MAYER·BROWN

Electronic Discovery & Information Governance

2017 TIPS OF THE MONTH - A Compilation

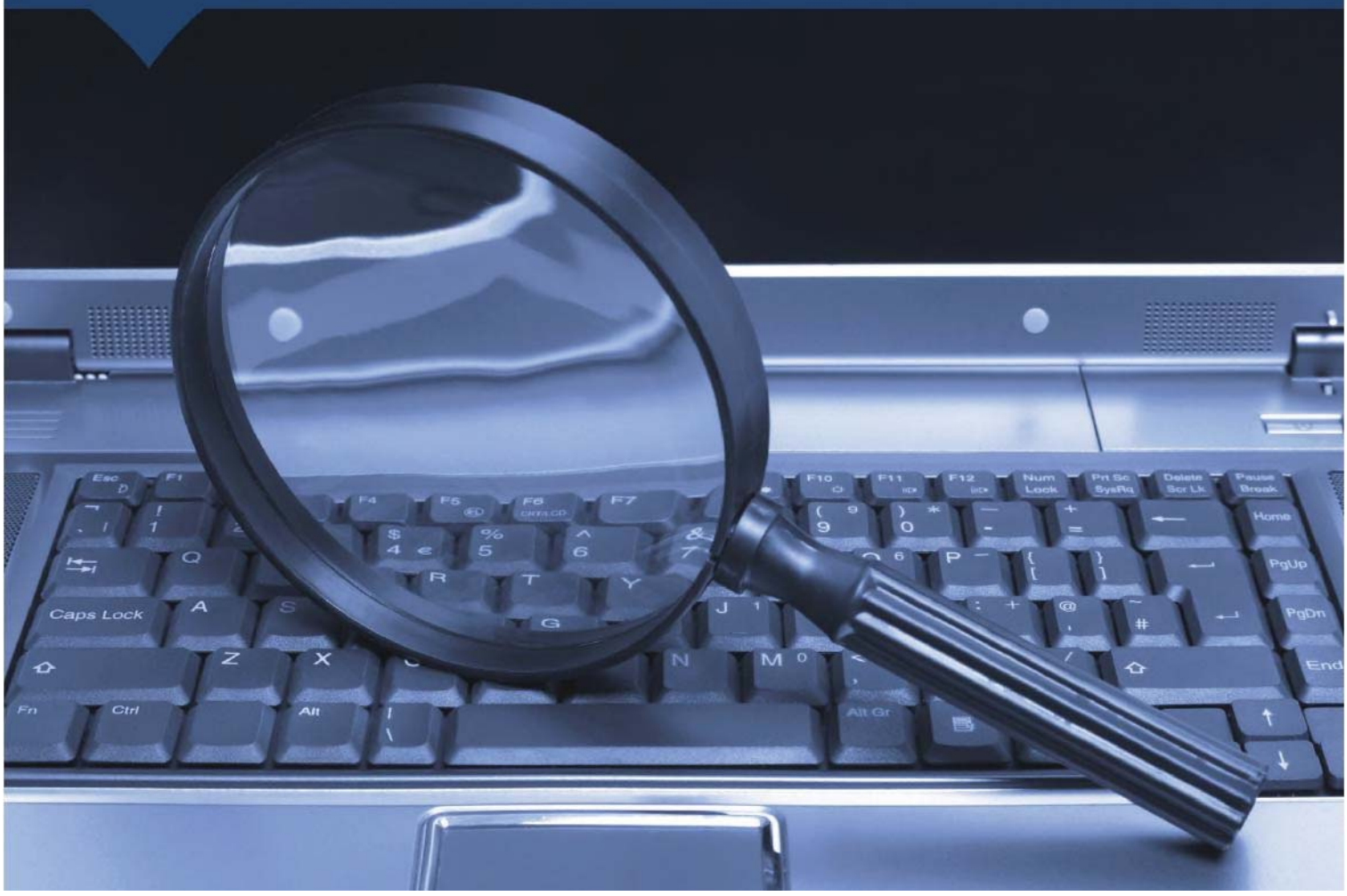


Table of Contents

Introduction

In 2017, several principles in electronic discovery and information governance were reaffirmed, albeit with contemporary variations to account for the ever-shifting technological landscape. The most recent revisions to the Federal Rules of Civil Procedure ("FRCP" or "Federal Rules") were widely discussed, with courts affirming established doctrines, and the legal scholars at the Sedona Conference provided further guidance on best practices for the treatment of electronically stored information ("ESI") in litigation. At the same time, new developments in e-discovery emerged last year. Discussions surrounding cybersecurity and data privacy evolved; self-authentication of evidence expanded under the Federal Rules; and two federal districts began participating in an initial discovery pilot program that radically alters parties' discovery responsibilities.
These topics—and others—were discussed in Mayer Brown's Electronic Discovery & Information Governance practice's Tip of the Month series in 2017.

Proportionality

Over the past year, legal practitioners continued to grapple with the expanding scope of electronic discovery. Courts and legal scholars alike stressed the importance of balancing parties' discovery needs in prosecuting or defending cases with limiting the sometimes-crippling costs of document preservation, collection, review and production.

- **Amendments to Federal Rule 26**. One of the noteworthy changes to the Federal Rules in December 2015 concerned the so-called proportionality principle governing the scope of discovery, which seeks to rein in unrestrained discovery requests and concomitant costs. While some version of the proportionality principle has been part of the Federal Rules ever since 1983, the drafters of the 2015 amendments sought to restore proportionality as an explicit component of the scope of discovery in FRCP 26(b)(1), particularly in relation to ESI. In the past year, judicial decisions that discussed both proportionality and limiting discovery to reasonably accessible data did not address the tension between the two. Instead, courts have defaulted to the traditional burden evaluation. Parties resisting overbroad discovery requests should be prepared to argue that information sought is either not reasonably accessible due to undue burden or cost or is not proportional to the needs of the case, or both.
- **Sedona Conference**. The judges, lawyers, academics and other experts who comprise the Sedona Conference agree with this sentiment. In March 2017, the Sedona Conference Working Group on Electronic Document Retention and Production ("WG1") published the third edition of the influential Sedona Principles. WG1 sought to convey "a reasonable and balanced approach" to the treatment of ESI in the legal process. As did prior editions, the third edition promoted the need for proportionality—in both ESI preservation and production. Attempting to navigate the proportionality and accessibility concepts of Rule 26, WG1 advised that the primary sources of ESI to be preserved and produced should be those readily accessible in the ordinary course; only when ESI is unavailable through such primary sources should parties move down a continuum of less accessible sources, until the information requested is no longer proportional to the needs of the case.

New Developments

In addition to affirming the principles of proportionality and reasonable accessibility in a theoretical manner, rising litigation costs were addressed in practical ways for the very first time last year.

- **The Mandatory Initial Discovery Pilot Project**. In mid-2017, the District of Arizona and the Northern District of Illinois became the first districts to participate in the Federal Judicial Center's Mandatory Initial Discovery Pilot Project ("MIDP"). MIDP, which aims to reduce the cost and delay of civil litigation, substantially alters what would otherwise have been parties' obligations under the Federal Rules with respect to the scope of the initial disclosures and the timing for discovery. Litigants and counsel in these jurisdictions are advised to review carefully MIDP's requirements in order to avoid missing deadlines and risking a default. Lawyers in other jurisdictions also should be aware of the changes that MIDP institutes, in the event that additional districts decide to join the project.
- **Self-Authentication of ESI**. Federal Rule of Evidence 902 governs certain types of evidence that are considered to be self-authenticating, i.e., those that do not require extrinsic evidence of authenticity to be admitted at trial. Amendments to this rule, which took effect on December 1, 2017, change the process for admitting certain ESI into evidence. The amendments added two new paragraphs permitting a party to self-authenticate certain types of electronic evidence: 902(13) allows for self-authentication of records generated by an electronic process or system that produces an accurate result, and 902(14) permits self-authentication of data copied from an electronic device, storage medium, or file if the data is authenticated by a process of digital identification. Types of data that would fall under these rules could include web pages, emails, text messages and cell phone photos. Under the amended Rule 902, proponents seeking to introduce these types of ESI into evidence no longer need to summon a live witness to the stand in order to provide extrinsic evidence of authenticity; rather, a party will be required simply to provide a certification by a foundation witness to establish the authenticity of the evidence.

Technological Competence

The developments described herein are likely to affect nearly all litigants—as well as litigation counsel—as issues pertaining to electronic discovery permeate nearly every dispute. Failure to keep abreast of technological advancements could result in unwanted consequences.

- **Cloud-Based File Sharing**. Cloud storage sites have been used in litigation as a method of sharing information. Users, however, should ensure that they are familiar with how such systems work and should take measures to limit unauthorized access to the confidential information stored on these sites. A recent case in Virginia illustrates the point. In *Harleysville Ins. Co. v. Holding Funeral Home, Inc.*, No. 1:15-cv-00057, 2017 WL 1041600 (W.D. Va. Feb. 9, 2017), the plaintiff, an insurance company, uploaded its entire investigation file—including information potentially subject to the attorney-client privilege and work product doctrines—to a cloud-based Box account. However, the plaintiff negligently failed to establish any further access control over the file. When a hyperlink to that account was produced during discovery, defense counsel downloaded the entire file, including the potentially privileged information. Likening the plaintiff's conduct to "leaving its claims file on a bench in the public square," the magistrate judge found that the disclosure was not inadvertent and held that the plaintiff had waived any privilege claim over the information posted to the site. Although the district court sustained, in part, the

plaintiff's objections to the magistrate judge's order and reversed the waiver finding, the facts of the case nevertheless provide a cautionary tale.

- **Applicability to Lawyers**. Lawyers must also take special care to protect the confidential information they store and disseminate. The New York County Lawyers Association's ("NYCLA") Committee on Professional Ethics issued an opinion in 2017 providing guidance for lawyers on protecting a client's confidential information that is stored and transmitted electronically, as well as in the context of conducting e-discovery. The NYCLA opinion said that lawyers practicing in New York owe their clients a duty of competence that "expands as technological developments become integrated into the practice of law." The opinion states that a lawyer must use reasonable care when transmitting information electronically; must understand the risks associated with the use of technology, including the threat of cyber attacks and inadvertent disclosures; and must either personally possess, or associate with persons who possess, sufficient understanding of the technology at issue. The opinion details concrete steps lawyers can take to meet their duty of competence as it relates to e-discovery.

For inquiries related to this, please contact Noah Liben at nliben@mayerbrown.com or Ethan Hastert at ehastert@mayerbrown.com.

To learn more about Mayer Brown's Electronic Discovery & Information Governance practice, contact Michael E. Lackey at mlackey@mayerbrown.com, Eric Evans at eevans@mayerbrown.com or Ethan Hastert at ehastert@mayerbrown.com.

Visit us at mayerbrown.com.

ELECTRONIC DISCOVERY & INFORMATION GOVERNANCE

Tip of the Month

ESI Discovery Challenges of the Internet of Things

Scenario

A US consumer products manufacturer plans to launch a line of smart products for the kitchen ranging from coffee makers to refrigerators capable of gathering data on customer use and performance that will be used to improve the user experience. Further, the new product line includes a smartphone application that allows users to remotely control the appliances. Tasked with conducting a risk assessment of this product line before mass production, the general counsel wants to identify potential issues relating to data created and stored by these smart products.

The Internet of Things

Over the last few years, the use of connected devices has become widespread among consumers and businesses. From thermostats to cars, countless objects now can collect, store and transmit data. The vast network of these connected objects is often called the "Internet of Things" (IoT). IoT devices include smart home technology allowing consumers to control locks, alarm systems, lights and thermostats through their mobile phones; wearable devices monitoring health and fitness; smart cars that offer driver-assist features; and more. IoT technology also is increasingly being used by businesses. Smart manufacturing uses IoT to track assets, monitor inventory and automate factories. Health care providers use IoT technology to track pharmaceuticals, monitor patients' health and send information to doctors. And utilities use smart grid technology to gather data regarding power use and outages.

While this ability to send and receive data provides powerful tools to improve consumer experience and gather information about consumer behavior, IoT presents several information governance and discovery challenges concerning data privacy, information security, and data preservation and extraction.

Data Privacy

The data collected by IoT devices may be subject to privacy regulations and can raise other issues relating to consumers' expectations that certain information will remain confidential. Some voice-controlled IoT devices, such as smart televisions or smart speakers, can (advertently or inadvertently) record conversations users expect to be private. Similarly, connected devices with cameras may record video or capture images without consumer knowledge. Many IoT devices collect, store and transmit sensitive consumer information such as geolocation information, payment details and health data, all of which may implicate state and federal privacy laws. Depending on where the servers storing such data reside, foreign data privacy laws also could

apply.

To ensure compliance with data privacy laws, it is important that companies pay particular attention to the nature of the data being gathered by the device and where the data are being stored. To minimize the risks associated with the inadvertent disclosure of private information, best practices include establishing consent, use and disclosure policies regarding the collection, storage and use of data (including the use of just-in-time notices for the collection of more sensitive information) and minimizing the collection and use of personally identifiable information.

Information Security

IoT devices also present data security concerns. Hackers may target an IoT device to obtain information stored on or communicated by the device. Even more problematic, hackers may attempt to gain control of the device itself either to manipulate it or use it as backdoor into company servers, which puts the enterprise at risk of a large-scale data breach.

To guard against such attacks, companies should consider implementing security safeguards and practices, including engaging an IT security vendor to test the IoT devices and related network to identify potential vulnerabilities. Further, data collected or transmitted by an IoT device and data stored on company servers is substantially more secure if it is encrypted while at rest. If the company is using a third-party storage provider, that provider's security policies and procedures should be fully vetted. The company should also test its software update processes to ensure that security solutions can be delivered in an effective and efficient manner.

Discovery of IoT Devices

Just like traditional forms of electronically stored information ("ESI"), potentially relevant information from an IoT device will be discoverable in a litigation. But the discovery of ESI on IoT devices presents some unique challenges, which include the relationship of the data owner to the litigation, producing the data in a usable format, separating relevant information from the massive amounts of data collected by IoT devices and maintaining consumer confidentiality.

Data collected by an IoT device may reside on the device only temporarily, if at all, before being transferred to a remote server. Due to the cost savings of outsourcing data-hosting services, IoT device data is often stored on third-party servers. While the data may technically be in the possession and custody of the service provider, under most circumstances the device manufacturer maintains control over the data for purposes of triggering a party's preservation obligations under the Federal Rules of Civil Procedure. As part of a comprehensive information governance program, companies contemplating the use of a third-party data storage provider should evaluate the service provider's ability to comply with company data retention policies, including the preservation of data, and to retrieve and deliver company data when necessary.

Conclusion

In addition to their unique benefits, IoT devices present unique information governance and discovery challenges. Companies should consider the potential privacy implications of information gathered by IoT devices and implement data security procedures to prevent the inadvertent disclosure of data. Should litigation arise, data retention policies that ensure proper preservation of information and allow the sorting and production of data will help facilitate the discovery process.

For inquiries related to this Tip of the Month, please contact Lilya Mitelman at lmitelman@mayerbrown.com and Michael Battaglia at mbattaglia@mayerbrown.com

To learn more about Mayer Brown's Electronic Discovery & Information Governance practice, contact Michael E. Lackey at mlackey@mayerbrown.com, Eric Evans at eevans@mayerbrown.com, Ethan Hastert at ehastert@mayerbrown.com, or Edmund Sautter at esautter@mayerbrown.com.

Please visit us at www.mayerbrown.com.

ELECTRONIC DISCOVERY & INFORMATION GOVERNANCE

Tip of the Month

Preparing to Comply with the EU General Data Protection Regulation

Scenario

A multi-national manufacturing business has its headquarters in the United States but also has substantial manufacturing and research and development facilities in Europe. The US-based general counsel wants to be prepared to comply with the EU General Data Protection Regulations ("GDRP").

The new GDPR will come into force throughout the European Union on May 25, 2018. The GDPR will replace existing data protection laws throughout Europe and introduce significant changes and additional requirements that will have a wide-ranging impact on businesses around the world, irrespective of where they operate.

The GDRP Changes That Will Affect Your Business:

Some key changes and additional requirements introduced by the GDRP are:

1. **Worldwide application of European data protection law.** In a significant departure from the current requirements, in addition to businesses that are established in the European Union, organizations that are located outside the European Union that process personal data in relation to the offer of goods or services to individuals within the European Union, or as a result of monitoring individuals within the European Union, will have to comply with European data protection law. Non-EU-based businesses will need to consider whether they will be subject to the new rules and, if so, how they will comply.

2**. Tougher sanctions for non-compliance**. The maximum fine for a breach of European data protection law will be substantially increased to 4 percent of an enterprise's worldwide turnover or €20 million per infringement, whichever is higher.

3. **A new data breach notification obligation**. Organizations will now have to notify the relevant European data protection authority of a breach without undue delay and where feasible within 72 hours. A notification must also be made to the individuals affected without undue delay where there is a high risk to them.

4. **New data privacy governance, data mapping and impact assessment requirements**. Many organizations will now need to appoint a data protection officer to be responsible for implementing and monitoring that organization's compliance with the GDPR and to carry out assessments of an organization's data processing in certain circumstances. Organizations will now also be required to map their processing of EU personal data and undertake data protection

impact assessments for higher-risk processing.

5. **A requirement to implement "privacy by design**." Businesses must now take a proactive approach to ensure that an appropriate standard of data protection is the default position taken when EU personal data is being processed.

6. **Strengthening of individuals' rights to personal data.** Individuals in the European Union will have these rights: (i) to have their personal data removed from systems or online content (the "right to be forgotten"), (ii) to not be subjected to automated data profiling (where this would produce a legal effect) and (iii) to be given a copy of the personal data relating to them in a commonly used format and to have that information transmitted to another party (the "right to data portability"). Organizations must determine how they will enable individuals to exercise these rights.

Preparing for the GDPR:

If a preliminary assessment determines that your business will have to comply with the GDPR, you should consider taking these steps:

- **Inform your leadership and formulate a plan**. Senior management should be made aware of the changes to data protection law and how it will affect your business. Senior management should designate the individuals who will formulate a plan for implementing the GDPR requirements and who will educate the wider workforce on its operational impact.
- **Map your personal data.** A detailed investigation should be conducted into and a record created of the personal data your business is collecting in relation to the offer of goods or services to individuals in the European Union, the purposes for which it is being processed, the ways it was obtained and the parties that it is being shared with.
- **Examine the impact**. The information gathered from the personal data mapping exercise should be used to assess which parts of your business and which data processing activities must comply with the GDPR.
- **Address the risks**. Data protection impact assessments should be conducted to identify and minimize the risks associated with the processing of personal data by your business, particularly where there are high risks to the rights and freedoms of the individuals concerned by the activities that are being or are going to be carried out.
- **Update your data governance.** Policies, procedures and other governance controls within your business should be updated to detail how your organization will practically comply with the new requirements under the GDPR. Employees should receive training on and should be regularly updated about this.
- **Review your supply chain contracts**. The contracts with the service providers and other parties that your business shares personal data with should be reviewed and, where necessary, renegotiated to ensure that your organization is appropriately supervising the manner in which they process personal data and are complying with their obligations under the GDPR.
- **Assess your international transfers**. Assess the manner in which you currently carry out any international transfers of personal data and whether any mechanisms for carrying out these transfers within your organization or to third parties need to be updated to comply with the European data protection requirements.

For more information and to learn how Mayer Brown's GDPR Readiness Service can help you prepare for GDPR compliance, visit Mayer Brown's GDPR page or contact any of the following:

Oliver Yaros at +44 20 3130 3698, Mark Prinsley at +44 20 3130 3900, Charles-Albert Helleputte at +32 2 551 5982, Dr Guido Zeppenfeld at +49 69 7941 1701, Rebecca Eisner at +1 312 701

8577, Lei Shen at +1 312 701 8852, Rajesh De at +1 202 263 3366, David Simon at +1 202 263 3388, Kendall Burman at +1 202 263 3210 or Gabriela Kennedy at +852 2843 2380.

For inquiries related to this Tip of the Month, please contact Mark Prinsley at mprinsley@mayerbrown.com and Kim Leffert at kleffert@mayerbrown.com.

To learn more about Mayer Brown's Electronic Discovery & Information Governance practice, contact Michael E. Lackey at mlackey@mayerbrown.com, Eric Evans at eevans@mayerbrown.com or Ethan Hastert at ehastert@mayerbrown.com.

Please visit us at www.mayerbrown.com.

ELECTRONIC DISCOVERY & INFORMATION GOVERNANCE

Tip of the Month

Protecting Information on Cloud-Based File Sharing Services

Scenario

A company is in the process of setting up a cloud-based file sharing service. The general counsel is concerned about, among other things, protecting unauthorized access to confidential and privileged materials she and others intend to post to the site. She has sought advice from the company's outside counsel for advice on best practices for setting up and operating cloud-based document sharing services to protect the materials posted to such sites from inadvertent access.

Cloud-Based File Sharing Services

Cloud storage has revolutionized the way businesses share information, both within and outside the organization. Many cloud storage services—most prominently Dropbox and Box—include a feature that lets users share files with anyone who receives a hyperlink to that file. Anyone who has (or can guess) that hyperlink can access the file or account associated with it. Although this feature of cloud storage sites allows easy information sharing, there may be significant legal consequences if, during litigation, that hyperlink is the only means of access control. This issue recently arose in *Harleysville Insurance Company v. Holding Funeral Home, Inc., et al.*, No. 1:15-cv-00057 (W.D. Va., Feb. 7, 2017), in which a US district court held that a party that shares access to information using hyperlinks, without further access control, waives any claim of privilege or work product protection over that information.

Harleysville—Facts

The plaintiff, Harleysville Insurance Company, suspected that a defendant had set a fire that destroyed the defendant's property. During Harleysville's investigation of the defendant's insurance claim, a Harleysville employee sent to the National Insurance Crime Bureau ("NICB") a hyperlink to a file in a Box account that contained a surveillance video of the fire scene. There was no further access control for the file: anyone with the link could access the Box account and the information stored there. Later, Harleysville uploaded its entire investigation and claims file to the same Box account without applying any further access control.

During discovery, defense counsel subpoenaed NICB's documents related to the fire claim. NICB complied with the subpoena and included in its responsive production a copy of the email containing the link to the Box account. Defense counsel typed the link into a web browser, accessed the Box account and—without informing Harleysville's counsel—downloaded Harleysville's entire claims file, including potentially privileged information.

Only later did Harleysville's counsel realize that defense counsel had downloaded the claims file.

Harleysville moved to disqualify defense counsel, arguing that downloading the claims file was an improper, unauthorized access to privileged information. Defense counsel argued that by placing the claims file on an unsecured Box account, where anyone with the right link could access it, Harleysville waived any claim of privilege.

Harleysville—the Court's Decision

The US District Court for the Western District of Virginia agreed with defense counsel, applying Virginia law to hold that "Harleysville has waived any claim of attorney-client privilege with regard to the information posted" to the Box account. The court found that, because "anyone, anywhere" with the link to the Box account could access the claims file, Harleysville "conceded that its actions were the cyber world equivalent of leaving its claims file on a bench in the public square and telling its counsel where they could find it."

The court rejected Harleysville's argument that defendant counsel's access to the files amounted to ethical misconduct that would render the disclosure "involuntary" and void any waiver. Instead, it held that Harleysville's subjective "intention is not determinative of whether the disclosure was involuntary or inadvertent." Instead, because Harleysville intentionally uploaded the claims file to the insecure Box account, Harleysville permitted defense counsel to access it, and the disclosure was an inadvertent result of Harleysville's carelessness.

For similar reasons, the court also rejected Harleysville's attempt to claw the document back under Federal Rule of Evidence 502, which provides that, notwithstanding the disclosure of otherwise privileged information, the privilege is not waived if (1) the disclosure was inadvertent; (2) the holder of the protection took reasonable steps to prevent the disclosure; and (3) after the disclosure, the holder of the protection took reasonable steps to rectify the error, including requesting that the other party destroy or sequester the protected documents. The court held that (1) the disclosure was not inadvertent because Harleysville intentionally uploaded the claims file to the Box account, and (2) Harleysville had not taken "reasonable steps" to prevent the disclosure because it had uploaded its entire claims file in a manner that made it available to anyone with access to the hyperlink.

The *Harleysvill*e court's holding of waiver is particularly striking because it also held that defense counsel had failed to comply with their ethical obligation to inform Harleysville that they had come into possession of information subject to a potential privilege claim. The court, relying on Virginia state bar ethics rules and state court decisions, held that defense counsel had an obligation to notify Harleysville once they discovered they had potentially privileged information. But they did not. And, the court reasoned, defense counsel should have realized that the materials in the Box account may have been privileged once they examined them. Despite these failures, the court concluded that disqualifying defense counsel was inappropriate because Harleysville had waived privilege and work product protections over the claims file.

Practical Steps for Avoiding Waiver

The *Harleysville* court analogized uploading information to a cloud storage site without specific access control to leaving documents on a park bench for anyone in the world to see. To avoid such findings, companies should familiarize themselves with the access control features of any tool they use to share information and take affirmative technical steps to restrict access to any materials posted to such a site—especially confidential or privileged information. Such controls include password protections and limiting user access to only the documents that each particular user needs access to.

For inquiries related to this Tip of the Month, please contact Geoffrey Pipoly at

gpipoly@mayerbrown.com.

To learn more about Mayer Brown's Electronic Discovery & Information Governance practice, contact Michael E. Lackey at mlackey@mayerbrown.com, Eric Evans at eevans@mayerbrown.com or Ethan Hastert at ehastert@mayerbrown.com.

Please visit us at www.mayerbrown.com.

ELECTRONIC DISCOVERY & INFORMATION GOVERNANCE

Tip of the Month

Adherence to Federal Rules of Civil Procedure Can Prevent Trouble Down the Road

Scenario

Plaintiff's counsel serves the defense with a set of requests for production of documents. The requests specify that electronically stored information ("ESI") be produced in its native format with all metadata attached. Aware that metadata is difficult to redact consistently, defense counsel is justifiably concerned about waiver of attorney-client and other privileges. To avoid any such waiver, defense counsel wonders whether it can simply choose to produce the ESI in another format.

Federal Rule of Civil Procedure 34(b)

Federal Rule of Civil Procedure ("Rule") 34(b) specifically sets forth a procedure for the contents of a request for documents, ESI and tangible things, as well as the timing and content of responses and objections. A recent opinion, *Morgan Hill Concerned Parents Association v. California Department of Education*, No. 2:11-cv-3471 KJM AC, 2017 WL 445722 (E.D. Cal. Feb. 2, 2017), underscores the importance of knowing and adhering to Rule 34(b), especially with regard to discovery of ESI.

The *Morgan Hill* plaintiffs served the defendant with a set of document requests that specified that ESI should be produced "in their native electronic format together with all metadata and other information associated with each document in its native electronic format." The defendant responded to these document requests but did not object to the production of ESI in its native format or propose another form for the production of ESI. Instead, the defendant objected to each request on multiple other grounds. More than a year after its initial response, after an extensive meet-and-confer process, the defendant finally stated a specific objection to the production of ESI in its native format. Further, the defendant produced some ESI but did so in the standard image-database-plus-load-file format generally used for non-native production. After further unsuccessful meet-and-confer seeking native production, the plaintiffs filed a motion to compel production of ESI in its native format as it had specified, arguing that the defendant should have either produced the ESI in its native format or specifically objected to the format and stated an alternative. The defendant argued that its production was proper because it produced the ESI in a "reasonably usable" form and that it had made a timely objection to the plaintiffs' chosen format.

Failure to Comply with Rule 34(b) Results in Duplicate Production

The court agreed with the plaintiffs, stating that Rule 34(b) allows the requesting party to specify the form or forms in which production should be made. The responding party is not bound by the requesting party's election but may object to the requested format and specify an alternative

“reasonably usable” format of its own. If the responding party does not object timely––for example, in its first set of written objections and responses––then the objection may be waived and the responding party must produce the ESI in the format requested.

The court rejected the defendant’s argument that the plaintiffs could not demand production in a specific format just because it would ease the burden of review. Indeed, ease of review is a reason why a requesting party may specify a particular format.

The court further found that producing ESI in load-file format—which the court conceded to be “reasonably usable” and a standard and widely accepted format—did not trump the defendant’s legal obligation to produce the ESI in the format specified by the plaintiffs or to make a timely objection.

The defendant also argued that it would be unduly burdensome to require it to produce all of the requested ESI in its native format because it had already produced thousands of the same documents in load-file format. The court rejected this argument stating that the problem was of the defendant’s own making: had it followed the Rules and produced the documents as requested or made a timely objection, it would not have found itself required to make a partially duplicate production.

Practice Tips

- **Parties should meet and confer as soon as practicable to reach agreement regarding the production of ESI:** Meeting and conferring early in the process can prevent having to devote time and effort to litigating a motion to compel and having to incur the costs associated with reproducing ESI.
- **Objections to discovery must be timely:** Objections to the format of production may be waived if not made at the first formal opportunity.
- **The producing party should make specific objections to production format:** A party responding to a request to produce ESI should not simply refuse to produce the ESI in the requested format if it believes that the request is unreasonable or disproportionate or the information sought is irrelevant. Instead, it should object to the proposed form, propose an alterative form, and seek a protective order if an agreement cannot be reached.

For inquiries related to this Tip of the Month, please contact Kim Leffert at kleffert@mayerbrown.com or Jerel Dawson at jdawson@mayerbrown.com.

To learn more about Mayer Brown's Electronic Discovery & Information Governance practice, contact Michael E. Lackey at mlackey@mayerbrown.com, Eric Evans at eevans@mayerbrown.com or Ethan Hastert at ehastert@mayerbrown.com.

Please visit us at www.mayerbrown.com.

ELECTRONIC DISCOVERY & INFORMATION GOVERNANCE

Tip of the Month

Proposed Updates to *The Sedona Principles*, Third Edition

Scenario

A technology company has been sued by a non-practicing entity (also known, less politely, as a patent troll) in US federal district court for patent infringement regarding a recently released product that is generating only moderate revenue. The general counsel wants to minimize discovery costs, but the non-practicing entity has issued overbroad discovery requests. The general counsel is aware of recent amendments to the Federal Rules of Civil Procedure (Federal Rules) in favor of proportionality and has inquired whether any additional developments could support a streamlined discovery process.

Background of the Sedona Principles

The Sedona Conference is a nonprofit research and educational institute composed of judges, lawyers, academics and other experts who meet in working groups to discuss legal issues in the areas of antitrust, intellectual property and other complex litigation. One of the most notable of these is The Sedona Conference Working Group on Electronic Document Retention and Production (WG1).

WG1 first met in October 2002 to address the production of electronic information in discovery, which at the time was largely governed by rules and concepts designed for paper records. WG1 recognized the unique challenges that electronic discovery posed and developed a set of recommendations for electronic discovery best practices during litigation. WG1 published an initial draft of these best practices—known as the Sedona Principles—for comment in March 2003. Although the Sedona Principles did not publish in final form until January 2004, the draft version quickly influenced the legal community and was cited in court decisions such as the landmark case *Zubulake v. UBS Warburg*, 229 F.R.D. 422 (S.D.N.Y. 2004).

As advancements in technology led to a greater volume of and complexity in electronic discovery and the Federal Rules were amended, WG1 continued its dialogue in support of further updates to the Sedona Principles. WG1 published a second edition in 2007 and conducted numerous meetings from 2010 to 2016 based on the evolving viewpoints on electronic discovery best practices. In March 2017, WG1 published the third edition of the Sedona Principles and is seeking public comment through June 30, 2017.

Overview of *The Sedona Principles*, Third Edition

The third edition of the Sedona Principles comprises "fourteen succinct statements that embody the consensus view of WG1 on a reasonable and balanced approached to the treatment of electronically

stored information in the legal process." It also includes detailed commentary providing context and boundaries for application of the principles. Some of WG1's proposed principles to guide electronic discovery during litigation include:

- When balancing the cost, burden and need for electronically stored information, courts and parties should apply the proportionality standard embodied in Fed. R. Civ. P. 26(b)(1) and its state equivalents, which requires consideration of the importance of the issues at stake in the action, the amount in controversy, the parties' relative access to relevant information, the parties' resources, the importance of the discovery in resolving the issues and whether the burden or expense of the proposed discovery outweighs its likely benefit.
- As soon as practicable, parties should confer and seek to reach agreement regarding the preservation and production of electronically stored information.
- Discovery requests for electronically stored information should be as specific as possible; responses and objections to discovery should disclose the scope and limits of the production.
- The obligation to preserve electronically stored information requires reasonable and good faith efforts to retain information that is expected to be relevant to claims or defenses in reasonably anticipated or pending litigation. However, it is unreasonable to expect parties to take every conceivable step or disproportionate steps to preserve each instance of relevant electronically stored information.
- The primary sources of electronically stored information to be preserved and produced should be those readily accessible in the ordinary course. Only when electronically stored information is not available through such primary sources should parties move down a continuum of less accessible sources until the information requested to be preserved or produced is no longer proportional.
- Absent a showing of special need and relevance, a responding party should not be required to preserve, review or produce deleted, shadowed, fragmented or residual electronically stored information.

(The full list of Sedona Principles can be found on The Sedona Conference's web site.)

The Sedona Principles promote several common themes, such as cooperation among parties, early discussion of the issues, proportionality (in both preservation and production) and more particularly worded discovery requests and responses. Based on these themes, there are several positions litigants can advance in the face of unreasonable discovery demands. The third edition clarifies that proportionality considerations extend beyond the amount in controversy and include the role that the propounded discovery could play in resolving issues in the case. (*See* Comment 2.a.) Proportionality should permeate all aspects of discovery, including preservation, searches for relevant electronic information, privilege logs, production scheduling and data delivery specifications. (*See* Comment 2.b.) Consideration of discovery costs should include not only the expense of document collection and retention but also other litigation costs, including the interruption of routine business practices and the cost of discovery review. (*See* Comment 2.d.) Parties should also consider streamlined privilege logs that identify withheld documents by category as opposed to document-by-document. (*See* Comment 3.d.) The Sedona Principles also emphasize that Rule 34 inspections of electronic information systems are disfavored unless the requesting party can show that the operation of a particular system is at issue and there is no reasonable alternative to onsite inspection. (*See* Comment 6.d.) While these are some positions advanced by *The Sedona Principles*, Third Edition, parties should review the comments in full for additional analysis to further support efficient discovery procedures.

Conclusion

Litigants are already using the recent Federal Rule amendments to streamline electronic discovery, and the Sedona Principles offer another avenue of reason. Not yet published in final form, the third edition of the Sedona Principles is open to public commentary until June 30, 2017. In the meantime, litigants should consider citing the Sedona Principles, or their corresponding comments, as courts have historically considered them even in draft form.

For inquiries related to this Tip of the Month, please contact Clayton McCraw at cmccraw@mayerbrown.com.

To learn more about Mayer Brown's Electronic Discovery & Information Governance practice, contact Michael E. Lackey at mlackey@mayerbrown.com, Eric Evans at eevans@mayerbrown.com or Ethan Hastert at ehastert@mayerbrown.com.

Please visit us at www.mayerbrown.com.

ELECTRONIC DISCOVERY & INFORMATION GOVERNANCE

Tip of the Month

Disclosure Scope and Discovery Timing Changes under the MIDP

Scenario

A manufacturing company just was served with a complaint filed in the United States District Court for the Northern District of Illinois. The company's general counsel heard about some new discovery rules in some of the federal courts and inquires how those rules will change the way parties litigate in federal courts.

The Mandatory Initial Discovery Pilot Program (MIDP)

The federal courts in the District of Arizona and the Northern District of Illinois have begun participating in the Federal Judicial Center's Mandatory Initial Discovery Pilot Program ("MIDP"), which radically changes both the scope of parties' initial disclosures and the timing for discovery more generally. With limited exceptions, all civil cases filed in the District of Arizona beginning May 1, 2017, and in the Northern District of Illinois beginning June 1, 2017, are governed by these new rules.

Disclosure Scope Changes with the MIDP

The MIDP brings with it three crucial disclosure changes of which all litigants and practitioners subject to the program should be aware:

1. A motion to dismiss generally will no longer delay the time to answer the complaint. The court *may* defer the filing of an answer "for good cause" but only where the motion is based on lack of subject-matter jurisdiction, lack of personal jurisdiction, sovereign immunity, absolute immunity or qualified immunity. This means that, in most cases, a defendant seeking to dismiss a complaint will still have to prepare and file an answer.
2. With limited exceptions, 30 days after a responsive pleading is filed, the parties must serve an expanded set of initial disclosures that must include:
    a. The names and contact information of all persons likely to have discoverable information relevant to *any* party's claims or defenses, along with a description of the nature of the information that each person is believed to possess.
    b. The names and contact information of anyone to whom the disclosing party has given written or recorded statements relevant to any party's claims or defenses, along with copies of the same if within the party's possession, custody or control.
    c. A list of documents, ESI, tangible things, land, or other property that may be relevant

to any party's claims or defenses, regardless of whether in the disclosing party's possession, custody or control, along with the names and contact information of the custodians of any items not within the producing party's possession, custody, or control. Items may be listed in specifically described categories if they are sufficiently numerous that listing them individually would be impracticable. In addition, with the exception of ESI, all such evidence within a party's possession, custody or control must be produced or made available on the date of the initial disclosure.

d. For each of the disclosing party's claims or defenses, the relevant facts and legal theories on which it is based.

e. From each party asserting a claim for relief, a computation of each category of damages claimed and a description of the documents or other evidence on which that computation is based. Alternatively, the party may produce the materials directly in lieu of providing a description.

f. A specific identification and description of any insurance or other similar agreement, including indemnification agreements, under which somebody else may be liable to satisfy all or part of any possible judgment.

3. Absent a court order, ESI must generally be produced within 40 days of serving a party's initial disclosures. However, parties are required to confer "on matters relating to its disclosure and production" including with respect to each party's preservation obligations, custodians and search terms, the use of technology-assisted review, and the form in which ESI will be produced.

Parties are under a continuing duty to supplement their initial disclosures whenever new or additional information or documents are discovered or revealed and must do so within 30 days of discovering the additional information or documents.

Although, as before, parties are not to file their initial disclosures and later supplements with the court, parties must now file a notice of service of their initial disclosures and later supplements.

Timing Changes with the MIDP

The timing changes are perhaps the most significant, particularly as they relate to discovery of ESI. Under the MIDP, parties now have only 70 days following the responsive pleading deadline to identify, preserve, collect, process, review and produce ESI. Although the MIDP allows that each party's disclosures are to be "based on the information then reasonably available to it," leaving open the possibility of conducting "rolling" productions as parties churn through often significant quantities of ESI, the MIDP nevertheless puts substantial pressure on parties to speed up the process of collecting and producing ESI.

Conclusion

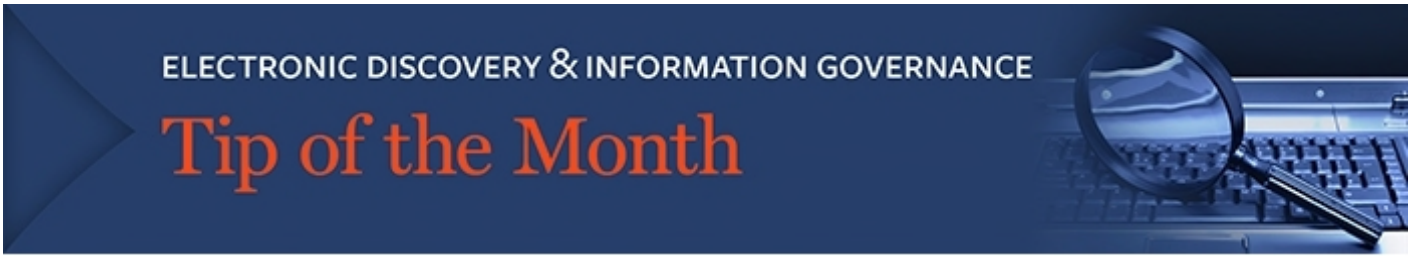
In summary, the MIDP imposes important changes on the timing and strategy of discovery and motion practice at the very beginning of federal court litigation. Although the MIDP has only been adopted by two federal district courts, it behooves lawyers in all jurisdictions to become familiar with these rules because they may be adopted in other jurisdictions.

For inquiries related to this Tip of the Month, please contact Corwin J. Carr at ccarr@mayerbrown.com or Kim Leffert at kleffert@mayerbrown.com.

To learn more about Mayer Brown's Electronic Discovery & Information Governance practice, contact Michael E. Lackey at mlackey@mayerbrown.com, Eric Evans at eevans@mayerbrown.com

or Ethan Hastert at ehastert@mayerbrown.com.

Please visit us at www.mayerbrown.com.



2017 Proposed Amendment to Federal Rule of Evidence 902

July 2017

Scenario

A multinational company is a defendant in a lawsuit that is expected to go to trial in 2018. The company believes that it will likely introduce evidence of web pages posted at various times, and wants to avoid the inconvenience of calling a live witness at trial to authenticate the web pages.

Authenticating Evidence at Trial

Generally, a party must produce sufficient evidence "to support a finding that the item is what the proponent claims it is" prior to introducing evidence into the record at trial. Fed. R. Evid. 901(a). Federal Rule of Evidence 902 provides that certain types of documents, such as government documents, certified copies of public records and newspapers, are self-authenticating and do not require extrinsic evidence of authenticity to be admitted at trial. Rules 902(11) and (12) also allow a party to rely on certification by a foundation witness to establish the authenticity of business records so long as the opponent is given a fair opportunity to challenge both the certificate and the underlying record.

Amendments to Federal Rule of Evidence Expand the Categories of Self-Authenticating Evidence

Proposed amendments to Rule 902 that are expected to take effect on December 1, 2017, will add two new paragraphs permitting a party to self-authenticate certain types of electronic evidence. The first, paragraph 13, will allow for self-authentication of a "record generated by an electronic process or system that produces an accurate result," such as a system registry report showing that an external device was connected to a computer. The second, paragraph 14, will allow for self-authentication of "[d]ata copied from an electronic device, storage medium, or file if authenticated by a process of digital identification," which will, among other things, permit self-authentication, using industry standard methodology, that a copy of an email is identical to the original email or that a forensic copy of cell phone text messages is identical to the original text messages. For evidence introduced under paragraph 13 or 14, a party will be required to provide certification by a foundation witness to establish the authenticity of the evidence, and the opposing party will have to be provided a fair opportunity to challenge both the certificate and the underlying record.

The intent of these amendments is to avoid the expense and inconvenience of calling on a witness at trial to certify the authenticity of electronic documents pursuant to Federal Rule of Evidence 901. The Advisory Committee found that "[i]t is often the case that a party goes to the expense of producing an authentication witness and then the adversary either stipulates authenticity before the witness is called or fails to challenge the authentication testimony once it is presented." Thus, proposed Federal

Rules of Evidence 902(13) and 902(14) will permit a party to avoid calling a live witness by providing, instead, a certificate by a qualified person certifying the authenticity of the electronic evidence.

Adopt Electronic Collection Best Practices to Benefit from the Amendments to Federal Rule of Evidence 902

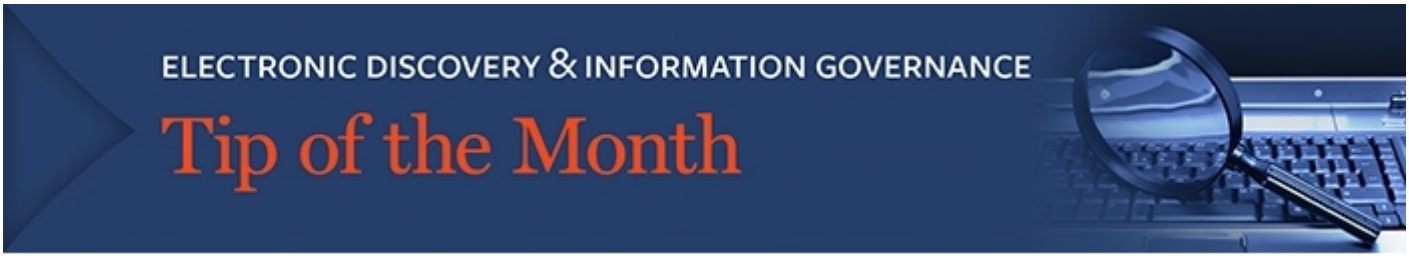
Parties wishing to follow the new self-authentication rules should ensure that their electronic collections are conducted in a forensically sound manner. In most cases, this will mean either bringing in a forensics specialist to conduct the collection or appropriately supervising self-collections, including, for example, designing the collection protocol, using forensic copying tools and documenting the collection.

Collection best practices performed by a person qualified to attest to the accuracy or reliability of the process that produced an exhibit or to the facts establishing that the exhibit is an accurate copy can eliminate the need to call an authentication witness at trial. Adopting this approach can save time, expense and inconvenience at trial.

For inquiries related to this Tip of the Month, please contact Kristina Portner at kportner@mayerbrown.com or Ethan Hastert at ehastert@mayerbrown.com.

To learn more about Mayer Brown's Electronic Discovery & Information Governance practice, contact Michael E. Lackey at mlackey@mayerbrown.com, Eric Evans at eevans@mayerbrown.com, or Ethan Hastert at ehastert@mayerbrown.com.

Please visit us at www.mayerbrown.com.



Recent Case Law Sheds Light on Application of Federal Rule of Civil Procedure 37(e)

August 2017

Scenario

After a lawsuit was initiated, the defendant company issued an internal litigation hold notice to its employees related to the plaintiff's claims. The hold notice directed the employees to preserve all potentially relevant documents, but it did not explicitly identify web browser histories as among the type of documents to be preserved, as this information was not deemed relevant based on the complaint and anticipated defenses. Many months later, the company was served with requests for production seeking the employees' web browser histories. The company's internet browser automatically deletes browser history after 120 days (unless instructed otherwise) and such information had already been deleted.

The company's general counsel wonders whether the company will be subject to sanctions due to the automatic deletion of the web histories under amended Rule 37(e) of the Federal Rules of Civil Procedure.

Overview of Amended Rule 37(e)

Under amended Rule 37(e), which became effective on December 1, 2015, a court may impose sanctions on an offending party "[i]f electronically stored information that should have been preserved in the anticipation or conduct of litigation is lost because [the] party failed to take reasonable steps to preserve it and it cannot be restored or replaced through additional discovery."

If these threshold elements are satisfied, Rule 37(e) establishes two different avenues parties can take to demonstrate sanctions are warranted. Under amended Rule 37(e)(1), if the court finds the party seeking the electronically stored information (ESI) has been *prejudiced*, the court may impose curative measures that are "no greater than necessary to cure the prejudice."

Further, under amended Rule 37(e)(2), regardless of prejudice, if the court determines that the offending party acted with *intent* to deprive the other of the information's use in litigation, the court may impose the harsher sanctions available, including presuming that the lost ESI was unfavorable to the offending party, instructing the jury that it may or must presume the information was unfavorable or entering default or dismissal.

Recent Case Law

The Duty to Preserve

Under Rule 37(e), a court may not impose sanctions for a failure to preserve ESI unless such ESI *should have been preserved*. Case law demonstrates that the duty to preserve under Rule 37(e) arises when a

party knows or should know that certain evidence is relevant to pending or future litigation. However, courts are interpreting amended Rule 37(e) as limiting this duty to preserve in a number of ways.

For instance, courts have interpreted this duty to preserve as being based on a "prospective standard." It is simply far too easy to determine what ESI should have been preserved using hindsight. Thus, courts have held that the determination of what ESI should have been preserved under amended Rule 37(e) should be viewed from the point of view of the party who controls the ESI at the time litigation is anticipated or ongoing, not when it is discovered that ESI was lost.

Further, courts have interpreted amended Rule 37(e) as limiting this duty to preserve to relevant ESI. Although the rule does not use the word "relevant," the Advisory Committee Notes do. The notes expressly acknowledge that the rule is based on a party's common law duty to preserve relevant information when litigation is reasonably foreseeable. This limitation makes sense, as there would be no prejudice to a party from the loss of irrelevant information.

Establishing Prejudice

A court may impose sanctions under amended Rule 37(e)(1) if the court finds that a party was prejudiced from the loss of the ESI. According to recent case law, there must be some concrete evidence regarding the particular nature of the missing ESI to establish prejudice and support relief under the amended rule. Without such evidence, the court cannot adequately evaluate the prejudice that it is being requested to mitigate.

In a recent case in the Northern District of Illinois, the court acknowledged that establishing prejudice can be a "tricky business" in cases where no one knows precisely what was lost. When the ESI no longer exists and cannot be viewed, it is difficult for a court to determine prejudice, for the party that failed to preserve the ESI to show absence of prejudice and for the party that seeks the ESI to establish prejudice.

Nonetheless, the court ultimately concluded that the circumstances did not warrant a finding of prejudice under Rule 37(e)(1). In support of this conclusion, the court noted the lack of evidence regarding the particular nature of the missing ESI and that it was "pure speculation" that the lost ESI would have benefitted the party seeking the imposition of sanctions. The speculation alone was not enough to support the relief requested.

Intent to Deprive

With respect to Rule 37(e)(2), courts have been applying the language strictly and have refused to impose the harsher sanctions allowed absent a showing that the offending party acted intentionally and was not merely negligent with regard to the lost ESI.

For example, in a recent case in the Eastern District of North Carolina, the court held that the party seeking relief under Rule 37(e)(2) failed to establish that the offending party acted with the "intent to deprive" that is required to support the relief sought. In so holding, the court reasoned that the circumstances at most indicated that the ESI was lost due to the offending party's negligence. Under Rule 37(e)(2), negligent conduct, even grossly negligent conduct, is insufficient.

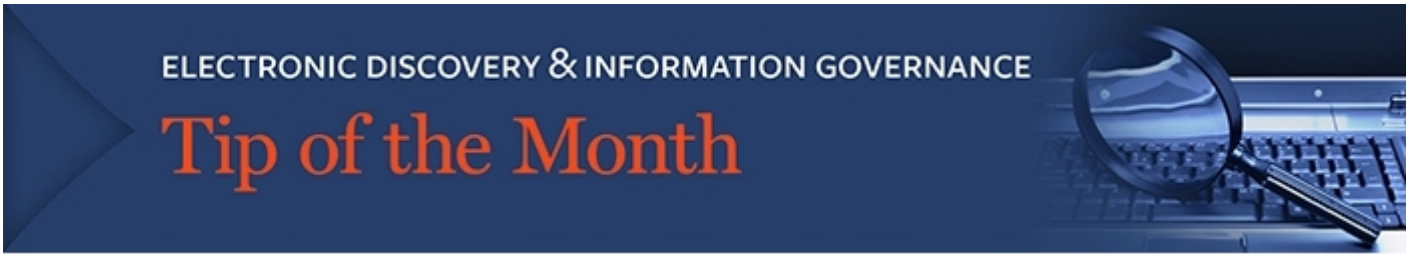
Conclusion

As recent cases illustrate, courts are strictly applying the language of Rule 37(e) in determining whether to impose sanctions for the loss or destruction of ESI. Once the threshold requirements are met, before imposing sanctions under Rule 37(e)(1) or (e)(2), courts are requiring that there be some evidence that the loss resulted in prejudice or that the offending party acted with intent to deprive the other of the use of the lost ESI. A lack of such evidence is likely to be fatal to the other party's request for sanctions.

For inquiries related to this Tip of the Month, please contact Gina Aiello Jordt at gjordt@mayerbrown.com or Ethan Hastert at ehastert@mayerbrown.com.

To learn more about Mayer Brown's Electronic Discovery & Information Governance practice, contact Michael E. Lackey at mlackey@mayerbrown.com, Eric Evans at eevans@mayerbrown.com or Ethan Hastert at ehastert@mayerbrown.com.

Visit us at mayerbrown.com.



New York Guidance on the Lawyer's Ethical Duty of Technological Competence

September 2017

Scenario

A Nevada-based financial services company has retained a law firm in connection with litigation pending in New York State that arose out of the company's alleged breach of a consumer protection statute. Given that the litigation will involve the review and production of sensitive electronically stored information (ESI) relating to the company's customers, the company has asked the law firm how it intends to securely collect, review and produce ESI and has inquired about the firm's technological competence with respect to electronic discovery.

New York County Lawyers Association Ethics Opinion on ESI

The questions from the company are timely: a recent opinion issued by the New York County Lawyers Association's (NYCLA) Committee on Professional Ethics provides guidance on the ethical duties lawyers must meet with respect to protecting a client's confidential information that is stored and transmitted electronically, as well as in the context of conducting e-discovery. The opinion indicates that a lawyer practicing in New York owes his or her clients a duty of competence that "expands as technological developments become integrated into the practice of law," and recognizes that the question of whether a lawyer satisfies his or her duty of technological competence depends on the particular circumstances of the representation.

Technological Competence and the Protection of Confidential Information

Drawing on prior opinions of both the New York State Bar Association and NYCLA, as well as the New York Rules of Professional Conduct, the NYCLA opinion observes that a lawyer's duty to protect client confidences and secrets extends not only to electronic communications with clients but also to confidential information that is stored and transmitted electronically. The opinion indicates that a lawyer must use reasonable care when transmitting information electronically to ensure that client confidences and secrets are maintained. Lawyers must understand the risks associated with the use of technology, including the threat of cyber attacks and inadvertent disclosures, and determine whether the use of such technology to store or transmit client confidences is prudent under the circumstances. The opinion also cautions that, to the extent that they represent clients outside of New York State, lawyers may be subject to the data protection laws of other states. Given these concerns, the opinion observes that lawyers must either personally possess, or associate with persons who possess, sufficient understanding of the technology at issue "to determine how to satisfy the lawyer's duty of reasonable care." The opinion indicates that whether the duty of reasonable care has been satisfied depends on circumstances such as "the subject matter, the sensitivity of the information, the likelihood that the information is sought by others, and the potential harm from disclosure."

Building on the principles laid out in the NYCLA opinion, lawyers can take several steps to ensure that their use of technology to communicate with clients and to store confidential information is consistent with the lawyer's duty of technological competence:

- Gain a sufficient understanding of relevant technologies (email, cloud storage, flash drives, etc.), either through education or association with others, to adequately weigh the risks and benefits associated with the use of such technologies
- Encrypt mobile communication and storage devices, especially when these devices leave the physical confines of the law firm
- Communicate with clients, vendors, co-counsel and employees through secure electronic means
- Research and comply with laws governing protection of personal data in the jurisdictions where the lawyer practices, as well as where his or her clients conduct business
- Whether required in their jurisdiction or not, seek out continuing legal education on subjects relevant to technology and the practice of law
- Educate employees and outside vendors on cybersecurity risks and best practices for maintaining client confidences

Technological Competence and Electronic Discovery

The NYCLA opinion also recognizes that e-discovery has become a significant part of most litigation, as well as government and regulatory investigations. Noting that federal and state rules govern a lawyer's obligations with respect to ESI, the opinion goes on to provide concrete guidance on steps that lawyers can take to meet their duty of competence as it pertains to e-discovery:

- Continually assess the lawyer's own e-discovery skills and resources and determine whether the lawyer must either acquire additional skills and resources or associate with e-discovery experts or other lawyers who possess the required skills and resources
- Conduct an *early* assessment of ESI issues that are likely to arise during the course of discovery, including issues relating to the preservation, collection and production of ESI
- Identify custodians of ESI and preserve and collect ESI in a manner that allows the lawyer to search for responsive ESI throughout the course of discovery
- Gain a thorough understanding of the client's systems for creating and storing ESI
- Advise clients of their options for preserving, collecting and producing ESI and their associated costs
- Supervise employees and outside vendors to ensure that work is done properly and in accordance with all relevant laws, rules and court orders

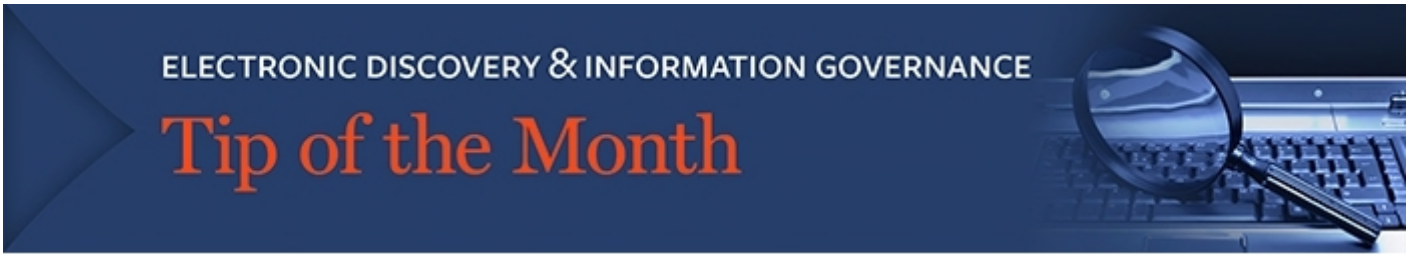
Conclusion

As the storage and transmission of sensitive information increasingly occurs by electronic means, lawyers must take steps to ensure that they continue to meet their duty to protect the confidences and secrets contained in ESI. Lawyers must also gain an understanding of the unique challenges posed by e-discovery and provide competent advice to clients concerning the preservation, collection and production of ESI.

For inquiries related to this Tip of the Month, please contact Jason Kirschner at jkirschner@mayerbrown.com or Christopher Mikesh at cmikesh@mayerbrown.com.

To learn more about Mayer Brown's Electronic Discovery & Information Governance practice, contact Michael E. Lackey at mlackey@mayerbrown.com, Eric Evans at eevans@mayerbrown.com or Ethan Hastert at ehastert@mayerbrown.com.

Visit us at mayerbrown.com.



While Everyone's Talking About Law Firm Cybersecurity, What You and Your Outside Counsel Might Do About It

October 2017

Scenario

The GC of a major, US-based corporation receives an email from a vice president in the chief security officer's business unit, reading, "Hey, did you see this article? Whenever I go to IT security conventions, I hear about cybersecurity issues at law firms. What are we doing about that?" The email also contains a link to a *LegalTech* article titled "Law Firms Fail on Cybersecurity, and Corporate Clients Are Cracking Down."

The legal press has extensively covered cybersecurity risks faced by law firms. Law firms are targets because they hold clients' most sensitive and confidential information. Almost every week there's a new headline underscoring this risk. But what should a client ask its outside counsel to do to keep the company's information secure?

The ACC's Model Controls

The Association of Corporate Counsel ("ACC") has put together a set of suggestions, a good start for a cybersecurity discussion between a company and its outside counsel: "Model Information Protection and Security Controls for Outside Counsel Possessing Company Confidential Information."

The Model Controls list 13 steps that law firms might take to protect confidential client information ("CCI"). In general terms, these steps align outside counsel's security policies and practices with a client's.

- Establish physical and electronic security measures and incident response protocols, including regular audits.
- Remove or return CCI within 30 days after a client request. This suggestion doesn't apply to back-and-forth emails, attorney work product, public information, information counsel retains under legal or ethical obligations or for disaster recovery, and information (such as deleted files) that requires specialized tools to access.
- Use at-rest encryption of CCI, whether it's stored with outside counsel or a third party vendor.
- Send CCI only via email with Transport Layer Security encryption, if a client requests this level of security.
- Require two-factor authentication for remote connectivity.
- Report security breaches within 24 hours of discovery using pre-established procedures
- Maintain physical security for data centers.
- Establish logical access controls for CCI on a need-to-know basis.
- Track systems, employees and contractors for security incidents.

- Perform regular hacking/penetration tests and code review.
- Establish industry-standard system and network security processes, such as regular antivirus and malware scans.
- Permit audits of facilities, systems and practices covering CCI.
- Get ISO 27001 certification, if a client requests it.
- Background check employees, contractors and contingent workers with access to CCI.
- Get cyber liability insurance.
- Have subcontractor and vendors with access to CCI adopt the client's security requirements

The Model Controls state that they are a list of possible security steps, not a "definitive statement on the subject." Instead, they're "practical information [for] in-house counsel." They don't "establish any industry standards for any purpose." But despite this disclaimer, the Model Controls are a valuable checklist of things to think about and discuss with outside counsel.

Two items in the Model Controls stand out as high-priority: encrypted email and vendor adoption of client requirements.

Encrypted Email

Many companies are still using unencrypted email to communicate with outside counsel. Anyone who intercepts an unencrypted email message can read it. Modern email programs (such as Outlook and Gmail) support encrypted email. Encrypted emails are much more difficult to read, even if they're intercepted. It may therefore be a good practice to encrypt any email that includes CCI using Transport Layer Security. Also, it is a good practice to use Secure File Transfer Protocol ("SFTP") to transfer CCI instead of File Transfer Protocol ("FTP"). Many law firms and vendors already support email encryption and SFTP. In fact, many of them strongly encourage clients to encrypt their email and file transfers.

Vendor Adoption of Client Requirements

Security only works if it applies everywhere that CCI is stored. That includes e-discovery and cloud storage vendors. The Model Controls recommend that clients insist that vendors accept their security requirements in writing, in an engagement agreement. This approach makes the vendor responsible for complying with the client's requirements. It also means that a company and its outside counsel share the responsibility of selecting vendors that can meet the client's standards. Many vendors already have procedures in place to meet industry-standard requirements. But others will struggle to meet them. Careful selection of a vendor with strong security procedures helps avoid risk, delay and expense.

Conclusion

Law firm and vendor cybersecurity matters. The ACC Model Guidelines lay out a good list of items for clients to think about and discuss with counsel to help protect the clients' confidential information.

For inquiries related to this Tip of the Month, please contact Eric Evans at eevans@mayerbrown.com.

To learn more about Mayer Brown's Electronic Discovery & Information Governance practice, contact Michael E. Lackey at mlackey@mayerbrown.com, Eric Evans at eevans@mayerbrown.com or Ethan Hastert at ehastert@mayerbrown.com.

Visit us at mayerbrown.com.

ESI Accessibility and Proportionality

November 2017

Scenario

A large manufacturing company employs thousands of people and generates a staggering amount of electronically stored information (ESI) daily. A plaintiff sues the company, alleging fraud based on events that occurred nearly 10 years ago, and serves document requests seeking electronic communications and other ESI from current and former employees as well as from other data sources. Some of the requested information can be collected from active and legacy databases sitting on servers located on three continents. Other data has long since been archived or overwritten under established business procedures. The general counsel seeks your advice about the company's legal obligations in responding to these discovery requests.

Is the Data Reasonably Accessible?

Certain types or sources of ESI are presumed to be "inaccessible." The seminal case of *Zubulake v. UBS Warburg LLC*, 217 F.R.D. 309 (S.D.N.Y. 2003) (*Zubulake I*) provided an avenue for litigants to resist production of ESI kept in an inaccessible format. Courts often cite *Zubulake I*'s five tiers of accessibility (from most to least accessible): (1) active, online data; (2) near-line data; (3) offline storage and archives; (4) backup tapes; and (5) erased, fragmented or damaged data.

Federal Rule of Civil Procedure 26(b)(2)(B) codified the idea that some information sources are less accessible than others, explaining that "[a] party need not provide discovery of electronically stored information from sources the party identifies as not reasonably accessible because of undue burden or cost." Therefore, the accessibility test is based not solely on the type of media or whether the producing party has technical difficulties in accessing the information but also on whether access is difficult "because of undue burden or cost."

Is the Discovery Proportional to the Needs of the Case?

The principle of proportionality in the discovery process had been incorporated into the Federal Rules of Civil Procedure (FRCP) since 1983. The 1983 Rules Committee Note explained that the change was intended "to guard against redundant or disproportionate discovery by giving the court authority to reduce the amount of discovery that may be directed to matters that are otherwise proper subjects of inquiry." The Rules Committee addressed proportionality again in 1993 (noting that "[t]he revisions in Rule 26(b)(2) are intended to provide the court with broader discretion to impose additional restrictions on the scope and extent of discovery") and in 2000 (emphasizing "the need for active judicial use of subdivision (b)(2) to control excessive discovery").

But many practitioners felt that previous amendments to the FRCP did not sufficiently limit discovery. FRCP 26(b)(1), as amended in December 2015, returned the proportionality factors to Rule 26(b)(1) in an effort to make proportionality an explicit component of the scope of discovery.

Tension Between What Is Accessible and What Is Proportional

There is inherent tension between the "not reasonably accessible" concept and the "proportionality" principle. The former is written in the negative: a party is authorized *not to* collect and produce ESI from sources the party deems to be *not* reasonably accessible. In contrast, the latter is written in the positive: a party *may obtain* relevant, non-privileged discovery that *is* proportional to the needs of the case. With the renewed emphasis on the proportionality principle, parties seeking discovery may now be in a better position to contend that the information sought is proportional to the needs of the case where litigants were once successful in resisting discovery deemed not reasonably accessible.

Conversely, the proportionality principle sometimes allows parties to limit discovery. In other words, proportionality applies even before the "not reasonably accessible" test: even information from accessible sources need not be produced if the discovery itself fails the proportionality test.

Among the limited number of cases issued since the adoption of the 2015 amendments that addressed both the proportionality principle and the accessibility rule, the one major commonality is that courts appear to be deferring to the traditional burden evaluation, a factor common to both analyses. And, as usual, "who wins" will depend on the details.

Key Considerations for Litigants

Litigants should remember that:

- When an adversary seeking discovery advances an argument that the requested information is proportional to the needs of the case, a persuasive "inaccessibility" counter-argument should detail the costs and burdens associated with gathering relevant data. A conclusory assertion that the requested information is cumulative, duplicative, or even burdensome—without supporting evidence—might not defeat a motion to compel.

- A burden can be established by means other than monetary expense. For example, in one case the defendant submitted a declaration explaining that it would require at least 10 employees working full-time for many weeks to even begin the effort to collect responsive documents. In denying the plaintiff's motion to compel, the court accepted the burden rationale even though the defendant did not quantify the burden with a dollar value. Diverting manpower from other business duties is another factor that can support a burden finding.

- However, the need to review documents for privileged information will generally not satisfy the "undue burden or cost" element of Rule 26(b)(2)(B). In one case, the court deemed certain requests to be proportional to the needs of the case and ordered discovery, rejecting the notion that the plaintiff had demonstrated inaccessibility simply because it would have to conduct a privilege review.

- Even ESI from otherwise accessible sources may be found to be not reasonably accessible due to undue burden or cost.

Conclusion

Whether there are grounds for a litigant to refuse to produce some of the requested ESI will depend on a host of factors, including, *inter alia*, the nature of the case and the requesting party; the purported relevance of the data; and the expense associated with identifying, collecting, formatting, reviewing and producing the data. The litigant should marshal its evidence to demonstrate that at least certain requested information is not reasonably accessible due to undue burden or cost and

should be prepared to argue further that such information is not proportional to the needs of the case. Because burden and expense often hinge on technological capabilities and limitations, the accessibility inquiry may ultimately depend on a standard that evolves as technology evolves.

For inquiries related to this Tip of the Month, please contact Noah Liben at nliben@mayerbrown.com or Ethan Hastert at ehastert@mayerbrown.com.

To learn more about Mayer Brown's Electronic Discovery & Information Governance practice, contact Michael E. Lackey at mlackey@mayerbrown.com, Eric Evans at eevans@mayerbrown.com or Ethan Hastert at ehastert@mayerbrown.com.

Visit us at mayerbrown.com.

Irrelevance May Not Justify Redaction

December 2017

Scenario

A party to a contract dispute is in the process of reviewing and producing data in discovery. The general counsel of the party knows that information that falls within the attorney-client or attorney work product privileges should be redacted from the data prior to production, but she also wants to know if there are other reasons, including that information is not relevant to the dispute at issue, to redact.

Parties to Litigation Cannot Redact Information Simply Because It Is Irrelevant

Federal Rule of Civil Procedure 26(b)(1) sets out a broad definition for the scope of discovery that does not, on its face, exclude irrelevant information. The rule states that the parties to a case "may obtain discovery regarding any nonprivileged matter that is relevant to any party's claim or defense and proportional to the needs of the case." However, a recent federal case clarifies that without some other protection from disclosure, there are indeed substantial risks to redacting information on the sole basis that it is "irrelevant" or "non-responsive."

The defendants in a recent case in the Eastern District of Wisconsin produced more than 6,000 documents, 600 of which were redacted in their entirety. Without asserting any privilege, the defendants argued that the redactions were necessary to protect confidential business information, relying on a 2016 case from the Southern District of Florida in which certain non-responsive redactions were allowed "because of [the defendants'] concern that the documents contained competitively sensitive materials that may have been exposed to the public, despite protective orders." The defendants here failed to explain why the protective order was insufficient to protect their confidential business information. As a result, they were relying solely on the argument that the redacted information was irrelevant as opposed to pointing to any other basis for excluding it from discovery.

The court granted the plaintiff's motion to compel production of the 600 documents, stating that the "potential for abuse exists" if litigants may unilaterally decide what is relevant, and it did not agree that a receiving party must "take the [producing party's] word" for whether redacted information would be irrelevant to the receiving party's claim. The court pointed out that despite an emphasis on proportionality in discovery, the Federal Rules of Civil Procedure still permit discovery of information that is inadmissible as evidence. The court noted that "[t]he practice of redacting for nonresponsiveness or irrelevance finds no explicit support in the Federal Rules of Civil Procedure" and allowing this practice "would improperly incentivize parties to hide as much as they dare."

Appropriate Reasons for Redaction

Attorney-Client Privilege

The attorney-client privilege protects certain communications between an attorney and a client. Generally, for the privilege to apply, there must have been a communication between an attorney and a client for the primary purpose of giving or obtaining legal advice or assistance with the expectation and maintenance of confidentiality.

Work Product Doctrine

The work product doctrine is a qualified immunity from discovery for information prepared by an attorney in anticipation of litigation. The purpose of the doctrine is to ensure that attorneys' representation of clients is not hamstrung by fears that their work product will be used against their clients.

Non-Public Personal Information

Federal Rule of Civil Procedure 5.2 requires that personally identifiable information, such as an individual's full social security number, full taxpayer identification number, full birth date, the name of an individual known to be a minor or a financial account number, be redacted from federal court filings. Unless the court orders otherwise, a court filing may include only (i) the last four digits of the social security number and taxpayer identification number, (ii) the year of the individual's birth, (iii) the minor's initials and (iv) the last four digits of the financial account number.

In addition, Title V of the Gramm-Leach-Bliley Act, its implementing regulations and some state rules enacted in response to the Act impose disclosure and procedural requirements on financial institutions regarding their customers' nonpublic personal information. The act provides that, ordinarily, "a financial institution may not, directly or through an affiliate, disclose to a non-affiliated third party any nonpublic, personal information." Nonpublic personal information includes any personally identifiable information about a customer, or list of customers, that is not publicly available.

Bank Examination Privilege

Confidential supervisory information between financial institutions and certain regulators may be protected under the bank examination privilege. The privilege broadly protects documents, examination reports, communications between financial institutions and regulators, and other information reflecting the opinions, deliberations or recommendations of regulatory agencies.

This privilege, however, "belongs" to the regulator, meaning that only the regulator can invoke it. The financial institution should identify information to which the privilege may apply and may notify the regulator of any requests to produce information potentially protected by this privilege. Regulators that may invoke the privilege include the Board of Governors of the Federal Reserve System, the Office of the Comptroller of the Currency, the Federal Deposit Insurance Corporation, the Consumer Financial Protection Bureau and some state banking agencies.

SAR Privilege

The Bank Secrecy Act requires banks to report "any suspicious transaction relevant to a possible violation of law or regulation." Implementing regulations , such as the Office of the Comptroller of Currency's implementing regulations, require banks to "file a Suspicious Activity Report [SAR] when they detect a known or suspected violation of Federal law or a suspicious transaction related to a money laundering activity or a violation of the Bank Secrecy Act." A bank may not disclose the existence of the SAR or any information that would reveal its existence and may not waive the SAR

privilege. The SAR privilege protects reports, memoranda and other documents that reflect or relate to evaluation of a potential SAR filing.

Conclusion

As recent case law illustrates, a party to litigation runs a substantial risk if it justifies redaction of information based solely on "irrelevance." Instead, counsel should consider whether some other rule, regulation or substantive law protects that information from disclosure. Protections would include the attorney-client privilege, the work product doctrine, rules regarding the disclosure of non-public personal information, the bank examination privilege and the SAR privilege.

For inquiries related to this Tip of the Month, please contact James Coleman at jcoleman@mayerbrown.com.

To learn more about Mayer Brown's Electronic Discovery & Information Governance practice, contact Michael E. Lackey at mlackey@mayerbrown.com, Eric Evans at eevans@mayerbrown.com or Ethan Hastert at ehastert@mayerbrown.com.

Visit us at mayerbrown.com.