleted electronically stored information

Deleted information may at one time have been a "useful" document generated in the ordinary course of business that had value to the organization, although that value may have expired. However, this historic fact alone does not justify the retrieval and review of deleted information. Case law indicates that only exceptional cases turn on "deleted" or "discarded" information (whether paper or electronic). Employees and organizations properly and routinely delete or destroy documents and electronically stored information that no longer have business value, so long as the information was not subject to regulatory, investigatory, or litigation preservation obligations when deleted or destroyed.

Accordingly, as a general rule and absent specific circumstances, organizations should not be required to preserve deleted electronically stored information in connection with litigation. While most computer systems will have a plethora of deleted information that could in theory be "mined," there should not be a routine obligation for such preservation and discovery. If, as usual, deleted information is not accessed by employees in the ordinary course of business, there is presumptively no reason to require the routine preservation of such information. The relevance will, at best, be marginal in most cases, while the burdens involved will usually be great. In exceptional cases, however, there may be good cause for targeted preservation of deleted and residual data.

Parties should communicate early about the possible relevance of deleted electronically stored information in order to avoid costly and unnecessary preservation, on one hand, or claims of spoliation, on the other.

For a related discussion of form or forms of production, including the preferred process for reaching agreement on these topics, see *generally Principle 12,* infra. *For a more specific discussion of forensic collection,* see *Principle 8 at Comment 8.c.*

RESOURCES AND AUTHORITIES

Charles Alan Wright, Arthur R. Miller, & Richard L. Marcus, *Federal Practice and Procedure* § 2008.2 (2d ed. 2006).

Tex. R. Civ. P. 196.4 ("The responding party must produce the electronic or magnetic data that is responsive to the request and is reasonably available to the responding party in its ordinary course of business. If the responding party cannot—through reasonable efforts—retrieve the data or information requested or produce it in the form requested, the responding party must state an objection complying with these rules.").

Shira A. Scheindlin & Jeffrey Rabkin, *Electronic Discovery in Federal Civil Litigation: Is Rule 34 Up to the Task?,* 41 B.C. L. Rev. 327, 372 (2000) (Under former Rule 34(a), "[e]mbedded data, Web caches, history, temporary, cookie and backup files—all of which are forms of electronically stored information automatically created by computer programs rather than by computer users—do not obviously fall within the scope of the term 'documents'.").

10. A responding party should follow reasonable procedures to protect privileges and objections in connection with the production of electronically stored information.

Comment 10.a. Potential waiver of confidentiality and privilege in production and the use of "clawback" agreements and procedures.

Because of the large volumes typically involved when electronically stored information is produced, parties should consider entering into agreements among themselves, including nonwaiver agreements, which outline the procedures to be followed to protect against any waiver of privileges or work product protection due to the inadvertent production of documents and data. Notably, the validity and impact of such nonwaiver agreements as to nonparties may vary greatly among jurisdictions. Similarly, the ethical obligations of counsel may vary. These nonwaiver agreements typically provide for the sequestering, return and/or destruction of the inadvertently produced information. Such agreement may include "clawback" arrangements that allow the producing party to "claw back" or "undo" the production. (As noted below, a "clawback" agreement is substantively different from a "quick peek" agreement. *See* Comment 10.d).

Counsel should discuss the need for such a provision at the outset of litigation and should approach the court for entry of an appropriate nonwaiver order. Under the 2006 Amendments, the discussions should take place at the Rule 26(f) conference and counsel can use Form 35 for inclusion in the Rule 16(b) Scheduling Order.

If an order is entered by a court endorsing the approach selected, the order should provide that the inadvertent disclosure of a privileged or work product document does not constitute a waiver of privilege, that the privileged document should be returned (or certification that it has been deleted), and that any notes or copies discussing the privileged or work product information will be destroyed or deleted.

The 2006 Amendments to the Federal Rules provide for a procedure whereby a claim of inadvertent production of privileged information or work product material can be made and the receiving party is obligated to sequester, destroy, or return the allegedly privileged information, or sequester it pending a court hearing. Fed. R. Civ. P. 26(b)(5). It is important to note that Rule 26(b)(5)(B) only provides the procedure for dealing with claims of inadvertent production and does not provide guidance regarding the substantive privilege law, including whether the inadvertent production results in waiver.

RESOURCES AND AUTHORITIES

Conference of Chief Justices, *Guidelines for State Trial Courts Regarding Discovery of Electronically Stored Information,* Guideline 4(D) (Aug. 2006) (parties should discuss procedures to be used if privileged electronically stored information is inadvertently disclosed); Guideline 8 (setting forth recommended factors for a court to use in determining if a party has waived the privilege because of an inadvertent disclosure).

ABA Civil Discovery Standard (1999)(rev. Aug. 2004) Standard 32(a), (c) and (e), *available at* http://www.abanet.org/litigaton/discoverystandards/2004civildiscoverystandards.pdf.

Charles Alan Wright, Arthur R. Miller, & Richard L. Marcus, *Federal Practice and Procedure* § 2016.3 (2d ed. 2006).

John M. Facciola, *Sailing on Confused Seas: Privilege Waiver and The New Federal Rules of Civil Procedure,* 2006 Fed. Cts. L. Rev. 6 (2006).

Joseph L. Paller Jr., *Gentlemen Do No Read Each Other's Mail: A Lawyer's Duties Upon Receipt of Inadvertently Disclosed Confidential Information,* 21 Lab. Law. 247 (Winter/Spring 2006).

Denis R. Kike, *Waiving the Privilege in a Storm of Data: An Argument for Uniformity and Rationality In Dealing with the Inadvertent Production of Privileged Materials in the Age of Electronically Stored Information,* 12 Rich. J.L. & Tech. 15 (2005).

John K. Villa, *The Inadvertent Disclosure of Privileged Material: What is the Effect on the Privilege and the Duty of Receiving Counsel?* 22 No. 9 ACC Docket 108 (Oct. 2004).

Jonathan M. Redgrave & Kristin M. Nimsger, *Electronic Discovery and Inadvertent Productions of Privileged Documents,* 49 Fed. Law. 37 (July 2002).

In re Qwest Communications Int'l, Inc. Sec. Litig., 450 F.3d 1179, 1200 (10th Cir. 2006) (refusing mandamus request regarding the order compelling disclosure in discovery of information furnished to government because of waiver of privilege; refusing to recognize "selective" waiver concept).

Hopson v. Mayor and City Council of Baltimore, 232 F.R.D. 228, 239-41 (D. Md. 2005) (arguing that risks of inadvertent waiver can be mitigated through use of scheduling orders, protective orders or discovery management orders agreed to by the parties and determined reasonable by the courts that protect produced documents from waiver; court further notes that such agreements will not excuse parties from making reasonable pre-production efforts to protect privileged material and recommends parties assume complete pre-production privilege review as required unless such review can be shown with particularity to be unduly burdensome or expensive).

Comment 10.b. Protection of confidentiality and privilege regarding direct access to electronically stored information or systems

Special issues may arise with any request to secure direct access to electronically stored information or to computer devices or systems on which it resides. Protective orders should be in place to guard against any release of proprietary, confidential, or personal electronically stored information accessible to the adversary or its expert.

Similar concerns exist regarding the potential disclosure of attorney-client privileged or work product information that may occur during such an inspection. There is no guarantee that a nonwaiver order in one jurisdiction will be fully honored in another if protected information is disclosed. Accordingly, even with a protective order in place, court-ordered inspections of computer systems should be used sparingly. Further, such orders should be narrowly tailored to the circumstances and accompanied by a sufficient protective order.

The 2006 Amendments to Rule 34(a) clarify that the right to "test or sample," as well as the right to "inspect," extends to both electronically stored information and the system on which it is stored. The Committee Note makes it clear, however, that this change is "not meant to create a routine right of direct access to a party's electronic information system, although such access might be justified in some circumstances. The Note further states that the inspection or testing "may raise issues of confidentiality or privacy" and mandates that "[c]ourts should guard against undue intrusiveness resulting from inspecting or testing such systems." Fed. R. Civ. P. 34 Committee Note (2006).

The 2006 amendments also permit, but do not require or provide for a court to order, that a party may make available business records in the form of electronically stored information to enable an opponent to derive an interrogatory answer in lieu of the party answering. Fed. R. Civ. P. 33(d). The Committee Note restricts this option to situations in which the burden of deriving an answer is substantially the same for either party. The party electing to respond by referencing electronically stored information must do so in a way that allows the interrogating party to locate and identify the information as "readily as can the party served." The Note goes on to say that in some circumstances the ability to satisfy these circumstances may require the responding party to provide technical support, information on application software, or other assistance. In fact, the Note specifically cautions that if necessary to afford the requesting party an adequate opportunity to derive or ascertain the answer to the interrogatory, the party electing to reference electronically stored information "may be required to provide direct access to its electronic information system." Fed. R. Civ. P. 33(d) Committee Note (2006).

Because of the risk of unintended costs and opening IT infrastructures to opposing parties, parties and counsel should carefully consider if and when they will elect to refer to a production of electronically stored information in a Rule 33(d) election rather than providing a substantive response to the interrogatory. Indeed, the Committee Note to the Rule acknowledges that because of "the responding party's need to protect sensitive interests of confidentiality or privacy," the party may choose to derive the answer itself rather than invoke Rule 33(d).

RESOURCES AND AUTHORITIES

In re Ford Motor Co., 345 F.3d 1315, 1317 (11th Cir. 2003) (granting mandamus to prevent implementation of district court order allowing inspection of databases as an abuse of discretion).

Comment 10.c. Use of special masters and court-appointed experts to preserve privilege

In certain circumstances, a court may find it beneficial to appoint a "neutral" person (e.g., a special master or court-appointed expert) who can help mediate or manage electronic discovery issues. The December 1, 2003 amendment to Rule 53 (Special Masters) clarifies that special masters are available to federal courts to address electronic discovery issues in appropriate cases where the matters cannot be addressed effectively and timely by an available district or magistrate judge. *See* Fed. R. Civ. P. 53(a)(1)(C).

Using a court-appointed "neutral" person to mediate electronic discovery issues may prove beneficial for a number of reasons. First, using such a person to mediate disputes and, if necessary, conduct initial inspections of any disputed documents, generally eliminates any privilege-waiver concerns regarding such inspections. Second, the "neutral" person may be able to speed the resolution of disputes by fashioning fair and reasonable discovery plans based upon specialized knowledge of electronic discovery and/or technical issues in light of specific facts in the case. *See id.*

Special care should be used in crafting the appointment order (and any protective order) to tailor the scope of the appointment and to protect against the disclosure or loss of any privileges or protections. It should also be noted that such appointments likely will remain the exception, and not the rule, as most parties should be able to address electronic discovery issues through cooperative efforts in the disclosure and discovery process, and any remaining disputes often can be decided by an available district court or magistrate judge of the district.

RESOURCES AND AUTHORITIES

Shira A. Scheindlin and Jonathan M. Redgrave, *Revisions in Federal Rule 53 Provide New Options for Using Special Masters in Litigation,* 76 New York State Bar J. 18 (Jan. 2004).

Playboy Enters., Inc. v. Welles, 60 F. Supp. 2d 1050, 1055 (S.D. Cal. 1999) (use of computer specialist was appropriate to review hard drive for relevant data, and no view of privileged material by specialist would constitute waiver of privilege).

Comment 10.d. Protection of confidentiality and privilege regarding "quick peek" agreements

Given the enormous volume of electronic documents generated and retained in today's business environment, and in light of the demands of litigation, there is an increasing interest in production under a "quick peek" agreement to protect against waiver of confidentiality and privilege.

In a "quick peek" production, documents and electronically stored information are produced to the opposing party before being reviewed for privilege, confidentiality, or privacy. Such a production requires stringent guidelines and restrictions to prevent the waiver of confidentiality and privilege. Under a "quick peek" agreement, if the requesting party selects a document that appears to be privileged, the producing party can identify the document as privileged and withdraw it from production without having waived any privilege.

A "quick peek" procedure or order should not be lightly entered and requires the voluntary consent of the producing party. While providing the advantage of reducing the costs of preproduction reviews for privilege and confidentiality (and maybe even responsiveness), there are potential risks and problems that should be carefully considered.

First, the voluntary production of privileged and confidential materials to one's adversary, even in a restricted setting, is inconsistent with the tenets of privilege law that, while varying among jurisdictions, usually require the producing party to meticulously guard against the loss of secrecy for such materials. The fact that an adversary sees the voluntarily produced document in any circumstance arguably serves as a waiver or loss of privilege or protection.

Second, despite the strongest possible language in any "quick peek" order to protect against waiver of privileges, there is currently no effective way to extend the scope of the order to restrict persons who are non-parties to the agreement from seeking the production of privileged materials that have been produced under such an order. For example, parties in mass tort and product liability cases, who are subject to multiple suits by different counsel in different states, face the risk that their "quick peek" agreement entered in one action may not protect the party from waiver arguments in other actions, even if they have a strong protective order in the first action. Given the differences in privilege laws among jurisdictions, this uncertainty presents a serious and legitimate impediment to any widespread acceptance of a "quick peek." While the proposed Rule of Evidence 502 being discussed by the Advisory Committee may eventually result in a uniform federal and state approach to issues relating to such agreements on waiver, this is not the current situation.

Third, counsel have an ethical duty to guard zealously the confidences and secrets of their clients. It is possible that questions could arise as to whether voluntarily entering into a "quick peek" production could constitute a violation of Model Rule of Prof'l. Conduct R. 1.1 (2002)(requiring a lawyer to use diligence and care in representation) or Model Rule of Prof'l. Conduct R.1.6 (2002) (protection of client secrets and confidences) if the manner of the production results in later waivers of privileges and protections. While this may seem unlikely, it has already arisen in the context of inadvertent productions. D.C. Bar Ethics Opinion 256 (1995) (examining whether actions of producing counsel violated standard).

Fourth, the genie cannot be put back in the lamp. The disclosure of privileged communications and work product to an adversary can adversely affect the client's interest, notwithstanding non-waiver provisions.

Fifth, there are a host of issues regarding the possible privacy rights of employees and nonparties that may be implicated in a voluntary "quick peek" production. Careful consideration should be given to a company's privacy commitments to employees and customers, its contractual privacy agreements with nonparties, and judicial process exceptions within the applicable privacy laws or regulations before a party enters into a "quick peek" agreement.

Accordingly, given the possible loss of privilege and property rights that could accompany a waiver determination, courts should not compel use of a "quick peek" procedure over the objection of a producing party. Even when large volumes of electronic documents are involved, parties are well-advised to search for privileged documents.

In those very limited instances in which a "quick peek" order may be practicable and in the parties' interests (as reflected by voluntary consent), the court should enter an order that: (1) indicates that the court is compelling the manner of production; (2) states such production does not result in an express or implied waiver of any privilege or protection for the produced documents or any other documents; (3) directs that the reviewing party cannot discuss the contents of the documents or take any notes during the review process; (4) permits the reviewing party to select those documents that it believes are relevant to the case; and (5) orders that for each selected document, the producing party either (a) produces the selected document, (b) places the selected document on a privilege log, or (c) places the selected document on a non responsive log (i.e., regardless of the privileged status, the document is not relevant to the litigation.).

RESOURCES AND AUTHORITIES

Conference of Chief Justices, *Guidelines for State Trial Courts Regarding Discovery of Electronically Stored Information,* Guideline 4(D) (Aug. 2006) (advocating agreement for process to be used if privileged electronically stored information is inadvertently disclosed); Guideline 8 (setting forth recommended factors for a court to use in determining if a party has waived the privilege because of an inadvertent disclosure).

Report of the Advisory Committee on Evidence Rules, Proposed Rule 502(b) (June 30, 2006) *available at* http://www.aspenlawschoo.com/books/mueller_evidence/updates/excerp_ev_report_pub.pdf.

Charles Alan Wright, Arthur R. Miller, & Richard L. Marcus, *Federal Practice and Procedure* § 2016.3 (2d ed. 2006).

Kenneth S. Broun & Daniel J. Capra, *Getting Control of Waiver of Privilege in the Federal Courts: A Proposal for a Federal Rule of Evidence 502,* 58 S.C. L. Rev. 211 (2006).

John M. Facciola, *Sailing on Confused Seas: Privilege Waiver and the New Federal Rules of Civil Procedure,* 2006 Fed. Cts. L. Rev. 6 (2006).

Shira A. Scheindlin and Jonathan M. Redgrave, *Discovery of Electronic Information, in 2 Bus. & Commercial Litig. in Fed. Courts,* Ch 22 (Robert L. Haig ed. 2005 & Supp. 2006).

ABA Civil Discovery Standards (1999) (rev. Aug. 2004), Standard 32(d)(ii) and (f), *available at* http://www.abanet.org/litigaton/discoverystandards/2004civildiscoverystandards.pdf..

Transamerica Computer v. IBM, 573 F.2d 646, 651 (9th Cir. 1978) (finding no waiver of privilege when IBM produced privileged information without intending to waive privilege under "accelerated discovery proceedings [which] [i]mposed such incredible burdens on IBM" that they were "in a very practical way" compelled to produce privileged documents).

Hopson v. The Mayor and City Council of Baltimore, 232 F.R.D. 238 (D. Md. 2005) (reviewing the law of privilege waiver and the effect of clawback agreements, and formulating an order most likely to withstand anticipated challenges).

Murphy Oil USA, Inc. v. Fluor Daniel, Inc., No. Civ. A. 99-3564, 2002 WL 246439, at *7 (E.D. La. Feb. 19, 2002) (noting that court cannot compel the disclosure of privileged communications in clawback arrangement).

Comment 10.e. Privacy, trade secret, and other confidentiality concerns

Electronic information systems contain significant amounts of information that may be subject to trade secret, confidentiality, or privacy considerations. Examples of such information include proprietary business information such as formularies, business methods, sales strategies, marketing and forecasting projections, and customer and employee personal data (e.g., social security and credit card numbers, employee and patient health data, and customer financial records).

Privacy rights related to personal data may extend to customers, employees, and non-parties. Although the identification and protection of privacy rights are not directly addressed in the 2006 amendments, ample protection for such information during discovery is available through a Rule 26(c) protective order or by party agreement. In negotiating protections for such information, a party should consider the scope of the applicable privacy rights, as defined in the operative contract or rule of law, including whether such scope includes a judicial process exception. When potential discovery of documents or electronically stored information located outside of the United States is involved, the parties should pay specific attention to the foreign privacy or blocking statutes, for example, the Data Protection Act enacted by the European Union.

See also Comment 10b, *supra*, dealing with the confidentiality, privacy and privilege issues implicated under amended Rules 33(d) and 34(a) of the Federal Rules when direct access to business records are made available voluntarily or when a court is requested to order testing, sampling or inspection of electronically stored information or the information systems on which it resides.

RESOURCES AND AUTHORITIES

The Sedona Guidelines on Confidentiality and Public Access (2007), available at http://www.thesedonaconference.org.

11. A responding party may satisfy its good faith obligation to preserve and produce relevant electronically stored information by using electronic tools and processes, such as data sampling, searching, or the use of selection criteria, to identify data reasonably likely to contain relevant information.

Comment 11.a. Search method

In many cases, electronically stored information is found in broad groupings based on the "container" and not the "content," such as an email "inbox" or "outbox," or on a shared drive, or on a web server. In many instances, such unstructured or semi-structured data is not archived in a manner that can be used to readily identify relevant information.

Because of the enormous volume of information involved, as well as the cost and time savings made possible by technology, it is often advisable, if not necessary, to use technology tools to help search for, retrieve, and produce relevant information. For example, selective use of keyword searches can be a reasonable approach when dealing with large amounts of electronic data. Examples of search terms include the names of key personnel, date ranges, and terminology related to a specific event. It is also possible to use technology to search for "concepts," which can be based on ontologies, taxonomies, or data clustering approaches, for example.

Organizations should internally address search terms and other filtering criteria as soon as possible so that they can begin a dialogue on search methods as early as the initial discovery conference. Parties should understand the use of search methods may involve an iterative approach with search terms and concepts subject to expansion or refinement as the case progresses. Absent an agreement on the search methods to be used, parties should expect that their choice of search methods will need to be explained, either formally or informally, in subsequent legal contexts, including in depositions, evidentiary proceedings, and possibly even at trial.

> *Illustration i.* The relevant custodians each have 2 GB of information on their hard drives. Rather than read every file, the producing party reaches agreement with the requesting party on a series of search terms that capture the key concepts in the allegations of the complaint, combined with restrictions for the relevant time frame, to identify potentially responsive information. The party then reviews this subset to produce (or log) the relevant documents. The producing party has satisfied its search obligations.

Courts should encourage and promote the use of search and retrieval techniques in appropriate circumstances. For example, use of search terms could reveal that a very low percentage of files (such as emails and attachments) on a data tape contain terms that are responsive to "key" terms. This may weigh heavily against a need to further search that source, or it may be a factor in a cost-shifting analysis. Such techniques may also reveal substantial redundancy between sources (i.e., duplicate data is found in both locations) such that it is reasonable for the organization to preserve and produce data from only one of the sources. *See* Comment 11.c., *infra*.

Ideally, the parties should agree on the search methods, including search terms or concepts, to be used as early as practicable. Such agreement should take account of the iterative nature of the discovery process and allow for refinement as the parties' understanding of the relevant issues develops. The search terms employed must be reasonably calculated to yield relevant data. If not, courts may need to order additional searches, which will increase the cost and burden of discovery.

RESOURCES AND AUTHORITIES

Steven C. Bennett, *E-Discovery by Keyword Search,* 15 No. 3 Prac. Litigator 7 (2004).

George L. Paul and Jason R. Baron, *Information Inflation: Can the Legal System Adapt?* 13 Rich. J.L. & Tech. 10 (2007) *available at* http://law.richmond.edu/jolt/v13i3/article10.pdf.

Treppel v. Biovail Corp., 233 F.R.D. 363, 374 (S.D.N.Y. 2006) (stating that requesting party's refusal to agree upon identification of custodians or search terms to be applied to electronically stored information was a "missed opportunity," but did not excuse responding party's obligation to locate and produce responsive documents).

Zubulake v. UBS Warburg LLC, No. 229 F.R.D. 422, at *7-8 (S.D.N.Y. July 20, 2004) (*"Zubulake V"*) faulting counsel for failing to interview key players in litigation or do key-word search of databases in course of creating and enforcing litigation hold).

Comment 11.b. Sampling

Parties should consider the use of sampling techniques, when appropriate, to narrow the burden of searching voluminous electronically stored information. By reviewing an appropriate sample of a large body of electronically stored information, parties can often determine the likelihood that a more comprehensive review of the materials will yield useful information.

For example, in the seminal case of *McPeek v. Ashcroft,* 202 F.R.D. 31 (D.D.C. 2001), Magistrate Judge Facciola ordered the "backup restoration of the emails attributable to" a particular individual's computer during a one-year period. Judge Facciola viewed this restoration as "a test run," which would allow the court and the parties to better determine whether a further search of the backup tapes was justified. Upon reviewing the results of the sample restoration, Judge Facciola held that further restoration of backup tapes was largely unjustified and ordered very limited discovery of emails contained on backup tapes. *Id.* at 34.

Fed. R. Civ. P34(a) expressly permits sampling of electronically stored information. In ruling on a party's request to inspect computer systems, the court must consider issues of burden and intrusiveness.

RESOURCES AND AUTHORITIES

McPeek v. Ashcroft, 202 F.R.D. 31, 34-35 (D.D.C. 2001) (in sexual harassment case where plaintiff sought restoration and searches of extensive archived emails, magistrate judge ordered a "test run" search of one individual's email from a one-year period, observing that the results would dictate the need for further searches).

McPeek v. Ashcroft, 212 F.R.D. 33, 34 (D.D.C. 2003) (discussing results of previously ordered "test run" searches and concluding that further restoration of backup tapes not warranted).

Zubulake v. UBS Warburg LLC, 217 F.R.D. 309, 324 (S.D.N.Y. 2003) (*"Zubulake I"*)("Requiring the responding party to restore and produce responsive documents from a small sample of backup tapes will inform the cost-shifting analysis.").

Comment 11.c. Consistency of manual and automated collection procedures

Depending on the nature of the sources of data, both manual and automated procedures for collection may be appropriate in particular situations. Whether manual or automated, the procedures must be directed by legal counsel to assure compliance with discovery obligations.

Manual collection is performed by the document authors or custodians themselves, by litigation support or information services personnel, or by others. In a manual collection, the items may be copied or transmitted by the end-user. This should be accomplished under a defined written protocol. Self-collections by custodians may give rise to questions regarding the accuracy of collections if directions and oversight are poor or non-existent.

Automated or computer-assisted collection involves using computerized processes to collect data meeting certain criteria, such as search terms, file and message dates, or folder locations. Automated collection can be integrated with an overall electronic data archiving or retention system, or it can be implemented using agents specifically designated to retrieve information on a case-by-case basis. Regardless of the method chosen, consistency across the production can help ensure that responsive documents have been produced as appropriate.

RESOURCES AND AUTHORITIES

Serra Chevrolet, Inc. v. General Motors Corp., 446 F.3d 1137, 1147 (11th Cir. 2006) (affirming portion of district court's ruling related to failure to comply with discovery order where defendant did not conduct a manual search of its files until several months after being ordered to produce all documents related to a particular subject).

12. Absent party agreement or court order specifying the form or forms of production, production should be made in the form or forms in which the information is ordinarily maintained or in a reasonably usable form, taking into account the need to produce reasonably accessible metadata that will enable the receiving party to have the same ability to access, search, and display the information as the producing party where appropriate or necessary in light of the nature of the information and the needs of the case.

Comment 12.a. Metadata

An electronic document or file usually includes not only the visible text but also hidden text, formatting codes, formulae, and other information associated with the file. These many types of ancillary information are often lumped together as "metadata," although some distinctions between different types of metadata should be recognized.

For example, the two most common distinctions are between "application" metadata and "system" metadata. Application metadata is created as a function of the application software used to create the document or file. Common application metadata instructs the computer how to display the document (for example, the proper fonts, spacing, size, and color). Other application metadata may reflect modifications to the document, such as prior edits or editorial comments. This metadata is embedded in the file it describes and moves with the file when it is moved or copied. System metadata reflects information created by the user or by the organization's information management system. Such information may, for example, track the title of the document, the user identification of the computer that created it, the assigned data owner, and other document "profile" information. System metadata generally is not embedded within the file it describes, but is stored externally elsewhere on the organization's information management system. Depending on the circumstances of the case, the content value of a particular piece of metadata may be critical or may be completely irrelevant. It may be important, therefore, when planning the scope of discovery to determine the types and locations of metadata associated with the various application data types that will be targeted in the discovery and determine whether or not they may play an ongoing role.

Aside from its potential relation to the facts of the case, metadata may also play a functional role in the usability of electronically stored information. For example, system metadata may allow for the quick and efficient sorting of a multitude of files by virtue of the dates or other information captured in metadata. In addition, application metadata may be critical to allow the functioning of routines within the file, such as cell formulae in spreadsheets.

Care should be taken when using metadata, as the content of a given piece of metadata may convey information that is contextually inaccurate. For example, when a Microsoft Word™ document is created, the computer on which that document is saved may automatically assign the document an "author" based on the information available on that computer. That document may be used as a template by other persons, but the "author" information is never changed. Thus, subsequent iterations of the document may carry as an "author" a person with no knowledge of the content of the document. Accordingly, a proper and thorough analysis should be undertaken in order to properly assess how the metadata was created.

The extent to which metadata should be preserved and produced in a particular case will depend on the needs of the case. Parties and counsel should consider: (a) what metadata is ordinarily maintained; (b) the potential relevance of the metadata to the dispute (e.g., is the metadata needed to prove a claim or defense, such as the transmittal of an incriminating statement); and (c) the importance of reasonably accessible metadata to facilitating the parties' review, production, and use of the information. In assessing preservation, it should be noted that the failure to preserve and produce metadata may deprive the producing party of the opportunity later to contest the authenticity of the document if the metadata is material to that determination. Organizations should evaluate the potential benefits of retaining native files and metadata (whether or not it is produced) to ensure that documents are authentic and to preclude the fraudulent creation of evidence.[37]

RESOURCES AND AUTHORITIES

Shira A. Scheindlin and Jonathan M. Redgrave, *Discovery of Electronic Information, 2 Bus. & Commerical Litig. in Fed. Courts,* §22:22 (Robert L. Haig ed., 2005 & Supp. 2006).

Kentucky Speedway, LLC v. NASCAR, Inc., Civ. No. 05-138-WOB, 2006 W.S. Dist. Lexis 92028 (E.D. Ky. Dec. 18, 2006) (court declines to require defendant to supplement production of electronically stored information, relying on a perceived emerging presumption against the production of metadata and citing Sedona Principle 12 (2005 edition)).

In re Priceline.com Inc. Sec. Litig., 233 F.R.D. 88, 91 (D. Conn. 2005) ("Defendants shall produce responsive information contained in stored data files to plaintiffs in TIFF or PDF form with Bates numbering and appropriate confidentiality designations, shall produce searchable metadata databases, and shall maintain the original data itself in native format for the duration of the litigation.").

Williams v. Sprint/United Mgmt. Co., 230 F.R.D. 640, 643 (D. Kan. 2005) (*"Williams I"*)(finding that if production of spreadsheets are ordered to be produced in form in which they are maintained, metadata should be produced, citing *The Sedona Principles* for definition and discussion of metadata).

Comment 12.b. Formats used for collection and production: "ordinarily maintained" v. "reasonably usable"

Electronically stored information is fundamentally different from paper information in that it is dynamic, created and stored in myriad different forms, and contains a substantial amount of nonapparent data. Because of these differences, approaching the production of electronically stored information as though it is just the modern equivalent of a paper document collection will likely lead to a failure to fully consider the complex issues involved and a failure to select the most relevant and functional form of production for a particular type of electronic information.

[37] Several attorney disciplinary bodies have issued opinions on the dangers of counsel inadvertently transmitting attorney-client confidences as metadata embedded within electronic documents and the efficacy of receiving counsel searching for and viewing such metadata. *See, e.g.,* New York Ethics Op. 749 (2001); ABA Comm. on Ethics And Prof'l Responsibility, Formal Op. 06-442; New York Ethics Op. 749 (2001); Maryland Bar Assoc. Comm. on Ethics Op. 2007-09. The Working Group expresses no opinion on these decisions, and it should be noted that the issues discussed in these opinions usually arise in a transactional context, before any duty to preserve electronically stored information relevant to anticipated or pending litigation arises. In transactional settings, counsel is free to routinely employ so-called "metadata scrubbers" to remove unwanted metadata before transmitting electronic documents to clients or to other counsel. In deciding to do so, counsel should weigh the dangers of transmitting client confidences or attorney-client communication against the benefits that metadata provides for later document management, indexing and review, and may choose to "scrub" only certain categories of particularly sensitive metadata. Once litigation is anticipated, however, routine metadata scrubbing of relevant documents must be reexamined in light of the preservation duty.

Electronic information is created and stored by a computer in a file format "native" to the software application used to create or utilize the information. However, electronically stored information can be produced in any number of formats, some more useful than others. For example, although an email message may be readily understood when presented as plain text printed on paper, this is not the case with audio or video files. All electronic documents and files, to one extent or another, contain information that is not apparent when displayed on a screen, printed on paper, or heard on speakers. The extent to which a production of electronically stored information includes such data depends on the form of production. For example, electronic information produced in the form in which the file was created (or "native format") will contain application metadata such as formulae in spreadsheets or "tracked changes" in word processing documents.

An electronic document or file produced in native format may also be accompanied by system metadata, such as the date the file was created or the identity of the computer on which it was created. However, electronic information produced in a static, two-dimensional form, such as an image file (e.g., TIFF or PDF, explained below), while having some practical advantages, does not contain any of the original metadata. Certain types of electronic information, such as databases, simply cannot be converted from their native, dynamic, three-dimensional form without significant loss of information and functionality.

Accordingly, there should be two primary considerations in choosing the form of production: (1) the need for, or probative value of both apparent and metadata; and (2) the extent to which the production of metadata will enhance the functional utility of the electronic information produced and allow the parties to conduct a more cost-effective and efficient review. These considerations should be weighed against the negative aspects associated with each format. [38] For example, production in a "native" format entails both advantages and disadvantages. Native production, which generally includes the entire file and associated metadata, may afford the requesting party access to the same information and functionality available to the producing party and, from a technical perspective, usually requires minimal processing before production. However, information produced natively may be difficult or impossible to redact or Bates number, and files in their native forms must be viewed using applications capable of opening and presenting the information without alteration. Suitable applications are not always accessible to requesting parties, who may also lack the equipment or expertise required to use such applications.

A native file production that includes a substantial volume and variety of file types could become very expensive and burdensome for the requesting party. In addition, since certain metadata could contain or reveal privileged, secret, or other sensitive information, an organization may determine that it must review such metadata before producing it, which can substantially impact the speed of production.

In current practice, many parties, local rules and courts have endorsed the use of image production formats, principally the Tagged Image File Format ("TIFF") and Adobe Portable Document Format ("PDF") formats. Standing by themselves, image file productions are the equivalent of printed pages from the screen. They have the advantage of a static format that can be Bates numbered and redacted, and, compared to native files, it is harder (but not impossible) to alter the data inadvertently or deliberately. However, simple image productions require significant processing that is time consuming and costly. The image productions, by themselves, also lose searchable text and metadata that might enable better understanding and utility of the evidence.

In an effort to replicate the usefulness of native files while retaining the advantages of static productions, image format productions are typically accompanied by "load files," which are ancillary files that may contain textual content and relevant system metadata. Again, however, there are potentially significant costs inherent in this process, and it does not work well for certain types of electronically stored information such as spreadsheets and dynamic databases.

---

[38] *See The Sedona Canada Principles,* Principle 8, Comment 8.b (2006), *available at* http://www.thesedonaconference.org.

The routine preservation of metadata pending agreements or decisions on the ultimate form of production may be beneficial in a number of ways. Preservation of metadata may provide better protection against inadvertent or deliberate modification of evidence by others and the systematic removal or deletion of certain metadata may involve significant additional costs that are not justified by any tangible benefit. Moreover, the failure to preserve and produce metadata may deprive the producing party of the opportunity later to contest the authenticity of the document if the metadata would be material to that determination.

In amending Rule 34(b) to accommodate the production of electronically stored information, the Advisory Committee acknowledged that wherever possible, parties should first attempt to reach agreement on the various form or forms of production, given that different types of data may serve different purposes and the need for native production and metadata may vary. The Advisory Committee also recognized that the default forms of production appropriate to paper discovery did not have direct equivalents in electronic discovery. However, the goals furthered by providing default forms of production governing paper discovery should be the same in electronic discovery – to encourage forms of production that would be inexpensive for the producing party and reasonably useable for the requesting party; and to avoid costly data conversion on the one hand, and the electronic equivalent of the "document dump" on the other hand. Therefore, without mandating any particular form of production, Rule 34(b) provides that in the absence of agreement or a specific court order, a producing party should produce electronically stored information either in the form in which it is "ordinarily maintained" or in a "reasonably usable" form.

The form in which electronically stored information is "ordinarily maintained" is not necessarily synonymous with the form in which it was created. There are occasions when business considerations involve the migration or transfer of electronically stored information to other applications or systems. For example, customer information may routinely be gathered by an organization from Internet-based forms, then collected in a relational database for further business use. The information may be incorporated into Microsoft Word™ documents, such as memoranda or correspondence, which may later be transferred into static electronic images for long-term storage and retrieval. In such cases, the form in which the electronically stored information is maintained understandably varies from that in which it was obtained or created. Absent an attempt to deliberately downgrade capabilities or characteristics for the purposes of avoiding obligations during specific litigation, migration to alternative forms for business purposes is not considered inconsistent with preservation obligations.

What constitutes a "reasonably usable" form will depend on the circumstances of a case, given that the need for email, documents, spreadsheets, or dynamic databases can all vary. As noted earlier, selection of a "reasonably usable" form is best handled by an agreement between the parties regarding the distinct categories of electronically stored information sought in a case. But where such an agreement is not reached, the Committee Note to Rule 34(b) explicitly states that "[i]f the responding party ordinarily maintains the information it is producing in a way that makes it searchable by electronic means, the information should not be produced in a form that removes or significantly degrades this feature." Accordingly, a party should produce electronically stored information in "reasonably usable" forms, though not necessarily "native format."

In determining the appropriate forms of production in a case, requesting parties and counsel should consider: (a) the forms most likely to provide the information needed to establish the relevant facts of the case; (b) the need for metadata to organize and search the information produced; (c) whether the information sought is reasonably accessible in the forms requested; and (d) the requesting party's own ability to effectively manage and use the information in the forms requested.

Producing parties and counsel should consider: (a) the relative risks of inadvertent production of confidential, privileged, and work product information associated with different forms of production; (b) difficulties in redaction, tracking, and use of native files; (c) whether alternative (e.g., "nonnative") forms of production provide sufficient usability (e.g., by providing adequate accompanying information through load files) such that the producing and requesting parties have the same access to functionality; and (d) the relative costs and burdens with respect to the proposed forms of production, including the costs of preproduction review, processing, and production.

Illustration i. A party demands that responsive documents, "whether in hard copy or electronic format," be produced. The producing party objects to producing the documents in native electronic format and states that production will be made through PDF or TIFF images on CD-ROMs with load files containing electronically searchable text and selected system and application metadata. The requesting party raises no further objection, and the producing party produces photocopies of the relevant hard copy memoranda, emails and electronic records in a PDF or TIFF format accompanied by a load file containing the searchable text and selected metadata for each item of electronically stored information. This production of electronically stored information satisfies the goals of Principle 12 because the production is in usable form, e.g., electronically searchable and paired with essential metadata.

Illustration ii. Plaintiff claims that he is entitled to a commission on a transaction, based upon an email allegedly sent by the president of defendant corporation agreeing to the commission. Defendant asserts that there is no record of the email being sent in its email system or the logs of its Internet activity, and that the email is not authentic. In these circumstances, it is appropriate to require production of not only the content of the questioned email but also of the email header information and metadata, which can play a crucial role in determining whether the questioned message is authentic.

Illustration iii. Plaintiff alleges that the defendant engaged in a fraud regarding software development. The plaintiff seeks a preliminary order permitting direct access to the hard drives of the software engineers involved and demonstrates that the computer program sold by defendant appears to incorporate plaintiff's source code. In this case, production of the source code in native format may be appropriate, as well as targeted forensic examination of the hard drives concerning the development of the source code. The court should impose such conditions as it deems appropriate to protect legitimate property and privacy interests of the defendant and its employees.

RESOURCES AND AUTHORITIES

Kentucky Speedway, LLC v. NASCAR, Inc., Civ. No. 05-138-WOB, 2006 U.S. Dist. Lexis 92028 (E.D. Ky. Dec. 18, 2006) (court declines to require defendant to supplement production of electronically stored information, relying on a perceived emerging presumption against the production of metadata and citing Sedona Principle 12 (2005 edition)).

In re Priceline.com Inc. Sec. Litig., 233 F.R.D. 88, 91 (D. Conn. 2005) ("Defendants shall produce responsive information contained in stored data files to plaintiffs in TIFF or PDF form with Bates numbering and appropriate confidentiality designations, shall produce searchable metadata databases, and shall maintain the original data itself in native format for the duration of the litigation.").

Compare Williams v. Sprint/United Mgmt. Co., 230 F.R.D. 640, 652 (*"Williams I"*) (D. Kan 2005) ("[W]hen a party is ordered to produce electronic documents as they are maintained in the ordinary course of business, the producing party should produce the electronic documents with their metadata intact, unless that party timely objects to the production of metadata, the parties agree that the metadata should not be produced, or the producing party requests a protective order."), *with Williams v. Sprint/United Mgmt. Co.,* 2006 WL 3691604 (D. Kan. December 12, 2006) (*"Williams II"*) "Defendant raises legitimate concerns about producing the transmittal e-mails with their attachments in their native format, including the whether production in native format would permit the redaction or removal of privileged information. […] Moreover, even assuming that Defendant could produce the transmittal e-mails together with their attachments in native format with the privileged information redacted, Plaintiffs have not sufficiently explained why they need the transmittal e-mails in their native format.").

Comment 12.c. Procedure for requesting and producing metadata under the Federal Rules

Amended Rule 26(f), concerning the conference of parties and planning for discovery, broadly requires parties to address issues related to electronically stored information early in cases where such discovery is at issue. Specifically, Rule 26(f)(3) mandates that the parties meet, confer, and develop a proposed discovery plan that indicates the parties' views and proposals regarding, among other topics, "any issues relating to disclosure or discovery of electronically stored information, including the form or forms in which it should be produced." To the extent that the parties believe that production of metadata is needed because of either relevance or usability, that should be raised at this conference as it will be a consideration in determining both the need to preserve information in a particular form and the ultimate form or forms of production. By fostering early and ongoing communication between the parties on the issue, the amendments to Rules 26(f) and 34 are designed to lessen the likelihood that disputes over form of production (including metadata issues) will impact the orderly progression of discovery.

Absent an agreement or a court order, Rule 34 establishes a distinct procedure for electronically stored information. Under Rule 34(b), a party serving a request for the production of electronically stored information may, but is not required to, specify the form or forms in which the information should be produced. To the extent that the requesting party seeks a "native" production or some other form of production with accompanying metadata, the revised rule places a burden on the party to make that request explicit. If the requesting party specifies a form or forms of production, the responding party may object to the requested form or forms of production and state the reasons for the objection. Regardless of whether a requesting party fails to state a preferred form of production, or the responding party objects to a requested form, the responding party must state the form or forms in which it intends to produce electronically stored information. In both cases, the producing party should indicate with specificity the forms of production it proposes to use and the requesting party should scrutinize the proposed forms.

Absent party agreement or court order providing otherwise, the responding party must produce electronically stored information in one of two "default forms," the form "in which it is ordinarily maintained," or a form that is "reasonably usable." *See* Comment 12b, *supra*. In addition, absent an agreement or order, a party need not produce the same electronically stored information in more than one form.

Any disputes regarding form or forms of production may be brought before a court for resolution in a variety of ways. The parties may raise any inability to reach agreement at the Rule 16(b) conference so that the court can give initial guidance. The court may place the issue on the calendar for formal resolution, recognizing the possible need for evidence from experts, IT personnel and business users. Parties may also raise the issue by motions – either a motion to compel by the requesting party under Rule 37 or a motion for a protective order by the responding party under Rule 26(c). However, the rules require, and the courts encourage, the parties to attempt to meet and resolve any dispute before filing such motions.

Finally, it is worth noting that a growing tendency in some federal courts is to issue formal local rules or informal guidelines, standards, or "default" case management recommendations addressing electronic production formats. There is much to be gained by such experimentation, but a serious risk exists that these will lead to rigidity and defeat the purpose of the Amended Rules to require parties, not courts, to make the tough choices that fit the particular discovery needs of a case.

RESOURCES AND AUTHORITIES

D. Kan., *Guidelines for Disc. of Electronically Stored Information, available at* http://www.ksd.uscourts.gov/guidelines/electronicdiscoveryguidelines.pdf.

D. Md. Loc. R., *Suggested Protocol for Disc. of Electronically Stored Information, available at* http://www.mdd.uscourts.gov/news/news/ESIProtocol.pdf.

N.D. Ohio Civ. App. K, *Default Standard for Discovery of Electronically Stored Information ("E-Discovery"), available at* http://www.ohnd.uscourts.gov/Clerk_s_Office/Local_Rules/AppendixK.pdf.

Comment 12.d. Parties need not produce the same electronically stored information in more than one format

Provided that the forms of production are reasonable, a party should not be required to produce the same information in both hard copy and electronic format, or in both native format and another electronic format. The 2006 Amendments state that production in more than one format is not required, absent an agreement or order. *See* Fed. R. Civ. P. 34(b)(2)(iii). If a court requires production of the same information a second time in a different format because of an unclear or tardy request, the court should consider shifting some or all of the cost of the second production to the requesting party.

RESOURCES AND AUTHORITIES

Williams v. Owens Illinois, Inc., 665 F.2d 918, 933 (9th Cir. 1982) (appellants in employment discrimination case not entitled to computer tapes when they already had access to wage cards containing the same information, even though using the cards "may be more time-consuming, difficult, and expensive").

In re Bristol-Meyers Squibb Sec. Litig., 205 F.R.D. 437, 443 (D.N.J. 2002) (plaintiff not required to pay half of defendant's scanning costs for electronic documents, even though defendant had already produced documents in paper form; although plaintiff was entitled to electronic version, it was already obligated to pay half of photocopying costs for the paper documents and should not be forced to pay for "double-discovery").

Williams v. Sprint/United Mgmt. Co., 230 F.R.D. 640, 652 (D. Kan 2005) (*"Williams I"*) ("When a party is ordered to produce electronic document spreadsheets as they are maintained in the ordinary course of business, the producing party should produce the electronic documents with their metadata intact, unless that party timely objects to the production of metadata, the parties agree that the metadata should not be produced, or the producing party requests a protective order.").

13. Absent a specific objection, party agreement or court order, the reasonable costs of retrieving and reviewing electronically stored information should be borne by the responding party, unless the information sought is not reasonably available to the responding party in the ordinary course of business. If the information sought is not reasonably available to the responding party in the ordinary course of business, then, absent special circumstances, the costs of retrieving and reviewing such electronic information may be shared by or shifted to the requesting party.

Comment 13.a. Factors for cost-shifting

The ordinary and predictable costs of discovery are fairly borne by the producing party. However, Rule 26 has long empowered courts to shift costs where the demand is unduly burdensome because of the nature of the effort involved to comply.

Traditionally, the consideration of cost-shifting by the courts has been at the discretion of the court.[39] Amended Rule 26(b)(2)(B) specifically notes that an order compelling the production of electronically stored information that is "not reasonably accessible"[40] may be subject to conditions, including "payment by the requesting party of part or all of the reasonable costs of obtaining information from sources that are not reasonably accessible." The Rule then identifies seven factors to be considered, and it is likely that courts addressing production under this rule will routinely consider, if not order, cost-shifting or cost sharing. The types of information that typically may (but not always) fall within Rule 26(b)(2)(B) include deleted data, disaster recovery/backup tapes, residual data, and legacy data.

Importantly, parties should recognize that cost-sharing and cost-shifting remains separately available under Rule 26(b)(2)(C) and Rule 26(c). In particular, even though electronically stored information is reasonably accessible (e.g., it exists on a corporate storage area network), the aggregate volume of data requested may be disproportionate to the needs in the case and/or the respective resources of the parties (e.g., a large multinational company suing a small company) such that a condition of further discovery can be the shifting of some or all costs of such discovery.

The factors for cost-shifting for the production of burdensome electronically stored information (whether reasonably available or accessible or not) should include (in order of importance):

1. whether the information is reasonably accessible as a technical matter without undue burden or cost
2. the extent to which the request is specifically tailored to discover relevant information
3. the availability of such information from other sources, including testimony, requests for admission, interrogatories, and other discovery responses
4. the total cost of production, compared to the amount in controversy
5. the total cost of production, compared to the resources available to each party
6. the relative ability of each party to control costs and its incentive to do so
7. the importance of the issues at stake in the litigation, and
8. the relative benefits to the parties of obtaining the information.

Finally, consideration of the "total cost of production" includes the estimated costs of reviewing retrieved documents for privilege, confidentiality, and privacy purposes. It also includes consideration of opportunity costs or disruption to the organization, *e.g.,* the need to redirect IT staff from business projects to retrieve or review the data. Accordingly, Rule 26 broadly defines the burdens that can be considered by a court in the proportionality analysis.

---

[39] Notably, the Advisory Committee Note also provides that "a requesting party's willingness to share or bear the access costs may be weighed by the court in determining whether there is good cause."

[40] Principle 13 uses the term "available" whereas the Federal Rule uses "accessible." In practice, there should be no practical difference as the focus should be on how the information is generally stored and used (i.e., in the regular course of business or not) and how hard (i.e., burdensome and expensive) it is to retrieve and review it.

RESOURCES AND AUTHORITIES

Conference of Chief Justices, *Guidelines For State Trial Courts Regarding Discovery of Electronically Stored Information,* Guideline 7 (Aug. 2006) ("Reallocation of Discovery Costs") (listing seven factors for courts to use in determining whether to shift part or all of the costs of discovery costs of information which is not accessible).

Comment, *The Growth of Cost-Shifting in Response to the Rising Cost and Importance of Computerized Data in Litigation,* 59 Okla. L. Rev. 115 (2006).

ABA Civil Discovery Standards, (1999) (rev. Aug. 2004) Standard 29(b)(iv) *available at* http://www.abanet.org/litigation/discoverystandards/2004civildiscoverystandards.pdf (listing factors to consider in allocating costs of discovery of any form of electronic information or related software).

Corrine L. Giacobbe, *Allocating Discovery Costs in the Computer Age: Deciding Who Should Bear the Costs of Discovery of Electronically Stored Data,* 57 Wash. & Lee L. Rev. 257 (2000).

Martin H. Redish, *Electronic Discovery and the Litigation Matrix,* 51 Duke L.J. 561 (2001).

Tex. R. Civ. P. 196.4 (mandating that requesting party "pay reasonable expenses of any extraordinary steps required to retrieve and produce" any information requested which is not "reasonably available").

Rowe Entm't, Inc. v. William Morris Agency, Inc., 205 F.R.D. 421, 431 (S.D.N.Y. 2002) (shifting costs of production of email from backup tapes in order to protect parties from undue burdens and costs under Rule 26(c) after a balancing approach involving specificity, likelihood of recovery of critical information, availability of information from other sources, purposes for which maintained, relative benefit, total costs associated with production, relative ability to control costs and resources), *affirmed*, No. 98 Civ. 8272(RPP), 2002 WL 975713 (Patterson, J.) (S.D.N.Y. May 9, 2002).

Wiginton v. CB Richard Ellis, Inc., No. 02-C-6832, 229 F.R.D. 568, 573 (N.D. Ill. Aug. 9, 2004) (holding that the "importance of the requested discovery in resolving the issues of the litigation" should be considered for cost-shifting in addition to the factors in the *McPeek, Rowe,* and *Zubulake* cases, and finding that these factors required defendant to bear 25 percent and plaintiffs 75 percent of the costs of restoring defendant's backup tapes, searching them and transferring them to an electronic viewer).

Zubulake v. UBS Warburg LLC, 217 F.R.D. 309, 318-22 (S.D.N.Y. 2003) (*"Zubulake I"*) (noting that "whether production of documents is unduly burdensome or expensive turns primarily on whether it is kept in an accessible or inaccessible format," and formulating seven-factor test for determining whether cost-shifting might be appropriate).

Zubulake v. UBS Warburg LLC, 216 F.R.D. 280, 290 (S.D.N.Y. 2003) (*"Zubulake III"*) (applying seven-factor test and shifting one-fourth of costs associated with restoring and searching backup tapes, but excluding cost of production, such as costs incurred when reviewing documents for privilege, from consideration in determining that total cost of production).

Comment 13.b. Cost-shifting cannot replace reasonable limits on the scope of discovery

Shifting the costs of extraordinary electronically stored information discovery efforts should not be used as an alternative to sustaining a responding party's objection to undertaking such efforts in the first place. Instead, such efforts should only be required where the requesting party demonstrates substantial need or justification. The courts should discourage burdensome requests that have no reasonable prospect, given the size of the case, of significantly contributing to the discovery effort, even if the requesting party is willing to pay.

> *Illustration i.* A requesting party demands that the producing party preserve, restore, and search a backup tape for information about a topic in dispute. The requesting party produces some evidence that relevant information, not available elsewhere, may exist on the tape. The information, not being readily available, is costly to acquire, and the producing party seeks a protective order conditioning its production upon payment of costs, including the costs of review. Absent proof that the producing party has intentionally deleted information that is relevant to the issues in the case, the protective order should be granted and the requesting party should pay for at least a portion of the costs associated with the request.

Comment 13.c. Non-party requests must be narrowly focused to avoid mandatory cost-shifting

Since 1991, Rule 45 of the Federal Rules has required persons issuing subpoenas to take reasonable steps to avoid imposing undue burdens or expense on the requested party and, if objection is made, any order to compel production "shall protect [the requested party] from significant expense." As important, the Committee Notes to the 1991 amendments state:

> A non-party required to produce documents or materials is protected against significant expense resulting from involuntary assistance to the court .... The court is not required to fix the costs in advance of production, although this will often be the most satisfactory accommodation to protect the party seeking discovery from excessive costs. In some instances, it may be preferable to leave uncertain costs to be determined after the materials have been produced, provided that the risk of uncertainty is fully disclosed to the discovering party.

In support of this proposition, the Committee cited a 1982 decision from the Ninth Circuit in a case where non-parties produced more than six million documents, and the costs of non-party discovery exceeded two million dollars. In light of the potentially enormous burdens involved with non-party discovery involving electronically stored information, parties seeking information from non-parties have a substantial interest in narrowly tailoring requests in light of a greater likelihood that a court may impose cost-sharing or cost-shifting. Indeed, parties seeking information from non-parties should be prepared to address these issues at informal meetings to determine if disputes can be resolved by agreement instead of rulings on a motion to quash or a motion to compel.

RESOURCES AND AUTHORITIES

United States v. Columbia Broadcasting Sys., Inc., 666 F.2d 364, 371 (9th Cir. 1982) ("[n]on-party witnesses are powerless to control the scope of litigation and discovery and should not be forced to subsidize an unreasonable share of the costs of a litigation to which they are not a party.").

14. Sanctions, including spoliation findings, should be considered by the court only if it finds that there was a clear duty to preserve, a culpable failure to preserve and produce relevant electronically stored information, and a reasonable probability that the loss of the evidence has materially prejudiced the adverse party.

Comment 14.a. Intentional, reckless, or grossly negligent violations of preservation obligations

Due to the complexity of modern electronic information systems, the large volumes of electronically stored information, and the continuing changes in information technology, there exists a potential for good faith errors or omissions in the process of identifying, preserving and producing relevant electronically stored information, which involves both humans and technology. This reality is based in part on recognition that routine business operations necessarily include functions that continuously modify, overwrite and delete data.

Case law indicates that there must be a sufficient level of culpability to support the imposition of spoliation sanctions. Accordingly, neither spoliation findings nor sanctions should issue without proof of a knowing violation of an established duty to preserve or produce electronically stored information or a reckless disregard amounting to gross negligence. Usually, the knowing violation will be found in the context of a specific provision of an existing discovery order, subpoena, preservation order, or similar explicit preservation obligation. However, the common law duty of preservation arises when a party, either plaintiff or defendant, reasonably anticipates litigation.[41]

The nature, scope and execution of preservation obligations are covered generally in Principle 5. Other related Principles are Principle 2 (role of proportionality standard), Principle 3 (necessity for early consultation), Principle 6 (proper role of producing parties in selecting methods of preservation), Principle 7 (burden of proof in proving inadequate preservation), Principle 9 (limits on duty to preserve deleted information), Principle 11 (use of sampling in regard to preservation) and Principle 12 (preservation of metadata).

RESOURCES AND AUTHORITIES

Residential Funding Corp. v. DeGeorge Fin. Corp., 306 F.3d 99, 108 (2d Cir. 2002) (stating that sanctions may be appropriate for negligent failure to take adequate steps to preserve and produce ESI in a timely manner).

Stevenson v. Union Pac. R.R. Co., 354 F.3d 739, 746-47 (8th Cir. 2004) (adverse inference instruction should not be given on the basis of negligence alone; there must be a finding of bad faith or some other culpable conduct, such as the ongoing destruction of documents during litigation and discovery even after they have been specifically requested).

Morris v. Union Pac. R.R. Co., 373 F.3d 896, 900-01 (8th Cir. 2004) (warning that an adverse inference instruction is a powerful tool which, when not warranted, creates a substantial danger of unfair prejudice, ruling that there must be a finding of intentional destruction indicating a desire to suppress the truth, and, in light of the trial court's conclusion that defendant did not intentionally destroy an audiotape of a collision, reversing and remanding for a new trial).

[41] *Compare Hynix Semiconductor, Inc. v. Rambus, Inc.*, No. C-00-20905 RMW (N.D. Cal. January 4, 2006) ("reasonable anticipation of litigation" when party is defendant) *with Rambus, Inc. v. Infineon Technologies AG,* 220 F.R.D. 264 (E.D. Va. 2004) ("reasonable anticipation of litigation" when same party, under same circumstances, is plaintiff).

Coleman (Parent) Holdings, Inc. v. Morgan Stanley & Co., Inc., No. 502003CA005045XXOCAI, 2005 WL 679071 (Fla. Cir. Ct. Mar. 1, 2005) (after concluding that defendant had sought to thwart discovery and failed, through willful and gross abuse, grossly negligent and negligent conduct with respect to discovery obligations to timely locate and produce relevant information from more than 1,000 backup tapes, court determines that (i) *defendant* would bear the burden of proving to the jury by the greater weight of the evidence that it lacked knowledge of fraud and did not aid, abet or conspire to perpetrate fraud and (ii) court would read to the jury a statement of "conclusive" findings of fact concerning the discovery failures from which the parties could argue in favor of whatever inferences the facts may support); *further opinion* 2005 WL 674885 (Fla. Cir. Ct. Mar. 23, 2005) (determined that partial default should be entered, following which jury returned verdicts of $605 million in compensatory damages and $850 million in punitive damages), r*ev'd and remanded on other grounds,* ---So.2d ---, 2007 WL 837221 (Fla. Dist. Ct. App. Mar. 21, 2007).

Zubulake v. UBS Warburg LLC, 229 F.R.D. 422, 431-33 (S.D.N.Y. 2004) (*"Zubulake V"*) (for willful destruction where certain key employees destroyed email after being repeatedly told by counsel not to, and counsel failed to interview key players in litigation or do key word search of databases in course of creating and enforcing litigation hold).

Comment 14.b. "Negligent" versus "culpable" spoliation

Some courts have invoked the tort concept of negligence in addressing spoliation of evidence claims. It is critical, however, to understand that establishing a standard of care (e.g., negligence) does not answer the question of whether any sanction is warranted. In considering sanctions, the focus should be on culpability and prejudice. As to culpability, the question is whether in the circumstances of the case, a party is sufficiently culpable for the loss of electronic data. "Culpability" in most jurisdictions does not include what could be considered "negligent conduct." Even courts that state that culpability may include negligent destruction – or, more precisely, negligent failure to preserve -- do equate such conduct with an entitlement to sanctions for data loss. Regardless of the label applied, courts begin by examining whether the party took reasonable good faith efforts to preserve relevant electronic data. The more evidence that the failure was intended to prevent discovery of specific information, the more likely spoliation instructions or other sanctions will be imposed. If a party has specifically requested documents in electronic format, allowing those documents to be destroyed, even if hard copies of those documents still exist, can lead to sanctions.

On the other hand, if a court finds that relevant information has been negligently lost, resulting in prejudice to the requesting party, but without the level of culpability that would lead to sanctions, the court may nevertheless order remedial measures designed to put the parties in roughly the position they would have been but for the negligence of the responding party. Such remedial measures may include ordering further discovery or allocating costs.

RESOURCES AND AUTHORITIES

Residential Funding Corp. v. DeGeorge Fin. Corp., 306 F.3d 99, 108 (2d Cir. 2002) (stating that sanctions may be appropriate for negligent failure to take adequate steps to preserve and produce electronically stored information in a timely manner).

Stevenson v. Union Pac. R.R. Co., 354 F.3d 739, 746-47 (8th Cir. 2004) (adverse inference instruction should not be given on the basis of negligence alone; there must be a finding of bad faith or some other culpable conduct, such as the ongoing destruction of documents during litigation and discovery even after they have been specifically requested).

Morris v. Union Pac. R.R., 373 F.3d 896, 900-01 (8th Cir. 2004) (warning that an adverse inference instruction is a powerful tool which, when not warranted, creates a substantial danger of unfair prejudice, ruling that there must be a finding of intentional destruction indicating a desire to suppress the truth, and, in light of the trial court's conclusion that defendant did not intentionally destroy an audiotape of a collision, reversing and remanding for a new trial).

Comment 14.c. Prejudice

A party seeking sanctions must prove that there is a reasonable likelihood that it has been materially prejudiced by the alleged spoliation. Destruction of tangentially relevant information, or information that is duplicative and has been produced from other sources, does not constitute prejudice.

An award of sanctions without a showing of prejudice is particularly inappropriate in the context of the discovery of electronically stored information, which often involves large volumes of complex data, in which it can be difficult to identify, preserve, and produce all relevant information with complete accuracy. In addition, in light of the significant confusion and disagreement about the proper treatment of metadata in cases and relevant literature – from preservation through production – it would be inappropriate to award sanctions simply due to the loss of metadata without a demonstration of actual prejudice.

The timeliness of a challenge to production failures may indicate prejudice, or the lack of it. The amended Federal Rules of Civil Procedure, as well as *The Sedona Principles,* since their inception, have urged an early constructive dialogue in cases between parties regarding respective preservation obligations and expectations. A corollary to this early discussion is that untimely challenges to production failures should not provide a basis for the imposition of sanctions.

> *Illustration i.* A party seeks production of electronically stored information but makes no objection to the production of electronic materials without metadata. Shortly before trial, it files a motion for sanctions and requests an adverse instruction based on the failure to produce metadata. Having not raised the issue earlier, the party has waived the right to seek metadata or sanctions.

RESOURCES AND AUTHORITIES

Zubulake v. UBS Warburg LLC, 220 F.R.D. 212, 221 (S.D.N.Y. Oct. 22, 2003) (*"Zubulake IV"*)("In order to receive an adverse inference instruction, Zubulake must demonstrate not only that UBS destroyed relevant evidence as that term is ordinarily understood, but also that the destroyed evidence would have been favorable to her.").

Comment 14.d. Good faith

Many cases involving spoliation and sanctions examine the "good faith" of the party that lost the evidence. Rule 37(f) now incorporates this standard, stating that a sanction should not issue if electronically stored information is lost as a result of the "routine, good-faith" operation of an electronic information system.

Good faith has both subjective and objective aspects in the context of electronic discovery. Considerations of a party's "good faith" may include the following inquiries: (a) was there a standard litigation hold process and was it followed? (b) did the party adequately communicate litigation hold instructions to employees? (c) did the party periodically distribute litigation hold reminders? (d) did the party adequately investigate and identify the locations that were reasonably likely to contain unique and relevant electronically stored information? (e) has the party been cooperative and forthcoming in Rule 26(f) and Rule 16(b) discussions? (f) has the party been reasonable and forthcoming in written discovery responses and depositions? (g) did the party take steps to secure relevant, unique electronically stored information that would otherwise be overwritten or deleted by automatic processes? (h) did the party take reasonable steps to ascertain whether orphaned or legacy data contain relevant information? and (i) was the electronic system designed and implemented solely with the intent of meeting business and technical needs or with the intent of thwarting discovery?[42] There is no talismanic test of "good faith," but organizations that can answer most if not all of these questions in the affirmative should be presumed to have acted in good faith absent proof to the contrary.

[42] *See* Fed. R. Civ. P. 37 Committee Note ("Many steps essential to computer operation may alter or destroy information, for reasons that have nothing to do with how that information might relate to litigation. […] Good faith in the routine operation of an information system may involve a party's intervention to modify or suspend certain features of that routine operation."). Fed. R. Civ. P. 37(f) is anticipated to be renumbered Fed. R. Civ. P. 37(e) effective December 1, 2007. *See* footnote 3, *supra*.

RESOURCES AND AUTHORITIES

Stevenson v. Union Pac. R.R. Co., 354 F.3d 739, 745-49 (8th Cir. 2004) (adverse inference instruction for pre-litigation destruction of evidence through a document retention program cannot be based on negligence alone but requires a finding of bad faith).

Lewy v. Remington Arms Co., 836 F.2d 1104, 1112 (8th Cir. 1988) (in reviewing whether documents destroyed pursuant to an existing retention policy constituted sanctionable conduct, court should determine whether the length of retention is reasonable given the particular type of document, whether lawsuits that would require production of these documents have been filed and their frequency, and whether the document retention policy was instituted in bad faith).

Comment 14.e. The good-faith destruction of electronically stored documents and information in compliance with a reasonable records management policy should not be considered sanctionable conduct absent an organization's duty to preserve the documents and information.

Where a party destroys documents or electronically stored information in good faith under a reasonable records management policy, no sanctions should attach. This does not mean a party may use its records management policy as a pretext for destroying documents or electronically stored information with impunity. Once a party reasonably determines that electronically stored information in its custody or control may be relevant to pending or reasonably foreseeable litigation, the party should take reasonable steps to preserve that electronically stored information, even if its records management program calls for its routine destruction. Determining a party's duty to preserve requires answering two separate questions: "when does the duty to preserve attach?" and "what evidence must be preserved?" Failure to properly preserve information may result in sanctions, including monetary fines, instructions to the jury commanding them to infer that the destroyed documents would be adverse to the interests of the responding party, and, in extreme cases, default judgments. Therefore, an organization's records management policy should recognize that the organization will sometimes have to suspend its ordinary retention and disposition of records and should include procedures designed to implement such suspensions.

However, if a party does not reasonably anticipate litigation, the destruction of documents in compliance with a reasonable records management policy should not be considered sanctionable conduct. Instead, the fact that the destruction occurred in compliance with a preexisting policy should be considered *prima facie* evidence of the good faith of the organization. In the absence of a duty to preserve records, courts have consistently refused to sanction parties who have destroyed records pursuant to a records retention program. Likewise, if duplicative or redundant information is routinely destroyed, but all relevant information has been preserved, courts have consistently refused to sanction parties in the absence of prejudice to the requesting party.

RESOURCES AND AUTHORITIES

Arthur Andersen LLP v. U.S., 544 U.S. 696, 704 (2005) ("'Document retention policies,' which are created in part to keep certain information from getting into the hands of others, including the Government, are common in business …. It is, of course, not wrongful for a manager to instruct his employees to comply with a valid document retention policy under ordinary circumstances.").

Morris v. Union Pac. R.R., 373 F.3d 896, 902 (8th Cir. 2004) (failure to interrupt recycling of audiotape despite occurrence of potentially discoverable information is not sanctionable in light of lack of intentional destruction indicating a desire to suppress the truth).

Stevenson v. Union Pac. R.R. Co., 354 F.3d 739, 747 (8th Cir. 2004) (holding that "some indication of an intent to destroy the evidence for the purpose of obstructing or suppressing the truth" is required to issue an adverse inference sanction where information is destroyed through the routine operation of a document retention policy).

Appendix A
Table of Authorities

Federal Cases

State Cases

Federal Statutes and Regulations

Federal Court Rules

State Court Rules

Ethics and Professional Responsibility Citations

Books, Articles, and Commentaries

John K. Villa, *The Inadvertent Disclosure of Privileged Material: What is the Effect on the Privilege and the Duty of Receiving Counsel?* 22 No. 9 ACC Docket 108 (Oct. 2004) 52
Kenneth J. Withers, *Electronically Stored Information: The December 2006 Amendments to the Federal Rules of Civil Procedure*, 4 Nw. J. Tech 8 Intell. Prop. 171(2006), *available at* http://www.law.northwestern.edu/journals/njtip/v4/n2/3 . . . . . passim
Gabrielle R. Wolohojian & David A. Giangrasso, *Expert Discovery and the Work Product Doctrine – Is Anything Protected?* 48-APR B. B.J. 10 (Mar./Apr. 2004) 24
Charles Alan Wright, Arthur R. Miller, & Richard L. Marcus, *Federal Practice and Procedure* § 2008.1 (2d ed. 2006). 18, 33
Charles Alan Wright, Arthur R. Miller, & Richard L. Marcus, *Federal Practice and Procedure* § 2008.2 (2d ed. 2006) 19, 47, 50
Charles Alan Wright, Arthur R. Miller, & Richard L. Marcus, *Federal Practice and Procedure* § 2016.3 (2d ed. 2006). 51, 55
Charles Alan Wright, Arthur R. Miller, & Richard L. Marcus, *Federal Practice & Procedure*, § 2218 at 449 (2d ed. 1994). 1
Gregory G. Wrobel, *et al., Counsel Beware: Preventing Spoliation of Electronic Evidence in Antitrust Litigation*, 20-SUM Antitrust 79 (2006) 31, 41

Appendix B

Suggested Cititation Format

This publication may be cited as follows:

> *The Sedona Principles, Second Edition: Best Practices, Recommendations & Principles for Addressing Electronic Document Production (The Sedona Conference® Working Group Series, 2007).*

The recommended short citation form is simply:

> *The Sedona Principles, Second Edition (2007).*

It may be appropriate to cite specific pages, principles, or comments. For example:

> *The Sedona Principles: Best Practices, Recommendations & Principles for Addressing Electronic Document Production, Second Edition 3-4 (The Sedona Conference® Working Group Series, 2007).*

> *The Sedona Principles, Second Edition (2007), Principle 11.*

> *The Sedona Principles, Second Edition (2007), Cmt. 5.e.*

Appendix C

Working Group Members & Observers (as of May 3, 2007)

Woods Abbott
Raytheon Company

E. Regan Adams
Credit Suisse

Whitney Adams
Cricket Technologies

Sharon A. Alexander
Jones Day

Thomas Y. Allman
Mayer Brown Rowe & Maw LLP

Keith Altman
Finkelstein & Partners LLP

Andreas Antoniou
Paul, Weiss, Rifkind, Wharton & Garrison LLP

James R. Arnold
KPMG

Hon. Leonard B. Austin
Supreme Court of the State of New York
Observer

John Bacevicius
Gartner, Inc.

Denise E. Backhouse
Morgan Lewis & Bockius LLP

Wanda Bailey
McGuireWoods LLP

Jennifer V. Baker
Navigant Consulting Inc.

Craig Ball
Craig D Ball PC

Katherine L. Ball, M.D.
Johns Hopkins University, Division of Health Sciences Informatics

Laura Bandrowsky
Duane Morris LLP

John A. Bannon
Schiff Hardin LLP

Theodore S. Barassi
Symantec Corp.

Thomas I. Barnett
Sullivan & Cromwell

Jason R. Baron
National Archives and Records Admin.
Observer

Diane Barrasso
Barrasso Consulting LLC

Andre Barry
Cline, Williams, Wright, Johnson & Oldfather, LLP

Courtney Ingraffia Barton
LexisNexis Applied Discovery

Bobbi Basile
Ernst & Young LLP

Cynthia Bateman
Georgia Pacific Corporation

James A. Batson
Liddle & Robinson, LLP

John F. Baughman
Paul, Weiss, Rifkind, Wharton & Garrison LLP

Kirby D. Behre
Paul, Hastings, Janofsky & Walker, LLP

Lawrence P. Bemis
Kirkland & Ellis LLP

Adam S. Bendell
Strategic Discovery Inc.

Steven C. Bennett
Jones Day

Kara Benson
Faegre & Benson LLP

Hon. Richard E. Best, Ret.
Action Dispute Resolution Services
Observer

R. Eric Bilik
McGuireWoods LLP

Joanna Blackburn
Starbucks Coffee Company

Stephanie Blair
Morgan Lewis & Bockius LLP

Alan Blakley
RLS Legal Solutions

Marjorie Rosenthal Bloom
U.S. Pension Benefit Guaranty Corporation
Observer

Christopher Boehning
Paul, Weiss, Rifkind, Wharton & Garrison LLP

Hildy Bowbeer
3M

John J. Bowers
Womble Carlyle Sandridge & Rice PLLC

Kevin F. Brady
Connolly Bove Lodge & Hutz LLP

Richard G. Braman
The Sedona Conference
Ex Officio

Allison Brecher
Marsh & McLennan Co.

Appendix C

Working Group Members & Observers cont.

Kerry A. Brennan
Pillsbury Winthrop Shaw Pittman LLP

Julia Brickell
Altria Corporate Services, Inc.

Kelli J. Brooks
KPMG

Charlene Brownlee
Davis Wright Tremaine LLP

Greg Buckles
Attenex Corporation

Macyl Burke
ACT Litigation Services

Chistine M. Burns
Cohasset Associates, Inc.

Paul E. Burns
Gallagher & Kennedy, P.A.

William P. Butterfield
Cohen, Milstein, Hausfeld & Toll, PLLC

Kara Buzga
Milberg Weiss Barshad & Schulman LLP

Jonathan S. Campbell
Capital One Services, Inc.

Mary Beth Cantrell
Amgen Inc.

Jacquelyn A. Caridad
Morgan Lewis & Bockius LLP

Diane Carlisle
Baker Robbins & Company

Scott A. Carlson
Seyfarth Shaw LLP

Hon. John L. Carroll, Ret.
Cumberland School of Law at Samford University
Observer

Vincent Catanzaro
DuPont

Barbara Caulfield
Affymetrix, Inc.

M. Kate Chaffee
Faegre & Benson LLP

Lloyd B. Chinn
Proskauer Rose LLP

Thomas A. Clare
Kirkland & Ellis LLP

Michael A. Clark
EDDix LLC

Matthew Clarke
Ryley Carlock & Applewhite

R. Noel Clinard
Hunton & Williams LLP

Matthew Cohen
Alix Partners

Andrew M. Cohen
EMC Corporation

Adam Cohen
FTI

Sigmund J. Collins
Philip Morris U.S.A

Clark R. Cordner
Wilmer Cutler Pickering Hale and Dorr LLP

Alfred W. Cortese Jr.
Cortese PLLC

Christopher V. Cotton
Shook Hardy & Bacon LLP

Jim Coulson
Huron Consulting Group LLC

David Couzins
Wilmer Cutler Pickering Hale and Dorr LLP

Moze Cowper
Amgen Inc.

William Craco
Johnson & Johnson

Joyce Craig-Rient
Finnegan Henderson Farabow Garrett & Dunner LLP

Tim Crouthamel
State Farm Insurance Company

Conor R. Crowley
DOAR Litigation Consulting

Wendy Butler Curtis
Fulbright & Jaworski, LLP

M. James Daley
Redgrave Daley Ragan & Wagner LLP

Jonathan A. Damon
LeBeouf, Lamb, Greene & MacRae

Chirstopher M. Davis
Steptoe & Johnson LLP

Martha Dawson
K&L Gates

Robert J. C. Deane
Borden Ladner Gervais LLP

Daniel T. DeFeo
The DeFeo Law Firm, PC

John Paul Deley
Energy Information Administration
Observer

Jonathan E. DeMay
Condon & Forsyth LLP

Radi Dennis
Sentry Consulting Group

William B. Dodero
Bayer Corporation

Manuel J. Dominguez
Berman Devalerio Pease Tabacco Burt & Pucillo

Paul F. Doyle
Proof Space

Phillip J. Duffy
Gibbons P.C.

David E. Dukes
Nelson, Mullins, Riley & Scarborough, LLP

Peg Duncan
Department of Justice, Canada
Observer

Victoria Edelman
LexisNexis Applied Discovery

Deborah Edwards
Duke Energy Corporation

Elizabeth F. Edwards
McGuireWoods LLP

Robert A. Eisenberg
Capital Legal Solutions

Laura E. Ellsworth
Jones Day

Todd Elmer
H5

Amor A. Esteban
Shook Hardy & Bacon LLP

Eric J. Evain
Connolly Bove Lodge & Hutz LLP

Cameron J. Evans
Honigman Miller Schwartz and Cohn, LLP

Hon. John M. Facciola
United States District Court District of Columbia
Observer

Mary Faria
Altria Corporate Services, Inc.

Jeffrey C. Fehrman
Electronic Evidence Labs

Joan E. Feldman
Navigant Consulting Inc.

Steve Fennell
Steptoe & Johnson LLP

Carmen Oveissi Field
Daylight Forensic & Advisory LLC

Kenneth Fields
Superior Court of AZ
Observer

Eric R. Finkelman
Ciba Specialty Chemicals Corporation

Jeffrey Flax
Administrative Office of the U.S. Courts
Observer

Jason B. Fliegel
Mayer Brown Rowe & Maw LLP

Joseph E. Foster
Akerman Senterfitt

Thomas Freeman
Reed Smith LLP

Amy Freestone
Faegre & Benson LLP

Eric M. Freidberg
Stroz Friedberg LLC

Suzanne Frost
Faegre & Benson LLP

Thomas E. Gaeta
Navigant Consulting Inc.

Randy Gainer
Davis Wright Tremaine LLP

David J. Galbenski
Lumen Legal

James H. Gallegos
Burlington Northern and Santa Fe Railway

Victoria B. Garcia
New Mexico State Court System
Observer

Aaron Gardner
Paul, Weiss, Rifkind, Wharton & Garrison LLP

Daniel K. Gelb
Gelb & Gelb LLP

Anthony I. Giacobbe Jr.
Zeichner Ellman & Krause LLP

Stanley M. Gibson
Jeffer Mangels Butler & Marmaro LLP

Daniel C. Girard
Girard Gibbs LLP

Edward Glynn
PricewaterhouseCoopers LLP

Dean Gonsowski
Xiotech, Inc.

Working Group Members & Observers cont.

James E. Gordon
Navigant Consulting Inc.

Ross Gotler
Paul, Weiss, Rifkind, Wharton & Garrison LLP

Richard Graham
Pension Benefit Guaranty Corporation
Observer

Ronald J. Green
Bank of America

Jay E. Grenig
Marquette University Law School

Ashley Griggs
Electronic Evidence Discovery, Inc.

Joseph P. Guglielmo
Whatley Drake & Kallas LLC

Matthew Hagarty
America Online, Inc.

Brian Hail
Haynes & Boone LLP

David H. Haines
Exterro

Julie Anne Halter
K&L Gates

Lori A. Ham
Poyner & Spruill LLP

Jennifer Hamilton
Deere & Company

Daniel J. Harbison
Connolly Bove Lodge & Hutz LLP

Earl Harcrow
Haynes & Boone LLP

Matthew S. Harman
King & Spalding LLP

Sherry B. Harris
Hunton & Williams LLP

Hope Haslam
Merrill Lextranet

Jeff Hatfield
Jordan Lawrence Group

Kris Haworth
LECG

Ronald J. Hedges
Nixon Peabody

Michael Henga
Pillsbury Winthrop Shaw Pittman LLP

Peter C. Hennigan
Faegre & Benson LLP

William Herr

Michael Heyrich
Citigroup Inc.

Josephine H. Hicks
Parker Poe Adams & Beinstein

Cathy Hilf
McGuireWoods LLP

Ted S. Hiser
Jones Day

Julie Hoff
Redgrave Daley Ragan & Wagner LLP

W. Michael Holm
Womble Carlyle Sandridge & Rice PLLC

Tim Hood
Redgrave Daley Ragan & Wagner LLP

Virginia W. Hoptman
Womble Carlyle Sandridge & Rice PLLC

Steve Horvath
Zantaz Inc.

Karen Hourigan
Redgrave Daley Ragan & Wagner LLP

Kelly Hoversten
Gray Plant Mooty

Geoffrey M. Howard
Bingham McCutchen LLP

Oleh Hrycko
H & A Computer Forensics

Kenton J. Hutcherson
The Hutcherson Law Firm

David W. Ichel
Simpson Thacher & Bartlett LLP

David A. Irvin
Womble Carlyle Sandridge & Rice PLLC

Conrad Jacoby
Attorney & Consultant

John Janes
Deloitte

Harvey Jang
Symantec Corp.

William R. Jenkins Jr.
Jackson Walker, LLP

John H. Jessen
Electronic Evidence Discovery, Inc.

Kevin F. Joerling
ARMA International

Monica Johnson
Faegre & Benson LLP

Mary Jo Johnson
Wilmer Cutler Pickering Hale and Dorr LLP

Appendix C

Working Group Members & Observers cont.

Glenn Johnson
King & Spalding LLP

Deborah A. Johnson
Orchestria

Jeffrey J. Joyce
Jones Day

Deborah Juhnke
Blackwell Sanders Peper Martin LLP

Randolph A. Kahn
Kahn Consulting Inc.

Sidney Kanazawa
Van Etten Suzumoto & Becket LLP

Dr. Hironao Kaneko
Tokyo Institute of Technology

Larry Kanter
Alvarez & Marsal

Gregory S. Kaufman
Sutherland Asbill & Brennan

Conrad S. Kee
Jackson Lewis LLP

Gaither Keener Jr.
Lowe's Companies, Inc.

John B. Kennedy
LeBeouf, Lamb, Greene & MacRae

Anne Kershaw
A. Kershaw PC, Attorneys and Consultants

Priya Keshav
Tusker Group LP

David J. Kessler
Drinker Biddle & Reath LLP

Laura M. Kibbe
Pfizer Inc.

Elizabeth Kidd
LexisNexis Applied Discovery

Dennis Kiker
Moran Kiker Brown PC

John K. Kim
Johnson & Johnson

Mike Kinnaman
Attenex Corporation

Shannon Capone Kirk
Ungaretti & Harris

David Kittrell

Gene Klimov
DOAR Litigation Consulting

Melissa L. Klipp
Drinker Biddle & Reath LLP

Liane R. Komagome
Hewlett Packard

Steven S. Krane
Barton Barton & Plotkin LLP

Antigone Kriss
Chambers of Judge Kimberly Moore
Observer

K. J. Kuchta
Forensics Consultation Solutions, LLC

James S. Kurz
Womble Carlyle Sandridge & Rice PLLC

Bradley R. Kutrow
Helms Mulliss & Wicker

Janet Kwuon
Reed Smith LLP

Francis Lambert
Zantaz Inc.

Edwin M. Larkin
Winston & Strawn LLP

Monica Wiseman Latin
Carrington, Coleman, Sloman & Blumenthal, L.L.P.

Brandon Lee
Deloitte Financial Advisory Services LLP

R. Michael Leonard
Womble Carlyle Sandridge & Rice PLLC

Ronald J. Levine
Herrick Feinstein LLP

Pauline Levy
McDonalds Corporation

Robert Levy
Haynes & Boone LLP

Paul Lewis
Protiviti

Julie Lewis
Digital Mountain, Inc.

Thomas Lidbury
Mayer, Brown, Rowe & Maw LLP

Joe Looby
FTI

Ralph Losey
Akerman Senterfitt

Lorrie L. Luellig
Ryley Carlock & Applewhite

Patricia Clarke Lukens

James K. Lynch
Latham & Watkins LLP

Appendix C

Working Group Members & Observers cont.

Cecil Lynn
LexisNexis Applied Discovery

Sheila Mackay
Daegis

Audra Hale Maddox
Womble Carlyle Sandridge & Rice PLLC

Heidi Maher
Renew Data Corp.

Michelle Mahoney
Mallesons Stephen Jaques

Sheri Malec
McDonalds Corporation

Carrie Mallen
McKesson Corporation

A. John P. Mancini
Mayer Brown Rowe & Maw LLP

Joseph Mann
Merrill Lextranet

Browning E. Marean III
DLA Piper

Robert Markham
Cohasset Associates, Inc.

David G. Martin
Medtronic, Inc.

James H. Martin
Office of the Attorney General of New Jersey
Observer

Ann Marie Mason
Metropolitan Life Insurance Co.

Geoffry C. Mason
Sidley Austin LLP

Kathleen M. Massey
Motorola Inc.

J. W. Matthews III
Haynesworth Sinkler Boyd, P.A.

Wayne Matus
Mayer Brown Rowe & Maw LLP

Tom Matzen
Xact

J. J. McCracken
Cooper Tire & Rubber Company

Anne B. McCray
McGuireWoods LLP

Gregory McCurdy
Microsoft Corporation

Nancy McMahon
Department of Justice
Observer

William McManus
Ryley Carlock & Applewhite

Stephanie Mendelsohn
Genentech

James L. Michalowicz
ACT Litigation Services

Lucie Miller
Eli Lilly & Co.

Bill Millican
ARMA International

Scott Milner
Morgan Lewis & Bockius LLP

Denise M. Mineck
Life Investors Insurance Company of America

Robert D. Moody
Berenfeld, Spritzer, Shechter & Sheer

Tim Moorehead
BP America, Inc.

Jack Moorman
PricewaterhouseCoopers LLP

Steve Morrissett
Finnegan Henderson Farabow Garrett & Dunner LLP

Helen Bergman Moure
K&L Gates

Shelia Murphy
Metropolitan Life Insurance Co.

Justin Myers
Rambus

Simon Nagel
Dechert LLP

Paul J. Neale Jr.
DOAR Litigation Consulting

Jon A. Neiditz
Lord Bissell & Brook LLP

John Nemazi
Brooks Kushman PC

Mollie Nichols
First Advantage

Jonathan Nystrom
Cataphora

John Oakley
Berenfeld, Spritzer, Shechter & Sheer

Kate O'Brien
Digital Mandate

Kate Oberlies O'Leary
General Electric Company

Timothy L. O'Mara
Latham & Watkins LLP

Maureen O'Neill
Paul, Hastings, Janofsky & Walker, LLP

Appendix C

Working Group Members & Observers cont.

Patrick Oot
Verizon Communications

Timothy M. Opsitnick
JurInnov Ltd.

Greg Osinoff
Digital Mandate

Robert D. Owen
Fulbright & Jaworski, LLP

Laura Lewis Owens
Alston & Bird, LLP

Neil Packard
e-Diligent, Inc.

Deidre Paknad
PSS Systems Inc.

Robert W. Pass
Carlton Fields

Thomas Pasternak
DLA Piper

John Patzakis
Guidance Software

George L. Paul
Lewis & Roca LLP

Richard Pearce-Moses
Arizona State Library
Observer

Cheryl L. Pederson
Cargill Inc.

Peter Pepiton II
CA Inc.

Ginger Heyman Pigott
Reed Smith LLP

Justin David Pitt
Bass, Berry & Sims PLC

Jeanette Plante
U.S. Department of Justice, Justice Management Divison, Office of Records Mangement Policy
Observer

Vivian Polak
LeBeouf, Lamb, Greene & MacRae

Anthony Polk
Electronic Evidence Discovery, Inc.

Ashish S. Prasad
Mayer Brown Rowe & Maw LLP

James Proscia
Brooks Kushman PC

Michael J. Prounis
Evidence Exchange

Charles R. Ragan
Redgrave Daley Ragan & Wagner LLP

Sreenu P. Raju
Sreenu P. Raju, P.L.C.

Donald C. Ramsay
Stinson Morrison Hecker LLP

Jonathan Redgrave
Redgrave Daley Ragan & Wagner LLP

Jeffrey Reed
Maron & Marvel PA

Heather Reed
Capital One Services, Inc.

Daniel L. Regard
LECG

Mark V. Reichenbach

Anthony Reid
Deloitte Financial Advisory Services LLP

David Remnitz
FTI

Ann Marie Riberdy
Wilmer Cutler Pickering Hale and Dorr LLP

Mark (Rick) E. Richardson III
Glaxo Smith Kline

Mary K. Riley
Bank of America

John T. Ritter
Bank of America

Karin A. Roberts
Eli Lilly & Co.

Paul M. Robertson
Redgrave Daley Ragan & Wagner LLP

William C.E. Robinson
GEICO Insurance Company

E. Casey Roche III
Discovery Mining Inc.

Michael S. Roe
Ashland Inc.

Dave Rogers
Ernst & Young LLP

Herbert L. Roitblat
Orcatec LLC

James E. Rooks Jr.
Association of Trial Lawyers of America

Andrea D. Rose
Crowell & Moring LLP

John J. Rosenthal
Howery LLP

Hon. Lee H. Rosenthal
United States Courthouse
Observer

Ira P. Rothken
Rothken Law Firm

Appendix C

Working Group Members & Observers cont.

Charles Rothman
H & A Computer Forensics

Kenneth Rowe
Chief Security Officers

Ashley Rowe
Metlife

Jane K. Rushton

Stuart K. Sammis
Corning Incorporated

Joseph R. Saveri
Lieff Cbraser Heimann & Bernstein, LLP

Leigh R. Schachter
Verizon Wireless

Gregory P. Schaffer
Alltell Corporation

Karen Schak
Deloitte

Hon. Shira A. Scheindlin
United States District Court
Southern District of New York
Observer

David Schieferstein
Philip Morris U.S.A

Ryan Schmelz
Riberian Enterprises Inc.

Christopher Schnabel
Paul, Weiss, Rifkind, Wharton & Garrison LLP

Eric J. Schwarz
Ernst & Young LLP

Dan P. Sedor
Jeffer Mangels Butler & Marmaro LLP

P. Brian See
Seyfarth Shaw LLP

Steven Shankroff
Skadden ARPS

Jeffrey C. Sharer
Sidley Austin LLP

Jackson Sharman III
Lightfoot Franklin & White

Kenneth Shear

Gregory Shelton
Williams Kastner & Gibbs PLLC

Robert W. Shely
Bryan Cave LLP

James D. Shook
EMC Corporation

Mark Sidoti
Gibbons P.C.

Sonya L. Sigler
Cataphora

Tom J. Sikora
El Paso Corporation

Dominique Simard
Ogilvy Renault LLP

Robert R. Simpson
Shipman & Goodwin LLP

Julie Sinor
PricewaterhouseCoopers LLP

Amy Sipe
ACT Litigation Services

Peter B. Sloan
Blackwell Sanders Peper Martin LLP

Thomas J. Smedinghoff
Wildman, Harrold LLP

Arthur L. Smith
Husch & Eppenberger

Jessica Cullen Smith
McDermott Will & Emery

Howard Smith
Barton Barton & Plotkin LLP

Ken Sokol
Electronic Evidence Discovery, Inc.

Catherine J. Sosso
Union Pacific Railroad Company

Carolyn Southerland
Baker Botts LLP

Judith Starr
Pension Benefit Guaranty Corporation
Observer

Stephen R. Stegich III
Condon & Forsyth LLP

Heidi Stenberg
Ernst & Young LLP

Kimberly Baldwin Stried
KBS Consulting - Lake County Physicians Association

Cheryl Strom
McDonalds Corporation

Ariana J. Tadler
Milberg Weiss Barshad & Schulman LLP

Steven W. Teppler
Steven W. Teppler, Esq.

Jeane Thomas
Crowell & Moring LLP

Appendix C

Working Group Members & Observers cont.

Paul Thompson
Dartmouth College

Hon. Samuel A. Thumma
Maricopa County Superior Court
Observer

Christina (Tina) Torres
Microsoft Corporation

Robert W. Trenchard
Wilmer Cutler Pickering Hale and Dorr LLP

John Turner
AnaComp

Judy Van Dusen
VanKorn Group, Limited

Jason Velasco

A. J. Venit
Bank of America

Peter Wacht
National Court Reporters Association

Jim Wagner
DiscoverReady

Lori Ann Wagner
Redgrave Daley Ragan & Wagner LLP

Vincent Walden
Ernst & Young LLP

Kathryn Hannen Walker
Bass, Berry & Sims PLC

Alston Walker
Stroock & Stroock & Lavan LLP

Skip Walter
Attenex Corporation

Paul L. Warner
Jeffer Mangels Butler & Marmaro LLP

Hon. Ira B. Warshawsky
Supreme Court of New York, Commercial Division
Observer

Ryan Wasell
Weyerhaeuser Company

Emroy Watson
Yamaha Motor Corporation

Hon. David Waxse
United States Distict Court
District of Kansas
Observer

Laurie A. Weiss
Fulbright & Jaworski, LLP

Brian Westenberg
Daimler Chrysler Corp.

David Wetmore
Ernst & Young LLP

Maggie Whitney
Sidley Austin LLP

Robert B. Wiggins
Morgan Lewis & Bockius LLP

James "Chuck" Williams
MetaLINCS

Jack Williams
Powell, Goldstein, Frazer & Murphy

Robert F. Williams
Cohasset Associates, Inc.

Scott L. Winkelman
Crowell & Moring LLP

Thomas P. Wisinski
Haynes & Boone LLP

Kenneth J. Withers
The Sedona Conference
Ex Officio

Edward C. Wolfe
General Motors Corporation

Gregory B. Wood
Fulbright & Jaworski, LLP

Todd I. Woods
Lowe's Companies, Inc.

Sarah E. Worley
Pre-Trial Solutions, Inc.

Susan B. Wortzman
Lerners LLP

Joel Wuesthoff
Ibis Consulting

Chris Yowell
Celerity Consulting

Jason Yurasek
Bingham McCutchen LLP

Patrick Zeller
Guidance Software

The Sedona Conference Working Group Series & WGS℠ Membership Program

> **"DIALOGUE DESIGNED TO MOVE THE LAW FORWARD IN A REASONED AND JUST WAY."**

The Sedona Conference® Working Group Series ("WGS℠") represents the evolution of The Sedona Conference® from a forum for advanced dialogue to an open think-tank confronting some of the most challenging issues faced by our legal system today.

The WGS℠ begins with the same high caliber of participants as our regular season conferences. The total, active group, however, is limited to 30-35 instead of 60. Further, in lieu of finished papers being posted on the website in advance of the Conference, thought pieces and other ideas are exchanged ahead of time, and the Working Group meeting becomes the opportunity to create a set of recommendations, guidelines or other position piece designed to be of immediate benefit to the bench and bar, and to move the law forward in a reasoned and just way. Working Group output, when complete, is then put through a peer review process, including where possible critique at one of our regular season conferences, hopefully resulting in authoritative, meaningful and balanced final papers for publication and distribution.

The first Working Group was convened in October 2002, and was dedicated to the development of guidelines for electronic document retention and production. The impact of its first (draft) publication—*The Sedona Principles; Best Practices Recommendations and Principles Addressing Electronic Document Production* (March 2003 version)—was immediate and substantial. *The Principles* was cited in the Judicial Conference of the United State Advisory Committee on Civil Rules Discovery Subcommittee Report on Electronic Discovery less than a month after the publication of the "public comment" draft, and was cited in a seminal e-discovery decision of the Federal District Court in New York less than a month after that. As noted in the June 2003 issue of Pike & Fischer's *Digital Discovery and E-Evidence, "The Principles*...influence is already becoming evident."

The WGS℠ Membership Program was established to provide a vehicle to allow any interested jurist, attorney, academic or consultant to participate in Working Group activities. Membership provides access to advance drafts of Working Group output with the opportunity for early input, and to a Bulletin Board where reference materials are posted and current news and other matters of interest can be discussed. Members may also indicate their willingness to volunteer for special Project Team assignment, and a Member's Roster is included in Working Group publications.

We currently have active Working Groups in the areas of 1) electronic document retention and production; 2) protective orders, confidentiality, and public access; 3) the role of economics in antitrust; 4) the intersection of the patent and antitrust laws; (5) *Markman* hearings and claim construction; (6) international e-information disclosure and management issues; and (7) e-discovery in Canadian civil litigation. *See* the "Working Group Series" area of our website www.thesedonaconference.org for further details on our Working Group Series and the WGS℠ Membership Program.

Visit www.thesedonaconference.org

THE SEDONA CONFERENCE® WORKING GROUP SERIES

WGS℠

THE SEDONA GUIDELINES

Best Practices Addressing Protective Orders, Confidentiality & Public Access in Civil Cases

A Project of The Sedona Conference®
Working Group on Protective Orders,
Confidentiality & Public Access (WG2)

MARCH 2007

THE SEDONA GUIDELINES:
Best Practices Addressing Protective Orders, Confidentiality & Public Access in Civil Cases

Editorial Team:
Professor Laurie Dore, Drake University, Des Moines, IA
Ronald J. Hedges, Counsel, Nixon Peabody, New York, NY;
(formerly U.S. Magistrate Judge, U.S. District Court for the District of New Jersey 1986-2007)
Kenneth J. Withers, Director of Judicial Education & Content,
The Sedona Conference®, Sedona, AZ

Advisory Editorial Team:
The Hon. J. Thomas Marten, District of Kansas, Wichita, KS
Prof. Stephen Saltzburg, George Washington University, Washington, DC
Prof. Jay Tidmarsh, Notre Dame Law School, Notre Dame, IN

REPRINT REQUESTS:
Requests for reprints or reprint information should be directed to
Richard Braman, Executive Director of The Sedona Conference®,
at tsc@sedona.net or 1-866-860-6600.

Dedication to H. Brent McKnight (1952-2004)

H. Brent McKnight, a member of the Steering Committee of this Working Group, passed away suddenly and unexpectedly in the year between the group's first meeting and the publication of its first draft Principles & Best Practices. Years before, Brent had been a Morehead Scholar who spent an internship working for Senator Sam Ervin, reading through 1,100 boxes of Watergate documents. As a Rhodes Scholar, studying religious philosophy under Bishop Stephen Neill at Oxford, Brent decided that justice was a true goal of religion and that justice would be his career. Prosecutor, state court judge, United States Magistrate Judge, United States District Judge, teacher, writer, scholar, husband, father, colleague and friend: through all this he infused his desire to see justice. And through all this, we were struck by the fact that he kept asking us to make sure he was getting it right. We were amazed at his humility wedded to intelligence; his sense of humor wedded to hard work. To you, Brent, we dedicate our work. May it help others advance the justice to which you devoted your life.

Alan Blakley

Foreword

The Sedona Conference® is a nonprofit law and policy think tank based in Sedona, Arizona, dedicated to the advanced study, and reasoned and just development, of law and policy in the areas of complex litigation, antitrust law and intellectual property rights. It established the Working Group Series (the "WGS℠") to bring together some of the nation's finest lawyers, consultants, academics and jurists to address current issue areas that are either ripe for solution or in need of a "boost" to advance law and policy. (See Appendix A for further information about The Sedona Conference® in general and the WGS℠ in particular). This publication is the result of nearly two years of nationwide dialogue conducted by our Working Group Two (WG2), which is devoted to Best Practices and Guidelines Addressing Protective Orders, Confidentiality and Public Access in Civil Cases.

The impetus for the formation of WG2 came from members of the federal judiciary, court clerks, and practitioners concerned with the effect that nationwide electronic Case Management/Electronic Case Filing ("CM/ECF") would have on the patchwork of local filing rules and practices that had developed over the years. On the one hand, electronic access to traditionally public court records promised to help the courts realize their role as a co-equal branch of government, by making the courts transparent and accountable, and by educating the public as to the courts' role in a democratic society. On the other hand, the possibility that electronic court filings would immediately be accessible by the public via the Internet, without any intervening review by court personnel, meant that personal and proprietary information could suddenly enter the public domain without the cloak of "practical obscurity" provided by manual filing of, and access to, paper court documents physically located at the courthouse.

This question, and the larger ramifications for society as a whole, concerned United States Magistrate Judge Brent McKnight of North Carolina, a member of the Judicial Conference Advisory Committee on Civil Rules, who in 2004 was chairing a subcommittee discussing the much narrower issue of public access to settlement agreements filed with the federal courts. Together with members of the Litigation Section of the Federal Bar Association, he approached The Sedona Conference with the idea of establishing a Working Group to study this issue and develop a set of guidelines or best practices for courts and practitioners working through the complicated process of framing local rules and procedures to accommodate CM/ECF. The group first met in April of 2004 in Sedona. That initial meeting was unique in bringing together attorneys who primarily represented corporate defendants, attorneys who primarily represented individual plaintiffs, public interest groups, and news media. Each came with their own experiences and concerns, and each came with certain ideas of what they wanted. But in the process of dialogue, their divergent views came together, as they listened to each other and began the process of genuine accommodation of each others' interests.
A major blow was dealt to the efforts of WG2, and we all experienced deep personal loss, with the untimely death of Judge McKnight just a few months after that first meeting. But the group resolved to continue the dialogue and draft a document that reflected, as much as possible, the scholarship, balance, wisdom and practicality that Judge McKnight strove to achieve.

The resulting Public Comment Draft was published in May of 2005, and was circulated widely to judges, practitioners, academics, and other interested parties. With the assistance of the American Judicature Society, the Dallas Bar Association, the Samuel I. Newhouse Foundation and others, public "town hall" meetings were held in four major cities to present the Public Comment Draft and air a wide range of comments and responses. The projected six-month Public Comment Period was extended an additional six months, and a special effort was made to reach out to sectors of the legal profession who believed that their views were underrepresented in the initial effort. Dozens of constructive comments were received, and a second meeting of the Working Group was held in Sedona in April 2006. During that meeting, several significant revisions were agreed upon, and an editorial committee was established to integrate the revisions and comments into a final version for publication. In November of 2006, a revised version was presented to the Working Group for further comment. A special Editorial Advisory Committee was drawn from The Sedona Conference's Advisory Board, consisting of a federal judge and two distinguished legal academics not previously associated with WG2 to review the subsequent draft to make sure that it presented an accurate and balanced portrayal of the current law, and an unbiased set of recommended best practices. In February of 2007 the final version of this publication was completed, the

culmination of the longest public comment period and most extensive Working Group dialogue in the experience of The Sedona Conference.

This Working Group's efforts to work towards completion of a post-public comment draft were subjected to an orchestrated campaign to derail publication. A number of WG2 members ended up resigning from the Working Group, and a number told us they did not want their names, or their firm names, included in the roster we typically publish in Working Group Series publications, though their names do appear on the "Opposing Views" piece (see below). Indeed, after this work product was completed even one of the editorial team members who had devoted significant time and energy to this effort and to incorporate wherever consistent with the law the views of members who are now listed on the "Opposing Views" piece had to withdraw his and his firm's name from this work product. This "politization" of Working Group efforts was new to The Sedona Conference and is, frankly, quite distressing. This presented the editors with a conundrum, for while the publication now reflects significant constructive input from members who have resigned or are on the "Opposing Views" piece, since a number of (former) members have resigned or withdrawn their names from the roster, the resulting roster would leave the misimpression that the publication reflects only input from those listed, instead of reflecting all the efforts to reach accommodation and compromise through dialogue. Rather than publishing an unrepresentative roster, the Editorial Committee has opted to remove the roster of WG2 members from this publication in its entirety.

The authors of the "Opposing Views" piece* argue a lack of consensus "in this still controversial area" and, on Working Group calls, sought to delay publication to allow for further dialogue. It was the view of The Sedona Conference, however, that the authors of the Opposing Views simply have a different view of the role of the judiciary in our society and the need for public oversight of the core adjudicatory function that led to the formation of WG2 in the first place; no amount of dialogue or word-smithing would overcome this gap. While "controversy" developed within WG2 surrounding this issue, the Guidelines themselves are not, in the views of the Editorial Team and Advisory Editorial Board, "controversial;" they simply seek to clarify the law.

As noted above, The Sedona Conference Working Group Addressing Protective Orders, Confidentiality and Public Access was formed out of a desire to help bring some clarity and uniformity to practices involving protective orders in civil litigation and determinations affecting public access to documents filed or referred to in court. It is hoped that the result of the Working Group's robust dialogue, and the principles and commentary that follow, will be of immediate benefit to the bench and bar as they approach matters relating to confidentiality protective orders, sealing orders, and public access.

I want to thank the entire Working Group for all their hard work, and especially the Editorial Committee (including the unnamed member) who have guided this effort for the past year. A special thank-you is also in order to our Advisory Editorial Board who helped us to ensure the work product reflects the law and struck a proper balance. We also want to note that the Working Groups of The Sedona Conference could not accomplish their goals without the financial support of the annual sponsors of The Sedona Working Group Series listed at http://www.thesedonaconference.org/sponsorship.

To make suggestions or if you have any questions, or for further information about The Sedona Conference®, its Conferences or Working Groups, please go to http://www.thesedonaconference.org or contact us at tsc@sedona.net.

Richard G. Braman
Executive Director
The Sedona Conference®
March 2007

* *The "Opposing Views" piece is on our website under "Publications>WG2." It is worth noting that half of the signatories on the opposing views piece became members of WG2 after publication of the public comment version in May 2005, and more than a year after formation of the Working Group and its first face-to-face meeting. Two of the signatories never became WG2 members. It is more akin to a "public comment" than a WG2 effort.*

The Sedona Guidelines: Best Practices Addressing Protective Orders, Confidentiality & Public Access in Civil Cases

Chapter 1: Discovery

Principle 1: There is no presumed right of the public to participate in the discovery process or to have access to the fruits of discovery that are not submitted to the court.

Principle 2: Absent an agreement between the parties or a court order based on a showing of good cause, a litigant is not precluded from disclosing the fruits of discovery to non-parties.

Principle 3: A protective order entered under Fed. R. Civ. P 26(c) to facilitate the exchange of discovery materials does not substitute for the individualized judicial determination necessary for sealing such material, if filed with the court on a non-discovery matter.

Principle 4: On a proper showing, non-parties should be permitted to intervene to challenge a protective order.

Chapter 2: Pleadings, Court Orders, Substantive Motions & Dockets

Principle 1: In civil proceedings, the public has a qualified right of access to documents filed with a court that are relevant to adjudicating the merits of a controversy. In compelling circumstances, a court may exercise its discretion to deny public access to submitted documents to protect the privacy, confidentiality or other rights of the litigants.

Principle 2: The public has a qualified right of access to court dockets that can only be overcome in compelling circumstances.

Principle 3: There is a qualified right of access to judgments, judicial opinions and memoranda, and orders issued by a court that can only be overcome in compelling circumstances.

Principle 4: Notice of motions to seal and supporting materials should be reflected in the publicly accessible docket.

Principle 5: Non-parties may seek leave to intervene in a pending case to oppose a motion to seal, to have an existing sealing order modified or vacated, or to obtain a sealing order.

Chapter 3: Proceedings in Open Court

Principle 1: The public has a qualified right of access to trials that can only be overcome in compelling circumstances.

Principle 2: The public has a qualified right of access to the jury selection process.

Principle 3: Absent a compelling interest, the public should have access to trial exhibits.

Chapter 4: Settlements

Principle 1: There is no presumption in favor of public access to unfiled settlements, but the parties' ability to seal settlement information filed with the court may be restricted, due to the presumptively public nature of court filings in civil litigation.

Principle 2: Settlements filed with the court should not be sealed unless the court makes a particularized finding that sufficient cause exists to overcome the presumption of public access to judicial records.

Principle 3: Settlement discussions between parties and judges should not be subject to public access.

Principle 4: Absent exceptional circumstances, settlements with public entities should not be confidential.

Principle 5: An attorney's professional responsibilities may affect considerations of confidentiality in settlement agreements.

Chapter 5: Privacy & Public Access to the Courts in an Electronic World

I. Four Basic Policy Approaches

1. Open electronic access, with minimal limits.
2. Generally open electronic access, coupled with more significant limits on remote electronic public access.
3. Electronic access only to documents produced by the courts.
4. Systematic reevaluation of the content of the public case file, combined with limited access to electronic files.

II. Common Features of Recently-Developed Court Rules and Policies on Public Access to Court Records

1. A statement of the overall purpose for the rule or policy.
2. Definitions of key terms used in the rule.
3. A procedure to inform litigants, attorneys, and the public that (a) every document in a court case file will be available to anyone upon request, unless sealed or otherwise protected; (b) case files may be posted on the Internet; and (c) the court does not monitor or limit how case files may be used for purposes unrelated to the legal system.
4. A statement affirming the court's inherent authority to protect the interests of litigants and third parties who may be affected by public disclosure of personal, confidential, or proprietary information..
5. A list of the types of court records that are presumptively excluded (sealed) from public access by statute or court rule.
6. A statement affirming that the public right to access court records and the court's authority to protect confidential information should not, as a general matter, vary based on the format in which the record is kept (e.g., in paper versus electronic format), or based on the place where the record is to be accessed (i.e., at the courthouse or by remote access).

7. As an exception to feature 6 above, a list of the types of court records that -- although not sealed -- will not be available by remote electronic public access.
8. A list of the types of information that either: a) must not be filed in an open court record, or b) if filed, must be redacted or truncated to protect personal privacy interests. These provisions mainly apply to personal identifiers such as the SSN, account numbers, and home addresses of parties.
9. Procedure for a court to collect and maintain sensitive data elements (such as SSN) on special forms (paper or electronic) that will be presumptively unavailable for public access. Such procedures generally build on technology to segregate sensitive information so that public access can be restricted in appropriate situations.
10. Procedure to petition for access to records that have been sealed or otherwise restricted from public access, and a statement of the elements required to overcome the presumption of non-disclosure.
11. Procedure to seal or otherwise restrict public access to records, and a statement of the burden that must be met to overcome the presumption of disclosure.
12. An affirmation that a rule on public access to court records does not alter the Court's obligation to decide, on a case-by-case basis, motions to seal or otherwise restrict public access to court records.
13. Guidance to the courts concerning data elements that are contained in electronic docketing systems that must (or must not) be routinely made available for public access.
14. Guidance for attorneys and/or litigants concerning: (a) the extent to which public case files will be made available electronically; and (b) the need to exercise caution before filing documents and information that contain sensitive private information, which is generally defined elsewhere in the rule.
15. An explanation of the limits, if any, on the availability of "bulk" and/or "compiled" data from public court records. Some rules specify that such data will only be made available to certain entities, for certain defined purposes, and pursuant to agreements to refrain from certain uses of the records obtained.
16. A statement concerning the fees that a court may charge for public access to court records.

Table of Contents

Introduction

We live in an open and democratic society that depends upon an informed citizenry and public participation in government. Open public meetings laws and federal and state freedom of information laws facilitate such participation by providing citizens with a right of access to information concerning their government. Indeed, the First Amendment protects "the stock of information from which members of the public may draw." *Richmond Newspapers, Inc. v. Virginia*, 448 U.S. 555, 576 (1980).

At the same time, our society places high premiums upon personal privacy, property rights, and individual autonomy. The United States Supreme Court has elevated some aspects of privacy to a constitutional (albeit rather amorphous) right. Our country has long valued entrepreneurial confidentiality as a key to social and material progress, promoting individual initiative, private enterprise, and technological innovation and the right to protect the property created by that enterprise. Courts have made clear in the civil litigation context that litigants may have privacy and proprietary rights in certain of the information produced during the discovery process. *Seattle Times v. Rhinehart,* 467 U.S. 20 (1984). Nevertheless, the primary responsibility to protect those rights at each stage of the litigation rests on the attorney for the producing party.

This inherent tension between public access to information about government activities and the desire to protect personal privacy, intellectual property and confidential business information comes to a head in the debate concerning confidentiality in litigation. As with the legislative and executive branches of government, our democratic society depends upon public participation in and access to the judicial process. Access to the courts both improves the operation of the judicial system and fuels the informed discussion essential to democracy. Public access to judicial proceedings facilitates public monitoring of our publicly-created, staffed, and subsidized judicial system. Fair and open judicial proceedings and decisions encourage public confidence in and respect for the courts - a trust essential to continued support of the judiciary. A public eye on the litigation process can enhance prompt, fair and accurate fact-finding and decision-making. Perjury is deterred, witnesses may step forward, and judgments may be tempered with greater care and deliberation. A public trial also educates citizens about the justice system itself as well as its workings in a particular case.

Unlike the legislative and executive branches of government, however, the primary function of the courts is the resolution of the "cases and controversies" before them, and public access to certain stages of civil lawsuits casts light beyond the judicial process itself. Indeed, civil litigation most often involves disputes between private parties who are drawn into the courts reluctantly or even involuntarily. These court proceedings may require the disclosure of intimate personal or financial information or the disclosure of trade secrets or confidential marketing, research, or commercial information may be at stake. Public access to the pretrial, trial or settlement stages of those cases thus might jeopardize legitimate privacy or proprietary interests of the litigants. Moreover, public access may hamstring the litigants' ability to resolve their dispute in a mutually agreed manner.

Many threshold questions were addressed by WG2: Do litigants give up a measure of their privacy and autonomy when they enter the doors of the public courthouse in order to resolve their disputes? To what extent should court rules on protective orders, confidentiality and public access take into consideration the possibility that producing parties (or non-parties) did not voluntarily choose the dispute resolution forum?

How is a court to honor the right of public access to judicial proceedings while protecting privacy and property interests? In which cases must such privacy and proprietary interests bow to a broader public interest?

Virtually every federal circuit court of appeals and state court of last resort that has spoken on these matters has determined that courts are required to weigh the public interest in the particular proceeding or stage of the litigation against the private interest in maintaining the confidentiality of the material under consideration.[1]

On the public interest side, the general rule announced by the United States Supreme Court is that the public's right of access to material produced in connection with a particular pretrial or trial proceeding arises when (1) the proceeding has historically been open and (2) public access plays a significant role in the proper functioning of the process. *Press-Enterprise Co. v. Superior Court*, 478 U.S. 1, 8 (1986); *Globe Newspaper Co. v. Superior Court*, 457 U.S. 596, 605-06 (1982). In doing so, the Court and the case law relying on this general rule have made distinctions between, for instance, discovery as historically private exchanges conducted by the parties, and trials as historically open proceedings in which the public has an interest, directly or as a matter of public accountability. *Baxter International v. Abbott Labs*, 297 F. 3d 544 (7th Cir. 2002).

On the private interest side, statutes and court rules have declared some types of proceedings (e.g., juvenile, child abuse, adoption, and guardianship) to be presumptively closed to the public, and certain types of information (e.g., the "personal identifiers" specified in proposed Fed. R. Civ. P. 5.2, http://www.uscourts.gov/rules/Rules_Publication_August_2005.pdf#page=55, including Social Security numbers, dates of birth, financial account numbers and names of minor children) to be presumptively eligible for exclusion from part or all or the court record available to the public. Case law has also given great weight to the private interest in protecting bona fide trade secrets and confidential proprietary information, such as marketing plans, employee training manuals, computer source code, and customer lists. Less weight has been given to unsupported claims of confidentiality for broadly designated business information. *Citizens First National Bank of Princeton v. Cincinnati Insurance Co.*, 178 F. 3d 943 (7th Cir. 1999).

[1] "[T]he ordinary showing of good cause which is adequate to protect discovery material from disclosure cannot alone justify protecting such material after it has been introduced at trial. This dividing line may in some measure be an arbitrary one, but it accords with long-settled practice in this country separating the presumptively private phase of litigation from the presumptively public." *Poliquin v. Garden Way Inc.*, 989 F.2d 527, 533 (1st Cir. 1993). *Compare Pansy v. Borough of Stroudsburg*, 23 F.3d 772, 786-87 (3d Cir. 1994) (confidentiality order over unfiled settlement agreement); *Phillips v. General Motors Corp.*, 307 F.3d 1206, 1210-12 (9th Cir. 2002) (confidentiality order over unfiled settlement information) *with* In Re *Providence Journal*, 293 F.3d 1, 9-11 (1st Cir. 2002) (access to trial exhibits); *Lugosch v. Pyramid Co.*, 435 F.3d 110, 119-20 (2d Cir. 2006) (access to summary judgment materials); *Hartford Courant Co. v. Pelligrino*, 380 F.3d 83, 90-96 (2d Cir. 2004) (access to dockets); In Re *Cendant Corp.*, 260 F.3d 183, 192-93 (3d Cir. 2001) (access to bids and bidding auction); *Leucadia v. Applied Extrusion Technologies*, 998 F.2d 157, 161-65 (3d Cir. 1993) (access to nondiscovery pretrial motions); *Virginia Dept. of State Police v. Washington Post*, 386 F.3d 567, 574-77 (4th Cir. 2004) (access to summary judgment materials); *Second v. Van Waeyenberghe*, 990 F.2d 845, 848 (5th Cir. 1993) (access to transcript and final order of permanent injunction as part of settlement agreement); *Baxter Internat'l, Inc. v. Abbott Labs.*, 297 F.3d 544, 545-56 (7th Cir. 2002) (access to documents on appeal); *Grove Fresh Distrib., Inc. v. Everfresh Juice Co.*, 24 F.3d 983, 896-97 (7th Cir. 1994) (access to court files); In Re *Neal*, 461 F.3d 1048, 1052 (8th Cir. 2006) (access to creditor list in bankruptcy proceeding); *Kamakana v. City and County of Honolulu*, 447 F.3d 1172, 1178-81 (9th Cir. 2006) (access to summary judgment materials); *EEOC v. National Children's Center*, 98 F.3d 1406, 1409-10 (D.C. Cir. 1996) (access to consent decree).

Attorneys must regularly consider the differing levels of protection (or conversely, the levels of public access) that may be afforded to materials exchanged in the course of discovery, and materials filed with the court. Further, when considering materials to be filed, attorneys and courts must distinguish between the levels of protection (or conversely, the levels of public access) afforded to materials being filed in relation to a nondispositive matter and materials that relate to the merits of the case.

In the discovery context, there is no presumption of public access to unfiled discovery. *Seattle Times Co. v. Rhinehart*, 467 U.S. 20 (1984). There is also no prohibition against a party disseminating information obtained through discovery. Attorneys may seek to enforce their clients' privacy and proprietary interests by agreement or may seek a protective order under Fed. R. Civ. P. 26(c) by showing "good cause." In the context of filing material with a court, a threshold presumption of public access exists. If the material relates to a nondispositive matter, a "good cause" determination by the court in issuing an order to seal is sufficient to overcome the presumption of public access. *Chicago Tribune Company v. Bridgestone/Firestone, Inc.*, 263 F.3d 1304 (11th Cir. 2001). However, if the material relates to the merits of the case, an order to seal must be supported by a determination of compelling need that overcomes the presumption of public access. *Leucadia, Inc. v. Applied Extrusion Technologies, Inc.*, 998 F. 2d 157 (3d Cir. 1993). Thus, materials "designated as confidential under a protective order… will lose confidential status (absent a showing of 'most compelling' reasons) if introduced at trial or filed in connection with a motion for summary judgment." Manual for Complex Litigation, §11.432 (4th Edition 2004).

The relative strength of the public's interest in access versus a litigant's interest in privacy, property or confidentiality evolves with the stage of litigation, so that what constitutes "good cause" to restrict public access during discovery or non-dispositive stages of the proceeding does not equate to the "compelling need" necessary to restrict public access at another stage. This complexity appears to have generated widespread confusion in practice. The reported case law, supported by comments received by the Working Group in response to the Revised April 2005 Public Comment Version of this publication, demonstrates that litigants frequently move to seal docket entries, court filings, or whole proceedings, citing standards applicable only in the discovery or non-dispositive context. Likewise, judges across the country are routinely presented with stipulated discovery protective orders that the parties claim govern filings on the merits. Under the pressure of court workloads, some judges may be tempted to improperly forgo the individual determinations necessary to seal court documents, and instead issue orders in accordance with the parties' stipulations. *See, e.g., Citizens First National Bank of Princeton,* 178 F. 3rd 943, 944 (7th Cir., 1999) ("Instead of [making a determination] he granted a virtual carte blanche to either party to seal whatever portions of the record the party wanted to seal. This delegation was improper."). More recently, the process of modernizing and automating court filing and case management systems has revealed age-old informal practices under which court clerks or counsel themselves routinely sealed filings without any judicial determination whatsoever.

The electronic age and the requisite process of modernization has also led to a new concern. The conversion of presumptively public court records from paper-based filing systems accessible only at the courthouse itself, to electronic records potentially available via remote Intranet or Internet connections, has changed the analysis of the weight to be given to privacy concerns. While in the past, the likelihood that an individual or business would go to the effort of using court files to access personal information for private gain was remote, the automation of these records has made the harvesting of personal information for commercial use a viable, and

indeed quite profitable, business. This has given rise to a new legal dialectic which recognizes a responsibility on the part of government to protect the confidentiality of personal information, and perhaps confidential business information, that it requires citizens to provide as part of the civil and criminal justice systems.

For these reasons, the Working Group determined that the bench and bar would benefit from suggestions for "best practices" regarding public access to court files and proceedings in civil litigation, together with illustrations reflecting common situations that litigants and judges are likely to face.

Chapter One deals with discovery, and it is placed first because it is clearly distinct from other aspects of litigation, in that it is largely private and party-controlled – until the fruits of discovery are filed with the court for consideration of the merits of the case. Chapter Two deals with the important administrative functions of the court—the procedures for filing, maintaining the docket, and handling court-generated documents such as opinions and judgments. Here the applicable standards for sealing are different from the standards for discovery protective orders, due to the greatly increased public interest in the workings of the court and the greatly narrowed focus of the materials involved to those that deal with the merits of the case. Chapter Three goes to the core judicial function with the greatest public interest—the trial itself, including jury selection and the evidence presented. Chapter Four takes up the question of settlements, which was not a primary focus of the Working Group, but has been a lightning rod for press coverage and legislative attention. Here the analysis is extended to consider settlements as private agreements between parties until the parties choose, or feel compelled, to invoke the supervisory or enforcement powers of the courts. Finally, Chapter Five explores the implications of the transformation of the courts from repositories of largely paper-based information to managers of digital information. In particular, Chapter Five examines the increased attention given to protecting personal information as courts redesign their processes and explore novel questions of public access in an electronic age.

Chapter 1. Discovery

Principle 1 **There is no presumed right of the public to participate in the discovery process or to have access to the fruits of discovery that are not submitted to the court.**

The American federal civil litigation system is premised on the just, speedy and inexpensive resolution of disputes. Fed. R. Civ. P. 1. The scope of discovery under the Federal Rules of Civil Procedure is intended to be broad. Parties may obtain discovery regarding "any matter, not privileged, that is relevant to the claim or defense of any party," and for good cause shown, may obtain broader discovery relevant to the subject matter of the dispute. The information requested and produced during the discovery phase of civil litigation "need not be admissible at trial if [it] appears reasonably calculated to lead to the discovery of admissible evidence." Fed. R. Civ. P. 26(b)(1).

Unlike the civil law system in Europe and elsewhere, in the American civil litigation system the parties themselves develop the facts they need for trial through the discovery process outlined in the Federal Rules of Civil Procedure and state equivalents. These rules delegate to private parties the inquisitorial powers of the court, including the right to inspect and copy documents, the right to conduct depositions, and the right to compel non-parties to testify or produce documents. *Seattle Times Co. v. Rhinehart*, 467 U.S. 20 (1984) ("Thus, the [Federal Rules of Civil Procedure] often allow extensive intrusion into the affairs of both litigants and third parties." 467 U.S 20 at 30; "The Rules do not distinguish between public and private information." 467 U.S. 20 at 36) The court does not usually involve itself in the conduct of civil discovery, although it enforces procedural rules and may be called upon to decide discovery disputes. Generally, the fruits of discovery (documents, answers to interrogatories, deposition testimony, etc.) are not filed unless these are being used as evidence, either at trial or in connection with a discovery dispute or other pretrial proceeding, or unless the court orders that these be filed. Fed. R. Civ. P. 5(d).[2]

Pretrial discovery that is simply exchanged between the parties is not a public component of a civil trial. *See, e.g., Seattle Times Co. v. Rhinehart*, 467 U.S. 20, 33 (1984) ("pretrial depositions and interrogatories are not public components of a civil trial . . . and, in general, they are conducted in private as a matter of modern practice"). There is thus no presumed right of public access to the discovery process or the fruits of discovery in the hands of a party. However, as discussed below, a party is not prohibited from voluntarily disclosing any information received during discovery unless the party has agreed otherwise or unless the court, upon a showing of good cause, enters a protective order pursuant to Fed. R. Civ. P. 26(c) or its state equivalents. A party's ability to enter into such agreements, and the court's ability to enter such orders, may be limited by statute or rule. *See e.g.*, Fla. Stat. Ann. §69.081; Texas R. Civ. P. 76a.

[2] It is sometimes argued that discovery requests are made to threaten the release of "sensitive" information and coerce settlement. This is a matter of professional responsibility within the scope of ethics rules and not addressed by the Working Group. See Model Rules of Professional Conduct (2001), Preamble: A Lawyer's Responsibilities (5) ("A lawyer should use the law's procedures only for legitimate purposes and not to harass or intimidate others"); Rule 3.4(d) ("A lawyer shall not... in pretrial procedure, make a frivolous discovery request...")

Best Practices

1. Attorneys should cooperate in efficiently exchanging information in civil litigation. Such cooperation includes an early, full discussion of the scope of discovery and the treatment of potentially discoverable materials that the parties deem confidential or private, to avoid later pretrial litigation of this issue.

2. A party may object to the discovery of otherwise relevant and non-privileged information it claims is confidential or private. Such an objection should be the basis for negotiation with the requesting party over the procedure for producing the requested discovery to protect legitimate privacy and confidentiality interests, If no agreement is reached, a party may apply to the court for a protective order under Fed. R. Civ. P. 26(c) or its state equivalents.

3. If the parties agree to produce information under the terms of a stipulated protective order, the court should enter such order upon a showing of good cause, subject to a later determination of the confidentiality of specific documents in the event of a challenge to the confidentiality designation.

Examples

1. The attorneys representing the parties in a class action race discrimination lawsuit against a large corporation confer pursuant to Fed. R. Civ. P. 26(f) and map out the discovery phase of the litigation. The lawsuit alleges discrimination in pay and promotions throughout the company. It is anticipated that the plaintiff will serve a broad discovery request seeking current and historical information regarding employee pay and promotions. It is also anticipated that the defendant will object to public disclosure of employee pay, citing employee morale and competitive interests. The attorneys negotiate a procedure for the production of the relevant information in bulk form, redacting any "personal identifiers" in the data, and enter into a confidentiality agreement or stipulate to a protective order that would permit large volumes of information to be reviewed and exchanged without compromising privacy and confidentiality interests.

2. Same facts as Example 1, but the attorneys were unable to reach agreement. The plaintiff serves its discovery request, as anticipated, and the defendant objects. Under the court's rules, the attorneys must attempt to resolve discovery disputes before filing any motions. During the required meeting, the defendant flatly refuses to produce the requested data, and the plaintiff threatens to obtain the data from other sources and publish it on the Internet. The plaintiff then moves to compel discovery and the defendant counter-moves for a protective order. Three months and several hundred billable hours later, the court grants both motions in part, fashioning a protective order similar to that reached voluntarily in Example 1.

Principle 2 Absent an agreement between the parties or a court order based on a showing of good cause, a litigant is not precluded from disclosing the fruits of discovery to non-parties.

Absent an agreement between the parties or an order to the contrary, a party is free to share the fruits of discovery obtained during litigation with others who are not parties to the lawsuit. *Phillips v. General Motors Corp.*, 307 F.3d 1206, 1210 (9th Cir. 2002); *Harris v. Amoco Prod. Co.*, 768 F.2d 669, 683-84 (5th Cir. 1985).

In some cases, a producing party has legitimate reasons to limit the dissemination of certain information exchanged in the normal course of discovery. Because broad discovery is generally allowed, and given the nature of certain disputes in the civil justice system, the rules of discovery often require disclosure of private, confidential information involving matrimonial, financial, medical or family matters, or in commercial cases, trade secrets and other confidential business information. In order to facilitate the efficient exchange of information during discovery, parties may enter into agreements or stipulations designed to maintain the confidentiality of material produced during discovery.

In the absence of an agreement between the parties, a producing party has the right to object to the production of particular material on the basis of "annoyance, embarrassment, oppression, or undue burden," and seek a protective order under Fed. R. Civ. P. 26(c). In appropriate cases, a party may seek an order "that a trade secret or other confidential research, development, or commercial information not be revealed or be revealed only in a designated way." Fed. R. Civ. P. 26(c)(7). The court is required to make a finding of "good cause" to support a protective order.

To avoid a costly and time-consuming document-by-document determination of "good cause" by the court during the discovery, parties who anticipate that the scope of discovery will likely include private or confidential information often seek the court's *imprimatur* under Fed. R. Civ. P. 26(c) on a stipulated agreement regarding confidentiality. These "umbrella" protective orders, most often found in large or complex cases, are frequently entered without judicial assessment of the specific documents or information the disclosure of which will be limited by the protective order, although a more generalized finding of "good cause" is still required. Parties may demonstrate reliance on a protective order entered as a case management tool. However, such an order is insufficient justification by itself for the court to enter a sealing order if documents subject to the protective order are to be filed.

In determining whether good cause exists to issue or uphold a protective order under Fed. R. Civ. P. 26(c), a court is required to balance the parties' asserted interest in privacy or confidentiality against the public interest in disclosure of information of legitimate public concern. *Pansy v. Borough of Stroudsburg*, 23 F.3d 772, 786 (3d Cir. 1994). Judicial restraints placed only upon the disclosure and use of information exchanged in discovery do not restrict "a traditionally public source of information," *Seattle Times Co. v. Rhinehart*, 467 U.S. at 33. "When directed solely at discovery materials, protective orders are not subject to the high level of scrutiny required by the Constitution to justify prior restraints; rather, courts have broad discretion at the discovery stage to decide when a protective order is appropriate and what degree of protection is required." Manual for Complex Litigation, at 11.432, p. 66 (4th Edition, 2004) (citing *Seattle Times Co. v. Rhinehart*, 467 U.S. at 36–37). Therefore, given that the public shares the parties' interest in a judicial system that can efficiently resolve disputes, the good cause standard generally should be considered to be satisfied if the parties can articulate a legitimate and particularized need for privacy or confidentiality, in those instances where the protective order will apply only to the disclosure of information exchanged during discovery. If a challenge is

made, "good cause" must be shown based on the circumstances existing at the time of the challenge. *Leucadia, Inc. v. Applied Extrusion Techs., Inc.*, 998 F. 2d 157 (3d Cir. 1993). Because of the limited scope and provisional nature of the umbrella protective order, the court need not conduct a detailed inquiry into the nature of the information at issue, which courts are sometimes unwilling or often practically unable to do, where much or all of the information at issue may not be used in connection with the determination of the merits of the dispute.

Best Practices

1. Attorneys should counsel their clients that, absent an agreement or order issued upon a showing of good cause, there is no restriction on dissemination of documents and other information exchanged during discovery. A party desiring restrictions on dissemination of the fruits of discovery should approach the opposing party as soon as it becomes apparent that some type of restriction on dissemination is necessary.

2. Attorneys should assess in each case whether a protective order restricting dissemination of information produced during discovery is necessary.

3. An umbrella protective order or confidentiality agreement should provide a procedure for confirmation or challenge of the confidentiality designations made as to particular documents, including timely notice to the producing party that the designation is being challenged to enable the producing party to promptly seek protection and to prove that the particular information qualifies for judicial protection.

4. Attorneys should avoid excessive and unjustified designation of documents as "confidential" under a protective order.

Examples

1. Using the race discrimination lawsuit example outlined under Principle 1 above, at the same time the attorney representing the corporate defendant notifies the attorney representing the plaintiff that she is willing to produce her client's payroll and promotion database, she states that it contains private financial information on the employees of her client. She says she will only produce this database if the plaintiff's counsel is agreeable to enter a protective order. The plaintiff's attorney agrees and they negotiate a proposed protective order which:

    a. defines the information and documents it will protect, encompassing the type of information that could upon proof be the appropriate subject of a protective order;

    b. establishes a procedure whereby plaintiff's attorney may notify defendant's counsel if she believes that certain documents designated as "confidential" by the defendant should not be treated as such; and

    c. provides that within a specified period after being notified of plaintiff's counsel's objection to certain confidentiality designations, if defendant's counsel wishes to maintain the confidentiality of the challenged documents, the defendant's counsel must seek a protective order pursuant to Fed. R. Civ. P. 26(c). The protective order makes clear that if the confidentiality designation is challenged, the court is to make a *de novo* determination of whether there is good cause to restrict the dissemination of the challenged information.

Principle 3 **A protective order entered under Fed. R. Civ. P 26(c) to facilitate the exchange of discovery materials does not substitute for the individualized judicial determination necessary for sealing such material, if filed with the court on a non-discovery matter.**

Protective orders sometimes purport to do more than restrict the parties from sharing the fruits of discovery. They often include a provision allowing materials deemed "confidential" to be filed with the court under seal without any further order. Such an agreement between the parties may be appealing. Courts are understandably disinclined to interfere with a matter agreed upon by the parties, particularly considering the court's limited time and resources. However, no agreement between the parties should substitute for the individualized and particularized showing that must be made before any materials are filed under seal, at least for non-discovery purposes. Moreover, given the presumption of public access to filed materials, that showing must be made under the stricter standards described in Chapter 2 rather than the "good cause" standard of Fed. R. Civ. P. 26(c) used for the issuance of protective orders.

Although protective orders with "sealing" provisions appear to be common, federal circuit courts have questioned the enforceability of protective orders that serve to seal material filed with the court, primarily because such sealing implicates the public's qualified right of access to court records. For example, according to the Third Circuit, "[T]he burden of justifying the confidentiality of each and every document sought to be covered by a protective order remains on the party seeking the protective order; any other conclusion would turn Rule 26(c) on its head." *Leucadia, Inc. v. Applied Extrusion Techs., Inc.*, 998 F.2d 157, 166 (3d Cir. 1993). Similarly, the Sixth Circuit held that protective orders under Fed. R. Civ. P. 26(c) authorizing the sealing of documents that either party "considers ... to be of a confidential nature" is facially overbroad. *Procter & Gamble Co. v. Bankers Trust Co.*, 78 F. 3d 219, 227 (6th Cir. 1996).

Particularly in cases with large quantities of material to be produced in discovery, a threshold showing of "good cause" over broad categories of material may be sufficient for the issuance of a protective order under Fed. R. Civ. P. 26(c). The purpose of the order would be to facilitate the cooperative exchange of voluminous discovery. Protective orders must not confuse the confidentiality of material produced in discovery with the filing of such materials under seal. That issue is discussed in detail in Chapter 2.

Best Practices

1. Attorneys should advise their clients that a protective order entered without an evidentiary showing only restricts the dissemination of designated documents and information so long as the need for confidentiality is not successfully challenged by another party or by an intervening third party, and so long as the information does not need to be filed in court or used as evidence at trial. The party wishing to prevent the dissemination of information may eventually be required to prove the basis for protecting specific information, even if not required to do so at the time the information is produced.

2. Protective orders which purport to cover both the exchange of documents in discovery and the filing of documents with the court would better conform with the legal standard if such protective orders were: (1) narrowly drafted; (2) kept the burden on the designating party to demonstrate good cause whenever the need for confidentiality is questioned; and (3) provided a procedure to establish a proper basis for sealing at the time the material is actually filed with the court for any purpose other than a discovery dispute.

3. Protective orders entered without evidentiary findings should provide a mechanism to establish whether information designated as confidential should be sealed if filed with the court. For instance, such an order could provide that a party "lodge" a protected document with the court pending a motion to seal from the designating party.[3] If the designating party files a motion to seal the court record within a reasonable period of time, a determination is then made as to whether the particular information should remain under seal. The fact that information was designated as confidential pursuant to the protective order is not dispositive in determining that the information should be sealed in connection with a determination on the merits.

4. As an alternative to the practice outlined above, the parties could agree in the protective order to provide reasonable notice to the designating party that it intends to file documents designated as confidential in court. The designating party should move within a reasonable period of time to have the specific documents sealed. Again, a judicial determination must be made as to whether the sealing of the particular records is warranted.

Examples

1. In the class action race discrimination lawsuit outlined under Principle 1 above and the protective order discussed as an example under Principle 2 above, the plaintiff's counsel intends to file the payroll and promotion database which has been designated as confidential as an exhibit in opposition to a motion for summary judgment. Pursuant to the terms of the order, plaintiff's counsel notifies defendant's counsel in advance of the filing that the designation is challenged, triggering the defendant's obligation to file a motion for a sealing order with respect to the challenged information. Alternatively, plaintiff's counsel temporarily files the payroll and production database with the opposition papers, ensuring that the material is not made public and likewise triggering the defendant's obligation.

2. Using the above example, plaintiff's counsel also notifies defendant's counsel that pages from one of defendant's outdated employee handbooks will be filed in connection with a summary judgment motion. These pages had been designated as confidential pursuant to the protective order. Defendant's counsel decides that it is not necessary to seek to have this outdated information sealed. Plaintiff's counsel is permitted to file the information in open court, and the confidentiality designation with respect to that information is waived.

[3] A "lodged" document is a document submitted to the court in conjunction with the filing of a motion to allow the document to be filed under seal. The "lodged" document itself is not considered part of the filing. If the court denies the motion, the document is returned to the submitting party. *See, e.g.*, N D. Cal. Civ. L. R. 79-5(d). ("Sealed or Confidential Documents: Motion to File Under Seal")

Principle 4 **On a proper showing, non-parties should be permitted to intervene to challenge a protective order that limits disclosure of discoverable information.**

A party involved in parallel or subsequent litigation should be permitted to present arguments that a protective order should be modified to allow it access to the allegedly confidential documents. A court deciding whether its protective order should be modified to allow a party to such litigation access to documents should consider the standards of relevance and efficiency articulated in Fed. R. Civ. P. 26, including considerations of annoyance, embarrassment, and oppression under Fed. R. Civ. P. 26(c). However, the public disclosure of information of a private or sensitive nature in one lawsuit should not necessarily subject a party to repeated disclosure of the same information in subsequent litigation, if there is good cause for protecting it from disclosure.

Most courts that have considered the question hold that the media, public interest groups, and other third-parties have standing to intervene in a civil case for the limited purposes of opposing or seeking modification or rescission of a protective order entered pursuant to Fed. Rule Civ. P. 26(c) when they assert that the public interest is served by disclosure. *See Grove Fresh Distributors v. Everfresh Juice Co.*, 24 F.3d 893, 896 (7th Cir. 1994); *Pansy v. Borough of Stroudsburg*, 23 F.3d 772, 777 (3d Cir. 1994); In re *Alexander Grant & Co. Litigation*, 820 F.2d 352, 354-55 (11th Cir. 1987); *CBS v. Young*, 522 F.2d 234, 237-38 (6th Cir. 1975). Courts have found standing without any showing that persons subject to an order limiting disclosure of discovery materials would be willing to disclose absent the protective order; rather, the cases presume that since the only practical effect of the protective order is to prevent an otherwise willing speaker from communicating to a willing listener, the party seeking to intervene meets the redressable injury requirement of standing simply because the order impedes "the news agencies' ability to discover newsworthy information from potential speakers." *Davis v. East Baton Rouge Parish School Board*, 78 F. 3d 920, 927 (5th Cir. 1996).

The courts are in disagreement as to the burden of proof when motions are made to modify or vacate an existing protective order. One standard provides that, assuming the order to have been validly entered in the first instance, the moving party must show sufficient reasons to release the protected information. *See Phillips v. General Motors Corp.*, 307 F.3d 1206, 1213 (9th Cir. 2002). Another approach leaves the burden of proof on the party that sought the order in the first instance to justify continued confidentiality, but adds reliance on the existing order as a factor to be considered. See *Pansy v. Borough of Stroudsburg*, 23 F.3d 772, 789-90 (3d Cir. 1994).

Best Practices

1. When intervention is allowed to oppose a motion for a protective order that has not yet been entered, or for purposes of challenging a general protective order, the court should consider and balance the public interest in the disclosure sought, the legitimate privacy interests that favor non-disclosure, and the extent to which the information is relevant to the controversy. The party seeking to limit disclosure has the burden of demonstrating that the balance of interests satisfies the "good cause" standard of Fed. R. Civ. P. 26(c).

2. If a protective order has already been entered after full consideration of the merits, including a review of the contents of the documents that are prohibited from disclosure under the order, the intervenor should be required to demonstrate circumstances or considerations not already considered by the court.

3. In entering into a confidentiality agreement or seeking a protective order, parties should anticipate non-party demands for discovery materials through subpoena, or that non-parties will object to producing information pursuant to subpoena because the requested information is claimed to be confidential. Agreements should also include provisions that expressly allow parties to provide materials to requesting regulatory agencies that offer appropriate protection for confidential materials.

4. When collateral litigants intervene, the issuing court "should satisfy itself that the protected discovery is sufficiently relevant to the collateral litigation that a substantial amount of duplicative discovery will be avoided...." *Foltz v. State Farm Mutual Automobile Ins. Co.*, 331 F.3d 1122, 1132 (9th Cir. 2003). The court should balance this policy of avoiding duplicative discovery against the countervailing interests of the parties opposing modification, including their reasonable reliance on the order's nondisclosure provisions. In many cases, any legitimate interest in continued secrecy can be accommodated by placing the collateral litigants under the use and non-disclosure restrictions of the original protective order. Modification merely removes the impediment of the protective order in the collateral litigation. The collateral court retains authority to determine the ultimate discoverability of, and the protection to be afforded to, specific materials in the collateral proceedings. *Foltz*, 331 F. 3d at 1133.

Examples

1. Using the example of the class action race discrimination lawsuit discussed under Chapter 1, Principle 1, a class member has opted out of the class and is pursuing an individual race discrimination lawsuit against the same defendant in another jurisdiction. The attorney for the opt-out plaintiff calls the attorney representing the plaintiff class and asks for a copy of the payroll and promotion database that defendant produced in the class action. However, this has been designated confidential, so class plaintiffs' counsel cannot provide the database to the attorney for the opt-out plaintiff.

2. In the same case as above, the attorney for the opt-out plaintiff serves a Fed. R. Civ. P. 45 subpoena on the attorney for the plaintiff class seeking production of all documents produced by defendant in the class action. But counsel for the plaintiff class is under a court order not to disseminate the confidential material produced by defendant. The protective order provides that class plaintiffs' counsel tenders the subpoena to defendant's counsel, who is obligated by the protective order to defend the protective order and oppose the subpoena, negotiate an extension of the protective order, or waive protection.

3. In the same case as above, because the opt-out plaintiff's lawsuit involves allegations similar to those involved in the class action, and direct discovery requests for the information would be inevitable, defendant's counsel agrees that the material can be produced to the opt-out plaintiff so long as he is willing to enter a similar protective order.

4. In a toxic tort case, a protective order is entered at the commencement of discovery. After significant discovery has taken place, a member of the news media moves to intervene, asserting that the general public has a legitimate interest in documents or information exchanged during discovery. If the court determines that a colorable public interest has been asserted, intervention should be allowed.

5. Assume the same facts as stated in Example 4, except that the parties fail to agree upon a stipulated protective order and one party moves for entry of a protective order pursuant to Fed. R. Civ. P. 26(c). The media, asserting the public interest, should be permitted to intervene and be heard in opposition to the motion. The party asserting confidentiality bears the burden of proving that an order should issue under Fed. R. Civ. P. 26(c).

6. Assume the same facts as stated in Example 4, except that the parties to the litigation failed to agree on a stipulated protective order and one party moved for the entry of a protective order pursuant to Fed, R. Civ. P. 26(c). The judge ruled on the motion and issued an order, making appropriate findings of fact and conclusions of law. At a later date, the news media intervene, seeking access to documents subject to the order. The intervenors bear the burden of coming forward with evidence sufficient to overcome the initial presumption that the existing order remain in place, although the original proponent bears the ultimate burden of persuasion that the order continues to be necessary and narrowly tailored to protect legitimate privacy and confidentiality interests.

Chapter 1

Selected Bibliography

Manual for Complex Litigation, Fourth (2004), Sec. 11.432 (discussing the use of "umbrella" and "particularized" protective orders in complex litigation).

Florida Statutes Annotated, §69.081 (describing the procedure for entry of an order "which has the purpose or effect of concealing a public hazard," etc.).

Texas Rule of Civil Procedure 76a (declaring that certain court records are presumed to be open and setting forth standards for sealing same).

Seattle Times v. Rhinehart, 467 U.S. 20 (1984) (no public right of access to unfiled discovery materials).

Poliquin v. Garden Way, 989 F.2d 527 (1st Cir. 1993) (showing of "good cause" sufficient to protect discovery materials from disclosure insufficient to bar access to evidence introduced at trial).

SEC v. TheStreet.com, 273 F.3d 222 (2d Cir. 2001) (transcripts of depositions of NYSE officers held not to be "judicial documents" but no presumption against public access as third parties had been present).

Leucadia v. Applied Extrusion Tech., Inc., 998 F.2d 157 (3d Cir. 1993) (recognizes distinction for purposes of access between discovery materials filed as exhibits to "merits" motions and those filed in support of discovery motions).

Shingara v. Skiles, 420 F 3d 301 (3d Cir. 2005) (reviewing standards for issuance of umbrella orders and concluding such an order was not warranted in a case that "is neither complex nor involves 'large-scale discovery'" and good cause showing not made).

Pittston Co. v. United States, 368 F.3d 385 (4th Cir. 2004) (holds that party cannot object to sealing of materials when it had access to same and had agreed to sealing).

Procter & Gamble Co. v. Bankers Trust Co., 78 F.3d 219 (6th Cir. 1996) (protective order cannot allow parties to control access to judicial records).

Baxter Internat'l v. Abbott Labs, 297 F.3d 544 (7th Cir. 2002) (distinguishes between broad procedural orders entered for purposes of discovery as opposed to those entered at later stages of litigation).

Citizens First Nat'l Bank v. Cincinnati Ins. Co., 178 F.3d 943 (7th Cir. 1999) (broad protective order granting parties "a virtual carte blanche" to seal records invalid under Fed. R. Civ. P. 26).

In re *Remington Arms Co.*, 952 F.2d 1029 (8th Cir. 1991) (sets forth procedure to determine whether information sought in discovery is trade secret for purposes of Fed. R. Civ. P. 26(c)(7) protective order).

United Nuclear Corp. v. Cranford Ins. Co., 905 F.2d 1424 (10th Cir. 1990) (discusses access by collateral litigants to discovery materials subject to protective order).

Foltz v. State Farm Mut. Auto Ins. Co., 331 F.3d 1122 (9th Cir. 2003) (discusses access by collateral litigants to discovery materials subject to protective order; establishes "mechanics of the relevance inquiry" and which court should do what).

United States v. Microsoft Corp., 165 F.3d 952 (D.C. Cir. 1999) (depositions in an antitrust action are open to public pursuant to the Publicity in Taking Evidence Act).

A full bibliography, updated periodically, may be found on The Sedona Conference web site at www.thesedonaconference.org starting in July 2007.

Chapter 2. Pleadings, Court Orders, Substantive Motions & Dockets

Principle 1 **In civil proceedings, the public has a qualified right of access to documents filed with a court that are relevant to adjudicating the merits of a controversy. In compelling circumstances, a court may exercise its discretion to deny public access to submitted documents to protect the privacy, confidentiality or other rights of the litigants.**

Chapter 1 dealt with discovery materials exchanged between the parties, for which there is no qualified right or presumption of public access. In Chapter 2 we start with the act of filing a document with the court, such as a pleading, response, motion, or an exhibit. We also deal with the documents and records created by the court in relation to civil litigation, such as dockets, docket entries, memoranda, orders, or judgments. When a document is filed or created by the court, a qualified right or presumption of public access arises. However, this is just the starting point of the public access analysis. The strength of the presumption, and the consequent burden that must be met to overcome it, depends on the relationship of the document to the adjudicative process. The more important the document is to the core judicial function of determining the facts and the law applicable to the case, the stronger the presumption and the higher the burden to overcome it. Thus, a qualified right or presumption of public access attaches to all documents filed with the court that are material to the adjudication of non-discovery matters. *See* In re *Cendant Corporation*, 260 F. 3d 183, 192-93 (3d Cir. 2001); *Chicago Tribune Co. v. Bridgestone/Firestone. Inc.*, 263 F.3d 1304, 1312 (11th Cir. 2001).

Courts have found the qualified right or presumption of public access from either of two sources, the Constitution or the common law. The United States Supreme Court has found a First Amendment right of public access in criminal cases. A constitutional right to public access arises if the proceedings or documents have historically been open to the general public and "public access plays a significant positive role in the functioning of the particular process in question." *Press-Enter. Co. v. Superior Court*, 478 U.S. 1, 8 (1986). "If the particular proceeding in question passes these tests of experience and logic, a qualified First Amendment right of public access attaches." *Id.* That qualified right can be overcome "only by an overriding interest based on findings that closure is essential to preserve higher values and is narrowly tailored to serve that interest." *Id. See also Globe Newspaper Co. v. Superior Court*, 457 U.S. 596, 606-607 (1982) ("Where, as in the present case, the State attempts to deny the right of access in order to inhibit the disclosure of sensitive information, it must be shown that the denial is necessitated by a compelling governmental interest, and is narrowly tailored to serve that interest.").

Some federal courts have extended the First Amendment right of public access to court files and proceedings in civil cases. *See, e.g., Republic of Philippines v. Westinghouse, Elec. Corp.*, 949 F.2d 653, 659 (3d Cir. 1991); *Rushford v. New Yorker Magazine, Inc.*, 846 F.2d 249, 252-53 (4th Cir. 1988). Other courts have found a common law presumption in favor of public access for documents and proceedings in civil cases. *See, e.g., FTC v. Standard Fin. Mgt.*, 830 F.2d 404, 408 n.4 (1st Cir. 1987); *Brown & Williamson Tobacco Corp. v. FTC*, 710 F.2d 1165, 1179 (6th Cir. 1983); *Smith v. United States District Court*, 956 F.2d 647, 650 (7th Cir. 1992); *EEOC v. Erection Co.*, 900 F.2d 168, 169 (9th Cir. 1990); *NBC Subsidiary (KNBC-TV), Inc. v. Superior Court*, 20 Cal. 4th 1178, 1217 (1999). Some courts have found both a First Amendment right and a common law presumption. *See e.g., Lugosch v. Pyramid Co. of Onandaga*, 435 F.3d 110 (2d Cir. 2006) (documents submitted to a court for its consideration in a summary judgment motion are "judicial documents" to which a presumption of immediate access applies under both the common law and the First Amendment).

Public access serves important public interests, including informing the public of the cases that are before the court. The essential benefit of access is to ensure accountability to the public. Public scrutiny brings about accountability, fostering public trust that the judicial system is functioning justly, properly and efficiently, and that participants in the system are properly and honestly performing their duties. Another benefit of public access is educating the public on the workings of the courts and the civil justice system, which promotes public confidence in the judicial system.

While important interests are served by the First Amendment right or common law presumption of public access, the right is not absolute and the presumption may be overcome in appropriate circumstances. If the documents in question have little or no relation to the merits of the case or have not historically been available to the public, the presumption of public access that arises from the mere fact that these have been filed with the court is quite weak. For instance, if the documents have been filed in relation to a discovery dispute, the court may seal them under the same "good cause" standard that would support a particularized protective order under Fed. R. Civ. P. 26(c). Likewise, the presumption of public access to filed settlement documents that merely recite the terms of settlement and do not purport to assign liability or otherwise "adjudicate" the case is weak. *See Gambale v. Deutsche Bank AG*, 377 F.3d 133, 143-44 (2d Cir. 2004) (distinguishing between settlement amount and summary judgment documents).

The presumption of public access is much stronger in relation to "judicial documents," that is, documents that relate to the merits of the case and assist the court in fulfilling its adjudicatory function. Courts have the discretion to seal court documents to protect rights of privacy or confidentiality, provided the court determines that an "overriding interest" exists that can only be protected by such an order. *See, e.g., Chicago Tribune Co. v. Bridgestone/Firestone*, 263 F.3d 1304, 1313 (11th Cir. 2001); In re *Cendant Corp.*, 260 F.3d at 194; *Leucadia, Inc. v. Applied Extrusion Tech., Inc.*, 998 F.2d 157, 166 (3rd Cir. 1993); *NBC Subsidiary (KNBC-TV), Inc. v. Superior Court*, 20 Cal. 4th 1178, 1217 (1999). A circumstance that might justify the exercise of the court's discretion is to protect the confidential proprietary interests in trade secrets or other commercially sensitive information. *See Leucadia*, 998 F.2d at 166; *Joint Stock Soc'y v. UDV North America*, 104 F. Supp. 2d 390, 396 (D. Del. 2000). Whether or not the requisite need for sealing has been demonstrated is a matter of courts' supervisory powers and is "best left to the sound discretion of the court, discretion to be exercised in light of the relevant facts and circumstances of the particular case." *Nixon v. Warner Communications,* 435 U.S. 589, 598-99 (1978).

During the 18 month period between the publication of the "public comment" draft of this document in April 2005 and the final draft at the end of 2006, several commentators put forward the proposition that all actions to restrict or deny public access to the documents and proceedings related to civil litigation should be subject to the same "good cause" showing to overcome the presumption in favor of public access. While this notion has simplicity and surface appeal, it is contradicted by the great weight of the case law and advanced in a limited circumstance by only one federal circuit court decision. *Chicago Tribune Co. v. Bridgestone/Firestone*, 263 F. 3d 1304, 1313 (11th Cir. 2001) (holding that the "good cause" standard of Fed. R. Civ. P. 26(c) may also apply to restrict access to documents filed in relation to a failed summary judgment motion in a settled case). While all justifications for restricting public access must constitute "good cause" to be upheld, the requisite "good cause" will be dramatically different depending upon the particular documents and proceedings, and the particular stages of the litigation. The "good cause" needed to support an umbrella protective order under Fed. R. Civ. P. 26(c) will not suffice to support the sealing of those discovery documents when filed in court. To lump the varying expressions of burden under the common rubric of "good cause" creates confusion as to what standard actually applies, and does a disservice to attorneys and parties who may erroneously believe that the "good cause" that

supported an umbrella protective order in discovery will also support an order to seal a record on appeal. *See e.g. Baxter International v. Abbott Labs*, 297 F. 3d 544 (7th Cir. 2002).

Statutes and court rules recognize specific situations in which pleadings must be kept confidential. For example, under the qui tam provisions of the False Claims Act, 31 U.S.C. §3729 et seq., a complaint of a private person must be filed in camera and remain sealed for at least 60 days, and the government may move *in camera* for an extension of the sealing. 31 U.S.C. §§3730(b)(2) and (3). The purpose of the sealing requirement is to give the government an opportunity to review the complaint and determine whether to intervene. 31 U.S.C. §3130(b)(4) Similarly, the Trademark Counterfeiting Act of 1984, codified in relevant part at 15 U.S.C. Sec. 1116(d), provides that a court may, on *ex parte* application, issue a seizure order for goods and counterfeit marks, and that any such order, "together with the supporting documents," shall be filed under seal, "until the person against whom the order is directed has an opportunity to contest such order...." 15 U.S.C. §1116(d)(8). The purpose of the sealing is to avoid the loss or concealment of the items to be seized. 15 U.S.C. §1116(d)(4)(B)(vii). In both of these statutory examples, sealing is for a specific purpose and a limited time.

There are also categories of cases with records that invariably include information, the disclosure of which is discouraged as a matter of public policy. State legislatures have adopted statutes mandating that such categories of cases be closed to the public. *See, e.g.*, Indiana Code §31-39-1-2 (records in juvenile proceedings); Maryland Code, State Gov't. Art., §10-616(b) (records in adoption and guardianship proceedings); Maryland Code, Art., §10-616(b) (records in adoption and guardianship proceedings); Maryland Code, Art. 88A, §6(b) (records in child abuse or neglect proceedings); New York, Family Court Act, §166 (records of family court proceedings); New York, Domestic Relations Law, §235 (records in divorce, custody, and child support proceedings). Several state courts have, or are considering, court rules restricting remote access via the Internet in certain categories of cases. See, e.g., Indiana Administrative Rule 9(g); Maryland Rules 16-1006 and 16-1007; Vermont Rules for Public Access to Court Records, §6. The Judicial Conference of the United States has also determined that remote access via the Internet to at least one category of cases, Social Security appeals, should be restricted. *See* Report of the Judicial Conference Committee on Court Administration and Case Management on Privacy and Public Access to Electronic Case Files, September 2001.

A court might also determine that sealing an entire document is not necessary because the protection of privacy or other interests can be achieved by redacting the private information or allowing the use of fictitious names. In such cases, redaction or use of a pseudonym can preserve the important privacy rights or property interests, while protecting the public's right to access. *See Doe v. City of Chicago*, 360 F. 3d 667, 669-670 (7th Cir. 2004). In other cases, sealing may be warranted only for a limited period of time. *See* E-Government Act of 2002, Public Law 107-347, and proposed Fed. R. Civ. P. 5.2, (implementing the E-Government Act, §205(c)(3), to provide privacy protection for filings electronically transmitted to a court), approved by the Civil Rules Advisory Committee of the U.S. Judicial Conference. See http://www.uscourts.gov/rules/Rules Publication August 2005.pdf#page=55

Courts should adopt procedures to facilitate the orderly consideration of motions related to public access to filed documents. For example, a party may believe it has compelling reasons to request an order allowing it to file an entire document with the court under seal. The court may permit the party to "lodge" the document with the court (a step short of filing the document) and file an appropriate motion to have the document sealed upon filing. Under such a procedure, the court and opposing parties have access to the document while the motion is under consideration, and the public has notice of the pending motion to file the document under seal, but the document has not been made public through filing. *See, e.g.*, D.N.J. L. Civ. R. 5.3; Cal. R. Ct. 243.1 to 243.4

Best Practices

1. Courts should provide guidance to civil litigants regarding the procedures for seeking and the standards for obtaining protective orders and sealing orders through the promulgation of local rules, court-wide standing orders, and courtroom-specific standing orders.

2. In jurisdictions where lodging is permitted, litigants should temporarily file or "lodge" documents with the court awaiting a ruling on a motion to have the documents filed under seal. If the motion is granted, the documents will be filed under seal. If the motion is denied the documents will be returned to the party unfiled.

3. Whenever a party seeks to file documents previously subject to a protective order, appropriate notice should be given that would enable the producing party to move for protection of the documents.

4. In exercising its discretion to issue a sealing order, a court should consider the importance of the rights and interests (for instance, privacy rights, confidential information, or proprietary business information) that would be jeopardized by public access to the sealed material; whether the need for confidentiality outweighs the public's interest in disclosure; whether the sealing requested is broader than necessary to meet that need for sealing; and whether less restrictive alternatives might be available that would preserve the interest in confidentiality while permitting at least some public access such as redaction, limiting the duration of the sealing order or the use of pseudonyms. Absent extraordinary circumstances, sealing orders themselves should not be sealed.

5 Attorneys should counsel their clients regarding the standards for sealing party-filed documents, the risk that information may be made public, and measures that may be taken to minimize or avoid the compromise of such information.

6. Sealing requests should not be overly broad and attorneys should take reasonable steps to segregate material that should be filed under seal from material that may be filed without seal. For example, an entire document a party requests to file under seal should not be sealed if, as a practical matter, confidentiality can be adequately protected by more limited means, such as the redaction of specific information, the use of "Doe" pleadings, or the sealing of only a portion of the document, with the non-confidential material to be openly filed.

7. Orders granting or denying a motion to seal should be subject to immediate appellate review under the collateral order or other doctrine.

Examples

1. A plaintiff files a trademark infringement action alleging that the defendant is manufacturing "knock off" products. The plaintiff seeks an *ex parte* seizure order, pursuant to statute, based on a showing that the defendant intends to move or destroy the products. The complaint and the request for an immediate seizure order are temporarily filed along with a motion to have the documents filed under seal. The temporary filing is accompanied by a proposed order to be endorsed by the judge, also under seal, stating that the complaint will be unsealed upon either the execution or the denial of the requested seizure order.

2. The exclusive Midwestern distributor of a highly popular and profitable product of an East Coast manufacturer is engaged in a dispute with the manufacturer over the manufacturer's alleged shoddy accounting practices. For several months the parties engaged in unsuccessful settlement negotiations, until the distributor prepares to file suit. The plaintiff distributor requests that its attorney file the complaint under seal to avoid publicity and loss of good will. After review of the controlling law in the jurisdiction, the attorney determines that the plaintiff's generalized interest in avoiding publicity and losing goodwill will not provide the requisite showing to support a sealing order. The attorney so informs his client and counsels him regarding possible alternatives, including alternative dispute resolution.

3. The same facts as Example 2 above. The distributor files a motion for summary judgment supported by documents designated as "confidential" and produced under a Rule 26(c) protective order which detail proprietary and commercially sensitive information about the manufacturer's business. The distributor's attorney files the motion with the confidential information redacted and requests the court's permission to file an unredacted version under seal. The manufacturer's attorney promptly files a motion explaining the basis for sealing the unredacted version with an affidavit that establishes the significance of the information to the business, the competitive harm disclosure might cause, and the measures taken to date to keep the information confidential. The court grants the sealing motion and files an order, stating the grounds for sealing without revealing any of the information itself.

4. Several members of a wealthy family, all beneficiaries under a trust, file suit against another family member who is the trustee, alleging misappropriation of trust assets. In the complaint, the plaintiffs set forth sensitive family information, such as the value of the trust, their respective shares of the trust assets, and the holdings of the trust. The plaintiffs' attorney prepares two versions of the complaint: one version in which the paragraphs containing the sensitive family information have been redacted, to which the public would have access, and another version of the complaint to be the subject of a motion to seal.

5. A plaintiff who is HIV-positive brings suit against a dentist for refusal to treat him in violation of state law. The plaintiff is not known in his community as being HIV-positive. He files his complaint under the court's "Doe" procedure, in which information that would identify him personally is removed from the version of the pleading to which the public has access. The version of the complaint containing identifying information is filed under seal. The judge issues an order that information identifying the plaintiff in all subsequent pleadings is to be redacted from publicly accessible versions, with unredacted versions filed under seal.

6. A plaintiff intends to file a motion for summary judgment in fourteen days, which will be supported by documents it obtained from the defendant through discovery and designated by the defendant as confidential under a stipulated protective order. Pursuant to the terms of the particular protective order, the plaintiff informs the defendant of its intention to file, which permits the defendant to file a motion to seal the material in advance of the summary judgment filing date. The defendant files the motion to seal, and the plaintiff files a redacted version of its summary judgment motion and supporting information but separately files an unredacted version containing the confidential information with the court.

7. During the course of litigation, the court indicates it may impose sanctions on counsel for repeatedly missing court-imposed deadlines in the case. Counsel requests the court's permission to file a responsive brief and affidavit under seal simply explaining that "medical reasons" are detailed in its response regarding sanctions. The court exercises its discretion to seal the brief and affidavit, in part because the public's interest in access is weaker because the filings have no role in the determination of the merits of the case.

8. In the same matter, counsel files a dispositive summary judgment motion, and temporarily files select portions of the supporting evidence along with a motion to seal stating that "confidential and proprietary" business information is contained in the documents. The court indicates its initial intent to deny the sealing motion. Counsel then requests, and the court grants, permission for counsel to file a supplemental brief and affidavit establishing how the information in the documents is maintained in confidence, that it is not known to the public or business competitors, and how disclosure of the information may give competitors an unfair advantage. In light of the supplemental filings, the court assesses the strength of the presumption of public access, weighs it against the interests in confidentiality, and finds a compelling need to partially seal the documents.

Principle 2 The public has a qualified right of access to court dockets that can only be overcome in compelling circumstances.

The docket is the principal index of judicial proceedings. All the judicial business of the court should be noted on the docket. See Fed. R. Civ. P. 79(a). For each case, the individual docket should serve as a record of all activity and as an index of all documents, pleadings, appearances, the scheduling of hearings and trials, motions, orders, judgments, as well as miscellaneous items.

There is a presumption of public access to dockets. *See e.g., Hartford Courant Co. v. Pellegrino*, 380 F.3d 83, 93-94 (2nd Cir. 2004). Access to the docket is the primary means to determine if a particular case is being adjudicated or if a party is engaged in litigation. Access to individual case dockets is the primary means to monitor the course of any particular case. Access to the docket is also the primary means for the public (including the media, academics, and civic groups) to monitor the overall performance of the courts and the administration of justice. The effectiveness of particular laws or court rules is often measured by analysis of court dockets. Moreover, legislative decisions regarding the allocation of resources to the judicial branch of government are based in large part on statistical analysis of docket activity.

When permitted by law or statute, certain court documents may be sealed and certain proceedings may be closed to the public. However, it does not follow that corresponding dockets should be sealed, either in whole or in part. The existence of a case itself should never be kept secret, and whenever particular documents or proceedings are to be sealed, docket entries referencing that sealing should be made to give the public adequate notice.

On rare occasions, docket entries could reveal information that would jeopardize the privacy or confidentiality interests of parties involved. Statutes and court rules restrict public disclosure of particular types of information that might appear in docket entries, such as Social Security numbers or the names of minors. However, the restrictions imposed by such statutes and court rules do not justify the sealing of the docket itself.

Rare circumstances may justify the temporary redaction of particular information in docket entries to prevent the destruction of evidence or the loss of a remedy. When such redaction is required a judge should make appropriate findings of fact and conclusions of law in an order that should be noted on the docket and should expire by its own terms when the circumstances justifying the order have passed.

Many courts include narrative "minute entries" or summaries of proceedings directly on the docket when the proceeding generates no document. Clerks who compose such narrative entries should be careful not to include sensitive or confidential information explicitly restricted by statute, court rule, or order. A narrative entry that must be redacted or sealed should be composed as a separate document and placed in the case file, and an appropriate entry made on the docket.

Best Practices

1. The public should be given access to the docket except in the most compelling circumstances. Even if the merits of a case warrant issuance of a sealing order, the case must still be assigned a docket number and a docket index itself must be accessible to the public.

2. The identity of the judge to whom a case has been assigned should appear on the docket under all circumstances, as should the identity of counsel.

3. "Procedural" events should appear on the docket for public review. These include, for example, the nature of the case, the payment of the filing fee, and notations that motions have been made or affidavits filed.

4. There may be circumstances under which parts of individual docket entries should be sealed. If so, the existence of a sealing order based on findings of fact and conclusions of law should be reflected on the docket.

5. Care should be exercised to distinguish between situations in which a document or proceeding is sealed, and the extremely rare instances in which the corresponding docket entries should also be sealed.

Examples

1. A plaintiff seeks to file a trademark infringement action against a defendant and seeks an immediate *ex parte* seizure order. The plaintiff is aware that the defendant monitors the filing of suits against it. The plaintiff presents the complaint and the *ex parte* motion for a seizure order, arguing that if the defendant knows the existence of the litigation it will destroy or transfer the infringing products to an unknown location. Convinced that the standards for both the *ex parte* seizure order and a sealing order are met, the judge endorses the seizure order and dictates a temporary sealing order, reciting her findings of fact and conclusions of law. The complaint and orders are filed with the clerk, with instructions to assign the case a number and docket it with only the number, judge's name, entries for a complaint and seizure order under seal, and an entry for a temporary sealing order. The temporary sealing order is set to expire upon execution of the seizure order or after a reasonable period of time.

2. An infant plaintiff, by his guardian, commences a declaratory judgment action against an insurer that issued a homeowners' policy to the infant plaintiff's grandfather. The infant alleges that, while visiting his grandfather's home on various occasions, he was sexually assaulted by the grandfather. The infant seeks a declaration that the grandfather's acts fall within the policy coverage. The case is assigned a "John Doe" plaintiff name, in accordance with local practice regarding the identity of minors. The insurance company is named as defendant. The docket includes the names of counsel and of the judge and routine procedural entries. The complaint appears on the docket with the notation "Under Seal," followed by an entry for the sealing order. The sealing order, which is not itself under seal, states that the judge, after reviewing the complaint and hearing from counsel, finds that the allegations in the complaint involve a minor and include matters of a sensitive and private nature, which should be confidential and protected from public disclosure by the court and counsel, in the best interests of the child.

3. A plaintiff in a patent infringement action has moved for summary judgment against the defendant. As part of that motion, the plaintiff has submitted the affidavit of an expert economist containing financial information that is proprietary to the plaintiff and which, if made public, would have adverse competitive effects on the plaintiff. The motion for summary judgment is filed and the affidavit is filed separately under seal. Both filings are noted in the docket, including the name of the affiant expert.

Principle 3 There is a qualified right of access to judgments, judicial opinions and memoranda, and orders issued by a court that can only be overcome in compelling circumstances.

The public has a qualified right of access to judgments, judicial opinions and memoranda, and court orders. Public access to opinions and orders is essential to public understanding and monitoring of the judicial process. *See Republic of the Philippines v. Westinghouse Electric Corp.*, 949 F.2d 653, 663-64 (3d Cir. 1991); In re *Continental Illinois Securities Litigation*, 732 F.2d 1302 , 1308-09 (7th Cir. 1984). Access by the legal community to court opinions is essential to the development of the common law and *stare decisis*, which depends on the application of precedent as expressed in court orders, judgments, and the reasoning articulated in judicial opinions and memoranda. Absent a clear showing of a compelling interest that can only be protected by imposing confidentiality restrictions, access to judgments, judicial opinions and memoranda and court orders should not be restricted. If restrictions on access are found to be essential, those restrictions should be narrowly crafted so as to impose no greater restriction on public access than is necessary to protect the interest at stake.

Courts and attorneys must balance the need for access with the legitimate interests of the parties in privacy and confidentiality. Court documents should be written with the presumption of public access in mind, and with the understanding that *de facto* restrictions on access arising from the difficulties of retrieving physical files have been largely eliminated by technology. Consequently, judges and law clerks should not include unnecessary confidential information in filed documents. Attorneys who submit proposed orders for a judge's signature should also exercise similar editorial judgment.

When information restricted by a statute or court rule must be included in a document, or when courts are presented with confidential information that must be incorporated in rulings, an unredacted version should be filed under seal and made available to the attorneys and parties in the case. A redacted version should be filed for public access, with an explanation of the reason for the redactions. The sealing of an entire document, or the filing of a redacted document under circumstances not addressed by a statute or court rule, must be based on a finding by the judge, available in the public record, that the necessity for restricting public access to the document in question overcomes the presumption of public access to judicial decisions in that particular instance.

Best Practices

1. Judges should include in opinions and orders a full discussion of the facts relevant to their decisions, guided by the consideration that the purpose of opinions and orders is to provide to litigants, lawyers, the public, and appellate courts reasoned explanations for their decisions. Courts should avoid including information, the public disclosure of which may be harmful to a litigant or a third party. If there is a compelling reason to include such information in opinions or orders, courts should consider redacting or sealing the information the disclosure of which would be harmful to a litigant or third party.

2. When a court includes information restricted by statute, court rule, or an existing sealing order in an opinion or order, the court should issue both a redacted document, as to which there will be public access, and an unredacted document that will be filed under seal.

3. If an opinion, memorandum, order, or judgment is to be sealed in part or in whole, the judge should

set forth findings of fact and conclusions of law that will be available for public access, including a discussion of the right deemed to be threatened by public access to the full opinion, the lesser restrictive alternatives to sealing the court considered, and why these were rejected.

4. The court should review its decision to seal an opinion, memorandum, or order, upon request by the parties or a third party intervenor, or upon the occurrence of changed circumstances. The sealing order should be vacated if and when the grounds justifying the sealing order no longer exist.

Examples

1. A business entity commences an action against a competitor for the theft of information utilized by the plaintiff in a manufacturing process. The plaintiff's manufacturing process is proprietary and is a closely guarded secret. For the purpose of ruling on a motion for summary judgment, the judge must compare both parties' manufacturing processes in an opinion. The judge files a brief summary judgment order for public access, together with a finding that the manufacturing process constitutes a legally protected trade secret and that public access to the accompanying opinion would compromise the plaintiff's legal interest. The opinion is filed under seal.

2. Same facts as Example 1 above. The theft is alleged to have been committed by a former employee of the plaintiff who became employed by the defendant, and the defendant has not yet established its own manufacturing process. The relief sought by plaintiff is solely injunctive in nature. The judge, ruling on a motion for a preliminary injunction, addresses whether the former employee had access to the plaintiff's information and the likelihood of the plaintiff's success on the merits of the case, but carefully avoids describing the information in detail in the opinion and order.

3. Same facts as Example 1 above. The opinion issued by the judge totals thirty pages addressing a number of facts and legal issues, and the detailed comparison of the parties' manufacturing processes appears on only three pages. A sealing order covering all information about the manufacturing process, based on findings of fact and conclusions of law, is already in place in the case. The judge files the full opinion under seal and a redacted opinion, referencing the existing protective order, for public access.

4. An insurance broker brings an action against an insurer, alleging that she is owed commissions on the sale of the insurer's products, and that other brokers were paid at a higher rate than she was. During discovery, the parties stipulate to a protective order for the production of records of commissions paid by the defendant to other brokers. Both parties move for summary judgment and include in their papers the records of commissions paid to other brokers. In ruling on the motions, the judge does not treat the commission information as confidential, as the protective order applied only to non-filed discovery materials and no showing has been made to justify sealing.

Principle 4 Notice of motions to seal and supporting materials should be reflected in the publicly accessible docket.

The public has a qualified right of access to all papers, including briefs, submitted in support of and in opposition to motions filed with the court that address non-discovery matters. Consequently, motions to seal documents should be rare and made only when there is no feasible alternative. However, in some circumstances, papers filed with the court may contain information that implicates legitimate privacy or confidentiality interests, or otherwise warrants redaction or sealing, and may be proper subjects for a sealing order before filing. In the absence of court rules or orders specifying procedures for the filing of materials under seal, the parties themselves should agree to a procedure under which a party intending to publicly file papers or information which has been subject to a sealing or protective order, or intending to file under seal any new material, informs the other party in a timely manner of that intent, thus allowing the other party opportunity to object, consent, or confer on the appropriate confidentiality status of the material. A court is not required to give particularized notice to any specific constituency when deciding a motion to seal. *See Webster Groves Sch. Dist. v. Pulitzer Publ'g Co.*, 898 F.2d 1371 (8th Cir. 1990).

Best Practices

1. As stated under Principle 1, attorneys should take reasonable steps to minimize the use of confidential information in motions, proposed orders, or briefs, so as to minimize the need to redact or seal such documents. The inclusion of attachments, such as discovery material produced under a protective order, should likewise be minimized, and when necessary, should be presented in such a manner as to facilitate the temporary filing of only the protected attachments, and not the whole document, pending resolution of a motion to seal.

2. Attorneys who intend to submit a motion discussing or attaching material designated by another as confidential or subject to seal should inform the designating party of their intent to file the material and ask the designating party to promptly respond and confirm whether that party continues to contend that the material merits confidentiality.

3. For cases in which the parties are unable to agree upon what, if any, information should be included in any public filing, and in all cases in which new pleadings, substantive motions, and accompanying materials are submitted with the intention of being filed under seal, the court should permit (by way of local rule, standing order, or in a protective order under Rule 26(c)) a party to temporarily file the material with the court under seal, thereby providing notice to all parties of the intended action without compromising the purported private or confidential nature of the material itself, pending a prompt ruling on confidentiality.

Examples

1. A plaintiff intends to file a motion for summary judgment in fourteen days, which will include documents obtained from the defendant through discovery and designated by the defendant as confidential under a stipulated protective order. The plaintiff may inform the defendant of its intention to include specified documents in an upcoming filing and request that the defendant file a motion to seal the material in advance of the filing date. If the defendant files the motion to seal, the plaintiff temporarily files its summary judgment motion and the accompanying documents with the court, pending a decision on the defendant's motion to seal. If the defendant does not move to seal in advance of the filing, the plaintiff still temporarily files its summary judgment motion and the accompanying documents but also files a motion seeking a court order that the summary judgment motion be filed publicly and that defendant's confidentiality designation be removed. If the defendant does not respond or object, defendant will be deemed to have waived the confidential designation, the designation will be removed, and the summary judgment motion with the supporting documents will be publicly filed.

2. The same facts as above, except that the plaintiff agrees that the documents merit sealing. The plaintiff drafts its summary judgment motion, brief, and supporting declarations, limiting its use of confidential material and reference to confidential facts. It temporarily files its motion and accompanying materials with the court along with a motion to seal, and submits a redacted copy of the summary judgment motion and brief intended for public filing. The court reviews the documents proposed to be sealed and the documents proposed to be redacted, and rules upon the motion to seal.

Principle 5 **Non-parties may seek leave to intervene in a pending case to oppose a motion to seal, to have an existing sealing order modified or vacated, or to obtain a sealing order.**

Courts have recognized that the members of the public have standing, and grounds to intervene, to obtain access to documents filed with a court under seal. So too, non-parties who have an interest in privacy and confidentiality of materials filed with the court and available to the public also have standing to independently seek to seal such materials. When the parties agree to secrecy or limitations on disclosure based upon interests that may be narrower than those of non-party intervenors, the court is not likely to have the benefit of the adversary process in making its decision. In such circumstances, courts have the discretion to grant non-parties permission to intervene for the purpose of opposing a pending motion to seal, or moving to have an existing sealing order modified or vacated. *Cf. Chiles v. Thornburgh*, 865 F.2d 1197, 1213 (11th Cir. 1989). The proposed intervenor should demonstrate good cause for the intervention and that it has moved to intervene without undue delay.

The court issuing a sealing order retains jurisdiction to entertain motions to modify or vacate the order after a case is closed. *See Gambale v. Deutsche Bank AG*, 377 F.3d 133 (2d Cir. 2004) (court retains jurisdiction over its own records, and may modify or vacate a sealing order after a case is closed.).

Appellate review exists for a trial court order addressing a motion to intervene and to modify or vacate a sealing order, although federal courts are split as to whether the proper "vehicle" is a *mandamus* petition or an appeal under 28 U.S.C. § 1291. *See Virginia Dept. of State Police v. Washington Post*, 386 F.3d 567, 574 n.4 (4th Cir. 2004); *United States v. McVeigh*, 119 F.3d 806, 809-810 (10th Cir. 1997); *Bank of America Nat'l Trust and Savings Ass'n v. Hotel Rittenhouse Assoc.*, 800 F.2d 339, 341 n.2 (3d Cir. 1986). Whatever the vehicle, "all circuits that have considered the issue have found appellate jurisdiction ... under one doctrine or the other." *McVeigh*, 119 F.3d at 810.

Best Practices

1. The entry of a motion to seal on the docket reasonably in advance of a hearing or decision provides adequate public notice that the court may seal party filed documents,

2. Interested persons who make an appropriate showing under Fed. R. Civ. P. 24(b) should be permitted to intervene to oppose, seek modification of, or seek vacatur of a sealing order.

3. Orders regarding motions to intervene and motions to modify or vacate sealing orders should be subject to immediate appellate review under the collateral order doctrine or any other appropriate procedural mechanism.

Examples

1. Company A wishes to file a motion for summary judgment including financial materials it obtained through discovery pursuant to a protective order. Company A files a motion to seal in advance of or concurrently with its motion for summary judgment. The allegedly confidential material is temporarily filed under seal with the court pending a decision on the motion to seal. The motion to seal and the temporary filing under seal of the financial materials appear on the court docket. The local newspaper, which has been reporting on the case, moves to intervene to oppose Company A's motion to seal. The motion to intervene should be granted.

2. Same facts as in Example 1, and Company A obtains the order sealing material in connection with its summary judgment motion. Several months later a litigant in another action involving Company A discovers the sealing order and believes that the subject financial materials are relevant to the new action. The litigant's attorney moves to intervene and unseal the records. The court grants the motion to intervene. Subsequently, the court may, in its discretion, grant or deny the collateral litigant access to the sealed materials.

Chapter 2
Selected Bibliography

Hartford Courant Co. v. Pellegrino, 380 F.3d 83 (2d Cir. 2004) (addresses common law right of access to docket sheets).

In re *Application of Dow Jones & Co., Inc.*, 842 F 2d 603 (2d Cir), *cert. denied, sub nom.* Dow Jones ? Co. v. Simon, 488 U.S. 948 (1988) (entry of a protective order may give rise to redressable injury).

North Jersey Media Group, Inc. v. Ashcroft, 308 F.3d 198 (3d Cir. 2002) (analyzes media claim of access to "special interest" deportation proceedings under "experience and logic" test of *Richmond Newspapers*, 448 U.S. 555 (1980), and denies access; notes that some courts of appeals have extended First Amendment right to civil trials).

Virginia Dept. of State Police v. Washington Post, 386 F.3d 567 (4th Cir. 2004) (discusses distinction between First Amendment and common law rights of access and between summary judgment and discovery materials for purposes of access; discusses criminal investigation as compelling interest).

In re *Washington Post Co.*, 807 F.2d 383 (4th Cir. 1986) (extends common law right of access to documents submitted with regard to proceedings that fall within that right; reminds district courts to follow "procedural requirements" set out in earlier circuit decision).

Detroit Free Press v. Ashcroft, 303 F.3d 681 (6th Cir. 2002) (conducts same analysis as *North Jersey Media Group*, cited above; reaches opposite conclusion).

Webster Grove School Dist. v. Pulitzer Publishing Co., 898 F.2d 1371 (8th Cir. 1990) (upholds limitation on access to civil proceeding involving juveniles; does not decide whether First Amendment right of access extends to civil proceedings, but applies common law standards; holds that procedural information on docket should not have been sealed).

Chicago Tribune Co. v. Bridgestone/Firestone, Inc., 263 F.3d 1304 (11th Cir. 2001) (discusses right of access to sealed materials under First Amendment, common law and Rule 26(c); distinguishes between discovery motions and "merits" motions for purposes of access).

United States v. Valenti, 987 F.2d 708 (11th Cir. 1993) (affirms authority of district court to seal bench conference and articulate reasons later to satisfy a compelling interest; holds "dual-docketing system" unconstitutional).

Rule 5(d), Federal Rules of Civil Procedure (discovery materials not to be filed until "used in the proceeding" or until the court orders filing).

Rule 79, Federal Rules of Civil Procedure (requires maintenance of "civil docket" and chronological listing of entries thereon).

Rule 412(c), Federal Rules of Evidence (provides for sealing of documents and *in camera* hearing on requests to use sexual conduct evidence).

United States District Court, District of New Jersey, L. Civ. R. 5.3 (establishes comprehensive procedures for electronic filing, including motions to seal).

United States District Court, District of South Carolina, L. Civ. R. 5.03 (establishes procedure for motions to seal).

A full bibliography, updated periodically, may be found on The Sedona Conference® web site at www.thesedonaconference.org starting in July 2007.

Chapter 3. Proceedings in Open Court

Principle 1 The public has a qualified right of access to trials that can only be overcome in compelling circumstances.

Public access to trials[4] on the merits reflects a long tradition in the United States. Trials have long been considered open to the public. Public access to trials is essential to the monitoring and oversight of the judicial process. Public access also allows the public to share the "communal" experience of the trial. Constitutional and common law rights of access compel the conclusion that trials are at the heart of the right of public access both for historical reasons and to vindicate concerns for the legitimacy and accountability of the judicial system.

Legitimate interests exist that may justify narrow restrictions on public access to trials. For example, governmental interests exist in protecting certain types of information, such as those pertaining to classified national security information, undercover operations, and confidential informants. Privacy interests, such as those related to juveniles and to sensitive medical information, may justify limited trial closure in some contexts. Property interests also exist which may warrant restrictions, such as those related to trade secrets. Moreover, the judicial system itself may, as an institution, require a limited restriction on immediate public access for purposes of, for example, "sidebar" conferences.

The United States Supreme Court has established a right of public access to criminal trials derived from the First Amendment. The Court has also established standards that govern any restriction of public access to criminal trials. *See, e.g., Press-Enterprise Co. v. Superior Court*, 464 U.S. 501, 508-510 (1984); *Globe Newspaper Co. v. Superior Court*, 457 U.S. 596, 606-607 (1982). Similar considerations apply to civil trials. A party seeking to restrict public access to a civil trial should demonstrate a substantial likelihood that a compelling interest will be prejudiced by allowing public access and that no alternative other than closure can adequately protect the threatened interest. Any restriction on public access ordered by the court should be narrowly tailored. The trial court should also make findings of fact and conclusions of law adequate to justify the closure.

Best Practices

1. Closure of a civil trial on the merits is extraordinary and should be permitted only in rare circumstances where compelling interests leave no alternative.

2. Any closure must be no broader than absolutely necessary, and should be strictly limited to that portion of the trial that requires closure.

3. Alternatives to complete closure should be employed whenever possible. For example, counsel and witnesses may be directed to avoid references to particular facts or subjects (if such a direction will not deprive a party of the right to a fair trial) or, if a witness has a legitimate privacy interest justifying protection of his or her identity, testimony may be taken anonymously.

4. If closure is necessary, the court should consider providing access through other means (such as providing the public with a prompt transcript) if this can be done without compromising the compelling interest that required closure.

[4] As used herein, "trials" encompasses jury and nonjury trials as well as any judicial proceeding in court or on the record, except those conducted *in camera*.

5. Courts should require parties who contend that closure of a portion of a trial will be necessary to raise the issue through a written motion in advance of trial, to allow the court ample time for consideration, and to permit the full exploration of alternatives to closure (such as orders precluding references to certain matters and/or providing for substitutes for evidence that implicates confidentiality concerns). Such a closure motion should be heard at a hearing duly noticed and open to the public. The hearing on the motion should be recorded or transcribed.

6. Any order of closure should be based on a complete statement of the reasons for closure and of the findings of fact that support the closure order in sufficient detail to allow appellate review. The order should include express findings identifying the compelling interest that requires closure and the reasons why less restrictive alternatives are insufficient.

7. If the interest that led to closure loses its compelling importance with the passage of time, the transcript of the closed portion of the trial should be made available to the public.

8. The need to hold certain brief discussions during the course of a trial outside the hearing of the jury under circumstances where it is impractical to excuse the jury from the courtroom justifies the use of "sidebar" conferences that are inaudible to the jury and the public. Because such conferences involve the discussion and resolution of procedural and substantive issues integral to the conduct of the trial, however, these should remain subject to the right of public access and, absent compelling justification, transcripts of such proceedings should be promptly made available to the public (subject to whatever protections are necessary to keep matters from coming to the attention of the jury).

9. Conferences in chambers are occasionally used to address issues that arise in the course of a trial. Because it is not practical to admit the public to in-chambers conferences, the use of such conferences to address the merits of procedural and substantive issues (as opposed to, for example, scheduling matters or other routine discussions of no genuine public interest) should be avoided unless there are compelling circumstances that justify exclusion of the public (for example, where the subject under discussion involves a jury issue that implicates protected privacy rights of a juror). If procedural or substantive issues are discussed in chambers, the proceedings should be recorded and transcripts promptly made available to the public (unless, again, compelling circumstances justify confidentiality).

10. In-chambers proceedings should never be used to prevent public access to trial proceedings that could not be closed to the public if they took place in a courtroom.

11. Any closed trial proceedings must be transcribed or recorded in the same manner as open proceedings, so that access may be provided if the closure order is later reversed, or if the interests that require closure are later waived or no longer require protection.

Examples

1. On the first day of trial, the attorney for the plaintiff makes an oral application to the court to seal the trial, contending that his client might be embarrassed by public disclosure of "private facts." No notice of this motion appears on the public docket. The attorney presents no facts to support the likelihood, nature, or extent of the damage his client would suffer by the public disclosure of the "private facts," and the attorney does not present any reasons why a less restrictive alternative to sealing the trial would not satisfy the concern (for instance, sealing only particular testimony or evidence). Based on these deficiencies, the court denies the application.

2. Consistent with the local rules of the court, a plaintiff files a motion to seal expert testimony that will be offered by both parties in a patent infringement trial. The experts will testify on the damages sought by the plaintiff, and their testimony will be premised on financial data held confidential by the plaintiff. The plaintiff submits an affidavit with its motion, which explains the nature of the data and why it is confidential. The affidavit also explains the competitive harm that will be visited on the plaintiff if the data becomes public. The court hears the motion, makes findings of fact and conclusions of law, and holds that specified portions of the experts' testimony revealing the financial data will be sealed. The court's ruling is filed for public review.

Principle 2 The public has a qualified right of access to the jury selection process.

Public access to the jury selection process promotes fairness by allowing the public to verify the impartiality of jurors, who are key participants in the administration of justice. Moreover, public access enhances public confidence in the outcome of a trial because public access assures those who are not attending that others may observe the trial. Public access also vindicates the societal concern that wrongdoers are brought to justice by individuals who are fairly selected to be jurors. Consistent with these interests, courts should not conceal from the public information that might bear on the ability of jurors to decide the matter before them impartially. Public access fosters discussion of government affairs by protecting the full and free flow of information to the public.

There may be circumstances in which some restriction to public access is necessary to ensure the safety or well-being of individual jurors, or to address personal privacy concerns.[5] In certain civil cases, courts may order that access to juror identities be limited or deferred to protect the safety of jurors, or to ensure their verdict is a product of the evidence admitted at trial rather than outside interference. *See Richmond Newspapers, Inc. v. Virginia*, 448 U.S. 555 (1980); *In re Globe Newspaper*, 920 F.2d at 94; *In re Baltimore Sun Co.*, 841 F.2d 74 (4th Cir. 1988); *Sullivan v. National Football League*, 839 F. Supp. 6 (D. Mass. 1993).

Various interests are cited in opposition to public access to the juror selection process. These interests include juror privacy, ensuring that an adequate number of persons are willing to serve as jurors, protection of the integrity of the jury system and avoiding a circus-like atmosphere. But the difficulty in attracting qualified jurors, or the fact that a trial may be the subject of intense media coverage, are insufficient reasons to deny public access to the jury selection process. These reasons would render the right of access meaningless— the very demand for openness would defeat its availability. Thus, personal preferences of jurors, a judge's unwillingness to expose jurors to press interviews, or a judge's concern that jurors may disclose what transpired during deliberations do not, by themselves, warrant anonymous juries or restrictions on public access.

The qualified right of public access to the jury selection process does not extend to the deliberations of jurors, which traditionally occur in secret. In the case of jury deliberations, that secrecy is reinforced by substantive evidentiary rules that prevent jury verdicts from being impeached by testimony concerning the jury's internal deliberations in most instances.

However, in cases in which the conduct (or misconduct) of the jury itself becomes an issue that is the subject of testimony and/or other proceedings before a court, such proceedings, like other trial proceedings, are subject to the right of public access and should remain confidential only if compelling reasons (such as legitimate interests in juror privacy or in protecting a criminal investigation) justify confidentiality. Concealing a juror's misconduct is not by itself a legitimate privacy concern. While a court may take steps to prevent remaining jurors from being tainted by such proceedings, that is not in itself a reason for denying public access; rather, the steps to be taken should be similar to those used by the court to prevent jurors from having access to other possibly prejudicial information about a case (*i.e.*, instructions to avoid news coverage or, in some cases, sequestration). *See United States v. Edwards*, 823 F. 2d 111 (5th Cir. 1987).

[5] Proposed Fed. R. Civ. P. 5.2 would mandate that certain personal identifiers be redacted from documents filed with the United States Courts. Neither the text of the proposed rule nor the Advisory Committee Notes explicitly address documents created or filed by the courts themselves, such as juror information. While redaction of personal identifiers from juror information may be considered consistent with the overall intent of the proposed rule, redaction of such information by court personnel is inconsistent with the intent of the Advisory Committee to place such duties on litigants and counsel.

Courts may limit an attorney's or party litigant's ability to interview jurors regarding their verdict or deliberations, or may require a showing of good cause before allowing such post-verdict interviews. Such orders do not themselves implicate the public's right of access to any public information, but only limit the behavior of lawyers and litigants. However, courts ordinarily should not limit the public's ability to interview jurors after the conclusion of a trial. *Compare* In re *Baltimore Sun Co.*, 841 F.2d at 75-76; *State v. Neulander*, 801 A.2d 255 (N.J. 2002), *and* In re *Express News Corp.*, 695 F.2d 807, 810 (5th Cir. 1982); *United States v. Antar*, 38 F.3d 1348, 1364 (3rd Cir. 1994).

Best Practices

1. Empanelling an anonymous jury or closing jury *voir dire* ("jury secrecy" procedures) are extraordinary and should be undertaken only in rare circumstances where exceptionally important interests leave a trial court with no practical alternative. Although such circumstances have sometimes been found to exist in criminal cases (especially ones involving organized crime), it would be extremely rare for such circumstances to be present in a civil case. If initial questioning of jurors is conducted through written questionnaires, these should be available to the public.

2. Before answering oral or written questions from the court or the parties, potential jurors should be informed about whether and how the court will protect the confidentiality of any information provided. Such procedures help alleviate concerns that the government will compel them to disclose personal or confidential information without adequate privacy protections and thereby ensure that sufficient numbers of citizens will agree to serve and will not avoid service because of privacy concerns.

3. Any jury secrecy order should be no broader than absolutely necessary, should be strictly limited to highly personal juror information that requires protection, and should be entered only on the affirmative request of an individual juror. Alternatives to jury secrecy should be employed whenever possible.

4. If jury secrecy is necessary, a trial court should provide access through other means (*i.e.*, a transcript) if this could be done without compromising the overriding interest that required secrecy in the first place.

5. If the interest that led to jury secrecy loses its overriding importance with the passage of time, a transcript of the closed portion of the jury proceeding or the names of anonymous jurors could be made available to the public upon application to the court by an interested party. Stronger reasons to withhold juror names and addresses (such as jury tampering) normally arise during trial rather than after a verdict is rendered.

6 Trial courts should require parties who anticipate that jury secrecy may be necessary to raise the issue through written motions, to allow a trial court ample time for consideration and to permit the full exploration of alternatives to secrecy (such as change of venue). Such motions should be heard at a hearing duly noticed and open to the public.

7. Courts should freely allow nonparties who oppose jury secrecy to submit papers and make arguments addressing any secrecy motion. Intervention should be liberally granted for this purpose.

8. Any order of jury secrecy should be based on findings of fact that support the secrecy order, including express findings identifying the compelling interests that require secrecy and the reasons why less restrictive alternatives are insufficient.

9. Jury secrecy orders, while appearing to be interlocutory in nature, should be appealable by mandamus or under the collateral order doctrine.

10. Any closed jury proceeding should be recorded and transcribed, so that access may be provided if the secrecy order is later reversed, or if the interests that require secrecy are later waived or no longer require protection.

Examples

1. In a civil action brought by a government agency against a well-known entertainer, the defendant approaches the court on the first day of trial and requests that the *voir dire* be sealed. The defendant's argument is that juror candor in answering questions will be compromised by the attendance of the press. In deciding the motion, the court considers if adequate public notice was given that the request would be made. Second, the court considers the proposition that candor might be compromised, noting that the application is solely premised on the defendant's celebrity status and press coverage. In the absence of a showing of facts supporting the proposition, the court denies the motion.

2. During the jury selection process in a civil action arising out of the sexual abuse of minors, the court advises the prospective jurors that they will be asked during *voir dire* if they ever experienced or witnessed sexual abuse. Given the nature of such questions and the (presumably) private nature of "yes" answers, the court gives jurors an opportunity to answer at sidebar in the presence of counsel. The sidebar conferences are transcribed. Two jurors state that parents or other relatives sexually abused them. One of these jurors testified about the abuse at a criminal trial. The other never reported the abuse. The judge releases the transcript of the *voir dire* of the first prospective juror but, after determining that the second juror would suffer psychological harm if the abuse became public, seals the transcript as to her. The judge puts findings of fact and conclusions of law on the record to justify the sealing.

Principle 3 Absent a compelling interest, the public should have access to trial exhibits.

The right of public access to trial proceedings includes the right of public access to evidence admitted during a trial, including the testimony that is memorialized in the transcript. *See Nixon v. Warner Communications,* 435 U.S. 589, 609 (1978). Admitted evidence should be fully available to the public on a contemporaneous basis, and the standard for sealing evidence should be the same as that for closing a courtroom: That is, only compelling interests may justify sealing, and any order denying access must be based on findings of fact and conclusions of law demonstrating such an interest.[6]

It must be recognized, however, that logistical problems may foreclose contemporaneous access to trial exhibits in particular cases. This may simply be a question of practicality. *See e.g.* In re *Application of National Broadcasting Co.*, 635 F.2d 945 (2d Cir. 1980). In such circumstances, the court, the parties, and the person seeking access should confer in an attempt to arrive at a procedure acceptable to all. When circumstances warrant, the public interest may be satisfied by providing access to the trial proceedings when the exhibit is admitted, rather than access to the exhibit itself. When access is sought to evidence introduced through means of novel technology such as computer generated or enhanced imagery, the court may be vested with wider discretion in deciding whether and how access may be allowed. *See* In re *Providence Journal Co.*, 293 F.3d 1 (1st Cir. 2002). Moreover, public access to trial exhibits is inhibited by a prevailing practice in most American trial courts to return trial exhibits to the parties after the time for filing an appeal has expired, or an appeal has been taken and resolved. Because the physical exhibits are not maintained as public records, these are no longer subject to enforceable public access rights. *See Littlejohn v. Bic Corp.*, 851 F.2d 683 (3rd Cir. 1988).

Best Practices

1. Courts should reasonably and promptly accommodate requests for access to exhibits admitted at trial and not under seal.

2. Providing access to trial evidence so that copies, recordings and/or photographs can be made of the evidence should be routine. Access should be denied only in rare circumstances where compelling interests leave the court with no practical alternative. Any denial of access to trial exhibits should be no broader than absolutely necessary and should be strictly limited to evidence that requires protection. Alternatives to denial of access should be employed whenever possible.

3. A party that intends to request that the court seal evidence it expects to be admitted at trial should make its request by written motion before trial. The court should hear and decide motions to seal admitted trial exhibits after other parties have had time to oppose the request, or non-parties have had time to request leave to intervene to oppose the request. Absent the most exigent circumstances, trial courts should deny any request for denial of access that is not made in time to allow such notice.

4. The hearing on the motion should be recorded.

[6] The Working Group reached no consensus on a right of public access to excluded evidence. On the one hand, such evidence, by its very exclusion, has been deemed by the judge to be irrelevant to the jury function. On the other hand, access to excluded evidence may allow the evaluation of the judge's role as "gatekeeper" and the overall fairness of the trial. In addition, evidence marked during trial becomes part of the record on appeal, even if excluded, indicating that appellate courts consider excluded evidence to be part of the adjudicative process.

5. If denial of access is necessary, a trial court should consider providing access through other means (i.e., providing access at the conclusion of the trial) if this can be done without compromising the overriding interest that required denial of access. If the interest that led to denial of access loses its overriding importance with the passage of time, access to trial evidence should be granted at the earliest possible time.

6. Any order denying access to evidence should be based on a complete statement of the reasons for denial and of the findings of fact that support the order denying access, including express findings identifying the compelling interests that require denial of access and the reasons why less restrictive alternatives are insufficient.

Examples

1. A plaintiff receives documents in discovery from the defendant in a product liability case. Prior to trial, the documents are marked confidential pursuant to a protective order entered in the case, and the plaintiff is prohibited from disseminating them publicly. Plaintiff identifies the documents on an exhibit list exchanged before trial, and during the trial these are marked and admitted in evidence. At no time does the defendant move to have the trial exhibit sealed. The exhibits are available to the public.

2. Same facts as above, except that the trial has ended and the exhibits have been returned to the parties who introduced the exhibits, and the press seeks to obtain copies of the admitted exhibits from the plaintiff. Although the protective order once protected the documents from disclosure, the plaintiffs' attorney provides the exhibits to the press because they were admitted in open court. The defendant learns of the press's request and seeks to enforce the protective order to bar the plaintiff from providing the exhibits to the press. The court rejects the defendant's effort to invoke the protective order because the documents, having been received in evidence in open court, are no longer properly subject to protection.

3. A plaintiff receives documents in discovery from the defendant in a product liability case. The documents are marked "confidential" pursuant to a protective order entered in the case and the plaintiff is prohibited from disseminating them publicly. Plaintiff identifies the documents on an exhibit list exchanged before trial and the defendant requests that the documents only be admitted under seal. The defendant moves before trial to seal the exhibits on the basis that the exhibits contain proprietary information and trade secrets. The court holds a hearing and grants the motion, protecting genuinely proprietary information from disclosure. The court admits exhibits for which no compelling need for protection has been established.

Chapter 3
Selected Bibliography

In re *Providence Journal Co.*, 293 F.3d 1 (1st Cir. 2002) (right of access to attend criminal trial and pretrial proceedings extends to "documents and kindred materials;" defendants' right to fair trial constitutes compelling interest sufficient to allow restriction of access; common law, but not First Amendment, right of access held to encompass duplication of evidence, but where "cutting-edge technology" in issue, trial court given discretion to accommodate access).

ABC, Inc. v. Stewart , 360 F. 3d 90 (2d Cir. 2004) (vacating in part order closing *voir dire* examination of potential jurors; recognizes that after-the-fact release of transcript no substitute for presence; trial court failed to demonstrate interest in assuring juror candor sufficient to seal and failed to use available alternatives to sealing).

Publicker Indus., Inc. v. Cohen, 733 F.2d 1059 (3d Cir. 1984) (First Amendment and common law rights of access extended to civil proceedings).

In re *Application of National Broadcasting Co.*, 635 F.2d 945 (2d Cir. 1980) (common law right of access to inspect and copy judicial records extends to evidence introduced at trial, whether documentary or of other nature, under reasonable procedures to be determined by the court).

United States v. Antar, 38 F.3d 1348 (3d Cir. 1994) (presumptive right of access applies to voir dire of examination of potential jurors; concludes that trial court erred in sealing transcript without adequate notice and findings of fact; modifies trial court restrictions on post verdict interviews of jurors by press).

United States v. Simone, 14 F.3d 833 (3d Cir. 1994) (presumptive right of access applies to post verdict examination of jurors into possible misconduct; strikes down closure of examination given failure of trial court to articulate "overriding interest;" after-the-fact receipt of transcripts not equivalent to actual presence).

Little John v. BIC Corp., 851 F.2d 673 (3d Cir. 1988) (common law presumption of access applies to documents initially produced in discovery pursuant to protective order and later admitted into evidence at trial, but exhibits returned to party after trial are no longer judicial records and disclosure cannot be compelled).

In re *Perrigo Co.*, 128 F.3d 430 (6th Cir. 1997) (injunction prohibiting magazine from publishing materials filed under seal violated First Amendment; umbrella protective order pursuant to which documents filed under seal without good cause determination invalid).

United States v. McDougal, 103 F.3d 651 (8th Cir. 1996) (affirms refusal to allow media access to videotaped depositions of President Clinton, although introduced at criminal trial and transcript released; concludes that, under circumstances presented, videotape itself not a "judicial record;" rejects "strong" presumption of access recognized by other circuits and defers to sound discretion of trial court).

United States v. McVeigh, 119 F.3d 806 (10th Cir. 1997) (First Amendment right of access does not extend to suppressed evidence or evidence inadmissible at trial).

Goff v. Graves, 362 F.3d 543 (8th Cir. 2004) (affirms sealing of depositions of confidential prison informants in Section 1983 action; preservation of institutional security and protecting against retaliation are compelling interests to issue protective order and to seal portion of record).

28 C.F.R. Sec. 509 (sets out U.S. Department of Justice policy with regard to open judicial proceedings, civil and criminal).

A full bibliography, updated periodically, may be found on The Sedona Conference web site at www.thesedonaconference.org starting in July 2007.

Chapter 4. Settlements

Principle 1 There is no presumption in favor of public access to unfiled settlements, but the parties' ability to seal settlement information filed with the court may be restricted, due to the presumptively public nature of court filings in civil litigation.

A dichotomy currently exists between open courts and private alternative dispute resolution such as arbitration and mediation. In many cases, parties may be willing or able to waive litigation in favor of such private dispute resolution, where the confidentiality of both the process and its outcome can be contractually assured. Similarly, litigants possess broad discretion to contract privately for confidentiality as a condition to settling even litigated disputes. In such cases, confidentiality, like other settlement terms, becomes a matter of private agreement to be enforced pursuant to applicable contract law.

There is a strong public policy in favor of settlement. Confidentiality of settlement terms is generally believed to encourage such settlements, and in the majority of cases, the parties need not make their settlement public by filing it with the court. Courts will generally enforce private confidentiality agreements so long as they merely restrict the voluntary disclosure of information and do not prohibit disclosures required by law or court order. Because the agreements can be reached without any judicial involvement, and the settlement itself is rarely filed with the court, these confidential settlements do not implicate any right of public access. *See Gambale v. Deutsche Bank AG*, 377 F.3d 133, 143 (2d Cir. 2004); *Herrnretier v. Chicago Housing Authority*, 281 F.3d 634, 636-37 (7th Cir. 2002); *Pansy v. Borough of Stroudsberg*, 23 F.3d 772, 781, 788-89 (3d Cir. 1994); Laurie K. Doré, *Settlement, Secrecy, and Judicial Discretion: South Carolina's New Rules Governing the Sealing of Settlements*, 55 S.C. L. Rev. 791, 799-800 (2004).

In many cases, however, a confidential alternative to litigation may not be available to disputing parties. Likewise, settling parties may not wish to rely solely upon private agreement to ensure confidentiality and may choose instead to more deeply involve the court in their confidential compromise. *See* Laurie K. Doré, *Settlement, Secrecy, and Judicial Discretion: South Carolina's New Rules Governing the Sealing of Settlements*, 55 S.C. L. Rev. 791, 801-04 (2004). In utilizing a public court to resolve their dispute or enforce its confidential settlement, the litigants invoke the jurisdiction of a forum that is subject to public oversight and monitoring. As such, confidentiality may no longer be a matter within the exclusive control of the parties. Confidentiality agreements between the parties regarding settlement do not bind the court, and if the parties wish to file their settlement agreement under seal, the court must exercise independent judgment and comply with applicable legislative and judicial standards[7] before issuing any sealing order incident to a settlement. *See Gambale v. Deutsche Bank AG*, 377 F.3d 133, 139-42 (2d Cir. 2004).

Although contract doctrine in some jurisdictions may invalidate confidentiality clauses that are illegal, unconscionable, or contrary to public policy, a strong and well-established public policy favors alternative dispute resolution (ADR) and the private settlement of disputes. Thus, notwithstanding the potential public interest in the resolution of disputes involving statutory or public rights (*i.e.*, consumer or employee claims) or public health and safety, little public oversight of confidentiality in alternative dispute resolution or private settlement currently exists. Attorneys should thus ensure that their clients are fully aware of all available public and private dispute resolution processes and advised that confidentiality cannot be expected or assured in a public forum.

[7] See Chapter 4, Principle 2 below.

Best Practices

1. At or before the commencement of litigation, attorneys should confer with their clients to determine whether private dispute resolution is available and would be preferable to traditional litigation in the courts. Among other things, attorneys should present these options to clients in the context of the clients' needs or desires to maintain confidentiality.

2. Attorney should discuss with clients that certain disputes present "classic" matters for private resolution, such as breach of a commercial contract between business entities. In contrast, other disputes, such as those brought by individual consumers or employees to vindicate statutory rights or involving public entities or officials, may not be appropriate for private dispute resolution given the public interest in their resolution.

3. In discussing the above options with clients, attorneys should also discuss the available mechanisms for enforcement of any breach of confidentiality by adversaries.

Examples

1. Two parties to a commercial agreement include in that agreement a provision for mandatory arbitration or mediation. The agreement provides for a sale of goods by one party to the other. No public health or safety concerns are implicated. Under these circumstances, there is no need for public oversight of the dispute resolution process and the parties may ensure confidentiality through contract. Enforcement of any settlement would be through contract law principles.

2. An individual receives telecommunications services from a large business entity. The consumer, under the terms of a standard agreement that was mailed to him, is required to arbitrate any future dispute that he has with the business entity. Under the terms of a confidentiality provision in the arbitration agreement, no public access is available to the facts or nature of the dispute, the arbitration proceedings, the terms of any award or settlement, or the services rendered by the arbitrator in this particular case. This dispute, which may implicate the rights of similarly situated consumers, involves statutory claims that have both remedial and deterrent objectives and that arguably implicate a public interest broader than the immediate parties. The confidentiality of this alternative forum raises policy concerns absent from example 1 and not addressed by the Working Group.

3. A business entity intends to commence an antitrust action against a competitor. Rather than proceed to litigation, the parties agree to arbitrate or mediate. A settlement is reached under which the competitors agree to divide markets on a geographic basis, in violation of antitrust laws. A startup company formed by former employees with knowledge of the confidential settlement agreement files suit, alleging that the settlement violates antitrust laws. The settling parties should not have any expectation that the confidentiality of the settlement will be maintained, inasmuch as the legality of the settlement itself has been questioned and is relevant to the action.

Principle 2 Settlements filed with the court should not be sealed unless the court makes a particularized finding that sufficient cause exists to overcome the presumption of public access to judicial records.

Parties that resort to a public forum and that enter into a settlement thereafter may have legitimate interests that warrant confidentiality. However, given the public right of access to public forums, sealed settlements should be the exception and not the norm. Courts should assure that settlements that are filed with the court are not sealed unless good cause exists; and unless specific findings of fact and conclusions of law are made and are available for public review. Attorneys who choose to file a settlement with the court should not seek to seal that settlement unless they are satisfied that such a showing can be made.

Courts are public forums. As discussed in Chapter 2, there is a presumption of access to courts and to information filed with courts, including settlement agreements. Thus, information considered to be confidential by parties and filed with courts may, by the act of filing, become public records subject to public access. *Jessup v. Luther*, 277 F.3d 926 (7th Cir. 2002); *Bank of America Nat'l Trust & Savings Ass'n v. Hotel Rittenhouse Assoc.*, 800 F.3d 339 (3d Cir. 1986). This presumption of public access, however, is arguably weaker (and thus more easily rebutted) for "settlement facts" that relate to the specific terms, amounts, and conditions of a settlement involving non-governmental, private litigants than the presumption that attaches to information more central to the adjudicatory function of courts. *See Gambale v. Deutsche Bank AG*, 377 F.3d 133, 143-44 (2d Cir. 2004) (distinguishing between settlement amount and summary judgment documents). In considering whether to seal a settlement, then, a court might appropriately distinguish between settlement information that would not exist but for the settlement and "adjudicative" facts that may be relevant to the underlying merits of the settled controversy.

Parties may have legitimate interests in the confidentiality of all or part of a settlement. Parties may also have justifiably relied on a promise of confidentiality in entering into a settlement. At the same time, however, a sealed settlement may affect the interests of the general public and collateral litigants. To overcome the presumption of public access, then, parties must establish sufficient cause and satisfy applicable tests established by legislatures and courts to govern the sealing of a settlement, in whole or in part. In addition, the judge should make specific findings of fact and conclusions of law on any application to seal a settlement to determine whether the presumption of public access has been overcome.

Despite resort to a public forum, the parties may elect to avoid any question of access to the terms of a settlement by choosing not to file it. For example, parties may enter into a settlement agreement and then file a voluntary dismissal under Fed. R. Civ. P. 41(a)(1). Such a dismissal requires no judicial action and the settlement agreement would not be submitted to the court. Alternatively, a party could move for dismissal under Fed. R. Civ. P. 41(a)(2), the resolution of which does not require approval of any settlement agreement. Under either procedure (or their state equivalents), the settlement agreement does not become a public record. The unfiled settlement will not trigger any presumption of public access and will instead have the status of any other private contract. *Compare SmithKline Beecham Corp. v. Pentuch Group*, P.L.C., 261 F. Supp. 2d 1002, 1004-08 (N.D. Ill. 2003) (Posner, C.J., sitting by designation) (alleged illegality of settlement agreement not subject to review under either procedure) *with Fomby-Denson v. Department of the Army*, 247 F.3d 1366, 1374-75 (Fed. Cir. 2001) (declining *sua sponte* to enforce confidential settlement agreement as contrary to public policy).

Settlements that are both filed and sealed appear to be infrequent, at least in federal courts. R. T. Reagan, *et al.*, *Sealed Settlement Agreements in Federal District Court* (Federal Judicial Center, 2004). Confidential settlements,

however, are more common and of broader concern. Parties are largely free to agree between themselves to confidentiality provisions in settlements. If the parties enlist the court's assistance concerning the settlement, however, the court should independently scrutinize any confidentiality provision. For example, the parties may request that the court retain enforcement jurisdiction to oversee the fulfillment of the settlement terms, or they may file a separate action for specific performance of the settlement or to recover damages for its breach. In such cases, the court should not enforce any non-disclosure or confidentiality provision that is not supported by a specific and sufficient showing of good cause.

Best Practices

1. Before attempting to seal a settlement, attorneys should confer with their clients to ensure that legitimate privacy, commercial or similar confidences exist that warrant confidentiality.

2. When negotiating the terms of a settlement, attorneys should confer among themselves with regard to any need for confidentiality and attempt to reach agreement on legitimate grounds for confidentiality.

3. Attorneys should not seek to seal settlements unless they are satisfied that grounds exist for a sealing order.

4. In considering whether to seal a settlement or enter a confidentiality order incident to a settlement, courts should distinguish between "settlement facts," such as the amount, terms and conditions of a compromise, and "adjudicative facts" that are relevant to the merits of the underlying controversy. The former, which arise out of the settlement process itself, might warrant a sealing order. Care should be taken in extending any such order to the latter so as to avoid suppressing information relevant to other cases, public health or safety, or other legitimate public interest.

5. In negotiating a confidential settlement agreement, attorneys should incorporate into any confidentiality provision an explicit exception for disclosures required by law or court order.

Examples

1. An individual plaintiff and a corporate defendant have entered into a settlement of a personal injury action. The defendant, as a matter of corporate practice, does not reveal the monetary amount of any settlements. The defendant insists, and the plaintiff agrees, on a confidential settlement. The parties do not contemplate filing the settlement with the court, as there is no basis for a sealing order.

2. An individual plaintiff and a corporate defendant have entered into a settlement of a personal injury action. The defendant settled to avoid the publication of internal documents at trial and on the express condition that the amount of the settlement would be confidential. The parties want the terms of the settlement embodied in an order by which the court retains jurisdiction to enforce the settlement. They move to seal the settlement. While the settlement itself would be presumed to be a public document if filed, the presumption of public access is weak as to the amount of the settlement. The court seals only the amount of the settlement.

3. An individual plaintiff who developed certain software is in litigation with a corporate defendant. The litigation arises out of the corporate defendant's alleged failure to develop and market new applications arising out of the software. The parties enter into a settlement agreement. The terms of the settlement provide for the parties to share source codes of the defendant's applications. Both parties, who are in a very competitive field of business, deem the source codes highly confidential. The parties agree that the settlement should be confidential. Neither party trusts the other and both contemplate injunctive relief and contempt should the source codes be misused. They agree to file a motion to seal the settlement. The source codes are described in detail so that there can be no misunderstanding of the scope of the settlement in any future enforcement action. The court issues an order sealing only that part of the settlement that reveals the source codes.

Principle 3 Settlement discussions between parties and judges should not be subject to public access.

Courts primarily exist to resolve disputes. Disputes may be resolved in a number of ways, including settlement. A strong public policy supports settlement and the "just, speedy, and inexpensive determination of every action." Fed. R. Civ. P. 1. Thus, judges should be expected to encourage settlement and to participate in settlement discussions.

Judges are public officials, however, and, as such, are subject to oversight and monitoring by the public. Thus, when a judge participates in settlement discussions between the parties or is otherwise "injected" into the settlement process, the judge's actions are arguably subject to public monitoring and oversight. The desire or need for such oversight and monitoring may be heightened when settlement discussions affect public health and safety.

However, several factors argue against public access to settlement negotiations even when they may involve the court. First, settlement negotiations require candor, and public access might discourage a party from revealing information necessary for self-evaluation and compromise. Second, settlement discussions are often conducted on an *ex parte* basis, where information is exchanged with the judge for settlement purposes only and is never shared with the adversary. Third, and most significantly, in promoting settlement, the judge acts as a facilitator, rather than as an adjudicator. Because the judge is not engaged in "decision-making," the rationale for public oversight and monitoring is significantly diminished.

Indeed, in many cases, the parties may privately settle their dispute without filing their settlement or submitting it for approval or other action by the court. In these cases, the case is dismissed on stipulation. No judicial record exists and the judge has neither the need nor the power to approve or disapprove of the settlement. In such cases, where the judge has no approval role and serves merely as a mediator or facilitator for the parties' private negotiations, any presumption of public access is weak, if not non-existent.

If public access is to be denied on this premise, however, the judge should take care not to step into a judicial role concerning the settlement. To protect the confidentiality of their settlement, the parties should not file their agreement with the court or seek judicial "approval" of their compromise. If parties voluntarily elect to file their settlement agreement in order to facilitate its subsequent enforcement, their action may create a judicial record, trigger a presumption of public access, and forfeit the confidentiality of the settlement.

Best Practices

1. A judge may act as an intermediary or facilitator in settlement negotiations between the parties to a case. Alternatively, the judge may refer the case for confidential, court-annexed alternative dispute resolution such as mediation. So long as the court does not step into an adjudicatory role and the settlement agreement is not filed with the court, no presumption of public access to the settlement discussions or to any settlement agreement will result.

2. Absent a statute or rule which requires otherwise, attorneys should not ask a judge to "approve" a settlement that they wish to keep confidential, file that settlement with the court or request that the terms of the confidential agreement be entered as orders of the court. A judge should not seek to approve a private settlement unless required or requested to do so.

3. In cases where judicial approval of a settlement is legally required (*e.g.*, class actions), or in cases where the parties seek the court's *imprimatur* on their settlement so that it can be entered as a consent decree enforceable through injunction, contempt or summary judgment, the settlement must be filed and submitted to the court. In such cases, the settlement agreement becomes a presumptively public judicial record, and proceedings leading to its formal approval are subject to a qualified right of public access.

4. A judge should not *sua sponte* suggest to the parties that a settlement might be kept confidential. In a case pending in federal court, however, a judge might appropriately suggest, as an alternative, that the court retain jurisdiction to enforce a settlement.

5. If the terms of a settlement are presented to a judge, the judge may express concern about any term that might arguably be illegal, unethical or unenforceable. However, it may be difficult for a judge to independently "police" the provisions of a settlement in this manner, as there will be no adversarial development of any issue.

Examples

1. The parties to a commercial dispute appear before a judge for a settlement conference. The judge conducts the conference in chambers and engages in *ex parte* discussions with the parties in an attempt to facilitate a settlement. A settlement is reached. The terms of the settlement are not put on the record and the settlement agreement is never filed. The settlement is private and there is no right of public access.

2. The same facts as (1) above, but the settlement is submitted to the court as a stipulation, with a motion that it be adopted by the court as an order. If the judge grants the motion, the judge gives the settlement a public *imprimatur* and the settlement becomes a public record.

3. The same facts as (1) above, but the settlement includes a provision whereby the parties agree to divide their state into districts and not compete with each other in certain districts. The judge cautions the parties of the possible illegality of the settlement and refuses to approve or otherwise facilitate the settlement.

Principle 4 Absent exceptional circumstances, settlements with public entities should not be confidential.

Public entities and officials, whether at the federal, state or local level, are public actors. By definition, their actions affect the public, whom they represent. The public thus possesses a significant interest in the monitoring and oversight of public officials and entities, even in litigation. Public entities are generally subject to open public meeting and/or open public record laws. Such laws, which seek to facilitate public monitoring and government accountability, may require disclosure of settlements involving the government or other public entities. Thus, when a public entity enters into a settlement, no expectation of confidentiality should exist, whether or not the settlement is filed with the court.

For these reasons, there should be a strong presumption against the confidentiality of any settlement entered into with a public entity or of any information otherwise disclosable under a public records law. *See Pansy v. Borough of Stroudsburg*, 23 F.3d 772, 792 (3d Cir. 1994). A particularly strong presumption of public access exists with regard to any monies paid by public entities in settlement. Only exceptional circumstances (such as those involving intimate personal information, the privacy of minors, or law enforcement needs) should warrant the confidentiality of these types of settlements. *See generally* Laurie K. Doré, *Settlement, Secrecy, and Judicial Discretion: South Carolina's New Rules Governing the Sealing of Settlements*, 55 S.C. L. Rev. 791, 809-10 (2004).

Best Practices

1. An attorney representing an individual or entity in litigation against a public agency should, before entering into settlement negotiations with the agency, consult with his or her client to determine whether the client has any proprietary or privacy interest in the terms of the settlement for which protections should be sought under applicable public records law or a court order. Absent any such protection, the attorney should caution his or her client against any expectation of confidentiality

2. An attorney representing a public agency should, in the course of settlement negotiations with an adversary, caution the adversary against expecting any confidentiality of a settlement agreement, absent specific exemptions in the public records laws or a court order

3. In determining whether to seal a settlement of a matter involving a public entity or official, a court should carefully consider relevant federal or state law. On the one hand, judges should be hesitant to seal a settlement if the information would be otherwise disclosable under a federal or state freedom of information or open public records statute. On the other hand, information that would be exempt from disclosure under such a law or separate privacy-related statute might merit a confidentiality order.

Examples

1. A business entity sues a state agency for breach of contract. The action arises out of alleged delay damages incurred by the plaintiff after the defendant agency failed to accept goods on a certain date. The settlement agreed to by the parties includes, at plaintiff's insistence, a confidentiality provision. No legitimate basis for confidentiality exists.

2. An individual sues a state agency for wrongful disclosure of her private medical information. The defendant agency admits that it erred in disclosing the information. The parties enter into a settlement which, at plaintiffs' insistence, seals all facts relevant to the suit, including plaintiffs' medical information. The plaintiffs' information may be sufficiently confidential to justify sealing the settlement or issuing a confidentiality order.

Principle 5 An attorney's professional responsibilities may affect considerations of confidentiality in settlement agreements.

The obligation of an attorney to maintain a client's confidences is fundamental to the attorney-client relationship. An attorney must thus take steps to arrive at a settlement that protects a client's confidential information. Consistent with this obligation, an attorney must take client confidences into account during settlement negotiations and may seek an agreement to limit the voluntary disclosure of confidential information as a condition of settlement.

In all settlement negotiations, however, an attorney should consider and adhere to all applicable standards of professional responsibility. For example, certain nondisclosure provisions may violate ethical rules that prohibit restrictions on another attorney's practice of law. The ethical rules of a jurisdiction may similarly prohibit a settlement that purports to restrict an attorney from using information gained in one case in other related cases. Additionally, a confidential settlement should not prohibit the disclosure of information required by law or court order.

An attorney should also recognize that confidential information may concern public health and safety or may affect specific individuals (such as collateral litigants). Depending upon the ethical rules of a jurisdiction, attorneys may have limited discretion to reveal confidences when death, serious bodily injury or financial harm is imminent. *See Model Rules of Professional Responsibility*, Rule 1.6(b). Little guidance exists, however, concerning the factors that an attorney should consider in deciding to exercise this discretion. *See id.*, Rule 1.6, Comment 6. Moreover, unless otherwise required (*See, e.g.*, 17 C.F.R. 205, "Standards of Professional Conduct for Attorneys Appearing and Practicing Before the [Securities and Exchange] Commission in the Representation of an Issuer"), no mandatory duty to disclose exists.

Best Practices

1. Attorneys should familiarize themselves with applicable ethical rules and substantive law to determine what limitations exist on their negotiating confidential settlements that might include unethical, illegal, or otherwise unenforceable terms.

2. Attorneys should familiarize themselves with applicable ethical rules and substantive law to determine which circumstances may permit disclosure of otherwise confidential information.

3. Regardless of whether ethical rules prohibit a nondisclosure provision or whether an attorney has discretion to disclose a confidence, an attorney should discuss and attempt to resolve any concerns concerning confidentiality with his client.

Example

1. The parties to a products liability action are engaged in settlement negotiations. The product at issue is a widely distributed and well-known kitchen appliance. Through study of the defendant's highly confidential design documents, obtained during discovery under a protective order, the plaintiff learns of the existence of a design defect in the product's control panel that might cause a fire like that in plaintiff's case. Plaintiff's attorney knows of at least four other cases involving fires in the appliance. The defendant insists that it will not settle without a confidentiality agreement.

The attorney confers with his client about the proposed settlement and the defendant's confidentiality demand. The client decides to agree to the settlement and confidentiality demand. Absent an ethical rule or substantive law to the contrary in the jurisdiction, the information would be considered a "client confidence." The attorney may not voluntarily reveal any information covered by the confidentiality clauses of the settlement agreement.

Chapter 4
Selected Bibliography

28 C.F.R. § 50.23 (policy of the United States Department of Justice with regard to confidential settlements)

Eastern District of Michigan, Local Civil Rule 5.4 (placing temporal limit on sealing of settlement agreements)

District of South Carolina, Local Civil Rule 5.03 (establishing procedure for motions to seal and barring sealed settlements).

Poliquin v. Garden Way, Inc., 989 F.2d 527 (1st Cir. 1993) (recognizing court's inherent power to modify confidentiality order even after settlement).

Gambale v. Deutsche Bank, 377 F. 3d 133 (2d Cir. 2004) (recognizing "weak" presumption of access to settlement amount given reliance on confidentiality and lack of public interest concerning amount).

Pansy v. Borough of Stroudsburg, 23 F.3d 772 (3d Cir. 1994) (holding that because settlement agreement between police chief and borough was not filed with, interpreted or enforced by the district court, it was not a judicial record subject to right of access doctrine: "Simply because a court has entered a confidentiality order over documents does not automatically convert those documents into 'judicial records' accessible under the right of access doctrine." However, court allowed newspaper to intervene to challenge propriety of confidentiality order under state Right to Know Act and Federal Rule 26 and required that "good cause" support any confidentiality order).

Zurich American Ins. Co. v. Rite Aid Corp., 345 F.Supp.2d 497 (E.D. Pa. 2004) (vacating an order sealing an arbitration award in corporate governance case, after balancing public policy favoring disclosure against speculative concerns of party favoring secrecy).

Ashcroft v. Conoco, Inc., 218 F.3d 288 (4th Cir. 2000) (addressing impropriety of sealing confidential settlement in environmental tort lawsuit involving contaminated drinking water).

Ford v. City of Huntsville, 242 F.3d 235 (5th Cir. 2001) (vacating confidentiality order concerning settlement between city and employee because trial court failed to consider effect of order on Texas Public Information Act).

Goodyear Tire & Rubber Co. v. Chiles Power Supply, Inc., 332 F.3d 976 (6th Cir. 2003) (creating new federal common law privilege protecting "secrecy of matters discussed ... during settlement negotiations".

Herrnreiter v. Chicago Hous. Auth., 281 F.3d 634 (7th Cir. 2002) (defendant in employment discrimination proceeding gave up claim of confidentiality with respect to settlement agreement when it made the terms of that agreement a subject of litigation by filing a motion to implement the settlement).

Lynch, Inc. v. Samatamson, Inc., 279 F.3d 487 (7th Cir. 2002) ("No one supposes that there is any impropriety in a judge's conducting settlement discussions off the record").

Jessup v. Luther, 277 F.3d 926 (7th Cir. 2002) (reversing district court's denial of newspaper's motion to unseal settlement agreement in Section 1983 action because filed settlement agreement was a judicial record subject to public right of access).

Union Oil Company of California v. Leavell, 220 F.3d 562 (7th Cir. 2000) (finding order sealing virtually all judicial documents in case file unjustified; when the parties "call on the courts, they must accept the openness that goes with subsidized dispute resolution by public (and publicly accountable) officials . . . . only genuine trade secretes, or information within the scope of a requirement such as Fed. R. Crim. P. 6(e)(2) . . . may be held in long-term confidence").

Foltz v. State Farm Mut. Auto. Ins. Co., 331 F.3d 1122 (9th Cir. 2003) (discussing right of collateral litigants to obtain discovery, motions, and judicial records filed under seal in settled case).

Phillips v. General Motors Corp., 307 F.3d 1206 (9th Cir. 2002) (examining right of access in settled product liability case to information produced by manufacturer concerning total number and aggregate dollar amount of settlements in similar fuel-fed fire cases).

Chicago Tribune Co. v. Bridgestone/ Firestone, Inc., 263 F.3d 1304 (11th Cir. 2001) (remanding for Firestone to demonstrate need for confidentiality of discovery filed under seal in settled case).

EEOC v. Nat. Children's Ctr., Inc., 98 F.3d 1406 (D.C. Cir. 1996) (holding that trial court abused its discretion in sealing consent decree in EEOC action and remanding for further explanation of decision to seal portions of the record and determination of good cause to support protective order governing deposition transcripts).

Joseph F. Anderson, Jr., *Hidden from the Public by Order of the Court: The Case Against Government-Enforced Secrecy*, 55 S.C.L. Rev. 711 (2004).

A. F. Blakley, *To Squeal or Not to Squeal: Ethical Obligations of Officers of the Court in Procession of Information of Public Interest*, 34 Cumberland L. Rev. 65 (2003).

Laurie Kratky Doré, *Public Courts v. Private Justice: It's Time to Let Some Sun Shine in on Alternative Dispute Resolution*, 81 Chicago-Kent L. Rev. 463 (2006).

Laurie Kratky Doré, *Settlement, Secrecy, and Judicial Discretion: South Carolina's New Rules Governing the Sealing of Settlements*, 55 S.C.L. Rev. 791 (2004).

Laurie Kratky Doré, *Secrecy By Consent: The Use and Limits of Confidentiality in the Pursuit of Settlement*, 74 Notre Dame L. Rev. 283 (1999).

Robert. Timothy Reagan, et al., *Sealed Settlement Agreements in Federal District Court* (Federal Judicial Center, 2004).

James E. Rooks, Jr., *Settlements and Secrets: Is the Sunshine Chilly?*, 55 S.C.L. Rev. 859 (2004).

A full bibliography, updated periodically, may be found on The Sedona Conference web site at www.thesedonaconference.org starting in July 2007.

Chapter 5. Privacy & Public Access to the Courts in an Electronic World

Introduction

The growing use of electronic filing and imaging technology makes it possible for courts to offer broader public access to case files through remote electronic access. There is increasing awareness, however, of the implications such broad public access to case files, especially through the Internet, has for personal privacy, and proprietary business information. In the United States court community, many have suggested that case files - long presumed to be open for public inspection and copying unless sealed by court order - contain private or sensitive information, trade secrets, and proprietary information that should be protected from unlimited public disclosure and dissemination in the new electronic environment.[8] Others maintain that electronic case files should be treated the same as paper files in terms of public access and that existing court practices are adequate to protect privacy, confidentiality, and intellectual property interests.

Potential Privacy, Confidentiality, and Proprietary Implications of Public Access to Electronic Case Files

Before the advent of electronic case files, the right to "inspect and copy" court files depended on one's physical presence at the courthouse. The inherent difficulty of obtaining and distributing paper case files effectively insulated litigants and third parties from any harm — actual or perceived — which could result from misuse of private or proprietary information provided in connection with a court proceeding. The Supreme Court has referred to this relative difficulty of gathering paper files as "practical obscurity." *See United States Department of Justice v. Reporters Committee for Freedom of the Press*, 489 U.S. 749, 770-71, 780 (1989) (recognizing "the vast difference between the public records that might be found after a diligent search of courthouse files, county archives, and local police stations throughout the country and a computerized summary located in a single clearinghouse of information").

Case files may contain private, sensitive or proprietary information such as medical records, employment records, financial information, tax returns, Social Security numbers and other personal identifying information, as well as customer lists, business plans, research data, and other proprietary business information. Allowing access to case files through the Internet, depending on how it is accomplished, can make such information available easily and almost instantly to anyone who seeks it. Personal, sensitive, or proprietary information, unless sealed or otherwise protected from disclosure, can be downloaded, stored, printed, and distributed.

[8] Congress has expressed this viewpoint in the E-Government Act of 2002, Public Law No. 107-357. Section 205(c)(3) of the Act requires the Supreme Court to prescribe rules "to protect privacy and security concerns relating to electronic filing of documents and the public availability ... of documents filed electronically." Proposed Fed. R. Civ. P. 5.2 has been promulgated in response to this mandate. It should be noted that the E-Government Act and Proposed Fed. R. Civ. P. 5.2 address only issues of personal privacy and do not extend similar rule-based protections to business confidences or proprietary information. Strong concern for the protection of such information was expressed by many members of this Working Group, and this is reflected throughout these Guidelines. However, we acknowledge that there is a special role for rulemaking in the area of personal privacy, as well-developed common law doctrines of business confidentiality and proprietary information are often unknown or unavailable to private citizens.

The information contained in court records, particularly the personal information, is highly valued by data-mining companies that cull public records and integrate public record data with other sources of data and sell the information for profit. Because there are few, if any, legal limitations on how public court records may be used by those who obtain them, data-mining companies are able to freely exploit the information in court records for commercial purposes as marketing information or "competitive intelligence."

These circumstances place into conflict two important policy considerations. First, public court records must easily be available to allow for effective public monitoring of the judicial system; and second, private or sensitive information in court files that is not germane to the public oversight role may require protection from indiscriminate public disclosure.

In different jurisdictions, two primary positions appear to be emerging with respect to the privacy issues relating to electronic case files. The first is sometimes referred to by the shorthand expression, "public is public." This position assumes that the medium in which case files are stored does not affect the presumption that there is a right of public access. By this analysis, current mechanisms for protecting privacy and confidentiality - primarily through protective orders and motions to seal - are adequate even in the new electronic environment. Some have also suggested that the focus for access policies should be on determining whether information should be deemed "public" in any format - electronic or paper - rather than on limiting access to electronic case files.

Advocates of this position suggest that litigants do not have the same expectation of privacy in court records that may apply to other information divulged to the government. The judicial process depends on the disclosure, voluntarily or involuntarily, of all relevant facts, to allow a judge or jury to make informed decisions. In bankruptcy cases, for example, a debtor must disclose a Social Security number or taxpayer identification number and detailed financial information that the bankruptcy trustee needs to administer the case and that creditors need to fully assert their rights. Similarly, in many types of civil cases - for example, those involving personal injuries, criminal allegations, or the right to certain public benefits - case files often must contain sensitive personal information. To a certain extent, then, advocates of this position expect private litigants to abandon a measure of their personal privacy at the courthouse door.

A second position on the privacy issue focuses on the relative obscurity of paper as compared to electronic files. Advocates of this position observe that unrestricted Internet access undoubtedly would compromise privacy and, in some situations, could increase the risk of personal harm to litigants or others whose private information appears in case files. In other cases, proprietary, financial, marketing, or trade secret information must be disclosed. In these cases, advocates for this position urge that the reasons and justification for public assess be balanced against the legitimate needs of corporate litigants to have access to the courts for resolution of disputes without having to forfeit valuable proprietary information to the public and competitors.

The combination of electronic filing and remote access magnifies the potentially dire consequences of mistaken exposure of sensitive information. The accidental disclosure of such information cannot be reversed - mistaken dissemination on the Internet is fundamentally different from an inadvertent disclosure on paper in a courthouse. This reality increases the burden on attorneys and courts to carefully guard against such mistakes. It also has been noted that case files contain information on third parties who often are not able - or not aware how - to protect their personal privacy or to protect valuable proprietary information by seeking to seal or otherwise restrict access to sensitive information filed in litigation.

Advocates of the second position acknowledge that it is difficult to predict how often court files may be used for "improper" purposes in the new electronic environment. They suggest that the key to developing electronic access policies is not the ability to predict the frequency of abuse, but rather the assumption that even a few incidents could cause great personal or competitive harm. Advocates of this position also note that the judicial branch, like other branches of government, has an obligation to protect personal and proprietary information entrusted to it.

They argue that there is a "public interest in privacy" because of the compulsory nature of information disclosure in the context of litigation. That is to say, confidential information often is disclosed in litigation not by choice but by compulsion. On this view, the courts should explicitly recognize, in rules and policies on public access to court records, that although there may not be an expectation of privacy in case file information when there is no protective order, statutory right, or established court procedure that provides such protection, there has been an expectation of practical obscurity that will be eroded through the development of electronic case files. Appropriate limits on electronic access to certain file information may allow the courts to balance these interests in the context of the new electronic environment.

Emerging Themes in the Development of Electronic Access Policy and Procedures

In efforts to analyze the issues of privacy, confidentiality, and access to electronic court records, the courts are engaging in a debate that in many ways mirrors the broader societal debate over privacy in the Internet era. In the policy development process, courts are addressing two related questions. First, what is the appropriate role of the courts in collecting and maintaining public records? Second, have those courts that allow Internet access to case files changed their role from being passive "custodians" of court records to being active "publishers" of information? These key questions have motivated courts at both the federal and state levels to begin the development of new access policies in the context of electronic case files.

In addition, court policy-making committees also have begun to ask whether the reliance on a case-by-case approach to access issues should be reexamined in the context of Internet publication of court records: Is it prudent to rely on litigants as the primary means of protecting privacy and confidentiality in the context of case files? Judges, as a general matter, do not raise privacy or confidentiality issues on their own. Instead, privacy and confidentiality issues that might be asserted in the course of litigation historically have been addressed on a case-by-case basis, so that if a litigant does not challenge the entry of sensitive information into the record, it will be entered without further inquiry.

Many courts appear to be searching for an alternative to the case-by-case approach, crafting restrictions on remote public access to preserve an element of the practical obscurity of paper files while allowing the public to take advantage of rapid advances in technology to provide easier and cheaper ways to monitor the courts and particular cases. This search for an alternative has led several courts to propose or implement new "categorical" restrictions on access, in effect reversing the common law presumption of access either by presumptively sealing certain types of cases or categories of information or by maintaining open access at the courthouse but restricting remote access on the Internet. In the federal courts, for example, the Judicial Conference of the United States has developed a privacy policy that allows unlimited public access to Social Security case files only at the courthouse, but prohibits remote public access over the Internet. Minnesota has proposed a twist on "courthouse only" access, providing remote public access only to documents and information created or maintained by the courts themselves. Under the Minnesota proposal, documents created by litigants would only be accessible from the courthouse. Other new state court rules on public access - such at those from

California, Maryland, and Vermont - carve out limited categories of cases or information for presumptive sealing, adding new categories to existing statutory sealing requirements.

Finally, courts are increasingly focused on "logistics" issues such as data security, the proliferation of electronic documents, and the mechanics of implementing new sealing requirements or access restrictions in the context of electronic case files.

Sedona Working Group Assessment of the Main Approaches to Public Access Rules and the Most Common Rule and Policy Features

Recently-developed rules and policies on public access to court records appear to follow four basic policy approaches. In addition, a preliminary review reveals several issues that each court system seeks to address in developing these rules and policies. Although the Working Group has concluded that it is too soon to identify "best practices" in this area, it is helpful to assess how the new public access rules are consistent – or not – with the principles articulated in these guidelines.

The Four Basic Policy Approaches

1. Open electronic access, with minimal limits.

   Some court systems have developed rules or implemented new public access policies affirming that the existing public access system for paper records will continue to apply to electronic court records. This group, which includes the New York state courts and the U.S. federal courts, draws few distinctions between access to electronic and paper files. As a general matter, these court systems only restrict public access to certain personal identifying information in court records that may be used to facilitate the crime of identity theft, but they allow electronic public access to almost all unsealed court records.

   Under this approach, the litigant has the obligation to protect private or confidential information by seeking to seal court records or by other self-help mechanisms such as redaction or refraining from filing such information unless absolutely necessary.

   This approach, while consistent with the law as it developed before the advent of electronic case filing and potential Internet access to court records, does not take into account the shifting role of courts from "custodians" of records to "publishers," and engages in no examination of its consequences or desirability. With only minimal restrictions on electronic pubic access, this shift in the role of the courts role may not provide adequate protections for private or proprietary information in court records, and may not be necessary to fulfill the courts' role in providing appropriate public access to court records.

2. Generally open electronic access, coupled with more significant limits on remote electronic public access.

   A second group has adopted a middle ground that generally allows remote electronic public access, but at the same time places significant limits on the types of cases — or categories of information — that courts may make available electronically. These courts recognize that there are practical and policy reasons to be cautious about electronic public access, especially in the short-term future during the period of transition from paper to electronic court files. The California and Indiana access rules provide examples of this approach. As with approach #1 above, the obligation to protect personal privacy, confidentiality, or proprietary information will be largely left to individual litigants with little or no independent assistance of the court.

The Working Group views this approach as more balanced than approach #1, but suggests that it may still fall short of providing appropriate protections for private and confidential information in court records. One expects the court to take a more active role, recognizing that public access to court records should be restricted where forfeiture of privacy or proprietary rights would likely result from disclosure.

3. Electronic access only to documents produced by the courts.

A third group of courts permits remote access to documents created by the court, such as dockets and court orders, but does not permit remote access to documents created by the parties. This approach is adopted in the Minnesota and Vermont access rules.

The Working Group notes that while this approach appears to provide significant protections for private and confidential information submitted by the litigants as part of the court record, this approach does not appear to allow the public to conduct sufficient oversight of the courts. In many cases, it is important to review pleadings and other litigant-filed elements of the case file in order to effectively evaluate a court's decision and orders.

4. Systematic reevaluation of the content of the public case file, combined with limited access to electronic files.

A fourth broad policy approach is to systematically review the elements of the public case file with the policy goal of better accommodating personal privacy interests in the context of electronic court records. These courts seek to limit the filing of extraneous personal or confidential information in public court files, a strategy referred to as "minimization." Where such information must be filed, these courts would provide expanded protections before moving forward with electronic public access systems. The Florida court system has issued a report outlining this approach.

The Working Group views this as a promising approach because it focuses on limiting the filing of information that arguably should not be in the public case file, and on sealing or otherwise limiting public access to information that is truly private or confidential, yet also necessary for the adjudication of the dispute.

List of Common Features of Recently-Developed Court Rules and Policies on Public Access to Court Records

The Working Group concludes that, as a general matter, the common features of public access rule outlined below are consistent with the Principles in Chapter 2 on "Pleadings, Court Orders, Substantive Motions, and Dockets," and Chapter 3 on "Trials." As noted in those chapters, it is clear that there are some categories of cases that invariably involve information that should be subject to limited public disclosure. State law often mandates that such categories of cases be closed to the public. In addition, many cases involve personal information, the public disclosure of which may violate recognized privacy rights or expose litigants to identity theft or other abuse. In those cases, exclusion of such information from pleadings – or the redaction of such information as mandated in several court rules – will be necessary to protect litigants' privacy interests while minimally intruding upon the public's qualified right of access to judicial records.

1. A statement of the overall purpose for the rule or policy.

2. Definitions of key terms used in the rule.

3. A procedure to inform litigants, attorneys, and the public that (a) every document in a court case file will be available to anyone upon request, unless sealed or otherwise protected; (b) case files may be posted on the Internet; and (c) the court does not monitor or limit how case files may be used for purposes unrelated to the legal system.

4. A statement affirming the court's inherent authority to protect the interests of litigants and third parties who may be affected by public disclosure of personal, confidential, or proprietary information..

5. A list of the types of court records that are presumptively excluded (sealed) from public access by statute or court rule.

6. A statement affirming that the public right to access court records and the court's authority to protect confidential information should not, as a general matter, vary based on the format in which the record is kept (e.g., in paper versus electronic format), or based on the place where the record is to be accessed (i.e., at the courthouse or by remote access).

7. As an exception to feature 6 above, a list of the types of court records that — although not sealed — will not be available by remote electronic public access.

8. A list of the types of information that either: a) must not be filed in an open court record, or b) if filed, must be redacted or truncated to protect personal privacy interests. These provisions mainly apply to personal identifiers such as the SSN, account numbers, and home addresses of parties.

9. Procedure for a court to collect and maintain sensitive data elements (such as SSN) on special forms (paper or electronic) that will be presumptively unavailable for public access. Such procedures generally build on technology to segregate sensitive information so that public access can be restricted in appropriate situations.

10. Procedure to petition for access to records that have been sealed or otherwise restricted from public access, and a statement of the elements required to overcome the presumption of non-disclosure.

11. Procedure to seal or otherwise restrict public access to records, and a statement of the burden that must be met to overcome the presumption of disclosure.

12. An affirmation that a rule on public access to court records does not alter the Court's obligation to decide, on a case-by-case basis, motions to seal or otherwise restrict public access to court records.

13. Guidance to the courts concerning data elements that are contained in electronic docketing systems that must (or must not) be routinely made available for public access.

14. Guidance for attorneys and/or litigants concerning: (a) the extent to which public case files will be made available electronically; and (b) the need to exercise caution before filing documents and information that contain sensitive private information, which is generally defined elsewhere in the rule.

15. An explanation of the limits, if any, on the availability of "bulk" and/or "compiled" data from public court records. Some rules specify that such data will only be made available to certain entities, for certain defined purposes, and pursuant to agreements to refrain from certain uses of the records obtained.

16. A statement concerning the fees that a court may charge for public access to court records.

Conclusion

Courts have begun to address privacy and confidentiality issues that arise as court files are made accessible on the Internet. The federal courts and a growing number of state court systems have developed policies or court rules to balance the competing interests of public access and personal privacy. These policies and rules recognize that case files may contain sensitive personal, confidential or proprietary information that may require special protection in the context of Internet access. Through changes in rules, court policies - and likely also in case law - it is clear that the law in this area will continue to develop to respond to the fundamentally changed context of public access to court records in the Internet era.

It is also clear that the era of "practical obscurity" has past. Litigants and attorneys must be aware of the possible consequences of filing any private or confidential information.

Chapter 5
Selected Bibliography

Court Rules and Policy Statements

Federal Judicial Conference Privacy Policy, available at http://www.privacy.uscourts.gov/b4amend.htm

United States District Court, District of New Jersey, L. Civ. R. 5.3

California Special Rules for Trial Courts (Rules 2070 to 2077), available at http://www.courtinfo.ca.gov/rules/titlefive/titlefive.pdf

Indiana Administrative Rules (Rule 9), available at http://www.in.gov/judiciary/orders/rule/amendments/2004/0204-admin-rule9.pdf

Supreme Court of Florida, In re: Implementation of Report and Recommendations of the Committee on Privacy and Court Records, Administrative Order No.AOSC06-20, June 30, 2006, available at http://www.floridasupremecourt.org/clerk/adminorders/2006/sc06-20.pdf

Supreme Court of Florida, In Re: Interim Policy in Electronic Release of Court Records, Administrative Order No. AOSC06-21, June 30, 2006, available at http://www.floridasupremecourt.org/clerk/adminorders/2006/sc06-21.pdf

Maryland Rules of Procedure (Ch. 1000 - Access to Court Records), available at http://courts.state.md.us/access/ro-accesstoctrecords.pdf

Minnesota Recommendations of the Minnesota Supreme Court Advisory Committee on Rules of Public Access to Records of the Judicial Branch, available at http://www.courts.state.mn.us/cio/public_notices/accessreport.htm

New York Commission on Public Access to Court Records, Report to the Chief Judge of the State of New York, available at http://www.courts.state.ny.us/ip/publicaccess/index.shtml

Vermont Rules for Public Access to Court Records (and amendments), available at:
http://www.vermontjudiciary.org/rules/proposed/rules_pa.htm
http://www.vermontjudiciary.org/rules/proposed/rules_pamay1.htm
http://www.vermontjudiciary.org/rules/proposed/paAmend6b.htm

Rules Governing Dissemination of Electronic Case Records, available at http://www.vermontjudiciary.org/rules/proposed/ruleselectronic.htm

Cases

United States Supreme Court

U.S. Dept. of Justice v. Reporters Committee for Freedom of the Press, 489 U.S. 749 (1989) (interpreting the FOIA, recognizing a privacy interest in information that is publicly available through other means, but is "practically obscure").

United States District Courts

Holland v. GMAC Mortgage Corp., 2004 WL 1534179 (D. Kan. Jun 30, 2004) (noting that filing documents under seal in court which employs electronic filing will be burdensome because sealed filing must be in paper format).

Eldaghar v. City of N.Y. Dep't of Citywide Admin. Servs., 2004 U.S. Dist. LEXIS 3503 (S.D.N.Y. 2004) (denying motion for protective order, observing there is no protectable privacy interest in personal identifiers that are already available on Internet).

Websites

National Center for State Courts

http://www.courtaccess.org/

Reporters' Committee for Freedom of the Press

http://www.rcfp.org/courtaccess/viewstates.php

A full bibliography, updated periodically, may be found on The Sedona Conference web site at www.thesedonaconference.org starting in July 2007.

Appendix A: The Sedona Conference® Working Group Series & WGS℠ Membership Program

The Sedona Conference® Working Group Series ("WGS℠") represents the evolution of The Sedona Conference® from a forum for advanced dialogue to an open think-tank confronting some of the most challenging issues faced by our legal system today.

Working Groups in the WGS℠ begin with the same high caliber of participants as our regular season conferences. The total, active group, however, is limited to 30-35 instead of 60. Further, in lieu of finished papers being posted on the website in advance of the Conference, thought pieces and other ideas are exchanged ahead of time, and the Working Group meeting becomes the opportunity to create a set of recommendations, guidelines or other position piece designed to be of immediate benefit to the bench and bar, and to move the law forward in a reasoned and just way. Working Group output, when complete, is then put through a peer review process, including where possible critique at one of our regular season conferences, hopefully resulting in authoritative, meaningful and balanced final papers for publication and distribution.

The first Working Group was convened in October 2002, and was dedicated to the development of guidelines for electronic document retention and production. The impact of its first (draft) publication—*The Sedona Principles; Best Practices Recommendations and Principles Addressing Electronic Document Production* (March 2003 version)—was immediate and substantial. *The Principles* was cited in the Advisory Committee on Civil Rules Discovery Subcommittee Report on Electronic Discovery less than a month after the publication of the "public comment" draft, and was cited in a seminal e-discovery decision of the SDNY less than a month after that. As noted in the June 2003 issue of Pike & Fischer's *Digital Discovery and E-Evidence*, "*The Principles*...influence is already becoming evident."

The WGS℠ Membership Program was established to provide a vehicle to allow any interested jurist, attorney, academic or consultant to participate in Working Group activities. Membership provides access to advance drafts of Working Group output with the opportunity for early input, and to a Bulletin Board where reference materials are posted and current news and other matters of interest can be discussed. Members may also indicate their willingness to volunteer for special Project Team assignment, and a Member's Roster is included in Working Group publications. The annual cost of membership is only $295, and includes access to the Member's Only area for one Working Group; additional Working Groups can be joined for $100/Group.

We currently have active Working Groups in the areas of 1) electronic document retention and production; and 2) protective orders, confidentiality, and public access; 3) the role of economics in antitrust; 4) the intersection of the patent and antitrust laws; (5) *Markman* hearings and claim construction in patent litigation; (6) international issues in e-disclosure and privacy; and (7) Sedona Canada—electronic document production in Canada. *See* the "Working Group Series" area of our website for further details on our Working Group Series and the Membership Program.

> "DIALOGUE DESIGNED TO MOVE THE LAW FORWARD IN A REASONED AND JUST WAY."

wgs℠