E-DISCOVERY RISKS, TIPS, AND TECH ADVICE FOR THE NON-TECHY ATTORNEY

By: Atty. William C. Gleisner, III[1]

Introduction

I have long been interested in computer assisted litigation. For many years I was counsel for a major national civil rights organization. I often found myself in litigation against well represented government agencies and large corporations. To complicate matters, I often had cases pending in several different jurisdictions simultaneously and thus had to deal with different rules and practice procedures. To survive, beginning in the early 1990s I began experimenting with new technologies which would give me an edge in prosecuting difficult and complex litigation.

I was a very early Westlaw disciple, and the ability to do electronic research certainly helped level the playing field. Around 1994 or 1995, I discovered Summation litigation support software. This was a marvelous development because it enabled me to manage and Boolean search large numbers of transcripts with relative ease. A short time later I discovered Indata's Trial Director, which gave me the ability to manage exhibits and (when a dinosaur judge from back in the day would allow) to display and work with exhibits in court. I then discovered Image Capture Engineering's Legal Access Ware and

[1] Currently, Mr. Gleisner is a member of the Wisconsin Judicial Council, where he was one of the principal drafters of Wisconsin's new e-discovery rules. For almost ten years he was a Summation Certified Trainer. With Marquette University Law School Professor Jay Grenig, he co-authored a multi-volume treatise in 2005 entitled *eDiscovery & Digital Evidence*, which is updated annually and continues to be the e-discovery flagship of the Thomson Reuters Company. He has provided "of counsel" assistance to law firms in Wisconsin and throughout the United States concerning e-discovery issues. Mr. Gleisner was Chair of the Amicus Curiae Committee of the Wisconsin Association for Justice (formally, the Wisconsin Academy of Trials Lawyers) from 2000 until 2007 and has authored numerous briefs on its behalf in the Wisconsin Court of Appeals and Supreme Court. In 2005, he was the recipient of the Wisconsin Academy of Trial Lawyers' "Robert L. Habush Trial Lawyer of the Year" Award.

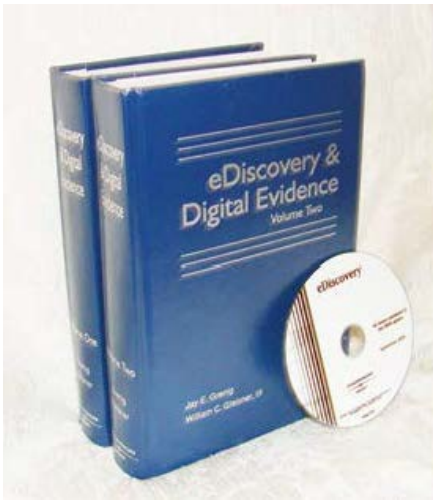
the world of high speed scanning. I bought a couple of large Ricoh scanners and suddenly litigation with large corporations and government agencies became a piece of cake!

In 1998, I became so fascinated with Summation software that I went to the time and trouble of becoming a Summation Certified Trainer. One thing led to another, and I decided to turn my law firm into an early version of a service bureau. I ended up training litigators at a number of large law firms around the country on how to use Summation and helped firms develop e-discovery techniques and strategies.

In 2002, I became co-counsel in some major products liability litigation pending in the U.S. District Court for the Eastern District of Tennessee. The defense counsel played hardball with me and even tried repeatedly to "snow" me with badly indexed and misleading CDs during discovery. I convinced the Judge in that case that the defendant was deliberately hiding evidence. He issued an order granting me the right to travel to the defendant's headquarters where I was permitted (over the strenuous and continuing objection of defense counsel) to search its servers in Detroit. The case settled shortly thereafter and I was completely hooked on e-discovery and electronic litigation.

In 2008, I was appointed to the Wisconsin Judicial Council (which is responsible for advising our Supreme Court concerning the Rules of Evidence and Rules of Civil and Criminal Procedure). On the Council I was appointed to a Committee which was tasked with developing e-discovery rules similar to those which were promulgated by the United States Judicial Conference and became effective in 2006. Together with Marquette University Law School Professor Jay Grenig, Milwaukee County Circuit Judge Sankovitz and then Circuit Court Judge Leineweber we drafted a comprehensive set of e-discovery rules. After more than one year of work and a number of hearings before our Wisconsin

Supreme Court, those rules became effective in 2011. I continue to serve on the Council (now as a representative of the State Bar) where we work constantly to "tweak" and improve those rules.



In 2005, I also had the privilege of co-authoring a treatise with Professor Grenig entitled *eDiscovery & Digital Evidence*, which was published by Thomson Reuters and which has been updated every year since. I am comfortable with the concept of e-discovery and electronic litigation; in fact, having been a litigator for 40 years, I can state with confidence that complex litigation was often mishandled by even the best trial lawyers before the advent of computer assisted litigation. What is sad and more than a little frightening is just how few lawyers have learned how to effectively discover, manage and present electronically stored information (ESI). I have no doubt that large amounts of relevant evidence go unsuspected and undiscovered every day. The failure to pursue ESI by means of e-discovery and to use that evidence in Court will soon become the subject of malpractice claims.

The outline with which I was furnished does not completely cover the topics I will address and so where I deem it necessary I will depart from the published outline. In my seminar presentation I will discuss and demonstrate a number of techniques for effective e-discovery. This White Paper is not intended to replace my seminar presentation or the slides which will accompany it. In particular, I assume that the audiences of the seminar are primarily trial lawyers or litigation support personnel. Accordingly, it is true that

lawyers need to know about e-discovery rules, case law, discovery techniques, ESI management and presentation; however, they should not (and I believe ethically cannot) become forensic experts. Therefore, this presentation will be geared to lawyers.

I. AN OVERVIEW OF E-DISCOVERY PRACTICE TECHNIQUES.

Frankly, on one level e-discovery and electronic litigation is not all that different from other types of litigation. As Judge Sankovitz says, "its old wine in new bottles." You still need to understand the facts of your case, and you need to do the necessary legal research. In my opinion, the differences have a lot to do with how you organize and equip your office and the type of experts you retain. In fact, it is fundamentally wrong to think of electronic litigation as a different practice species. Very rapidly, e-discovery and electronic ligation is becoming a facet of all litigation that is at all complex.

In this white paper I will summarize some of the more important rules and case law. I will also discuss how you should organize and equip your office. During my presentation at the seminar, I will provide demonstrations of how to actually conduct e- discovery, manage ESI and bring it to bear in Court.

It is important to bear in mind that the variety of tools and types of ESI are growing like mushrooms. You can't possibly become familiar with all of them, and you can't possibly learn all of the intricacies of each new or different ESI mutation. You need to develop a system and a methodology and know which experts to bring in to assist you.

A. The computer forensics toolkit.

I do not like this heading. Lawyers don't have "forensic toolkits." They have litigation toolkits that are geared to the e-discovery needs of their firm. If you are serious

about doing e-discovery (and you had better be serious because e-discovery can quickly become very costly), your office must be equipped with certain "tools" or software or you will do a disservice to yourself and your clients. As the lawyer, you will need to understand how the various tools work and what they can accomplish. You will also need to employ staff that can operate those tools effectively and competently. And there are definitely things which you cannot do in your office, and so you will need to retain competent service bureaus and forensic experts when necessary.

There are many choices for what you may put in your "toolkit" and I will discuss some of the other choices you may select below in Section F of this white paper. However, here I am going to describe what I use and how I use it. The "sine qua non" of effective litigation is effective discovery. So, let's start with the most important partner you can have when seeking e-discovery, your forensic expert.

i. The Forensic Expert

I use Digital Intelligence in New Berlin, Wisconsin.[2] I know that there are other companies, but I have come to trust Digital Intelligence. They provide everything; forensic software, hardware, training and court savvy experts. According to their web page:

> Whether the need is to obtain records from a litigation opponent or respond to a request for documents, Digital Intelligence can provide assistance in identifying, preserving and analyzing electronic evidence to avoid the pitfalls of spoliation unique to this type of evidence. Digital Intelligence focuses efforts on uncovering valuable electronic data and maintaining the integrity of this evidence. Digital Intelligence understands the pervasive nature of electronic documents and can assist with all aspects of electronic evidence management,

[2] http://www.digitalintelligence.com. 17165 W. Glendale Drive, New Berlin, WI 53151 866-DIGINTEL (866-344-4683).

> from consulting and data gathering to examination and production. Our expert staff can also help prepare or respond to electronic evidence discovery requests.

This is definitely what you need, but of course the cost is substantial. But to emphasize again; effective e-discovery can be very costly. One way around the cost is to learn how to plan, prepare and execute e-discovery requests and not rely on your forensic expert to do so. In many cases, you will receive responses which will allow you to narrow or eliminate the need for a forensic expert. Such an expert becomes indispensable if you are confronted with someone who is hiding evidence or is resisting the production of relevant evidence (such as emails, for example). I will discuss the capabilities of Digital Intelligence at greater length during my seminar presentation, but what you really need to know is their capabilities and that can be learned from their webpage.

ii. Managing ESI.

As you might imagine, I use Summation to manage, organize and search ESI (although I often do this in tandem with Trial Director, as discussed in the next section). Summation is now part of Access Data,[3] and itself provides a great many services similar to Digital Intelligence.

Summation has become a very sophisticated product and retails for approximately $1700 if you purchase a single user license for Summation Express. You will also need a work station with 4 gigabytes of ram to download the full Summation Express system. However, as part of Summation Express you can download just Iblaze, which requires only 1 gigabyte of ram and can perform a number of the functions you will require. See the data sheet which is attached to this white paper as Appendix A.

[3] http://www.accessdata.com/products/ediscovery-litigation-support/summation.

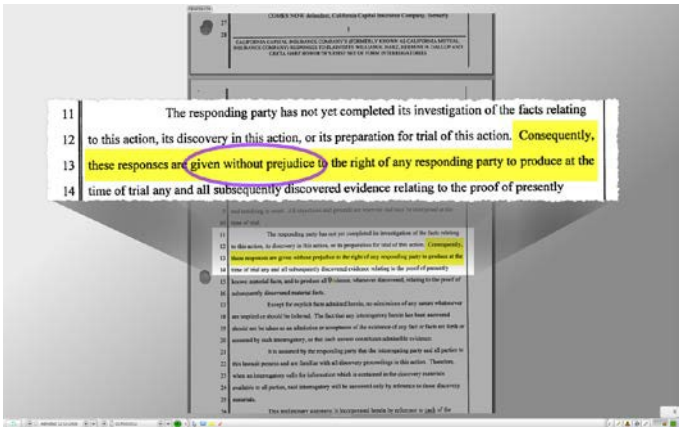
I will demonstrate Summation during the seminar, but here are just some of the very powerful ESI management tools that are available.

1. You can use the program to "log onto" a properly equipped court reporter's steno and have a real time feed of a deposition in progress.
2. You can load a large number of transcripts into the program and conduct sophisticated Boolean searches of those transcripts.
3. You can load evidence into the program (although for this you will need the 8 gigabyte Summation Express) and then create hyperlinks the transcript so that you can call up a reference exhibit while in a transcript.
4. You can conduct Boolean searches across evidence folders and transcripts.
5. You can link up transcripts and videotapes of transcripts (although again for this you will need the 8 gigabyte Summation Express) so that you can word search the transcripts and have a scrolling transcript as a video unfolds.
6. There are strong redaction tools and "production set" tools (including bate stamp tools) that will enable you to prepare appropriate discovery productions.
7. You can view many "e-doc" productions without having to acquire the native software (thus expediting document review).
8. With Summation Express, you can upload case material into secure cloud locations to share with co-counsel or experts.

iii. Exhibit Organization and Courtroom Presentations.

I use Indata Corporation's Trial Director[4] for exhibit organization and courtroom presentations. Admittedly, some of the functions of Summation and Trial Director overlap, but with Trial Director I can prepare trial books which contain thumb nails (or full copies) of exhibits. The program will add bar codes to the thumbnails or images when printed out and I can then use a bar code gun to call up exhibits once the Court orders the exhibits published.

Once the exhibits have been called up, I can use the program to do sophisticated zooms (see at right) and add or remove layers to an exhibit (such as an engineering drawing). It is easy to load images of evidence into Trial Director and it is very easy to manage the evidence once it is loaded. All my scanned evidence is loaded into this program. In my opinion, Trial Director is the perfect complement to Summation. If the seminar system permits, I will demonstrate this during the seminar.



iv. The Service Bureau

In addition to the forensic expert, you will need someone to scan in evidence and code it once it has been converted to ESI. This is not the job of the forensic expert. You could do this at your office but when the case is large enough this may well be an unworkable solution. Service bureaus are often local (in our area they are associated with

[4] http://www.indatacorp.com/TrialDirector.html. A license costs around $600.

the larger court reporter companies) but for the big jobs I would use a national organization. My preference is the company that makes Trial Director, namely the Indata Corporation. According to the Indata website:

> **Document Scanning:** InData can convert your exhibits into vastly more convenient electronic files, such as TIF or PDF images. You may also choose to use OCR (Optical Character Recognition) technology to read and extract the words within the documents. After the scanning process, our image technicians will review each image to verify the image quality, correct rotation setting, and page naming. **Document Coding:** Build a strong discovery database with coding services to catalog your scanned case documents. InData's operators search through documents and identify information based on your specific criteria. Coded information is then verified and checked for conformity and spelling. The coded documents can be imported into all litigation database software, enabling fast, efficient review by your litigation team.

v. Scanning and Advanced Management Software.

Scanners with automatic document feeders (ADF) were once hard to purchase, but no longer. What you need is software that will work well with a ADF and that is Adobe Acrobat 10.0 or higher. This is relatively inexpensive software (around $300) but it is truly miracle software. It will not only scan in your evidence, it will automatically OCR text (which means that it converts it into searchable text).

This software will also load “conversion” files into your Word and Excel programs and your web browser. Thus, it will be possible to do direct conversions of Word, Excel and web documents into a pdf format. Since a pdf is really just a photo of a file, the formatting of the original document is retained and it can easily be searched just like the original Word or Excel file. In fact, many Court e-filing systems require pdf filings and Adobe Acrobat 10.0 will handle such conversions with ease. There are a

number of other things that you can do with this software. For example, some courts require the filing of electronic briefs on CD or DVD. With this software you can create a completely hyperlinked brief which will enable a reader to call up a case or a video. You can also use the latest iteration of this software (Acrobat 11) to convert PDFs to Word and Excel.

B. Choosing to use e-discovery vendors.

Parties often are forced to litigate on a limited budget, and thus are tempted to forego technical assistance unless it is absolutely necessary. This means that many times focus is placed on the experts needed for trial, and parties assume they can amass enough evidence during discovery to provide those experts the information they require.

Many discovering parties do not think they require expert assistance at the discovery stage of litigation; however, when it comes to digital discovery this can be a very costly mistake. Counsel should consider what a forensic computer expert can accomplish by visiting Websites of forensic computer experts. If a party suspects the existence of significant relevant digital evidence, the party simply cannot afford to forego the assistance of a forensic computer expert during discovery. Investing in an expert will pay dividends when the defendant starts to resist production.

The expert can participate in meetings with the defendant's information technology staff, write memoranda to educate the court about technology issues, and testify at hearings on the need for digital data. Retaining this expert can save you hours that you would otherwise spend in depositions and preparation to understand the technology and where to find the data. A simple Internet search can find many companies that offer e-discovery consulting services. You have my recommendations who I have used and

why; quite frankly, beyond that I don't think it is my place to steer you to vendors with whom I am unfamiliar.

C. File systems, types and sources of Relevant ESI sources and repositories.

The sources of digital evidence are literally exploding. Take just the case of corporate infrastructures. From the perspective of lawyers, any discussion of digital data today has to begin with a recognition that "[t]he Internet as we now know it embodies a key underlying technical idea, namely that of open architecture networking." The network operating system (NOS) has greatly evolved from the early 1980s, but all modern NOSs take advantage of the open architecture of the Internet in a variety of ways. Regardless of how they are deployed (to support a LAN[5] or a WAN[6]), or the nature of their architecture, the modern NOS is designed so that it is capable of interconnecting with the Internet:

- To augment the power of the NOS
- To make use of the Internet for supplemental connectivity between linked computers
- To transfer data to remote users or locations.

And that is just the veritable tip of the ice berg. Add to that mobile devices, automobile computers, and a host of other digital devices which are developing, and you can understand why Bill Gates says that life and business are taking place at "the speed of thought."

[5] Local area network.

[6] A "WAN" is a Wide Area Network. There are many definitions of what constitutes a WAN, but the main characteristic is that they are designed to interconnect a large number of computers that may be separated by a few miles or a few thousand miles. More will be said about this concept later in this chapter.

In terms of complex litigation, the computer networks of large organizations, particularly international organizations, cannot be understood without taking into account the potential interaction of the modern NOS with and reliance on the Internet. In fact, the study of the modern NOS is really the study of how the lessons of the Internet have been incorporated into the management, transfer and preservation of data within the modern organization. The point of just this brief discussion is this: How can you possible conduct effective e-discovery if you don't thoroughly understand the computer system that the adversary is using? That is why I am such a strong proponent of conducting all e-discovery in two stages, as discussed below in Section G of this white paper.

D. Recovering, Archiving and Preserving ESI.

Quite simply, proper discovery methodology (Section G below) and the proper use of programs like Summation, Trial Director and Adobe Acrobat (Section IA above) will cover the issues raised in this section. I will amplify on this during the seminar.

E. Common e-discovery mistakes by attorneys.

A friend of mine once said "I don't have any interest in technical matters, like computers. After all, that's why I went to law school." Well, law schools should be changing to better prepare lawyers for the world of ESI (and they aren't); but that is a whole different topic. The fact of the matter is that lawyers who fail to take the time to properly equip themselves for e-discovery and electronic litigation have no business litigating complex litigation. Take for example the *Danis* case.

In *Danis v. USN Communications, Inc.*, 2000 WL 1694325 (N.D. Ill. 2000), counsel on both sides failed to understand the architecture and functionality of a NOS. In

Danis, the plaintiff filed a motion for sanctions, claiming that USN employees, acting at the direction or under the supervision of the individual defendants, "destroyed virtually all evidence of the massive fraud alleged in the plaintiff's complaint."[7] In ruling on the motion, the court observed:

> Sorting out what happened here has been a challenging task not only due the complexity of some of the issues presented, but—regrettably—due to the assertions of counsel that often have confused than clarified the issues. On a number of occasions, plaintiffs have asserted that certain documents were not produced when in fact it later turned out that the documents long ago had been produced. Conversely, defendants have on occasion informed the Court that they have produced certain documents, when in fact it turned out that they had not. Moreover, throughout these proceedings, the submissions by the lawyers too often have offered overblown rhetoric rather than accurate information and careful reasoning.[8]

In the court's opinion, one of the reasons for this confusion was that "neither side to this motion has demonstrated to this Court a complete mastery of what types of documents were generated by USN in the ordinary course of business, how they were used, or their significance."[9] In its opinion, the court described the various servers used by defendant USN and summarized how they worked:

> First, there was a UNIX server that contained a number of databases which could be accessed through different software application [sic]. . . . USN maintained NT servers. These servers were used by USN for e-mail, desk top computers, and local area networks. Through these systems, USN employees could generate correspondence and other original documents. In addition, information contained in the databases on the UNIX system could be accessed through the desk top computers on the NT servers, but when accessed and/or copied electronically, the information also would remain stored in the UNIX database. Charles Struble was the person with overall responsibility for all computer systems at USN.

[7] 2000 WL 1694325, at *2.
[8] Id. at *4.
[9] Id. at *2.

> Mr. Struble delegated direct responsibility for the two sides of the USN computer systems to two different people: Christopher Urban was responsible for the NT servers and desk tops and David Rohrman was responsible for the UNIX servers.[10]

A major part of the difficulties in *Danis* stemmed from the failure of counsel for both parties to understand the architecture of the corporate computer system. As a result, the plaintiffs did not pursue discovery intelligently, and the defense did not appropriately produce relevant documents. No one appears to have grasped that a large amount of missing relevant data might have been transferred to an FTP[11] server and downloaded to a UNIX server, or that a backup tape of the latter might still exist.[12] Recognizing this, the court criticized the failure of both plaintiff and defense counsel to learn the architecture and scope of defendant USN's NOSs:

> What emerges from this thicket concerning the [relevant] documents is that even as of the hearing, neither the plaintiffs nor defendants have full command over what documents they possessed. Perhaps the most apt comment is the one made by plaintiffs' counsel at the close of the hearing, in which he stated that the understanding of the documents "was very much a learning process" that continued even through the time of the hearing. It appears to have been a learning process for both sides. That learning process has been protracted and rendered more difficult—and costly—by the fact that the parties have failed to use the [computer] tools available to get a handle on what documents exist.[13]

Danis is unusual in that a Court has taken the time to address with great specify the consequences of failing to understand the architecture of NOSs and how that can seriously complicate the discovery and perseveration of digital evidence. But the failure to understand the architecture and operating parameters of an adversary's computer

---

[10] Id. at **10-11.
[11] See Jang, Mastering Red Hat Linux 9, p. 757 (SYBEX 2003) ("The File Transfer Protocol (FTP) is one of the oldest members of the TCP/IP protocol stack, yet it is still in common use today. As the name suggests, it is optimized for transferring files. While you can also download a file through an alternative protocol (such as HTTP) or an encrypted service (such as SFTP), FTP is faster.").
[12] Danis v. USN Communications, Id. at *11.
[13] Id. at *24.

system can doom even the most diligent and careful e-discovery effort; and often does. The first step in any serious effort at e-discovery is to understand where the ESI lives.

F. How to Conduct e-Discovery on a Tight Budget.

The short answer is; it can't be done. There is no way to avoid the expenditure of significant funds if you are going to pursue e-discovery and, in complex litigation, you will need to pursue e-discovery. However, there are economies that can be enforced. The Manual for Complex Litigation (Fourth Edition) suggests several ways to save time and money when discovery digital information is involved:

- *Phased or sequenced discovery of computerized data.…* Sections 11.41 and 11.422 [of the Manual] have discussed phasing discovery by issue. Computerized data, however, are often not accessible by date, author, addressee, or subject matter without costly review and indexing. Therefore, it may be appropriate for the court to phase or sequence discovery of computerized data by accessibility. At the outset, allowing discovery of relevant, nonprivileged data available to the respondent in the routine course of business is appropriate and should be treated as a conventional document request. If the requesting party requests more computerized data, consider additional sources in ascending order of cost and burden to the responding party, e.g., metadata or system data, archived data, backup data, and legacy data. The judge should encourage the parties to agree to phased discovery of computerized data as part of the discovery plan. But with or without a prior agreement, the judge may engage in benefit-and-burden analysis under Rule 26(b)(2)(iii) at each stage and enter an appropriate order under Rule 26(c), which may include cost sharing between the parties or cost shifting to the requesting party. See section 11.433.

- *Computerized data produced in agreed-on formats.* Information subject to discovery increasingly exists in digital or computer-readable form. The judge should encourage counsel to produce requested data in formats and on media that reduce transport and conversion costs, maximize the ability of all parties to organize and analyze the data during pretrial preparation, and ensure usability at trial. Wholesale conversion of computerized data to paper form for production, only to be reconverted into computerized data by the receiving party, is costly and wasteful. Particularly in multiparty cases, data production on CD-ROM or by Internet-based data transfer can increase efficiency. Section

11.444 discusses "virtual" document depositories.

- *Sampling of computer data.* Parties may have vast collections of computerized data, such as stored E-mail messages or backup files containing routine business information kept for disaster recovery purposes. Unlike collections of paper documents, these data are not normally organized for retrieval by date, author, addressee, or subject matter, and may be very costly and time-consuming to investigate thoroughly. Under such circumstances, judges have ordered that random samples of data storage media be restored and analyzed to determine if further discovery is warranted under the benefit versus burden considerations of Rule 26(b)(2)(iii).[14]

G. Successful e-Discovery Presupposes the Existence of a Solid e-Discovery Plan.

More than any other litigational exercise, e-discovery will only work if you have a sound discovery plan. The following is one version of a plan that I have employed some cases (how one proceeds will depend on the facts of each case).

- Preserve evidence existing on any Website by downloading its contents to Adobe Acrobat or, if that is impractical, with the assistance of a forensic expert before the lawsuit is commenced.

- Send out a letter before or immediately after a lawsuit is commenced demanding that all digital evidence be segregated and preserved. If there is reason to believe that will not be done, seek a protective order.

- Early in a lawsuit, serve interrogatories that seek only information about the other party's computer systems. These interrogatories should seek to carefully define possible sources of digital evidence and inquire whether those sources exist on a computer system and where they are stored. Also inquire as to what software programs and operating systems are being used by the party (including all of the technical specifications), and get the user and administrator manuals used in connection with all relevant software and operating systems that is not available commercially.[15]

[14] Manual for Complex Litigation (Fourth) § 11.423 (footnotes omitted).

[15] See Unnamed Physician v. Board of Trustees, 93 Cal.App.4th 607, 113 Cal.Rptr.2d 309 (2001) (in physician review hearing, hospital ordered to provide physician with all existing documents related to hospital's computer programs, except those of proprietary nature).

- Learn who does the computer work for a party (e.g., its Management Information System or Information System officers) by use of interrogatories or through a FRCP 30(b)(6) deposition.[16] After discovering who did or does the computer work for a party, depose those individuals. If possible, use these people to start to assemble a map of the computing infrastructure (servers, operating systems, databases, web servers, applications. If custom software is relevant, it may be useful to identify the persons (e.g., employees or consultants) who created it and may have knowledge of data sources, flows, storage and replicas.

- Only after you know the adversary's computer system, serve a second set of interrogatories that seeks disclosure of facts and evidence, and include in that set a separate section that specifically seeks disclosure of relevant digital evidence. When seeking digital discovery, ask that any evidence that exists in digital format be provided just as it exists in the computer systems of the defendant. This may occasion a number of battles, relating to format, metadata, privilege**,** convenience and cost. It is best to insist on evidence that exists digitally be provided in the native digital format if at all possible. Never accept hardcopies, PDFs[17] or TIFFs[18] of the evidence.

- Review all evidence received, in hardcopy or in digital format, promptly so that follow up requests for a native format production can be made if necessary. Use backup copies since you have the originals provided by respondent safely locked away (obviously, this is where a forensic expert will become very useful).

- If the case is important enough, do not settle for email productions in hardcopy or PDF format. Seek to get the "metadata"[19] associated with email productions. If you don't have the email program that was used

---

[16] See Fed.R.Civ.P. 30(b)(6). See generally, Grenig & Kinsler, Handbook of Federal Civil Discovery and Disclosure 2d §§ 5.20-5.24.

[17] PDF, short for portable document format, was developed by Adobe Systems Inc. as a unique format to be viewed through Acrobat viewers. A PDF file (created on one computer) can be viewed with an Acrobat viewer on most other computers and on other platforms. A page layout can be created on a Macintosh computer and converted to a PDF file. After the conversion, this PDF document can be viewed on a UNIX or a Windows machine.

[18] TIFF files are similar to PDF files, but they lack the sophistication of PDFs. TIFF is a less versatile format than PDF, requiring special software in order to be properly viewed and manipulated. On the other hand, a great deal can be done to modify and secure PDF files using relatively inexpensive Adobe Acrobat publishing software, to successfully work with TIFF files one often must resort to specialized and fairly expensive software, such as Summation litigation software. Adobe Acrobat publishing software can convert TIFF files into PDF files.

[19] Metadata is a term of art that means "data about data." It is hidden data that can be seen only when a digital document is viewed in its native format. Often, when a document is created by a particular program (such as Word), there is metadata about the document that can be viewed only if the data is opened by that program. For example, email may be stored in directories that can be accessed only by Microsoft Outlook or Outlook Express. When the hard copy of email comes from Outlook or Outlook Express, substantial metadata is missing, including header information concerning blind copies of documents, date stamps, and routing information.

to send and receive the discovered email, and, if it is not available commercially, make a demand for a copy of the software. Minimally, get the data exported with the mail headers intact. If there are large amounts of email or archived data, you will definitely need to involve a forensic expert.

- Once digital discovery is obtained, organize and manage it in order to easily search and retrieve information. Programs such as Concordance, Summation or Trial Director can be used to accomplish this task.

- If a credible demonstration can be made that crucial digital evidence is being withheld, sanctions may be sought. The federal courts have relatively extensive experience with sanctions for failures to allow digital discovery.

- If there is reason to believe significant digital evidence exists that is being withheld from, and as they say "the game is worth the candle," then consider retaining the services of a forensic computer expert to assist in "mining" for that evidence. Such a move is expensive, and should only be considered if there is a reasonable belief that evidence is being buried.

- If the case is big enough, seek onsite inspection of a defendant's computer system and, possibly, the appointment of a special master or court-appointed expert witnesses who can independently inspect the responding party's system. Some federal courts have set up procedures for making such inspections that can be adapted for other cases.[20]

H. Useful Websites.

Following this Paper, in Appendix B, the reader will find an article from the February 2011 *Wisconsin Lawyer* which I co-authored with Milwaukee County Judge Richard Sankovitz and Marquette Law Professor Jay Grenig entitled Panning for Gold: Social Networking's Impact on E-Discovery. This article contains references to techniques and web sites which the reader may find helpful in pursuing e-discovery contained in or associated with social networking sites (SNS). It also discusses and explains the "Wayback Machine," which may well be the most useful web tool available

[20] See, e.g., Playboy Enterprises, Inc. v. Welles, Inc., 60 F.Supp.2d 1050, 1055 (S.D.Cal.1999).

for Internet based e-discovery searches today. It is amazing how you can use this tool to visit websites which were taken down years ago.

There are a number of very useful web sites available to assist with e-discovery searches. However, one which I find especially useful is www.applieddiscovery.com/. If you are conducting e-discovery, it is worth the price of admission. Even if you have only a casual interest in e-discovery, just visiting the site will help orient you to available resources and authority. It has an excellent monthly e-newsletter which will help keep you up to date on new developments. According to its web page:

> Founded in 1998, **Applied Discovery** is a global leader in the delivery and management of electronic discovery services and support. Applied Discovery leverages an extensive portfolio of resources, relationships, and research to help clients solve today's and tomorrow's discovery challenges. Applied Discovery delivers multinational collection, analytics, processing, review and production services for law firms, corporations, and government entities engaged in audits, investigations, and litigation. Additionally, Applied Discovery is an active participant in key industry leadership groups to include the Electronic Discovery Reference Model, the E-Disclosure Information Project, the Sedona Conference, and the Text Retrieval Conference. Applied Discovery is also both US-EU and US-Swiss Safe Harbor Certified (U.S. Department of Commerce).

You can actually use the Applied Discovery site to find a forensic expert. While there are other sites, some of which I will discuss during my presentation, I recommend that you also visit Legal Tech, http://legaltechdirectory.com/ and Legal Technology News, http://www.law.com/jsp/lawtechnologynews/index.jsp.

II. DEPOSITIONS AND COURT PRESENTATIONS.

If you are going to pursue e-discovery you will have to do more than merely issue thoughtful interrogatories and pursue sanctions if they do not provide the necessary

information. You will also have to conduct depositions of witnesses who manage an adversary's computer system. In this regard, you will need to become familiar with FRCP 30(b)(6) depositions, or your state's equivalent.

A. Examining witnesses concerning e-discovery.

Often, you will not know who in an adversary public or private corporation is responsible for the management of digital assets. Even after interrogatory answers are furnished and requests to produce have been honored, it will still be hard to determine who knows where the "goods" are buried. That's where FRCP 30(b)(6) comes in, which provides:

> 6) *Notice or Subpoena Directed to an Organization.* In its notice or subpoena, a party may name as the deponent a public or private corporation, a partnership, an association, a governmental agency, or other entity and must describe with reasonable particularity the matters for examination. The named organization must then designate one or more officers, directors, or managing agents, or designate other persons who consent to testify on its behalf; and it may set out the matters on which each person designated will testify. A subpoena must advise a nonparty organization of its duty to make this designation. The persons designated must testify about information known or reasonably available to the organization. This paragraph (6) does not preclude a deposition by any other procedure allowed by these rules.

This is a very important tool and you should use it to uncover as much relevant information as you can about an adversary's computer system. Of course, you only need to use this once or twice in each lawsuit because interrogatories regarding an adversary's computer system (which should precede such a deposition) and a 30(b)(6) deposition will undoubtedly lead the identity of other deponents. Here's what professor Grenig and I have to say about such depositions in *eDiscovery & Digital Intelligence,* at pp. 176-177:

> Witnesses who agree to be designated as organization representatives must be adequately prepared to respond to questions concerning topics outlined

in the deposition notice.[21] Such preparation is necessary because the individuals so deposed are required to testify to the knowledge of the corporation, not the individual.[22] Questions asked the witness may include:[23]

- Number, types, and locations of computers currently used and no longer in use.
- Operating systems and application software the responding party is using, including the dates of use.
- File-naming and location-saving conventions of the responding party.
- Disk- or tape-labeling conventions.
- Backup and archival disk or tape inventories or schedules.
- Likely locations of digital records relevant to the subject matter of the case.
- Backup rotation schedules and archiving procedures, including any backup programs in use at any relevant time.
- Digital records management policies and procedures.
- Policies regarding use of computers and data.
- Identities of all current and former employees and consultants who have or had access to network administration, backup, archiving, or other system operations during the relevant period.
- Where and how data is stored.
- Whether the witness or employees use a home computer for work.
- Whether personal digital assistants are used and how.
- Whether the witness' assistants edit or store digital information.

[21] Calzaturficio S.C.A.R.P.A. s.p.a. v. Fabiano Shoe Co., 201 F.R.D. 33, 37 (D.Mass.2001); Prokosh v. Catalina Lighting, Inc., 193 F.R.D. 633, 639 (D.Minn.2000); Bank of New York v. Meridien BIAO Bank Tanzania, Ltd., 171 F.R.D. 135, 151 (S.D.N.Y.1997).

[22] Calzaturficio S.C.A.R.P.A. s.p.a. v. Fabiano Shoe Co., 201 F.R.D. 33, 37 (D.Mass.2001); Prokosh v. Catalina Lighting, Inc., 193 F.R.D. 633, 639 (D.Minn.2000); Poole ex rel. Elliott v. Textron, Inc., 192 F.R.D. 494, 504 (D.Md.2000).

[23] Nimsger, Digging for E-Data, Trial, Jan. 2003, at 56, 57; Krause & Coggio, Electronic Discovery: Where We Are, and Where We're Headed, J.Proprietary Rts., Mar.2004, at 16, 19.

B. Presenting your e-discovery data.

I have already told you how I present evidence in Court. But there are some other organizational tips with which I wish to furnish you. First, never assume that the Court will be comfortable with your plans concerning how you will use your electronic evidence. You should raise your probable use in the final pretrial. You should also inspect the Courtroom with the person or persons who will assist you and determine just how you will "choreograph" your presentations.

Second, you should prepare a "war room" near the courthouse for the purposes of organizing your evidence and reviewing developments which occur on a daily basis. I think Indata has excellent resources and personnel for creation and management of a war room, and I encourage you to visit their web site.

III. THE LAW.

Obviously I am a Wisconsin practitioner, but our e-discovery rules closely track the federal rules. But I feel that you are owed some insight into the law which has been growing up around the "brave new world" of e-discovery and electronic litigation So, for the sake of completeness, I am setting forth below the new Wisconsin rules along with some pertinent commentary which I have drafted that will help explain the purpose of each rule (where the Judicial Council commentary is lacking or thin) and which provides citations to and discussion of some of the relevant federal authority which has influenced the adoption of each rule for the benefit of the reader.

Wisconsin's New E-Discovery Rules

RULE I.

802.10(3)(jm): The need for discovery of electronically stored information.

COMMENTARY

This amendment adds another issue which the court and parties may wish to include in the scheduling order pursuant to Wis. Stat. §802.10(3). In effect, this section acts as a "consciousness-raising" device which is intended to focus the court and the parties on the need to address issues related to electronically stored information ("ESI") early in the litigation process. The Judicial Council Note following this section also suggests that a court confronted with ESI may wish to consider the appointment of a "referee" under Wis. Stat. §805.06 to help sort out complex or technical issues regarding ESI. While the use of a referee may prove beneficial to the court and parties, if their appointment becomes common place when dealing with issues involving ESI it may become necessary to consider an amendment to the rule governing referees because right now §805.06(2) specifies that the appointment of a referee "shall be the exception and not the rule." Based on the federal experience with special masters, referees may prove especially useful in smaller counties where ESI is not encountered often and where judicial resources are scarce. However, a skilled and technically knowledgeable referee may prove invaluable in any case involving large amounts of ESI and competing computer forensic experts because a referee will enable the court to access a neutral technical adviser to help decide complex issues.

In cases where a court decides a referee may be inappropriate or unnecessary, Wisconsin judges can exercise their authority under Wis. Stat. §907.06 to employ the services of a court-appointed computer expert at the expense of the parties to either assist the court in reviewing and ruling on highly technical issues or to facilitate the e-discovery process. Two cases which demonstrate how a court-appointed expert would work in

practice in a case involving e-discovery are *Playboy Enterprises, Inc. v. Welles,* 60 F. Supp. 2d 1050 (S.D. Cal. 1999) and *Simon Property Group, L.P. v. mySimon, Inc.,* 194 F.R.D. 639 (S.D. Ind. 2000).

RULE II.

804.01(2)(e) Specific limitations on discovery of electronically stored information.

1. No party may serve a request to produce or inspect under s. 804.09 seeking the discovery of electronically stored information, or respond to an interrogatory under s. 804.08 (3) by producing electronically stored information, until after the parties confer regarding all of the following, unless excused by the court:

a. The subjects on which discovery of electronically stored information may be needed, when such discovery should be completed, and whether discovery of electronically stored information shall be conducted in phases or be limited to particular issues.

b. Preservation of electronically stored information pending discovery.

c. The form or forms in which electronically stored information shall be produced.

d. The method for asserting or preserving claims of privilege or of protection of trial-preparation materials, and to what extent, if any, the claims may be asserted after production of electronically stored information.

e. The cost of proposed discovery of electronically stored information and the extent to which such discovery shall be limited, if at all, under sub. (3) (a)

COMMENTARY

This Rule, created by Supreme Court Order 09-01A (November 10, 2010), occasioned a great deal of debate during the consideration of the e-discovery rules. It was finally adopted on a split vote with a strong dissent by Justice Bradley and the Chief Justice. Justice Bradley made a number of points in her Dissent which are in part set forth below:

ANN WALSH BRADLEY, J. *(dissenting).*

> I fear that the majority is using a sledgehammer to crack a nut. The problems with electronic discovery in our state's courts are few. Nevertheless, the majority responds with a statewide mandate that is all-encompassing and immediate. Because I am concerned that this unnecessary new mandate has the potential to diminish both fairness and efficiency along with the potential of increasing the time and expense of litigation, I respectfully dissent… In moving immediately rather than cautiously majority fails to heed its own advice. … This court advised the Judicial Council that the Wisconsin rules should follow the federal rules of civil procedure, where appropriate, and benefit from the federal experience. Realizing the need to monitor the consequences of the new federal electronic discovery rules, the Seventh Circuit Court of Appeals moved cautiously. … Rather than enhancing fairness and increasing efficiency, I believe that a mandatory confer rule has the potential to diminish both. … Unlike the majority, I would follow the initial recommendation of the Judicial Council committee and make a meet and confer discretionary. Also, unlike the majority, I would follow the lead of the Seventh Circuit and cautiously continue to test how this newly mandated procedure is working. Accordingly, I urge judges, lawyers and litigants from around the state to monitor this new mandate, and if it is not working, petition the court for change.

RULE III.

804.08(3) OPTION TO PRODUCE BUSINESS RECORDS. If the answer to an interrogatory may be determined by examining, auditing, compiling, abstracting, or summarizing a party's business records, including electronically stored information, and if the burden of deriving or ascertaining the answer will be substantially the same for either party, the responding party may answer by: (a) specifying the records that must be reviewed, in sufficient detail to enable the interrogating party to locate and identify them as readily as the responding party could; and (b) giving the interrogating party a reasonable opportunity to examine and audit the records and to make copies, compilations, abstracts, or summaries.

COMMENTARY

This rule is substantially the same as Federal Rule of Civil Procedure 33(d). One of the concerns expressed by several members of the Supreme Court during the January 21, 2010 public hearing was the need to make certain that the new Wisconsin e-discovery

rules closely follow the federal e-discovery rules which were adopted in 2006. The Judicial Council also incorporated much of the federal advisory notes as the Council's own commentary. Therefore, members of the bench and bar are encouraged to carefully study the Judicial Notes following each of the new rules because in some instances they may signal a change in practice which will be different from current state practice and may apply in cases which do not involve e-discovery.

Wis. Stat. §804.08(3) states that a party producing ESI in response to an interrogatory must insure that the interrogating party can locate and identify the answer as readily as the producing party, but then goes on to state that the responding party must give the interrogating party "a reasonable opportunity to examine and audit the information…" According to the commentary under new §804.08(3) this means:

> Depending on the circumstances, satisfying these provisions with regard to electronically stored information may require the responding party to provide some combination of technical support, information on application software, or other assistance. The key question is whether such support enables the interrogating party to derive or ascertain the answer from the electronically stored information as readily as the responding party. A party that wishes to invoke Rule 33(d) by specifying electronically stored information may be required to provide direct access to its electronic information system, but only if that is necessary to afford the requesting party an adequate opportunity to derive or ascertain the answer to the interrogatory.

The foregoing commentary to §804.08(3) could prove challenging in a number of respects. However, one of the primary points of conforming new state e-discovery rules to the federal e-discovery rules is to allow the bench and bar to readily access the rich body of federal gloss which has developed over the years concerning e-discovery. Addressing the specifics of the commentary to §804.08(3) suggests a number of issues may be raised which will be new to the bench and bar. For example, how much technical support can be demanded by a discovering party? In the case of ESI which can only be read by so called "legacy proprietary software" which may no longer exist, one court has required a producing party to design a computer program to extract data from its computerized business records. *See Anti-Monopoly, Inc. v. Hasbro*, No. 94CIV2120,

1995 US Dist. Lexis 16355 (S.D.N.Y. Nov. 3, 1995). Of course, this type of ruling today ought to prompt defense counsel to seek to compel cost shifting to the requesting party. *See, e.g., Zubulake v. UBS Warburg,* 217 F.R.D. 309, 318-322 (S.D.N.Y. 2003); *Medtronic Sofamor Danek, Inc. v. Michelson,* No. 01-2373, 2003 U.S. Dist. LEXIS 8587 (W.D. Tenn. May 13, 2003); *Byers v. Illinois State Police*, No. 99 C 8105, 2000 US Dist. Lexis 9861 at *35-37 (N.D. Ill. June 3, 2002); and *Rowe Entertainment, Inc. v. William Morris Agency, Inc.*, 98 Civ. 8272, 2002 US Dist. Lexis 8308 at *23 (S.D.N.Y. May 9, 2002). The referenced commentary to §804.08(3) also raises a question as to what "direct access" means.

Does it mean that a discovering party will automatically have the right to go onto a defendant's property and directly examine the hard drives of an adversary's computer system? Again, the federal case law is very helpful. First, it is important to note that the latest method of granting access does not usually involve the actual physical presence of discovery counsel. Instead, it most often involves the imaging of a computer hard drive or hard drives and making those available to discovering counsel. Both the courts and the Sedona Conference (http://www.thesedonaconference.org) caution that imaging of a producing party's computer system must be approached with great care and forethought. According to *John B. v. Goetz*, 531 F.3d 448 (6th Cir. 2008):

> Courts have been cautious in requiring the mirror imaging of computers where the request is extremely broad in nature and the connection between the computers and the claims in the lawsuit are unduly vague or unsubstantiated in nature… [T]he Sedona Principles urge general caution with respect to forensic imaging in civil discovery: '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.... [M]aking 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.'

However, with regard to all aspects of e-discovery including access to a producing party's hard drives, in the electronic age producing counsel should be aware that a lack of candor or efforts to subvert discovery can have dire consequences which did not always occur prior to the wide use of ESI.

Direct access to a producing party's computer system can result where there is such a clear failure to preserve, or it can result from discoveries that the producing party has not produced all of the evidence that was requested in early discovery. In *Kilpatrick v. Breg*, recently discovered emails and memoranda were inconsistent with earlier depositional testimony. Agreeing that there were indications that responsive documents had not been produced, the court granted direct access to some of the producing party's system. *Kilpatrick v. Breg*, No. 08-10052-CIV, 2009 WL 1764829 at *4 (S.D. Fla. June 22, 2009).

RULE IV.

804.09(1) SCOPE. A party may serve on any other party a request within the scope of §804.01(2):
(a) to produce and permit the requesting party or its representative to inspect, copy, test or sample the following items in the responding party's possession, custody, or control.
1. any designated documents or electronically stored information, including writings, drawings, graphs, charts, photographs, sound recordings, images, and other data or data compilations stored in any other medium from which information can be obtained either directly or, if necessary, after translation by the responding party into a reasonably usable form; or
2. any designated tangible things; or
(b) to permit entry onto designated land or property possessed or controlled by the responding party, so that the requesting party may inspect, measure, survey, photograph, test, or sample the property or any designated object or operation on it.

COMMENTARY

Newly amended Wis. Stat. §804.09 is the heart of the new e-discovery rules. We will address §804.09(1) as a distinct rule from §804.09(2).

This is because the former defines the scope of e-discovery while the latter sets forth the procedure for prosecuting and defending an e-discovery request. To begin with, §§804.09(1) and (2) are modeled on FRCP 34(a) and (b). In fact, §804.09(1) is a very straightforward definition of the scope of e-discovery and can best be understood by quoting directly from the Judicial Council's Note, which in turn is taken from the Federal Advisory Comment to FRCP 34(a):

> Rule 34(a) is amended to confirm that discovery of electronically stored information stands on equal footing with discovery of paper documents. The change clarifies that Rule 34 applies to information that is fixed in a tangible form and to information that is stored in a medium from which it can be retrieved and examined. . . . [A] Rule 34 request for production of 'documents' should be understood to encompass, and the response should include, electronically stored information unless discovery in the action has clearly distinguished between electronically stored information and 'documents.' Discoverable information often exists in both paper and electronic form, and the same or similar information might exist in both. The items listed in Rule 34(a) show different ways in which information
>
> may be recorded or stored. Images, for example, might be hard-copy documents or electronically stored information. The wide variety of computer systems currently in use, and the rapidity of technological change, counsel against a limiting or precise definition of electronically stored information. Rule 34(a)(1) is expansive and includes any type of information that is stored electronically. A common example often sought in discovery is electronic communications, such as e-mail. The rule covers – either as documents or as electronically stored information – information 'stored in any medium,' to encompass future developments in computer technology. Rule 34(a)(1) is intended to be broad enough to cover all current types of computer-based information, and flexible enough to encompass future changes and developments.

RULE V.

804.09(2) PROCEDURE. (a) Except as provided in s. 804.015, the request may, without leave of court, be served upon the plaintiff after commencement of the action and upon any other party with or after service of the summons and complaint upon that party, and shall describe with reasonable particularity each item or category of items to be inspected. The request shall specify a reasonable time, place, and manner of making the inspection and performing the related acts. The request may specify the form or forms in which electronically stored information is to be produced.
(b) 1. The party upon whom the request is served shall serve a written response within 30 days after the service of the request, except that a defendant may serve a response within 45 days after service of the summons and complaint upon that defendant. The court may allow a shorter or longer time. The response shall state, with respect to each item or category, that inspection and related activities will be permitted as requested, unless the request is objected to, in which event the reasons for objection shall be stated. If objection is made to part of an item or category, the part shall be specified. The response may state an objection to a requested form for producing electronically stored information. If the responding party objects to a requested form, or if no form was specified in the request, the party shall state the form or forms it intends to use.
b) 2. Unless otherwise stipulated or ordered by the court, these procedures apply to producing documents or electronically stored information:
a. A party shall produce documents as they are kept in the usual course of business or shall organize and label them to correspond to the categories in the request;
b. If a request does not specify a form for producing electronically stored information, a party shall produce it in a form or forms in which it is ordinarily maintained or in a reasonably usable form or forms; and
c. A party need not produce the same electronically stored information in more than one form.

(c) The party submitting the request may move for an order under s. 804.12(1) with respect to any objection to or other failure to respond to the request or any part thereof, or any failure to permit inspection as requested.

COMMENTARY

This rule sets forth a whole new set of procedures which will govern the actual process of e-discovery and requires very careful study. The rule contains a number of specific requirements which must be understood before even attempting to prosecute or defend e-discovery.

THE ISSUE OF "FORM"

To begin with, s. §804.09(2) provides "The request may specify the form or forms in which electronically stored information is to be produced." In the case of ESI, "form" should be read as "format" and a decision as to what format one wishes to receive e- discovery should not be made lightly. Those who think that it is best to receive all evidence in hardcopy may well be making a grave mistake when dealing with ESI. First, if one elects to receive ESI in one form, that is the only form the producing party needs to supply during discovery. *See* §804.09(2)(b)2c; *Autotech Technologies v. Automationdirect.com*, 248 F.R.D. 556 (N.D. Ill. 2008) (court denied a motion to produce files in their native format with attached metadata after the producing party had already produced the same documents in .pdf and in hardcopy). Second, in the case of ESI there may be a great deal hidden within the ESI itself or closely related to the ESI which will be entirely unavailable if the ESI is produced in a paper form. Third, if you ask for ESI in paper you are trusting that opposing counsel and their client are being candid with you and, if they are not, you are also sacrificing the ability to detect their lack of candor.

At this point, I wish to stress that those prosecuting or defending an e-discovery request will do well to retain the services of a forensic computer expert. ESI may exist in a number of formats in an adversary's computer system, and ESI may also be converted into a number of formats by adversary counsel or adversary experts before it is produced.

I strongly recommend that one consider seriously asking that all ESI be produced in its native format. This is actually of benefit to both discovering and producing parties. In the case of discovering parties, this will afford them an opportunity to fully investigate and evaluate the ESI once produced. In the case of producing parties, providing discovery in a native format makes it easy to comply with the mandate of §804.09(2)(b)2a which provides: "A party shall produce documents as they are kept in the usual course of business or shall organize and label them to correspond to the categories in the request."

There are other formats that may be offered besides the native format. For example, a producing party may suggest that ESI be produced as "tiff" or "pdf" images and give as a reason that it will be far easier to manage and search. However, when dealing with any format other than native, there are facets of ESI discovery which can be lost as surely as if one produced the ESI in hardcopy. One example is "metadata."

METADATA

A book could be written about the concept of metadata. We will only touch the surface here and at the webcast presentation, but one must understand that given the right circumstances metadata may be crucial to the e-discovery process. Metadata as a concept is not that difficult to grasp. Think of it as information about ESI which can only be viewed when using the software originally designed to display the ESI to an authorized user. Originally, it was thought of as information which helped a computer operator store or retrieve computer information.

The definition has now broadened to include any information about ESI which is hidden from view. In this regard, the routing information of email may constitute metadata (and that information could be crucial if one were trying to show that administrators at a business had viewed certain email). Metadata might include word processing information about who helped draft a document. Metadata might even include information that is part of a database that is hidden from view when the database is displayed as a spreadsheet.

The battle concerning metadata will certainly rage for many years to come. As an example of the issues involved, consider the following. In *City of Phoenix v. Lake*, 207 P.3d 725 (Ariz. Ct. App. 2009) a citizen filed public records requests with a municipality, including all notes kept by seven police officers. Suspecting that the notes had been backdated, the citizen requested the metadata that accompanied those notes. Despite a strong public policy in Arizona favoring disclosure of public records, the *Lake* Court concluded that there was a distinction between a public record and a "metadata record," and that disclosure was only required for public records. The dissent in *Lake* took strong exception to the decision of the court, stating in part:

> The majority's approach suggests metadata is somehow different from the underlying public record, and therefore, metadata has a different 'nature and purpose' from the public record. This approach fails to recognize metadata is part of the requested electronic document. Suggesting metadata, standing alone, falls outside of the various formulations of a public record recognized in Arizona, misses the point-metadata does not stand alone. It is not an electronic orphan. It has a home; it exists as part of an electronic document.

Id. at ¶53.

How one determines the need for and scope of metadata requests is beyond the scope of this webcast. However, it is important to emphasize that it is by no means a foregone conclusion that metadata is relevant or discoverable. Some courts have expressed a great deal of skepticism concerning metadata. In *U.S. v. Zerjav,* No. 4:08CV00207 ERW, 2009 WL 2143756 (E.D. Mo. July 14, 2009) the court opened its opinion by stating "[w]hile the Parties may exchange metadata by agreement, the Court has no intention of requiring any party, in any case, to produce metadata without showing that other means of obtaining the discoverable material failed." Other courts have limited the circumstances under which discovery of metadata will be permitted. In *Kingsway Financial Services v. PriceWaterhouseCoopers,* No. 03 Civ. 5560, 2008 WL 5423316 (S.D. N.Y. Dec. 31, 2008) the court cited *Aguilar v. Immigration & Customs Enforcement Div. of the United States Dep't of Homeland Sec.*, 255 F.R.D. 350 (S.D.N.Y. 2008) for the proposition that in the absence of an issue concerning the authenticity of a document or the process by which it was created, most metadata has no evidentiary value.

THE DUTY TO PRESERVE ESI

Those who must produce ESI need to remember that they have an affirmative duty to preserve ESI if litigation is reasonably anticipated. This is a very important duty and is a fundamental *sine qua non* of e-discovery.

In general, the federal courts have issued many decisions which are often cited when preservation has not been done properly. *See, e.g., Danis v. USN Communications, Inc.*, No. 98 C 7482, 2000 WL 1694325 (N.D. Ill. Oct. 23, 2000). In *Metropolitan Opera Association v. Local 100, Hotel Employees,* 212 F.R.D. 178 (S.D.N.Y. 2003) the court severely sanctioned defense counsel, stating in part:

> (1) [Counsel] never gave adequate instructions to their clients about the clients' overall discovery obligations [regarding ESI], … (2) knew the [client] to have no document retention or filing systems and yet never implemented a systematic procedure for document production or for retention of documents, including electronic documents; [and] (3) delegated document production to a layperson who … did not even understand himself (and was not instructed by counsel) that a document included a draft or other non-identical copy, a computer file and an e-mail.

Id. at 222.

Producing counsel needs to meet with the information system ("IS") personnel of a client and take affirmative steps to see that ESI is preserved. He or she must set up procedures to police the preservation of ESI. *See, e.g., National Association of Radiation Survivors v. Turnage,* 115 F.R.D. 543, 557 (N.D. Cal. 1987); *In re Prudential Ins. Co. of America Sales Practices Litigation,* 169 F.R.D. 598 (D.N.J. 1997); *US v. Koch Industries,*197 F.R.D. 463 (N.D. Okla. 1998). *See also* duties of corporation and counsel discussed in *William. T. Thomson Co. v. General Nutrition Corp.,* 593 F. Supp. 1443, 1455 (C.D. Cal. 1984). In the case of *In re Old Banc One Shareholders Securities Litigation,* No. 00 C 2100, 2005 US Dist. LEXIS 32154 (N.D. Ill. Dec. 8, 2005) the court stated:

> In order to meet its obligations, Bank One needed to create a comprehensive document retention policy to ensure that relevant documents were retained and needed to disseminate that policy to its employees….

Id. at *11-12.

SPOLIATION

This is definitely not a concept which is new to Wisconsin. *See, e.g., See In re Estate of Jane Neumann,* 2001 WI App. 61, 242 Wis. 2d 205, 626 N.W.2d 821, where the court stated: "Courts have fashioned a number of remedies for evidence spoliation. The primary remedies used to combat spoliation are pretrial discovery sanctions, the spoliation inference, and recognition of independent tort actions for the intentional and negligent spoliation of evidence. … Wisconsin has recognized the first two remedies." *Id.* at ¶80. *See also Sentry Ins. v. Royal Ins. Co.,* 196 Wis. 2d 907, 918-19, 539 N.W.2d 911 (Ct. App. 1995) (upholding trial court's exclusion of evidence related to refrigerator where party's expert intentionally removed components, thereby precluding testing by opposing party); *Jagmin v. Simonds Abrasive Co.,* 61 Wis. 2d 60, 80-81, 211N.W.2d 810 (1973) (holding that spoliation inference [against party causing spoliation] is inappropriate where evidence was negligently destroyed, but may be appropriate where destruction is intentional). *And also see* Justice Gableman's decision in *American Family v. Golke,* 2009 WI 81, 319 Wis. 2d 397, 768 N.W.2d 729. However, spoliation in the context of e-discovery is qualitatively different from spoliation when dealing with hardcopy or physical evidence.

One of the most intriguing challenges relates to how one should go about proving the spoliation of ESI. For an interesting discussion of how to do this the reader is directed to the case of *In re Telxon Corp. Sec. Litigation*, No. 5:98CV2876, 1:01CV1078, 2004 WL 3192729 (N.D. Ohio July 16, 2004), which involved failures to disclose digital evidence, and the methods used by the plaintiffs' counsel to prove its existence.

The plaintiffs in *Telxon* argued as follows. Because "PwC … produced hardcopy documents in a version different from any version of the documents in electronic form, the conclusion is inescapable that PwC has not yet made available to Telxon and plaintiffs all of its electronic databases relevant to this action…" The *Telxon* plaintiffs also argued, "[t]he absence of electronic versions of internal audit work papers, and the absence of the electronic version of the 1998 work papers from which the hard copies were produced raises questions as to whether PwC is still withholding discoverable material." *Id.* at *22.

The Telxon plaintiffs attempted to show damage by arguing: "[T]he failure to note all modifications and all persons modifying documents on the hard copies produced during discovery caused Telxon and plaintiffs to choose not to depose certain persons or not to ask certain questions of the people whom they did depose…. T]he failure to produce documents in the order in which they were kept and the failure to produce all indices allowing the sorting of produced documents according to topic of interest slowed Telxon's and plaintiffs' discovery of relevant information and increased the cost of discovery." *Id.* at *23.

The Magistrate Judge in *Telxon* was persuaded and held as follows: "PwC failed at the start of discovery to check thoroughly its local servers and its archives for relevant documents, failed to compare the various versions of relevant documents on those databases, failed to produce documents as they were kept in the ordinary course of business, and failed to reproduce thoroughly and accurately all documents and their attachments. Prior to litigation PwC had permitted destruction of documents despite committing to their preservation." *Telxon* at *33.

804.12(4m) failure to provide electronically stored information. Absent exceptional circumstances, a court may not impose sanctions under these rules on a party for failing to provide electronically stored information lost as a result of the routine, good-faith operation of an electronic information system.

COMMENTARY

The following Judicial Council Note following §804.12(4m) explains the purpose of this new addition to §804.12:

> Section 804.12 (4m) is taken from F.R.C.P. 37(e). Portions of the Committee Note of the federal Advisory Committee on Civil Rules are pertinent to the scope and purpose of s. 804.12(4m): "The 'routine operation' of computer systems includes the alteration and overwriting of information, often without the operator's specific direction or awareness, a feature with no direct counterpart in hard-copy documents. Such features are essential to the operation of electronic information systems.
>
> [The rule] applies to information lost due to the routine operation of an information system only if the operation was in good faith.

Good faith in the routine operation of an information system may involve a party's intervention to modify or suspend certain features of the routine operation to prevent the loss of information, if that information is subject to a preservation obligation. A preservation obligation may arise from many sources, including common law, statutes, regulations, or a court order in the case.

The good faith requirement . . . means that a party is not permitted to exploit the routine operation of an information system to thwart discovery obligations by allowing that operation to continue in order to destroy specific stored information that it is required to preserve. When a party is under a duty to preserve information because of pending or reasonably anticipated litigation, intervention in the routine operation of an information system is one aspect of what is often called a 'litigation hold.' Among the factors that bear on a party's good faith in the routine operation of an information system are the steps the party took to comply with a court order in the case or party agreement requiring preservation of specific electronically stored information. … The protection provided by [this rule] applies only to sanctions 'under these rules.' It does not affect other sources of authority to impose sanctions or rules of professional responsibility. This rule restricts the imposition of 'sanctions.' It does not prevent a court from making the kinds of adjustments frequently used in managing discovery if a party is unable to provide relevant responsive information. For example, a court could order the responding party to produce an additional witness for deposition, respond to additional interrogatories, or make similar attempts to provide substitutes for some or all of the lost information.

RULE VII

805.07 (2) SUBPOENA REQUIRING THE PRODUCTION OF MATERIAL. (a) A subpoena may command the person to whom it is directed to produce the books, papers, documents, electronically stored information, or tangible things designated therein.

A subpoena may specify the form or forms in which electronically stored information is to be produced. A command in a subpoena to produce documents, electronically stored information, or tangible things requires the responding party to permit inspection, copying, testing, or sampling of the materials.

(b) Notice of a 3rd-party subpoena issued for discovery purposes shall be provided to all parties at least 10 days before the scheduled deposition in order to preserve their right to object. If a 3rd-party subpoena requests the production of books, papers, documents, electronically stored information, or tangible things that are within the scope of discovery under s. 804.01(2)(a), those objects shall not be provided before the time and date specified in the subpoena. The provisions under this paragraph apply unless all of the parties otherwise agree.

(c) If a subpoena does not specify a form for producing electronically stored information, the person responding shall produce it in a form or forms in which it is ordinarily maintained or in a reasonably usable form or forms. The person responding need not produce the same electronically stored information in more than one form.

COMMENTARY

The amendments to Wis. Stat. §805.07(2) extend the rules governing the discovery of ESI to situations in which information is sought from third parties.

APPENDIX A

Summation Express

Redesigned to run on the powerful and proven AccessData technology core, Summation Express is a web-based document, electronic data and transcript review platform that accommodates smaller teams.

Next Generation Features and Classic Summation Functionality

- Web-based with support for alternative browsers such as Safari & Firefox
- Built on AccessData core technology
- Data processing for over 700 file types
- ECA and final review in one
- Uncomplicated and intuitive workflows
- Offline mobile case review
- Granular security
- Classic Summation transcript support
- Ingest native, PSTs/NSFs and DII files
- Near native redaction
- Word boundary redaction
- Email threading
- Concept search
- Near duplicate analysis
- Advanced case data filtering with 100s of unique facets
- Audit & activity reports
- Exports:
  - Load files for multiple review platforms – including competitors' and EDRM XML
  - Reduced PSTs, TIFFs and PDFs

Summation Express offers both comprehensive early case assessment capabilities - data ingestion, processing, culling, export with load file creation and first pass review - and final review features - search, annotation, redaction, production tools and transcript support - in one product. This integration means that users can move data from the ECA stage directly to final review without creating a load file, exporting or re-processing. In fact, all stakeholders from IT to in-house teams to outside counsel can efficiently and securely collaborate in a single platform.

ECA

Summation Express features industrial strength processing using AccessData's time tested and powerful FTK™ engine. This includes high speed file and image ingestion with support for over 700 data types as well as modifiable processing options such as OCR, de-duplication and deNIST support with extensive reporting options including processing, de-duplication, export, and search with real time status.

Search

Search in Summation Express is 4D, meaning that users can index, invoke keywords, apply ECA-type filter facets, and refine with Excel-like column level filters to create a four dimensional search structure. Moreover Summation Express adds Boolean, stemming, phonic, fuzzy, in-document and white box concept search to the tool set. With search result relevancy ranking, advanced searching options and clear and concise search reporting, search in Summation Express is comprehensive and powerful.

Review & Annotate

Along with standard review features such as near native document viewing, email threading, and near duplicate comparison, Summation Express also has some truly next generation annotation features. These include redaction on near native files, which allows users to redact first and then image, meaning they TIFF a much smaller subset of documents – and 'word-boundary redaction' - meaning that instead of the redaction tool creating boxes that the user must lay over different pieces of text to redact a whole sentence, the user can actually drag the redaction tool over the sentence as if highlighting a section of text in MS Word.

Production

Summation Express combines the exporting power of our ECA tool with the functionality of a final review tool, meaning that users can export large native, image or blended data sets to multiple load file types, but still have the stamping and redacting tools necessary for a formal production to opposing counsel.

AccessData

Portability

One of Summation Express's classic strengths is its ability to allow users to "go mobile" or take a case offline, make changes to it, then sync it back up upon reconnection to the network. This feature is particularly useful for road warriors or those who need to take a case to a courtroom or other location without internet connectivity.

Transcripts

Summation Express features industry leading transcript support that historical users have come to depend on – including reports, color highlighting, condensed printing, exhibit linking, transcript notes and real time integration.

About Summation Express

Ideal for smaller case loads; Summation Express offers support for up to 2 million records across all cases and up to three concurrent users. Summation Express also features powerful processing capacity and is optimized for laptops and regular workstations.

Contact Us Today

Are you ready to let the AccessData Team help you power your discovery? To find out more about Summation Express or to schedule a demonstration, call 800.574.5199 / +1.801.377.5410, or email sales@accessdata.com

www.rediscoversummation.com

AccessData

ACCESSDATA CORPORATE HEADQUARTERS
384 South 400 West
Suite 200
Lindon, UT 84042 USA
801.377.5410

NORTH AMERICA SALES
800.574.5199
801.765.4370 (fax)
sales@accessdata.com

INTERNATIONAL SALES
Office: +44 (0)20 7010 7800
internationalsales@accessdata.com

GENERAL CONTACT INFORMATION:
+1.801.377.5410
+1.801.765.4370 (fax)

San Francisco, CA Office
425 Market Street, 7th Floor
San Francisco, CA 94105
801.377.5410

Houston, TX Office
14531 FM 529
Suite 225
Houston, TX 77095
801.377.5410

Sterling, VA Office
ph: 801.377.5410
21400 Ridgetop Circle
Suite 101
Sterling, VA 20166-6511

United Kingdom Office
ph: +44 0207 010 7800
3rd floor
1 Bedford Street
London
WC2E 9HG

Australian Office
ph: +61 (0) 2 8205 7828
Level 12
1 Pacific Highway
North Sydney, NSW 2060
Australia

Now Simpler and More Powerful, Rediscover the New Summation…

Redesigned to run on the powerful and proven AccessData technology core, Summation is a web-based document, electronic data and transcript review platform that accommodates the workflows of contemporary legal teams.

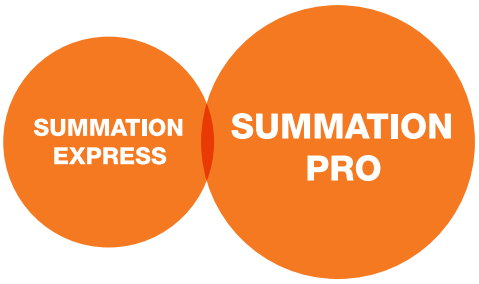
Simple to use and highly secure, Summation is also the first product to combine comprehensive data processing, early case assessment and final review features into a single platform– eliminating the need for iterative processing, data loading and review cycles.

Your Challenges, Your Solution

Modern litigation involves the review of all types of data during the discovery phase. The volume of this data, particularly electronic records, is growing at a rapid pace, and it is getting more and more difficult for legal teams to stay on top of their discovery obligations. Couple data growth challenges with the lack of collaborative support current software options offer IT departments, in-house legal teams and law firms and you have a perfect storm of cost and risk.

Enter Summation.

Summation lets legal teams use one product to strategically reduce the amount of data they analyze in final review via a repeatable process that eliminates fees generated by moving data between tools and providers. Summation also provides an intuitive and secure platform in which to analyze and produce all discovery data types - thereby saving users time and money while effectively reducing risk and promoting true collaboration.



Summation comes in multiple versions which range from supporting small teams and matters to the largest of organizations and cases.

Summation Express supports small collaborative teams and small to medium sized cases.

Summation Pro is built for unlimited team and case sizes and comes in two options depending on the amount of processing power an organization needs.

Next Generation Features and Classic Summation Functionality

- Web-based with support for alternative browsers such as Safari and Firefox
- Built on AccessData core technology
- Data processing, ECA, and final review all-in-one
- Uncomplicated and intuitive workflows
- Offline mobile case review
- Granular security
- Classic Summation transcript support
- Ingest native, PSTs/NSFs and DII files
- Near native redaction
- Word boundary redaction
- Email threading
- Concept search
- Near duplicate analysis
- Advanced case data filtering with 100s of unique facets
- Audit & activity reports
- Exports:
  - Load files for multiple review platforms – including competitors' and EDRM XML
  - Reduced PSTs, TIFFs and PDFs
  - Native Files
  - Forensic Archives

What's Included?

Summation offers both comprehensive early case assessment capabilities (data ingestion, processing, culling, export with load file creation and first pass review) and final review features (search, annotation, redaction, production tools and transcript support).

Moreover it offers these as reasonably priced subscription models with no throughput charges for processing, hosting or data export. But price is not the only advantage of accommodating these two pieces of the e-discovery process in one product. The integration also means that users can move data from the ECA stage directly to final review without creating a load file, exporting or re-processing. In fact, all stakeholders from IT to in-house teams to outside counsel can efficiently and securely collaborate in a single platform. Also, since Summation is purpose-built as a web based platform teams from around the globe can contribute.

Near Native Redaction

Summation allows users to redact on near native files, which facilitates a workflow of redacting first and then imaging only the redacted set. This means teams image a smaller subset of documents, which saves time and money.

Word Boundary Redaction

Summation offers 'word-boundary redaction' - meaning that instead of the user creating multiple boxes to lay over different pieces of text to redact a whole sentence, the redaction tool can be dragged over the sentence as if highlighting a section of text in MS Word. This allows the user to create a single redaction that covers a whole line and stops midway through a second line. When reviewing and redacting thousands of documents, this feature can be a real time-saver and help mitigate the potential for user error.

Transcript Support

Summation also offers industry-leading transcript support that historical users have come to depend on – including reports, annotations and real time integration.

- **Simple and Powerful**
- **Web Based with Offline Mobile Capability**
- **Highly Scalable – From Small Matters to the Largest Cases**
- **Flexible and Customizable**

AccessData

ACCESSDATA CORPORATE HEADQUARTERS
384 South 400 West
Suite 200
Lindon, UT 84042 USA
801.377.5410

NORTH AMERICA SALES
800.574.5199
801.765.4370 (fax)
sales@accessdata.com

INTERNATIONAL SALES
Office: +44 (0)20 7010 7800
internationalsales@accessdata.com

GENERAL CONTACT INFORMATION:
+1.801.377.5410
+1.801.765.4370 (fax)

San Francisco, CA Office
425 Market Street, 7th Floor
San Francisco, CA 94105
801.377.5410

Houston, TX Office
14531 FM 529
Suite 225
Houston, TX 77095
801.377.5410

Sterling, VA Office
ph: 801.377.5410
21400 Ridgetop Circle
Suite 101
Sterling, VA 20166-6511

United Kingdom Office
ph: +44 0207 010 7800
3rd floor
1 Bedford Street
London
WC2E 9HG

Australian Office
ph: +61 (0) 2 8205 7828
Level 12
1 Pacific Highway
North Sydney, NSW 2060
Australia

APPENDIX B

PANNING FOR GOLD:

Social Networking's Impact on E-Discovery

by Hon. Richard J. Sankovitz, Jay E. Grenig & William C. Gleisner III

What's new is old again. Not long ago, social networking – on platforms such as Facebook, MySpace, Twitter, YouTube, and the like – seemed exotic and avant-garde. But no longer. In 2011, social networking is commonplace.

In fact, social networking has so permeated the culture that competent lawyers cannot afford to ignore its customs and the trove of discoverable information to be found where it takes place. Just as lawyers last century needed to master the intricacies of email, so too this century with social networking. As one commentator puts it: "It should now be a matter of professional competence for attorneys to take the time to investigate social networking sites. You must pan for gold where the vein lies – and today, the mother lode is often online."[1]

This article summarizes practical recommendations and recent legal developments concerning:

- Helping clients understand how bad social networking habits can undermine their cases;
- Using commonly available resources to mine social networking sites (SNS) for discoverable information;
- Whether users of SNS have any right to shield what they post from discovery; and


Sankovitz


Grenig


Gleisner

Richard J. Sankovitz, Harvard 1983, is a Milwaukee County circuit court judge and teaches in the field of electronic discovery, presenting a program entitled "Electronic Discovery: New Wine in Old Bottles." He seeks to reassure judges and lawyers that they need not be specialists or technicians to master these new tools.

Jay E. Grenig, California-Hastings 1971, is a professor of law at Marquette University Law School. He is a member of the Wisconsin Judicial Council and reporter for the Local Rules Committee of the U.S. District Court for the Eastern District of Wisconsin. He is coauthor of *eDiscovery & Digital Evidence, Electronic Discovery and Records Management Guide* and *Wisconsin Practice Series: Civil Discovery* and former managing editor of *Electronic Discovery and Records Management Quarterly.*

William C. Gleisner III, Marquette 1974, has an extensive background in state and federal litigation and focuses on the technical and legal aspects of obtaining, organizing, and managing electronic evidence. He provides computerized litigation support and "of counsel" assistance to law firms nationwide, helping them to plan, formulate, and execute e-discovery strategy. With Prof. Grenig, he is coauthor of *eDiscovery & Digital Evidence* and was a Summation-certified trainer for nearly 10 years. He thanks his associate, Matthew W. Surridge, for his research and drafting assistance.

• Whether users of SNS may be held liable for the defamatory content of their posts.

The Ubiquity of Social Networking

It is commonplace for people to publish information about themselves, their activities, their histories, and their opinions on a variety of SNS platforms, including Facebook, MySpace, Twitter, and YouTube, not to mention on blogs, chatrooms, and so on. Seventy-five percent of people ages 18 to 24 have a profile on online social networks. One-third of adults ages 35 to 44 are active on online social networks, and nearly 20 percent of people ages 45 to 54 have profiles on a social network.[2]

Cautions for Clients and Prospective Jurors

The problem. People who use social networks might not consider that the information they post about themselves can be used against them or the organizations for which they work. In today's wired world, litigants – adverse parties and clients alike – may be in the habit of regularly posting experiences and opinions on SNS. They create videos and post them to YouTube, or they comment on videos created by others. They publish blogs and comment on blogs published by others. They chat in chatrooms. They create their own Web pages.[3] And other people may be posting unflattering or revealing information in cyberspace about the litigant without his or her knowledge. "In 2008, two weeks after being charged with drunk driving in an accident that seriously injured a woman, Joshua Lipton made the foolish decision to show up at a Halloween party in a prisoner costume with the label 'Jail Bird' on his orange jumpsuit. Someone posted the photo on Facebook and the prosecutor made effective use of the photo of this young man partying while his victim was recovering in a hospital. The judge called the photos 'depraved' and sentenced him to two years in prison."[4]

The problem is aggravated by clients and others who might not appreciate or candidly acknowledge the degree to which their online disclosures may affect their cases, or how they might be sprung on them in a deposition or at trial.

Deleterious online habits also afflict potential jurors. It has become almost commonplace for jury trials to be derailed by jurors who go online to post their opinions or information about their deliberations or to research extraneous information about the case before them. "A misbehaving juror in Arkansas posted eight tweets during a trial which resulted in a $12.6 million dollar verdict [against defendant Stoam]. During the trial, the juror's tweets included one that said, 'oh and nobody buy Stoam. It's … bad mojo and they'll probably cease to exist, now that their wallet is 12m lighter.'"[5]

Some solutions. Lawyers advising any kind of client involved in civil or criminal litigation – plaintiffs, defendants, individuals, corporate agents – should put Internet usage at or near the top of the list of things to discuss with the client at the outset of the litigation. Clients must be advised not only of the potential for damaging their own cases (and the need for candor in discussing what damage already may have been done) but also of the opportunity to discover useful information about adverse parties.

An attorney might even consider including a disclaimer or additional provision in retainer agreements, such as the following:

1) The client (and, if a corporate client, all of its officers and employees) promises not to post any information on the Internet about the subject *matter of the representation without* first consulting with counsel.

2) The client (including corporate employees) must be completely candid concerning all past Internet postings.

3) If the client is not candid about the client's Internet postings, counsel cannot be responsible for the consequences and reserves the right to withdraw.

4) Counsel cannot predict what will be found on the Internet regard-

ing a client and so reserves the right to withdraw as counsel after conducting counsel's own search of the Web for information concerning the client.

Discovery of Information Published on an SNS

The two most common legal issues that arise when a party attempts to discover another's SNS posts are 1) whether the person who posted the information has any right to shield posts from discovery; and 2) whether the operator of the SNS has any duty to respond to discovery requests.

Courts generally do not consider SNS posts privileged. In *Ledbetter v. Walmart Stores Inc.*,[6] Walmart sent subpoenas to Facebook, MySpace, and Meetup.com seeking information about the plaintiffs, who had filed an action seeking damages for physical and mental injuries and loss of consortium. The court denied the plaintiffs' motion for a protective order based on the physician-patient and spousal privileges, finding the plaintiffs had waived the privileges by filing the lawsuit. The court found the information was relevant and reasonably calculated to lead to the discovery of admissible evidence.

In *EEOC v. Simply Storage Management*,[7] a case involving multiple claims of sexual harassment, requests were made directly to the plaintiffs about postings they had made to Facebook and MySpace. The EEOC objected to the production of all SNS content (and to deposition inquiries on the same subjects) on the grounds that the requests were overbroad and unduly burdensome (because they improperly infringed on the claimants' privacy) and would harass and embarrass the claimants.[8]

The defendants claimed the nature of the injuries the claimants had alleged "implicates all their social communications (i.e., all their Facebook and MySpace content)."[9] The court first observed that the discovery of SNS "requires the application of basic dis-

Search Engines for Locating Posts on Social Networking Sites

Hundreds of search engines are available on the Web, and more are coming online all the time. The following are some helpful resources for locating evidence on social networking sites.

- Top Ten Search Engines, www.seoconsultants.com/search-engines
- AltaVista, www.altavista.com
- Ask, www.ask.com
- Bing, http://www.bing.com
- Cuil (billed as having the world's biggest index), www.cuil.com
- DuckDuckgo (eliminates clutter as it crawls), www.duckduckgo.com
- Exalead (based in France, use to search European sources), www.exalead.com/search
- Factbites (answers in sentences using encyclopedias and other higher content sites), www.factbites.com
- Google, www.google.com
- Google for searching blogs, http://blogsearch.google.com
- Hakia (looks for meaning through semantic connections of words to concepts rather than relying on the standard keyword match), www.hakia.com
- Highbeam (searches approximately 80 million articles from archives of 6,500 newspapers, magazines, and more), www.highbeam.com
- Kosmix (searches images, video, blogs, tweets), www.kosmix.com
- Quintura (clusters results in a tag cloud that can be manipulated to alter the search), www.quintura.com
- Technorati (searches blogs), www.technorati.com
- SearchQuilt, www.searchquilt.com
- Yahoo, http://search.yahoo.com

Specialty search engines – for videos:
- Bing, http://www.bing.com/videos/browse
- Google, http://video.google.com
- Yahoo Video, http://video.search.yahoo.com
- YouTube, www.youtube.com

Specialty search engines – for images:
- Bing, http://www.bing.com/images
- Google, http://images.google.com
- Yahoo, http://images.search.yahoo.com

"Meta-search" engines (to search several engines at one time):
- etools.ch (Swiss meta engine useful for searching European sites), http://www.etools.ch
- Fuzzfind (also searches social bookmarking sites), www.fuzzfind.com
- iSeek, www.iseek.com
- MetaCrawler (simultaneously searches white pages, yellow pages, Ask, Bing, Google, Yahoo, and more), www.metacrawler.com
- Polymeta, www.polymeta.com
- Yippy (searches images and Wikipedia), http://search.yippy.com
- Zuula, www.zuula.com

For more information about Web search tools, see Web Search Guide, www.Websearchguide.ca/index.html; and Applied Discovery, www.applieddiscovery.com.

Social Networking, Jurors, and Jury Instructions

Jurors are online and networking, too, and the bad habits of some continue to make headlines, including:

- the juror in England who polled her Facebook friends to decide whether to vote guilty or not guilty;
- the juror in Arkansas who posted eight tweets during a trial, including one tweet denigrating the defendant, against which the jury had awarded a $12.6 million verdict; and
- the juror in New York who, during deliberations, attempted to "friend" one of the witnesses.

Wisconsin Jury Instructions

Wisconsin courts were among the first courts in the nation to address these concerns by alerting jurors about online pitfalls and explicitly instructing them to avoid the Internet during trial. In 2009, the Wisconsin Criminal Jury Instructions Committee modified its standard jury instruction on jury communicotions (Wis JI-Civ 50) to address specifically the potential for Internet abuse:

"... Do not consult dictionaries, computers, websites or other reference materials for additional information. Do not seek information regarding the public records of any party or witness in this case. Any information you obtain outside the courtroom could be misleading, inaccurate, or incomplete. Relying on this information is unfair because the parties would not have the opportunity to refute, explain, or correct it.

"Do not communicate with anyone about this trial or your experience as a juror while you are serving on this jury. Do not use o computer, cell phone or other electronic device with communication capabilities to share any information about this case. For example, do not communicate by blog, e-mail, text message, Twitter, Facebook, other social networking sites, or in any other way, on or off the computer."

To Learn More ...

State Bar of Wisconsin PINNACLE™ will present the live **webcast "Amended Rules of Discovery,"** on Thursday, March 31, 12 – 1:30 p.m. In July 2010, the Wisconsin Supreme Court adopted new discovery rules recognizing the influx of electronic discovery and regulating how e-discovery is practiced. The court further amended the rules in November to require a mandatory pre-discovery conference before engaging in e-discovery. The rules became effective Jan. 1, 2011.

The webinar will:

- provide a summary of the discovery rules;
- discuss the impact of the new rules on lawyers' discovery duties; and
- relate the current status of amendments before the Wisconsin Judicial Council's Evidence & Civil Procedure Committee.

Credits: 1.5 CLE credits. Tuition: $95 members; $115 nonmembers; $0 Ultimate Pass holders. Register: (800) 728-7788; (608) 257-3838 Madison area.

See also

- "What You Need to Know: New Electronic Discovery Rules," by Hon. Richard J. Sankovitz, Jay E. Grenig & William C. Gleisner III, July 2010 *Wisconsin Lawyer*

covery principles in a novel context."[10]

The defendants in *Simply Storage* cited one case in which a court required production of the plaintiff's entire SNS profile.[11] The court also discussed the case law it was able to find dealing with the issue of SNS requests directed to a party. According to the court, "[a] person's expectation and intent that her communications be maintained as private is not a legitimate basis for shielding those communications from discovery. ... *Murphy v. Perger*, 2007 WL 5354848 (S. Cal. 2007), ... held that a requesting party is not entitled to access all non-relevant material on a site, but that merely [blocking a] profile from public access does not prevent discovery either. ... As in other cases when privacy or confidentiality concerns have been raised, those interests can be addressed by an appropriate protective order, like the one already entered in this case."[12]

The court in *Simply Storage* determined that the appropriate scope of relevance of an SNS request to a plaintiff was "any profiles, postings or messages (including status updates, wall comments, causes joined, groups joined, activity streams, blog entries) ... that reveal, refer or relate to any emotion, feeling or mental state...."[13] Overall, the *Simply Storage* court was unsympathetic to the privacy concerns asserted by the plaintiffs. According to the court, "[t]he court agrees with the EEOC that broad discovery of the claimants' SNS could reveal private information that may embarrass them.... Further, the court finds that this concern is outweighed by the fact that the production here would be of information that the claimants have already shared with at least one other person through private messages or a larger number of people through postings."[14]

Another case in which postings to an SNS were deemed public, not private, was *Moreno v. Hanford Sentinel Inc.*[15] A student and her family sued a principal and a school district for invasion of privacy and intentional

infliction of emotional distress because of the re-publication of a journal entry from a social networking website. The student had published an ode on her MySpace page that contained derogatory remarks about her hometown. The ode was taken down after six days but the school principal was responsible for getting it published in the local newspaper, which led to death threats and other unfortunate acts. The *Moreno* court held that once the ode had been published on MySpace it was no longer private or entitled to an expectation of privacy. According to the court, "[t]he student's] affirmative act made her article available to any person with a computer and thus opened it to the public eye. Under these circumstances, no reasonable person would have had an expectation of privacy regarding the published material.... [T]he fact that [the student] expected a limited audience does not change [this fact]. By posting the article on myspace.com, [the student] opened the article to the public at large."[16]

However, not every court will permit the discovery of information stored on online social networks, at least if the user makes definitive efforts to protect the privacy of the information rather than broadcasting it generally. To the extent that a posting to an SNS resembles a private communication that is otherwise privileged, such a posting may be protected from discovery under the federal Stored Communications Act (SCA).[17]

In *Crispin v. Christian Audigier Inc.*,[18] several defendants sought to obtain access to the SNS postings of a plaintiff by serving subpoenas directly on the SNS operators. The plaintiff attempted to quash the subpoenas by asserting rights conferred on the SNS operators by the SCA.

The *Crispin* court ruled that the SCA protects electronic communications that are configured to be private.[19] Thus, some Internet communications are protected and some are not:

"With respect to Webmail and private messaging, the court is satisfied that those forms of communications media are inherently private such that stored messages are not readily accessible to the general public. ... With respect to the subpoenas seeking Facebook wall postings and MySpace comments, however, ... it appears... that a review of plaintiff's privacy settings would definitively settle the question, [and so] the court does not reverse Judge McDermott's order, but vacates it and remands so that Judge McDermott can direct the parties to develop a fuller evidentiary record regarding plaintiff's privacy settings."[20]

SNS and Corporate Governance

Corporate record management administrators face unique and difficult challenges because of SNS. Some commentators have described social networking as an "e-discovery and records management nightmare."[21] According to these commentators:

"Is a tweet done on firm resources a 'record' for purposes of retention requirements and ESI preservation/production? ... Much of this remains unsettled ground. If you find that scary, you're not alone. ... Twitter, blogs, and social networks have given almost everyone a Goliath-sized headache. Whether you are thinking in terms of your own law firm or your clients, you must now consider these new technologies."[22]

One record management administrator has described tweets as "being no different from letters, e-mail, or text messages: they can be damaging and discoverable, which could be especially problematic for companies that are required to preserve electronic records, such as the securities industry and federal contractors."[23]

Besides impeding record

(continued on page 61)

(from page 17)

management, social networking could complicate the business world in other ways. Employers already face a number of difficulties arising from employee misuse of work computers.[24] Access to SNS websites or blogs actually may give rise to employee privacy rights that one would not expect to exist during the use of company computers.[25]

Employees, however, need to realize that emails they send or postings they make to an SNS concerning an employer can come back to haunt them.[26] Problematic situations include those associated with trade-secret theft via email or social networking posts[27] and an employee making disparaging remarks about an employer on what the employee thought was a secure network.[28]

Legal Implications for Badmouthing Others on an SNS

The spontaneity and immediacy of SNS postings tend to make them frank, sometimes too much so. Frank comments have the potential to do real damage to a client or a client's business.

But before considering legal action for defamation or business disparagement, lawyers need to reflect on the fact that there is a growing trend to treat blogs and social networks as news and thus protected, as are traditional news outlets, by the First Amendment and laws that shield press informants. In *O'Grady v. Superior Court*,[29] the court was confronted with a charge by Apple Computer that certain unknown persons had caused the publication of trade secrets. Apple issued subpoenas to the publishers of the websites on which the information was published. The *O'Grady* court concluded, "We decline the implicit invitation to embroil ourselves in questions of what constitutes 'legitimate journalis[m].' The shield law is intended to protect the gathering and dissemination of news, and that is what petitioners did here. We can think of no workable test or principle that would distinguish 'legitimate' from 'illegitimate' news. Any attempt by courts to draw such a distinction would imperil a fundamental purpose of the First Amendment."[30]

Searching for and Using SNS Data

Searches. What if a client long ago created a Web page that could prove embarrassing today? Even if the Web page was taken down years ago, a forensic investigator can use tools such as the "Wayback Machine"[31] to retrieve that Web page. According to the creator of the Wayback Machine, it can be used to "[b]rowse through over 150 billion Web pages archived from 1996 to a few months ago."[32] With the Wayback Machine, a forensic investigator can retrieve copies of a website even though it was taken down many years ago and the server where it had been located has ceased to operate.

In a recent legal malpractice case, a defendant firm claimed it had absolutely no knowledge of a particular specialty and nothing on its Web page or in ordinary searches of the Web indicated anything to the contrary. Representatives of the defendant firm swore under oath that the firm never had any expertise in that specialty. However, using the Wayback Machine, the plaintiff's attorney discovered a Web page published by the defendant firm six years earlier that was devoted entirely to that specialty, including statements about how much knowledge the defendant firm had concerning that specialty and maintaining an "ask the expert feature" about the specialty. This Web page revealed that many of the firm members who were now denying any knowledge of the specialty had claimed extensive knowledge six years earlier. In fact, using the Wayback Machine led to the discovery that the defendant firm had even published a client newsletter concerning the specialty.

All litigators should become familiar with the wide variety of search

engines that are available for conducting Web searches. The accompanying sidebar includes several search engines and their Web addresses. While some of the listed websites charge an access fee, they can be used to supplement private investigators' findings and can help obtain far greater information about an individual or a business than one might find using Google, for example. Highbeam will provide access to newspaper and magazine archives, which often can point to interesting discovery leads. It is not easy to search for blogs or blog entries using basic search engines. Thus, for such a chore, one should consider using advanced search engines like Google's blogsearch or Kosmix. Sometimes it is useful to use a search methodology that is not based on keywords. For example, a person can use Hakia to search using semantic connections. Case law or white papers dealing with e-discovery often will be important, and these may be found using the Lexis Applied Discovery site.

Litigators also should become familiar with Web crawlers.[33] A Web crawler is an Internet search device that continuously and automatically searches the Web for sites that address or mention topics the user specifies, for example, news items on a subject that interests the user. For example, Google "news alerts" help keep computer users apprised of news developments about particular issues. Litigators also might consider creating searchbots. "A Searchbot is your own personal search robot that continuously searches the Internet trying to find all the best Websites it can on your behalf. When you build a Searchbot you give it a personality and then program its search circuits with all the things you want to find. You can search for Websites based on factual information like tags and locations.... You can even ask your Searchbot a question and it will talk to other Searchbots to find you an answer."[34]

Admissibility of information obtained from an SNS. There is a difference between asserting SNS posts are discoverable and defending their admissibility in court. Milwaukee County Family Court Judge Michael J. Dwyer has stated that SNS posts are often irrelevant to the legal crux of a case.[35] Judge Dwyer also has stated that an SNS post will be considered inadmissible hearsay if one cannot authenticate the source of the post. According to Judge Dwyer, "If a party denies making the post, it's not admissible."[36] Milwaukee divorce attorney Richard J. Podell has stated that SNS "posts he's provided in cases were allowed as a rebuttal where a spouse denies an extramarital affair."[37] Regardless of their admissibility at trial, the fact is that SNS posts clearly are discoverable, may lead to other discoverable evidence, and may well present serious challenges for counsel before and during trial, especially if used as impeachment.

There is a world of difference in using SNS posts in the context of a civil dispute versus in a criminal dispute, but one obvious concern is whether an attempt by law enforcement to obtain communications posted on an SNS infringes the user's rights under the Fourth Amendment. In *United States v. Warshak*,[38] the court ruled that a suspect may have an expectation of privacy in email communications that bars the production of the information without a warrant. The court explained,

"If we accept that an email is analogous to a letter or a phone call, it is manifest that agents of the government cannot compel a commercial ISP to turn over the contents of an email without triggering the Fourth Amendment.... [T]he ISP is the functional equivalent of a post office or a tele-

phone company.... [I]f government agents compel an ISP to surrender the contents of a subscriber's emails, those agents have thereby conducted a Fourth Amendment search, which necessitates compliance with the warrant requirement absent some exception."[39]

Conclusion

In the social networking era, attorneys face an entirely new challenge that directly affects client representation. It is essential that attorneys and judges keep up to date with these developments. The law is just beginning to evolve in response to SNS data and its use, but the average lawyer cannot afford to ignore the very real potential for legal good and harm that may result from social networking.

Endnotes

[1]Sharon Nelson et al., *The Legal Implications of Social Networking*, 22 Regent U. L. Rev. 1, 14 (2010).

[2]Karen Barth Menzies & Wesley K. Polischuk, *Is Your Client an Online Social Butterfly?* Trial, Oct. 2010, at 23, 24.

[3]Online resources that can be used to create and host Web pages are emerging at a breathtaking pace. See www.intuit.com/Website-building-software or http://mediatemple.net.

[4]Nelson, *supra* note 1, at 12.

[5]*Id.* at 4.

[6]2009 WL 1067018 (D. Colo. Apr. 21, 2009).

[7]*EEOC v. Simply Storage Mgmt.*, 2010 U.S. Dist. Lexis 52766 (S.D. Ind. May 11, 2010).

[8]*Id.* at *4.

[9]*Id.* at *7.

[10]*Id.* at *8.

[11]*Bass v. Miss Porter's School*, 2009 WL 3724968 (D. Conn. Oct. 27, 2009).

[12]*Id.* at 8-9.

[13]*Id.* at 14-15.

[14]*Id.* at 18.

[15]172 Cal. App. 4th 1125, 91 Cal. Rptr. 3d 858 (Cal. App. 2009).

[16]*Id.* at 1130. *See also Commonwealth v. Proetto*, 771 A.2d 823, 831-32 (Pa. Super Ct. 2001).

[17]18 U.S.C. §§ 2701-2712.

[18]717 F. Supp. 2d 965 (M.D. Cal. 2010).

[19]*Id.* at 989.

[20]*Id.* at 991.

[21]Nelson, *supra* note 1, at 15.

[22]*Id.* at 15-16.

[23]*Id.* at 16. For an excellent general discussion of the duty to preserve, see Maria Perez Crist. *Preserving the Duty to Preserve: The Increasing Vulnerability of Electronic Information*, 58 S.C. L. Rev. 7 (2006).

[24]Louis J. Papa & Stuart L. Bass, *How Employers Can Protect Themselves from Liability for Employees' Misuse of Computer, Internet and E-mail Systems in the Workplace*, 10 B.U. J. Sci. & Tech. L. 110 (2004).

[25]*See Stengart v. Loving Care Agency Inc.*, 973 A.2d 330 (N.J. App. 2009) (holding employee's emails exchanged with her attorney through her personal, password-protected, Web-based email account were protected by attorney-client privilege).

[26]*See* Joshua C. Gilliand & Thomas J. Kelley, *Modern Issues in e-Discovery*, 42 Creighton L. Rev. 505, 518-21 (2009).

[27]*See, e.g., Rinkus Consulting Group Inc. v. Cammarata*, 688 F. Supp. 2d 598 (S.D. Tex. 2010) ("Rimkus argues that the September 30, 2006 email Bell forwarded to himself is evidence of trade secret misappropriation. At a discovery hearing held on September 2, 2009, this court allowed Rimkus to subpoena Google, an email provider, to obtain emails Bell sent and received." *Id.* at 626).

[28]*See Konop v. Hawaiian Airlines*, 302 F.3d 868 (9th Cir. 2002) In *Konop*, a pilot sued the airline, his employer, alleging that the airline had viewed his secure website, on which he posted bulletins critical of the airline, its officers, and the incumbent union, without authorization. Two other pilots who had permission to access the website allowed an airline officer to use their names to establish accounts and passwords and access the website. *Id.* at 872. *Cf. Intel Corp. v. Hamidi*, 30 Cal. 4th 1342 (Cal. Sup. Ct. 2003) (company sued former employee for trespass because he sought to send disparaging emails to current employees).

[29]139 Cal. App. 4th 1423, 44 Cal. App. 6 (Cal. App. 2006).

[30]*Id.* at 1457.

[31]Wayback Machine, www.archive.org/web/web.php. Other archive sites include the Bibliotheca Alexandrina, www.bibalex.org/Home/Default_EN.aspx; and the Library of Congress National Digital Library Program, http://memory.loc.gov/ammem/dli2/html/lcndlp.html. See http://en.wikipedia.org/wiki/Internet_Archive.

[32]www.archive.org/web/web.php.

[33]http://en.wikipedia.org/wiki/Web_crawler.

[34]www.searchbots.net/about.

[35]Jack Zemlicka, *High-Tech Hearsay*? 24 Wis. L. J. 1 (Daily Reporter Pub'g Co. Ed., Dec. 20, 2010)

[36]*Id.* at 7.

[37]*Id.*

[38]2010 WL 5071766 (6th Cir. Dec. 14, 2010).

[39]*Id.* at *12.