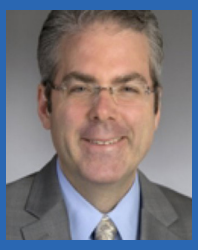
Federal Bar Association
Eastern District of Michigan Chapter:
Litigation Technology Committee/Social Media

WINTER 2015

www.fbamich.org | EDMI Model Order

Table of Contents



Greetings from the Litigation Technology Committee/Social Media of the Federal District Court for the Eastern District of Michigan.

On behalf of the Committee's co-chairs and the author/members of this Newsletter sub-committee *(including Stott Matthews, Megan McKnight, Mark St. Peter, Angela Emmerling Shapiro and Dante Stella)* we are pleased to provide this Newsletter and hope that you find it informative. Inasmuch as this is our first foray into issuing a newsletter, its content and format is subject to change in the future. Our goal for the newsletter is to provide a wide-range of differing viewpoints on an assortment of eDiscovery and other litigation support topics. You will also find a diverse and eclectic collection of articles for those who wish to delve deeper into these topics. We truly hope that you find this newsletter both interesting and informative. Enjoy!

DANIEL QUICK
Dickinson Wright
Committee Co-Chair

Federal Bar Association
PO Box 20759
Ferndale MI 48220
fbamich@fbamich.org

Courthouses:

Detroit 313.234.5300
Ann Arbor 734.741.2075
Flint 810.341.7890
Bay City 989.894.8830
Port Huron 313.226.2547

FEDERAL BAR ASSOCIATION
Eastern District of Michigan Chapter

Discovery of Backups In The Era of Cloud Computing

Dante Stella
Dykema

DANTE A. STELLA focuses his practice in litigation and investigations that involve complex legal, factual and data management issues. He also provides non-litigation counseling to clients on data retention, information infrastructure, and electronic discovery planning.

Mr. Stella heads Dykema's electronic discovery practice and co-chairs the Firm's Discovery Management Group. Mr. Stella is also a member of Dykema's Pro Bono Committee, representing the Detroit office.

Mr. Stella's investigative work (internal and external) includes planning, coordinating and executing responses to:

- United States Department of Justice (DOJ) Antitrust Division criminal subpoenas to suppliers and purchasers of various commodities, intermediate goods, and finished goods.
- FBI criminal subpoenas issued in public corruption investigations.
- Civil subpoenas directed to third parties in antitrust and other litigation.

Mr. Stella's commercial litigation work focuses on cases that involve complex facts, novel issues of law, and high stakes.

In his roles with Dykema's E-Discovery and Discovery Management groups, some of Mr. Stella's specialized projects include:

- Designing efficient discovery processes that result in targeted collection, intelligent processing, and efficient review of Electronically Stored Information (ESI) in response to litigation or government investigations.
- Helping clients create and implement effective litigation holds and defensible internal processes related to ESI.

Prior to joining Dykema, Mr. Stella interned for the Honorable Avern Cohn, United States District Judge for the Eastern District of Michigan.

313-568-6693 | *dstella@dykema.com*
www.dykema.com

Discovery of Backups In The Era of Cloud Computing

In civil litigation, backups (offline copies of active data) are generally outside the duty to preserve and produce information. Courts recognize that backups exist primarily (if not solely) for business continuity and that backups are generally inconvenient to hold, access, restore, and process for any purpose. As a result, disaster-recovery backups are generally off-limits in discovery. Courts see things differently where those backups are the sole source of important information in litigation.[1] A producing party typically will designate its offline backups "not reasonably accessible" under Fed. R. Civ. P. 26(b)(2)(B) – and may also argue that the effort or cost of accessing and searching them is not proportional to the needs of the case under the new Fed. R. Civ. P. 26(b)(1) coming into force on December 1, 2015. In response, a requesting party might argue that the backups contain something that no longer exists on active systems and is critically important to the case.

Historically, in addressing these disputes, courts have balanced accessibility and utility: can the data be accessed without undue burden or cost – and if it cannot be, who is going to pay for it? In the past, possession, custody, and control concepts rarely came into play because most business organizations maintained both their active data and their backups in their own facilities, on their own equipment, using their own personnel. The landscape has changed somewhat as some organizations have moved their information to "the cloud." Legal and practical considerations become more complicated where part or all of the data infrastructure belongs to an unrelated business.

The "cloud" is a vague concept in advertisements, but most articulations of it include two propositions: (1) the data is stored offsite (vis-à-vis its users), and (2) the data is accessed via the Internet. The National Institute of Standards and Technology (NIST) defines cloud computing as:

…a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.[2]

Two common varieties used by organizations are private clouds and public clouds. At a basic level, a private cloud dedicates resources (like servers) to a particular organization or group of related organizations. This includes arrangements such as offsite data centers and outsourced (hosted) servers (or virtual servers). By contrast, a public cloud uses a common set of resources to service many unrelated organizations. The discoverability of backups in a cloud environment is still an emerging area of law, and parties should proceed with caution and common sense according to what variety of cloud is involved.

Possession, Custody, or Control

Understanding Fed. R. Civ. P. 34 is crucial to understanding how cloud data might be discovered via direct document request or become the subject of third-party discovery directed to a cloud provider. Rule 34(a) constrains first- and second-party discovery to information in a party's "possession, custody, or control."[3] The key principles are:

- Documents are deemed to be within the "possession, custody, or control" of a party if the party has "actual possession, custody or control of the materials or has the legal right to obtain the documents on demand."
- "Control" comprehends not only possession of the documents, but also the right, authority, or ability to obtain them. Rule 34(a) therefore enables a party seeking discovery to require production of documents beyond the actual possession of the opposing party if such party has retained any rightt or ability to influence the person who possesses the documents.
- A party that has a legal right to obtain certain documents is deemed to have control of the documents, but the relationship between the party and the person or entity having actual possession of the document is central in each case.
- The party seeking the production of documents bears the burden of proving that the producing party has the control required under Fed. R. Civ. P. 34(a).[4]

Private clouds and public clouds interact differently with these principles.

Private Clouds and Backups

Private clouds run the gamut from an organization's own offsite data center to fully-outsourced IT departments. The more a private cloud resembles an in-house data system, the more closely the discovery of backups follows conventional principles. Even in situations where an unrelated third party holds the data, though, private clouds have features that make them amenable to discovery. Active data is generally under possession, custody, and/or control of the organization that created it. The organization has physical possession in cases where it owns the data center. And where the data center and infrastructure is owned by others, the organization has the legal right to access that active data – the essence of any cloud services agreement. Private cloud backups, likewise, are often subject to an organization's possession, custody, or control. The most clear-cut situation is where the organization owns the data center or a service agreement provides for the restoration of backups on demand. But other situations implicate other questions.

1. Can the organization retain and access backups outside its contract with a service provider? Even if there is no explicit contractual provision requiring a cloud provider to retain or process backups on demand, an organization using a private cloud can always ask. It is often possible to do something with backups where there is a close correspondence between an organization and the machines used to service it. Other forms of "influence," such as business leverage, also might be brought to bear.

2. Is the depth of the backups sufficient to provide any real benefit? Even outside of the basic possession, custody or control aspect, there is the question of benefit and cost. Private cloud providers may not keep the depth of backups that their customers would. Backups are only truly useful to the extent that they reflect data that has changed since the backup was made (call it the "delta"). Where the delta is small, backups are cumulative of what is presently on the system. On some systems like financial databases, there is no delta because as transactions accumulate, today's active system might contain everything found in backups – plus more. The delta - and the attendant cost/benefit analysis - informs discoverability under current Fed. R. Civ. P. 26(B)(2)(C) (limits on even permissible

discovery) and potential grounds for a protective order under Fed. R. Civ. P. 26(c).

3. Would suspending backups cause operational problems or threaten the integrity of the system? Especially in smaller private clouds, just as in on-site systems, mechanical aspects of backup systems inhibit retention of backups. Conflicts between a litigation hold and business needs can arise almost instantly. Usually these center around expansion capabilities: for example, there may be no extra tapes on hand at the service provider; a tape library may not be large enough to accommodate a greatly expanded backup set (in many systems, reconstructing a point in time may require the mounting of dozens of tapes); or a rack-mount backup appliance might be difficult or impossible to expand on the fly. Some problems are more insidious: as the amount of media increases, the reliability of a backup system may diminish. For example, where one backup is spread over many pieces of media, the risk of failure also increases proportionately to the amount of media involved. Think of it this way: if it takes 10 tapes to restore yesterday's data, all 10 tapes must function perfectly. In addition, the corruption of indices can threaten the reliability of backups for their primary purpose. When an index fails, it might be difficult or impossible to restore data for any purpose. These technical issues implicate Fed. R. Civ. P. 26(b)(2)(B), under which federal courts often equate significant technical burdens (and not necessarily insurmountable ones) with a source's not being "reasonably accessible."

Additional Considerations for Public Clouds

A public cloud is a single remote system that theoretically anyone can use. For example, an email provider like Gmail, Yahoo, or Hotmail uses a common pool of servers to handle email for all of its customers. One particular email account could be stored on the same equipment as thousands of others belonging to unrelated people and entities. The same is true of cloud storage (such as OneDrive or Google Drive) and software-as-a-service (such as SalesForce, Office Online, or Google apps). With public clouds, establishing the existence of useful backups, let alone "possession, custody, or control" can be much more challenging.

4. Is there actually a backup? The terms and conditions of public cloud contracts rarely make promises regarding backups. They often hint, via references to "cutovers," that when it comes to disaster recovery, there may not be backups any conventional sense, but rather a quick switch to a redundant system that is kept as a mirror-image of the live system. Mirrors are updated either contemporaneously or at close intervals. As such, there may not be any meaningful delta between the oldest copy of the data set and the newest (such as where a mirror is updated every 24 hours). Restoration of backups of those mirrors – if such backups even exist – would implicate Fed. R. Civ. P. 26(b)(2)(B) and Fed. R. Civ. P. 45(e)(1)(D) (both relating to reasonable accessibility). A public cloud service provider would argue, with good reason, that such backups would be not "reasonably accessible" as contemplated by those rules.

5. Whose backup is it anyway? To the extent that cloud service providers keep true backups, and not just mirrors, it is normally to further their own business goals of system integrity and uninterrupted up-time. Cloud service providers have considerable flexibility to achieve their goals, and there are questions of scale. The more customers a public cloud has, the more likely it is that a backup of one customer's data will reside on the same equipment or media as that of several, tens, hundreds, or thousands of other customers. In this way, conventional backups of public clouds – where they exist - are really backups of the provider's system, not that of any particular customer.

6. Does the service contract give the customer possession, custody, or control of backup data? As noted above, it is quickly becoming well-settled law under Fed. R. Civ. P. 34(a)(1) that if a customer has a legal right to access active electronic data at the time litigation arises, it is required to preserve and, if warranted, produce it in litigation.[5] Conversely, where a party to litigation has no legal right to access the data (or no longer has such a right), a requesting party has to look elsewhere.[6] Many contracts for cloud services (particularly those with larger vendors) do not give customers a right to access backups of their data, let alone any right to obtain restorations and exports for litigation. Although service contracts are often an issue in private cloud arrangements (see above), they can present a far bigger issue for public clouds, where terms of service are (a) uniform across customers, (b) indifferent to, if not hostile to, backup restoration at the request of a customer, and (c) difficult or impossible to change via negotiation. For possession, custody, and control, these are key questions:

- Does the contract express disaster recovery in any terms other than uptime and restoration if there is a system failure?
- Does the contract provide for accessing backups or archives at the organization's request?
- Would the organization ever have the bargaining power to obtain such a provision?
- Even outside of the contract, could the organization obtain retention or restoration of backup(s) at some additional cost?

If the answers to these questions are all "no," then there is a reasonable argument that an organization lacks possession, custody, or control over whatever a cloud vendor is doing to protect against disaster – and therefore should not be required to produce from backups. This may not be an intuitive result, but it is the logical conclusion from existing legal principles. Of course, where there are contractual rights buried in the agreements, litigants have been caught by surprise by judicial conclusions that they had preservation and production obligations.

Two things do bear mention. One is that organizations do not have any general obligation under U.S. law to arrange their cloud systems (public or otherwise), so that backups can be retained and processed in response to legal matters that are not even on the horizon. Backup systems are a response to operational considerations and the general data governance principle that records should be stored in such a way that assures their survival for the duration of their retention period. In "peacetime," U.S. law prescribes retention periods for a small number of regulated industries, but organizations are otherwise free to organize their data systems and retain (or dispose of) data according to everyday business needs.

The other is that different rules apply in federal criminal investigations, and under many circumstances, an investigating agency will order the preservation of all data it considers relevant, including all backups of such data. Although this may be impractical with public cloud systems, it is important to make an effort to learn what can be done with these systems (if anything) and document it.

The Bottom Line

At the end of the day, attorneys and their client organizations should understand that the rise of cloud services has changed the landscape of discovery of backups – simultaneously making them less interesting to litigation and raising barriers to their restoration and production.

[1] Zubulake v. UBS Warburg LLC, 220 F.R.D. 215, 218 (S.D.N.Y. 2003).

[2] The NIST Definition of Cloud Computing, Special Publication 800-145 (NIST, Sept. 2011) at 2.

[3] Fed. R. Civ. P. 34(a)(1).

[4] Tank Connection, LLC v. Haight, No. 13-cv-1392-JTM-TJJ, 2015 U.S. Dist. Lexis 72604 at *16 (D. Kan. June 4, 2015).

[5] Mazzei v. Money Store, No. 01-CV-5694, 2014 U.S. Dist. Lexis 99850 at *8 (S.D.N.Y. Jul. 21, 2014).

[6] Ablan v. Bank of Am. Corp., No. 11-CV-04493, 2014 U.S. Dist. Lexis 164751 at *12 (N.D. Ill. Nov. 24, 2014) (where a party does not have a legal right to access data at a data provider, Fed. R. Civ. P. 34 is not the appropriate mechanism for discovery but Fed. R. Civ. P. 45 may be).

Cell Phones, Chat and E-Discovery

J.Stott Matthews
Spectrum Computer Forensics
and Risk Management, LLC

J. STOTT MATTHEWS is the founder and Managing Partner of Spectrum Computer Forensics and Risk Management LLC which was established over a decade ago. Prior to Spectrum, Matthews had over sixteen years of experience in the high-tech, manufacturing, and finance industries.

Matthews has spoken on the subject of electronic discovery and computer forensics, with audiences including litigators, courts, paralegals, and corporations. His expert work has included depositions as well as appearing in Federal and State courts as a computerforensics expert; he has been referenced as a computer-forensic expert in two Federal Court opinions (2006 and 2012) and his cases have been referenced nationally.

Increasingly, Matthews' practice has included data-breach-related cases, especially those involving health-care and credit-card data. Conducting security audits is a parallel service provided to clients in this industry, with a focus on the Security section of HIPAA.

Matthews has held computer-forensic and computer-security certifications, including the EnCase® Certified Examiner (EnCE) and Certified Information Systems Security Professional (CISSP). The ENCE certifies both public and private sector professionals in the use of Guidance Software's EnCase® computer-forensic software and illustrates that an investigator is a skilled computer examiner. The CISSP® is an independent information security certification governed by the International Information Systems Security Certification Consortium, commonly known as $(ISC)^2$.

Matthews also is a Professional Investigator, licensed by the State of Michigan, as currently required by state law.

Among his prior positions, Matthews served (i) as Director of Finance in the high-tech joint venture between DaimlerChrysler, Ford and GM, where he was a member of the executive team, (ii) as Vice President - Controller of Chrysler Corporation's Japanese subsidiary, and (iii) in the Corporate Audit department of DaimlerChrysler.

Matthews earned his MBA from the Columbia Graduate School of Business and his BA in Economics and East Asian Studies from Bucknell University, with a concentration in the Japanese language. He is an honorably discharged veteran of the United States military.

(866) 977-9779
jstott.matthews@spectrumforensics.com
www.spectrumforensics.com

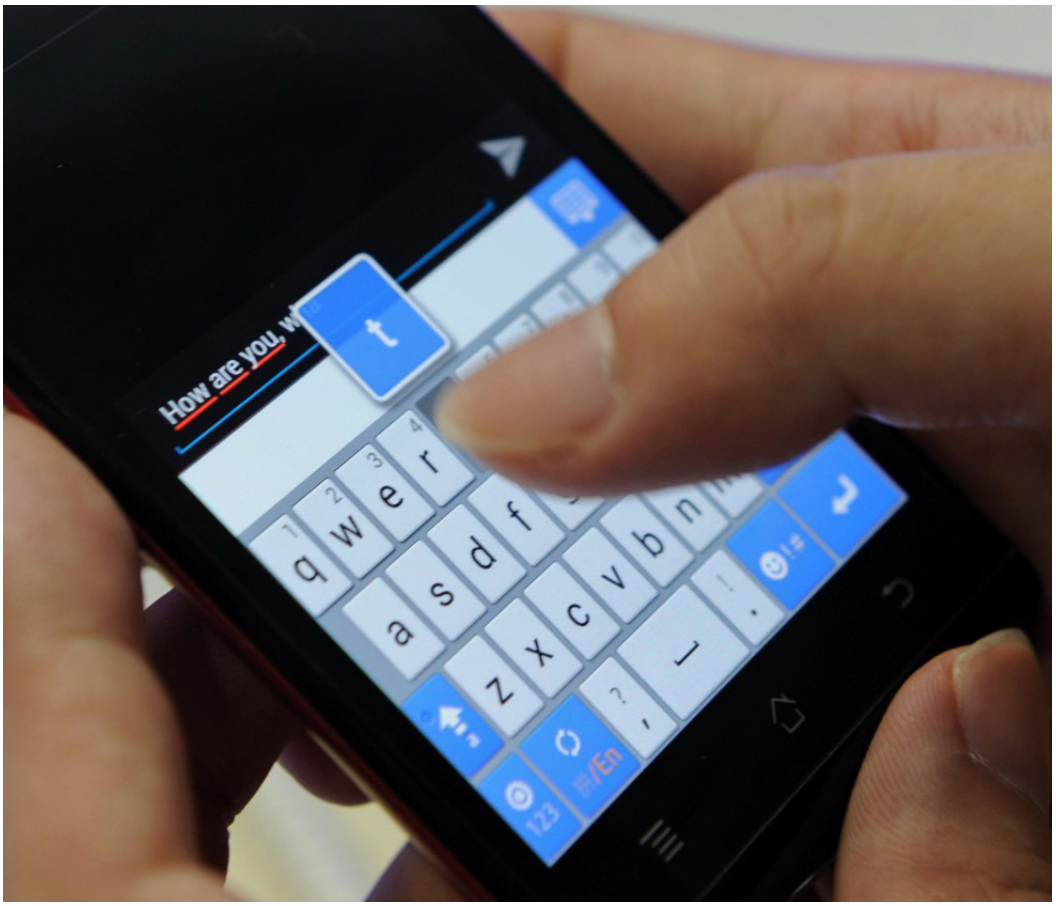
Cell Phones, Chat and E-Discovery

The cell phone in today's litigation environment is an essential source of electronically stored information ("ESI"). The most current set of high-end devices, like the iPhone 6, contain more processing power than the first PCs from the late 1980's and early 1990s. In recent years, there has been a rapid evolution in the use of cell phones. The ESI on a cell phone can be varied and broad—including photos, email, geo-location, Cloud-sourced business documents, and internet history. However, the most important data on a cell phone – in both criminal and civil litigation – is often the text messages, also known as "Chat" or "SMS" ("Simple Messaging Service").

As with any type of ESI, the ability to confirm the authenticity of a text message chain, string or thread (a "Chat") is an integral part of the litigation process. Since before the rise of Chat, litigators have leveraged the tools of computer forensics to establish the authenticity of files from laptop and desktop computers and computer servers. There was a time when it was fairly easy to assume that a litigant could go undetected in preparing a purely fictional Microsoft Word document or email message to serve as a key piece of evidence in a lawsuit. Computer forensics changed this; now, it is common knowledge that such shenanigans are often detectable. Just as computer forensics helped litigants establish and challenge authenticity with email and word processing documents, computer forensics is performing the same role for Chat.

Chat renders different challenges in terms of potential abuse for fake evidence creation than ESI such as email or word processing. It is common for Chat users to simply print or take a photograph of the "screen shot" of a Chat and present it to their lawyers as "proof" of the contents of a Chat. However, such photographs may fail to withstand evidentiary scrutiny because of the ease with which one can manipulate both the contact information and the Chat content. In order to understand the ease of creating a fake Chat, you can try the following on your own cell phone: (1) identify the contact information for a client or manager that you Chat with; (2) edit the contact information to replace the name with that of a relative (i.e. your mom or sister); and (3) take a screen shot of the resultant Chat history. If the result makes you uncomfortable, it should. It is easy to add or modify a user's contact information and generate a Chat that appears legitimate and alters the course of a lawsuit.

Criminal attorneys (especially those in Michigan familiar with the criminal prosecution of a former Detroit mayor) are now quick to recognize the particular evidentiary challenges of Chat, and this heightened awareness and scrutiny is seeping into civil litigation. As with other forms of ESI, the computer-forensics industry has developed tools and methodologies to capture the Chat that exists on a cellphone or similar device. These tools assist with establishing -- or challenging-- the authenticity of a Chat and give litigants greater certainty over the dates, times, content, and phone numbers related to a Chat. Where a Chat may be relevant, it is important for litigants and their attorneys to understand how this ESI was identified, preserved, and collected and to consider enlisting the assistance of a computer-forensics professional to assist where authenticity is important.



Practical Strategies for the Efficient Protection of the Attorney-Client Privilege

Megan McKnight
Plunkett Cooney

MEGAN MCKNIGHT is an attorney in Plunkett Cooney's Commercial Litigation and Banking, Bankruptcy and Creditors' Rights practice groups, who focuses her practice in the areas of financial and commercial litigation, as well as e-discovery and data privacy consulting.

A member of the firm's Bloomfield Hills office, Megan has extensive experience representing financial institutions and corporate clients in a range of matters, including commercial contract disputes, consumer financial services defense, loan defaults and workouts, complex collection actions, lender liability defense, fraud and other misconduct, and real estate disputes.

Megan is routinely consulted to troubleshoot and resolve electronic discovery issues. She's admitted to practice in the state, federal and bankruptcy courts in Michigan, and state and federal courts in Illinois.

248-901-4018 | *mmcknight@plunkettcooney.com*
www.plunkettcooney.com

Practical Strategies for the Efficient Protection of the Attorney-Client Privilege

The sanctity of attorney-client communications and attorney work-product is a bedrock principle of our legal system. It exists to encourage clients to be candid and truthful with their attorneys, so that the attorneys are empowered to provide the best advice and most effective representation. However, in our era of communication overload and big e-discovery—which shows no signs of slowing—preserving the attorney-client privilege and work-product protection during discovery is often a huge burden. Reviewing responsive information for privilege prior to production and logging documents withheld on the basis of privilege is tedious and expensive work. Privilege disputes, though occasionally interesting to the lawyers, rarely advance the merits of a lawsuit or pique the interest of clients. Unless the attorney-client privilege is declared a casualty of the end of privacy (or of sheer expense) attorneys should consider seeking both (1) a tailored FRE 502(d) Order and (2) a customized order that sets the expectation for asserting the privilege over particular information.

1. Obtain a FRE 502(d) Order

In order to reduce the risk of waiving an important attorney-client privilege or work-product protection, attorneys should consider seeking an order pursuant to Fed. R. Evid. 502(d) (a "FRE 502(d) Order") to the effect that no disclosure of privileged information will result in waiver. Alternatively, attorneys may seek an order that affirms the parties' agreement that any disclosure is ipso facto inadvertent, or that the steps being taken to attempt prevent the disclosure of privileged information are reasonable.

Prior to 2006, there was a real risk that the disclosure of privileged information —regardless of how determined a party had been to keep it confidential or how big the error that resulted in the disclosure —would result the waiver of that privilege. Since 2006, Fed. R. Evid. 502(b) has codified a three-pronged safe-harbor that protects a party's privilege where the party (1) inadvertently discloses privileged information, (2) takes reasonable steps to prevent the disclosure; and (3) takes reasonable steps to rectify the error. While the likelihood that an expansive waiver will result if a single document is miscoded is now reduced, the revised rule has created three new opportunities for litigation over "inadvertence," and "reasonable steps". Accordingly, attorneys and their clients should consider whether different parameters are appropriate for a given case.

FRE 502(d) Orders that override the safe-harbor requirements in Fed. R. Evid. 502(b) —with their associated fact-finding —are increasingly common and can provide enhanced predictability and further reduce the risk of a privilege waiver. The Federal Rules of Evidence Advisory Committee contemplated that parties may enter into such order, explaining in the Notes to the Fed. R. Evid. 502 that, "a court order may provide for return of documents without waiver irrespective of the care taken by the disclosing party; the rule contemplates enforcement of "claw-back" and "quick peek" arrangements."

Nonetheless, attorneys and clients should exercise caution as protecting truly sensitive privileged communications remains important. While a broad FRE 502(d) Order may protect your client from waiver (and you from malpractice), **information once learned by your adversary cannot be unlearned.** I have been on both sides of an inadvertent disclosure of privileged information. Recently, I was given a report prepared by a consulting expert hired by my adversary that thoroughly analyzed the strengths and weaknesses of my adversary's primary defense. Although I advised opposing counsel and destroyed the privileged memo, the knowledge I gained could not be returned. I believe that the disclosure of this memo changed the course of the litigation and led to a favorable settlement for my client. The accidental disclosure of this memo did not result in a privilege waiver but its harm was significant. Further, while the scope of the harm in my recent case was limited to that single dispute, the potential harm is significantly increased for parties that face repeated lawsuits with the same parties or opposing counsel, where the knowledge gained as a result of one error in one case can be a road map for the next case. In sum, while a FRE 502(d) Order can attempt to mitigate some of the risk and reduce some of the costs, it cannot protect a party from a minor mistake causing significant harm.

2. Tailor Privilege Log Requirements.

To reduce the burden of asserting the attorney-client privilege or attorney work-product protection, attorneys should consider prophylactically seeking an order that sets the parameters of how a party is to assert the privilege. The traditional practice of creating a document-by-document privilege log does not make sense when it means thousands or hundreds of thousands of records. The flexibility of Fed. R. Civ. P. 26(b)(5) has led federal courts to impose vastly disparate requirements on parties withholding documents on the basis of privilege or work product. Fed. R. Civ. P. 26(b)(5) requires that a party asserting the privilege disclose, "the nature of the documents, communications, or tangible things not produced or disclosed -- and do so in a manner that, without revealing information itself privileged or protected, will enable other parties to assess the claim." While the Federal Rules of Civil Procedure Advisory Committee's notes to Rule 26 (written in 1993!) contemplated the use of categorical privilege logs, widespread adaptation has been slow. Since different interpretations of Fed. R. Civ. P. 26(b)(5) can implicate widely varying resources, it is wise to set try to expectations early.

In 2009, the Hon. John M. Facciola and attorney Jonathan M. Redgrave developed one of the first systematic frameworks for addressing privilege issues in big e-discovery cases and popularized the concept of categorical privilege logs. Since that time, the use of categorical privilege logs —whereby a single entry will correspond to several documents, rather than document-by-document logging—has been gaining traction in both federal and state courts. In 2014, the rules of the state courts in New York were amended to include an express preference for categorical privilege logs. Federal courts have approved the use of various streamlined logging processes, including those set forth in the Facciola-Redgrave Framework, where document-by-document review and logging is unwieldy.

In many cases, a robust combination of (a) categorical limitations; (b) fully detailed document-by-document logging within specific categories; (c) use of available technological tools; and (d) early attention to common concerns, is the optimal approach to allow parties to focus on the truly controversial privilege assertions. While the factors that parties should consider to reduce the burden of asserting the privilege will vary on a case-by-case basis, the following are examples of common items for consideration:

Considering Common Categorical Limitations:

- Excluding communications to/from litigation counsel
- Excluding documents/communications created post-litigation
- Excluding or including documents to/from specific attorneys or consultants
- Limiting the logging of documents to particular date ranges

Using All Tools Available:

- Using predictive coding or other technology assisted review to identify privileged documents
- Using search terms and other delimiters to identify privileged documents
- Using sampling, either with opposing counsel or for the purpose of an in camera review with the court.

Addressing Email-Specific Concerns Early:

- Determining how email chains will be handled. Does one privileged email mean the entire chain should be withheld? Or, does a party have to redact the non-privileged emails in a given chain? Does each email in a chain have to be logged, or is logging the top (i.e., most recent) email in the chain adequate?
- Reaching agreement on how emails will be logged. Is it adequate to only include in the privilege log information that can be automatically populated your e-discovery software? How should the "subject" field should be treated?

As with FRE 502(d) Orders, attorneys and their clients should be cautious. There is a risk that parties will use more flexible logging standards to withhold documents whose claim to privilege is tenuous or bury responsive and relevant information. However, dedicating attention to how the privilege is asserted should force parties to focus on the truly controversial issues and deter parties from using privilege review and logging as a way to increase litigation costs and divert an adversary's attention from the merits of the case.

Conclusion

The use of FRE 502(d) Orders and orders that address expectations regarding assertions of the privilege may both reduce the risk of a privilege waiver and reduce the cost associated with protecting the privilege.

Technologically Simple

Mark St. Peter
Computing Source

MARK ST. PETER is CEO and Managing Director of Computing Source, an all-in-one legal technology and support firm with offices in Madison Heights, Detroit, Ann Arbor, Birmingham, Grand Rapids, Chicago and Indianapolis. In his role, St. Peter develops and executes the company's strategic vision, oversees long-term growth of the company, and manages day-to-day operations.

St. Peter founded Computing Source in 2001, and has spent the past 13 years developing the firm into the largest provider of legal support in Michigan—with the past two years being a time of much growth. Under St. Peter's leadership, the company grew from 20 to more than 100 team members, opened new offices in Ann Arbor, Grand Rapids, Chicago and Indianapolis, acquired demonstrative evidence and trial presentation firm Evidence Express, acquired MuniDeals, a financial printing company specializing in the distribution of municipal bond offering documentation, and more than doubled its services in order to serve as the single-source solution for law firms, corporate counsel and other clients throughout the region.

In addition to his work with Computing Source, St. Peter regularly serves as an expert witness for law firms, corporate counsel and judges. St. Peter is a Certified Fraud Examiner, a Certified Computer Examiner and an Associate Member of the American Bar Association.

(248) 213-1500
msp@computingsource.com
www.computingsource.com

Technologically Simple

A century-old observation remains surprisingly relevant in a litigation landscape that increasingly revolves around the ability to understand and leverage technology and high-tech tools

At a time when technology and technical issues seem to be adding new layers of complexity and new challenges to the litigation process, it is helpful to remind oneself that there truly is nothing new under the sun–and that the answers to some very modern challenges can be found in age-old wisdom that is anything *but* modern.

In fact, the ideas of an Italian economist named Vilfredo Pareto, who presented what became known as the "Pareto Principle" in the late 19th and early 20th centuries, are still very much relevant today. In fact, those ideas can be applied directly to the 21st-century practices of electronic discovery and computer forensic services.

The Pareto Principle was inspired by Pareto's pioneering work describing the unequal distribution of resources in society. It states that, in many cases, 80% of the effects of something can be attributed to 20% of the causes. While he developed this notion in the process of analyzing the distribution of wealth, this principle (which is also popularly referred to as the 80/20 Rule) holds true in a wide range of circumstances and can be applied to a number of data sets and scenarios.

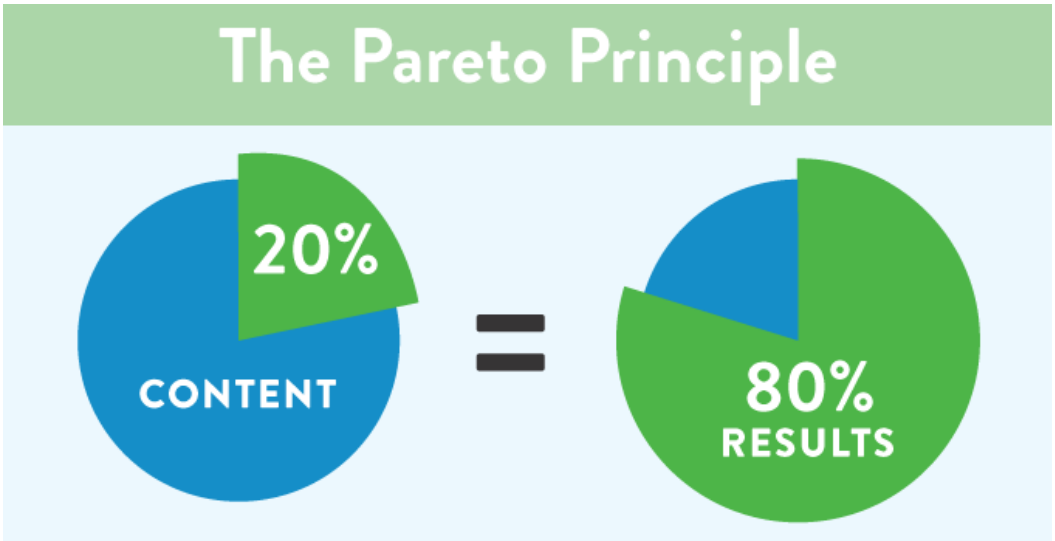
In fact, this analog analysis is perhaps even more relevant in the screen-lit world of today's increasingly digital reality. The Pareto Principle is a powerful tool precisely because it addresses complexity so neatly and so intuitively. While it might seem unusual to deploy ideas that were conceived and refined in a very different era and context to the newest problems of today, the message of the 80/20 Rule is clear: *simplicity works*.

As any experienced provider of digital forensic services can attest: simple beats complicated every single time. Pareto's Principle can be successfully applied to almost any case that requires sifting through or managing large amounts of information. In fact, the 80/20 Rule applies basically across the board in the practice of electronic discovery and computer forensics. Almost without exception, the vast majority of relevant/targeted material will be found in a relatively small subset of the larger data set.

Not only does this notion serve as a guiding principle, it also points the way to some very practical and useful strategies that be used to apply its insights when trying to separate the virtual wheat from the digital chaff. Narrowing the scope of search in any digital investigation is an important first step, and the Pareto Principle provides a formula for how to proceed. It also helps to correct a common misconception about computer forensics and digital evidence retrieval: that technical obstacles are the biggest stumbling block. The reality is that logistical challenges are the most formidable, and the time and expense involved in the e-discovery process can be significant. With that in mind, a framework like that set forth by the Pareto Principle is arguably the single best way to lower costs and tighten e-discovery timelines. While technical capabilities and high-tech experience will always be essential, technical experts and legal professionals who can effectively narrow their search window and find what they are looking for faster and more efficiently will be in the highest demand.

Consider a real-world example of the Pareto Principle in action. An investigation begins to gather evidence for potential litigation. As is so often the case, the first step is to search through all the email accounts of persons involved in the case to look for relevant data. Instead of a scattershot search, however, a wise first step would be to organize emails by quantity or frequency of appearance. A review of the top 100 or so names on the list of correspondence almost always reveals an unexpected or unusual name. It is remarkable how often this person turns out to be a key witness, or to be the source of important evidence or information.

Litigation attorneys would be wise to familiarize themselves with providers of electronic discovery and computer forensic services who practice these principles and techniques, think outside the box, and who can deliver the speed, accuracy and affordable quality that those techniques make possible. From forensic imaging of hard drives, to finding lost or deleted data, to detailed analyses of online activity, and the recovery and management of critical data, *simplicity* is key. That simplicity can make a difference both to the bottom line, and to the final outcome of a case. The challenges are new, and the principle is over one-hundred years old, but those priorities are timeless.



Less Predictable Uses of Predictive Coding

Angela Emmerling Shapiro
Butzel Long

ANGELA EMMERLING SHAPIRO is a litigation shareholder based in Butzel Long's Ann Arbor office and the Chair of the firm's Women's Leadership Committee. She has more than fifteen years of experience in all aspects of litigation but her passion is electronic discovery. Angela has earned her CEDS certification (Certified eDiscovery Specialist) and was named a 2014 "Top Lawyer" in the area of Information Management and eDiscovery by DBusiness Magazine.

Angela routinely works with clients to navigate complicated electronic discovery issues in the context of litigation and governmental investigations (DOJ, NHTSA, etc.) as well as antitrust and other internal audits. She oversees all stages of the electronic discovery life cycle, including information management, developing and executing preservation plans, working with IT and vendors to data map and collect data, creating efficient review workflows, assessing and utilizing technology assisted review where appropriate, managing contract reviewers, negotiating production protocols and approving final deliverables for production. She has also litigated electronic discovery issues, including spoliation.

(248) 258-2504
shapiro@butzel.com
www.butzel.com

Less Predictable Uses of Predictive Coding

Predictive coding as an alternative to large scale linear document review has received a great deal of attention over the past several years. Using a sophisticated algorithm to help predict whether a document is relevant (or to rank potential relevance) can lead to a more cost-effective, efficient, and even more accurate review.

Many litigation attorneys and clients still shy away from predictive coding, though, often because they are concerned about defensibility and work product issues. For example, the prospect of being called upon to disclose what documents were reviewed to "train" the predictive coding program while preparing your client's production makes attorneys and clients alike apprehensive – especially when privileged or completely irrelevant yet sensitive documents are at issue. These are valid concerns, at least until more uniform guidance is provided by the courts.

Predictive coding has other uses, though, that should not raise the same concerns yet still offer significant benefits.

For example, you can use predictive coding or other technology assisted review to identify strengths and weaknesses in your client's case at the earliest stage of anticipated litigation. This is called Early Case Assessment ("ECA"). Using a computer to help rapidly weed through your client's information can help identify the handful of truly key documents and witnesses from the outset. Thus, risks can be more thoroughly assessed and a meaningful settlement or litigation strategy developed before anyone steps foot in a courtroom.

Predictive coding can also be used to analyze incoming document productions. The ability to quickly digest and rank large data dumps from an opposing or third party can be critical when faced with aggressive discovery deadlines. Once documents are ranked you can then determine how best to tackle further analyses. For example, you might elect to review documents ranked in the top 10% yourself while associates look at the next 20% and contract attorneys sample from the remaining 70%.

Further, there are multiple ways predictive coding can be used to streamline the review of your client's own documents before production without using the technology to eliminate any documents from review (the point at which some will argue that training materials should be disclosed). For example:

- If you and opposing counsel negotiate traditional keyword searches to identify the universe of potentially relevant documents, you can use predictive coding to organize and prioritize review of that universe by your team, devoting more costly attorney resources to higher-ranked documents. This strictly involves prioritizing and organizing documents, not removing or skipping any from the review universe;
- You can rank documents by the likelihood of privilege and then assign the top tier of results to your privilege log team; or
- You can run predictive coding across the universe of documents reviewed by your team to compare coding decisions and to revisit inconsistently-coded documents before production.

Using predictive coding for ECA or to supplement/organize traditional reviews in the ways discussed above allows you to leverage some of the strengths of the technology without triggering an even arguable obligation to make disclosures to (or obtain buy-in from) opposing counsel or the court. These less predictable uses of predictive coding carry very little risk but huge potential for reward in cases with large amounts of data.

www.fbamich.org | EDMI Model Order

Dante A. Stella
Dykema
400 Renaissance Center
Detroit, MI 48243
TEL: (313) 568-6693
FAX: (313) 568-6893
dstella@dykema.com
www.dykema.com

J. Stott Matthews
Spectrum Computer Forensics & Risk Management
32440 Susanne Drive
Franklin, MI 48025
TEL: (866) 977-9779
jstott.matthews@spectrumforensics.com
www.spectrumforensics.com

Megan McKnight
Plunkett Cooney
38505 Woodward Ave.
Suite 2000
Bloomfield Hills, MI 48304
TEL: (248) 901-4018
FAX: (248) 901-4040
mmcknight@plunkettcooney.com
www.plunkettcooney.com

Mark St. Peter
Computing Source
29401 Stephenson Highway
Madison Heights, MI 48082
TEL: (248) 213-1500
FAX: (248) 213-1501
msp@computingsource.com
www.computingsource.com

Angela Emmerling Shapiro
Butzel Long
41000 Woodward Ave,
Stoneridge West
Bloomfield Hills, MI 48304
TEL: (248) 258-2504
FAX: (248) 258-1439
shapiro@butzel.com
www.butzel.com

Federal Bar Association
PO Box 20759
Ferndale MI 48220
fbamich@fbamich.org

Courthouses:

Detroit
313.234.5300

Ann Arbor
734.741.2075

Flint
810.341.7890

Bay City
989.894.8830

Port Huron
313.226.2547

FEDERAL BAR ASSOCIATION
Eastern District of Michigan Chapter