

DISCOVERY CENTER

A Data Analytics + eDiscovery Newsletter from Warner Norcross + Judd

hot topic

The Internet of Things and eDiscovery

Even when you don't know it, you're creating data — data that is stored somewhere for some indeterminate period of time. When you use your smartphone, one or more cell towers record and store your phone's unique identifier. If your phone's Wi-Fi is turned on, it's continually sending out a low power signal looking for available Wi-Fi networks. When it "pings" one, the Wi-Fi network also records your phone's unique identifier. A Fitbit records the user's heart rate, steps taken, calories burned, and stores that data in "the cloud." Newer cars have a "black box" similar to that in an airplane. In the event of a collision, the data can be used to show speed at impact, whether seats belts were in use, and whether the brakes were applied. Many other "smart" devices, from thermostats to refrigerators to home security systems, record and store data with little, if any, user interaction. Welcome to the Internet of Things ("IoT").

What is the IoT? Very simply, it's the connection of non-traditional computing devices to the Internet. The process started with our cell phones, but has branched out to our vehicles, our watches, our appliances, our home security systems, etc. Gartner estimates

that in 2016 the number of Internet-connected "things" was at 6.4 billion and predicts the number will grow to 20.8 billion by 2020. All of these billions of devices create and store data, at least temporarily. It is discoverable, like all electronic data. In fact, IoT data has already played a role in some interesting cases.

- In Ohio, a man was charged with arson when the data from his pacemaker did not correspond to his reported activities at the time of the fire.
- In Connecticut, a husband was charged with the murder of his wife when the data from her Fitbit conflicted with the husband's account of the crime.

continued on page 2

table of contents

Hot Topic: The Internet of Things and eDiscovery	page 1
Case Law: Summaries and Suggestions	page 3
A Closer Look: When the Duty to Preserve Evidence Arises	page 7
Technology: Utilizing Data Analytics to Improve Document Review	page 9
Warner Discovery Center	page 12



WHAT IS THE IoT?



continued from page 1

- In Arkansas, the audio recordings from a murder suspect's Amazon Alexa were subpoenaed for whatever evidence they might provide about what transpired inside the house on the night of the murder.
- In Illinois, Google's creation of "facial maps" from photographs automatically uploaded from Google Droid devices to the Google Cloud led to legal challenges under the Illinois Biometric Information Privacy Act.

While several of these cases concern criminal prosecutions, they still illustrate the pivotal role IoT data could play in litigation. Indeed, civil litigation, such as wrongful death or insurance fraud, could result from these highlighted cases. If we've learned anything, it's that electronic data, regardless of source, is treated like any other discoverable information. "Rule 34(a) is amended to confirm that discovery of electronically stored information stands on equal footing with discovery of paper documents." Committee Notes, 2006 Amendments, Fed. R. Civ. P. Rule 34(a). This means we need to take the same steps with IoT data as with any other physical or electronic data.

Pay special attention to whether litigation has been filed or is "reasonably foreseeable," triggering your duty to preserve evidence.

Determine if IoT data exists and is potentially relevant to the claims or defenses in the litigation.

If potentially relevant, determine if the IoT data is within your "possession, custody or control."

If so, determine if and how the IoT data can be preserved. Take reasonable steps to preserve the data and include it in your litigation hold.

Determine if the IoT data is "readily accessible" and can be collected, reviewed and produced.

Document all steps taken to identify, preserve and collect IoT data.

Raise any issues regarding the above as early as possible with your opponent and/or the court.

We are entering an era when the interconnectedness of things with the Internet will further complicate the discovery process by vastly expanding the number of electronic data sources and further exploding the volume of electronic data. The lack of IoT data standards regarding data format and storage exacerbate these complexities. In the meantime, all we can do is apply the lessons we've learned to date on handling electronic data in civil litigation.

APPLY THE LESSONS WE'VE LEARNED TO DATE




Summaries and Suggestions

A. ESI Protocol: Details can be Critical

City of Rockford v Mallinckrodt ARD, Inc, 326 FRD 489 (ND Ill 2018)

The City of Rockford, Illinois, among others, sued Mallinckrodt ARD Inc., a pharmaceutical manufacturer, on antitrust and racketeering grounds due to the company's pricing of the drug Acthar. The parties had generally agreed to the terms of an ESI protocol, including the search methodology used to create the universe of potentially responsive documents to review prior to production. But, the parties could not agree on what to do about documents not returned by using the agreed upon search methodology — technically referred to as the “null set.”



Defendant proposed that plaintiffs should review the documents produced under the search methodology. Then, if plaintiffs reasonably believed that categories of responsive documents were missing, the parties would meet and confer to discuss modifications to the agreed-upon search methodology.

Plaintiffs proposed that defendant select and review a statistical random sample of the null set and produce any responsive documents found therein. Then, the parties would meet and confer to discuss modifications to the agreed-upon search methodology.

The Court sided with the plaintiffs. Examining the proportionality factors in Rule 26(b)(1), the Court found that the importance of the issues in the case, the potential for significant damages, the defendant's possession of virtually all of the significant evidence, the defendant's resources, the criticality of ESI to resolving the issues, and the minimal burden and expense to defendant, all weighed in favor of the plaintiffs' proposal.

In cases where the burden of discovery is asymmetrical — one party possesses the vast majority of the relevant information — the proposal adopted by the Court has the potential to vastly expand that party's discovery obligations. Whenever entering into an agreed ESI protocol, the at-risk party should:

1) Resist any obligations to search the null set. Seek an agreement where the documents returned by the agreed-upon search methodology constitute the only set of documents to review. At most, agree to meet and confer if the other party can state a reasonable, good-faith basis for a belief that relevant documents are missing from the production.

2) Be prepared to show why sampling the null set is disproportionate to the needs of the case. Go through each of the proportionality factors in Rule 26(b)(1) and gather evidence (affidavits, cost estimates, etc.) to show that on balance the factors do not favor sampling the null set.

B. Rule 37(e) Spoliation Sanctions: Negligent Loss of Evidence Doesn't Warrant Stiff Sanctions

Barbera v Pearson Education, Inc, 2018 WL 4939772 (7CA Oct 12, 2018)

Employee filed a Title VII sex discrimination case against her employer alleging that she was not allowed to resign with severance pay as three similarly situated men had been allowed to do. During the course of discovery, she learned that defendant lost an email exchange she had with a senior manager regarding severance. Employee filed a Rule 37(e) motion for spoliation sanctions.

The magistrate judge found that the email should have been preserved and that its loss warranted sanctions under Rule 37(e). The magistrate did not find that defendant acted with “intent to deprive” the plaintiff of the email, limiting the

available sanctions to the less severe measures allowed under Rule 37(e)(1). The magistrate judge imposed a sanction precluding defendant from contesting plaintiff's characterization of the contents of the lost email at trial. Subsequently, the magistrate granted defendant's motion for summary judgment, and plaintiff appealed.

On appeal, plaintiff argued that the magistrate judge erred in not finding defendant intended to deprive her of the email and should have ordered that a jury be required to accept all of her proposed stipulations of fact, not just those related to the content of the email. The appellate court affirmed the magistrate's spoliation ruling. There was no evidence that defendant intended to deprive the plaintiff of the contents of the email. Even if sanctions were warranted under Rule 37(e)(2), the magistrate judge's sanction was sufficient to cure any prejudice from the loss of the email — which is the objective under both Rule 37(e)(1) and Rule 37(e)(2) — to impose the least severe sanction necessary to cure the prejudice resulting from the loss of ESI.

Accepting plaintiff's characterization of the lost email did not create any genuine issue of material fact for trial. So, the appellate court also affirmed the grant of summary judgment in defendant's favor.

Spoliation sanctions don't always have to be painful. In cases where prejudice results from the inexcusable loss of ESI, the spoliator should remember to:

- 1) Argue for the least severe sanction necessary to cure the prejudice regardless if the sanction is permitted under Rule 37(e)(1) or Rule 37(e)(2) — both require the court to impose the least severe sanction necessary to cure the prejudice.
- 2) Assess the impact of the sanction on dispositive motion practice. Summary judgment may still be possible even if the sanction mandates certain facts be taken as true.

C. Requests for Production: Requesting Metadata is Essential

Lawrence v City of New York, 2018 WL 3611963 (SDNY July 27, 2018)

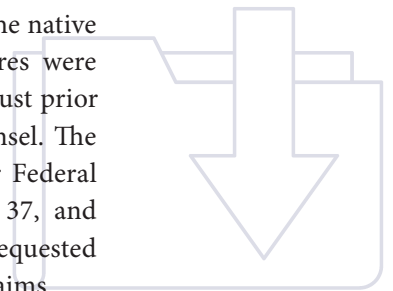
Plaintiff filed a civil rights action against police officers for injuries and damages suffered during a warrantless intrusion of plaintiff's apartment. During the incident, plaintiff alleges that the officers physically battered her, damaged her property and stole \$1,000.

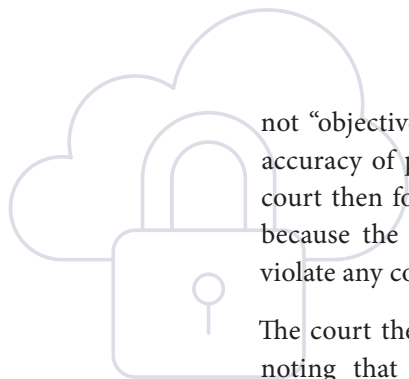
Plaintiff provided a series of photographs to her counsel that she represented were taken within a few days of the incident depicting the damages caused by the police officers. Counsel reviewed the photos, saved them to PDF files, bates-stamped them and produced them to defendants during the course of discovery.

During her deposition, plaintiff testified inconsistently as to who took the photos, first identifying her son and his friend, and later stating she took most of the photos and her son took a few, but none were taken by her son's friend. This confusion led the defendants to request plaintiff to turn over the smartphones used to take the photos. Plaintiff's counsel objected, but agreed to turn over the photos' native files.

An examination of the metadata from the native files revealed that 67 of the 70 pictures were taken two years after the incident and just prior to being turned over to plaintiff's counsel. The defendants moved for sanctions under Federal Rules of Civil Procedure 11, 26 and 37, and under the court's inherent authority, requested dismissal with prejudice of plaintiff's claims.

The court determined that defendants' rules-based grounds for dismissal were unavailable. The court found that Rule 11, which concerns pleadings, did not apply since the photos were a discovery matter. Next, the court found that Rule 26(g), which concerns discovery responses, did apply. However, the court found that the plaintiff's counsel was careless, but





not “objectively unreasonable” in certifying the accuracy of plaintiff’s discovery responses. The court then found that Rule 37(b) did not apply because the production of the photos did not violate any court order.

The court then examined its inherent authority, noting that “[b]eyond the powers conferred expressly by rule and statute, a federal court has inherent power to sanction a party for bad faith litigation conduct.” The court found that the “creation of staged photos was the beginning of a sustained effort by [plaintiff] to mislead defendants and this Court.” Fearing that any lesser sanction than dismissal with prejudice would encourage future litigants to attempt to perpetrate fraud on the court, the court concluded that plaintiff’s conduct “requires that the policy favoring adjudication on the merits yield to the need to preserve the integrity of the courts.”

In many cases, the criticality of ESI evidence depends on “when.” When was this email sent? When was this picture taken? In those cases:

- 1) If you are producing the evidence, **CHECK the metadata!** Not because you don’t trust the source, but because you could be risking your case if you don’t.
- 2) If you are requesting the evidence, **REQUEST the metadata!** Not because all opponents attempt to perpetrate a fraud on the court, but because even innocent mistakes happen that can impact the judicial truth-seeking function.

D. Requests for Production: Narrowly Tailored Is Required

McKey v US Bank National Association, 2018 WL 3344239 (D Minn July 9, 2018)

A terminated employee brought age discrimination and retaliation claims against her former employer. Defendant alleged that it terminated the employee due to poor performance. The employee originally requested that the defendant produce the complete personnel file of every employee who reported to her supervisor for the period January 2013 to present. Two days later, the employee narrowed her request to only personnel records pertaining to discipline, termination, performance conduct or performance evaluation and limiting the timeframe to January 2015 to the present. The defendant objected on the basis that the narrowed request was disproportionate to the needs of the case. The employee moved to compel.

The court ruled in favor of the employee and ordered defendant to produce the records under the narrowed request. Because the employee’s claims would likely require indirect evidence to succeed, the court found that the employment records of similarly situated employees were relevant and proportional to the needs of the case — even potentially dispositive. Moreover, the defendant made no showing of how production of the records would be unduly burdensome or of how the employee could obtain the requested information from an alternate source.

A SUSTAINED EFFORT ... TO MISLEAD DEFENDANTS AND THIS COURT.

continued on page 6



This case provides a good reminder that:

1) When it is time to file a motion to compel, courts look favorably upon narrowly tailored discovery requests.

2) When it comes time to oppose a motion to compel, courts expect to be shown why a discovery request is disproportionate — not simply being told the request is “unduly burdensome,” “too costly” etc. (as our next case demonstrates).

E. Discovery Responses/ Objections: Boilerplate Objections are Sanctionable

Wesley Corp v Zoom TV Products, LLC, 2018 WL 3722700 (ED Mich Jan 11, 2018)

Plaintiffs sued alleging that defendants had breached their settlement agreement relating to previously filed patent and trademark infringement litigation. Plaintiffs moved to compel defendants to produce documents and to amend their interrogatory responses. Defendants’ response to almost every interrogatory was:

[Defendants] object[] to this interrogatory as vague, overly broad, unduly burdensome, harassing, and/or seeking information that is irrelevant and/or not reasonably calculated to lead to the discovery of admissible evidence. Subject to, and without waiving its objection,...

And, their response to almost every document request was:

[Defendants] object[] to this request as vague, overly broad, unduly burdensome, harassing,

and/or seeking information that is irrelevant and/or not reasonably calculated to lead to the discovery of admissible evidence. Subject to, and without waiving its objection,

[Defendants] indicate[] it does not have any responsive documents within its possession, custody and control.

At the hearing on plaintiffs’ motion to compel, the parties agreed to a 45-day extension of the discovery deadline to allow defendants to amend their discovery responses. The court agreed to this extension, but did take defendants to task for their use of boilerplate objections — and granted plaintiffs’ request for attorney fees.

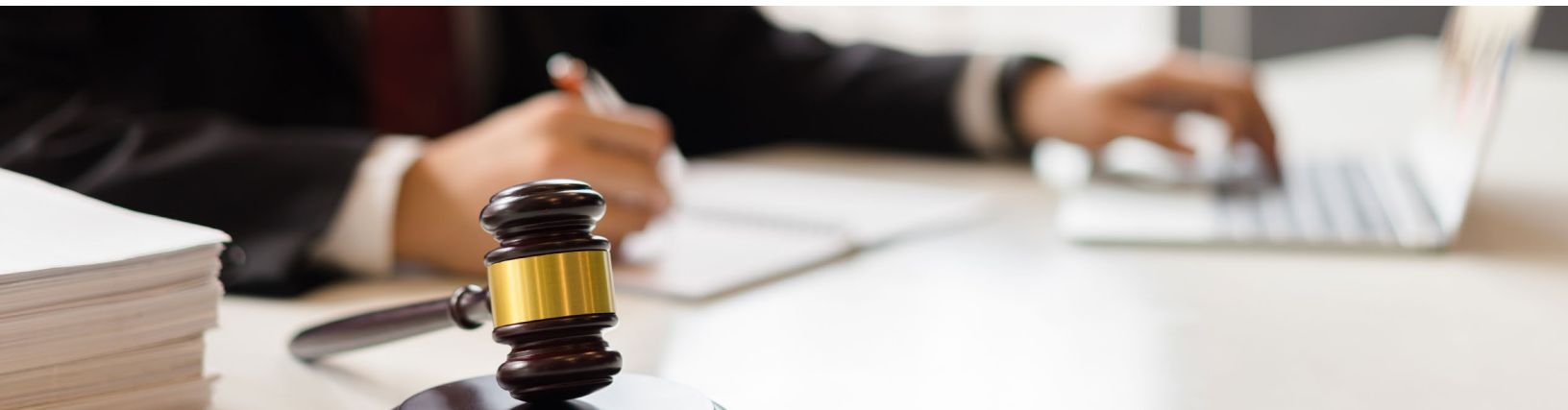
This court is not the first — nor will it be the last — to condemn the use of boilerplate objections. Indeed, perhaps the only thing more surprising than the pervasive reliance on boilerplate is the practice’s continued existence in the face of strong and widespread criticism by federal courts. (Citations omitted.) These cases, in their interpretation of the discovery rules and their denunciation of boilerplate, “are not aspirational, they are the law.” (Citation omitted.)

The court went on to state its displeasure at having to regulate the discovery process “where attorneys engage in foot-dragging and obstructionism.” The court promised that further interventions would be “accompanied by more significant sanctions...”

The lesson from this case is simple:

Do not use boilerplate objections.

MOVED TO COMPEL DEFENDANTS



When the Duty to Preserve Evidence Arises

When the focus turns to spoliation of electronically stored information (ESI) in federal court, all eyes turn to Federal Rule of Civil Procedure 37(e). The rule was amended in December 2015 to provide a uniform standard for the imposition of ESI spoliation sanctions. However, the amended rule provides no guidance on the threshold question of when the alleged spoliator's duty to preserve evidence arises. In that regard, the Advisory Notes state: "Many court decisions hold that potential litigants have a duty to preserve relevant information when litigation is reasonably foreseeable. Rule 37(e) is based on this common-law duty; it does not attempt to create a new duty to preserve." So, litigants are left to pre-amendment case law to determine the contours of the duty to preserve evidence.

Every jurisdiction uses a similar test for determining when the duty to preserve evidence is triggered. In Michigan, for instance, the Sixth Circuit Court of Appeals has held that "[t]he obligation to preserve evidence arises when the party has notice that the evidence is relevant to litigation or when a party should have known that the evidence may be relevant to future litigation." *Fujitsu Ltd v Federal Express Corp*, 247 F3d 423, 436 (6CA 2001). The court later adopted the same test with respect to ESI. *John B v Goetz*, 531 F3d 448, 459 (6CA 2008).

Once litigation is filed, there is no question the litigant's duty to preserve arises. But what about prior to the filing of litigation? What circumstances should lead a party to conclude prior to the filing of litigation that it should be preserving evidence? The more broadly that question is answered, the further back in time the duty to preserve can arise, and the greater the risk of spoliation sanctions becomes.

There is general agreement that certain events trigger the duty to preserve evidence prior to the filing of litigation. See, e.g., *Bagley v Yale University*, Civ. No. 3:13-CV-1890 (D Conn Dec

22, 2016) (duty arose before filing of suit and arguably when university staff exchanged emails noting plaintiff's threat of legal action); *Rimkus Consulting Group, Inc v Cammarata*, 688 F Supp 2d 598, 612-613 n 7 (SD Tex 2010) (duty arose for defendants when they were planning to institute a related legal action); *Jones v Bremen High Sch Dist 228*, No. 08-CV-3548 (ND Ill May 25, 2010) (duty to preserve documents arose when party received EEOC charges); *D'Onofrio v SFZ Sports Group, Inc*, No. 06-687 (DDC Aug 24, 2010) (duty to preserve evidence triggered on receipt of letter stating that sender intended to initiate litigation and requesting preservation of electronic documents); but cf. *Cache La Poudre Feeds, LLC v Land O'Lakes, Inc*, 244 FRD 614 (D Colo 2007) (no duty to preserve evidence where letters regarding dispute did not contain "unequivocal threat" of litigation).

A recent case rejected an attempt to broadly interpret the duty to preserve evidence and trigger the duty to preserve 14 years prior to the filing of litigation.

In Re Abilify (Aripiprazole) Products Liability Litigation, 2018 WL 4856767 (ND Fla Oct 5, 2018) concerns a side effect of Abilify, an antipsychotic drug prescribed to treat certain mental/mood disorders and in combination with other medication to treat depression. In the lawsuit patients alleged that using Abilify resulted in them becoming compulsive gamblers.

Plaintiffs sought emails from the 2002-2006 timeframe from defendant, but these emails were deleted pursuant to the defendant's document retention policy in place at the time. Plaintiffs moved for spoliation sanctions against defendant claiming that defendant's deletion of the emails violated its duty to preserve. Plaintiffs argued that defendant's duty attached based on:

1. Industry-wide knowledge during the 2002-2006 timeframe regarding potential side effects of drugs arguably in Abilify's class;

2. Federal regulations requiring defendant to maintain records concerning adverse drug experiences; and
3. The 2002 Pharmacovigilance agreement requiring the defendant to maintain safety-related correspondence for the benefit of the parties to the agreement.

The court rejected each of the plaintiffs' arguments and denied their motion for sanctions. The court first noted that the duty to preserve "arises once litigation is pending or reasonably foreseeable." *In re Abilify*, at *2. The court referred to the Sedona Conference principle which states that a "reasonable anticipation of litigation" arises only when "an organization is on notice of a credible probability that it will become involved in litigation, seriously contemplates litigation, or when it takes specific actions to commence litigation." *Id.*, at *3.

With regard to the industry-wide knowledge argument, the court found that it would take a "quantum leap" to find defendant's duty to preserve had been triggered based on scientific literature and litigation concerning a different drug prescribed for a different condition. The theory "improperly places too much emphasis upon events other than those generated by the plaintiff or those who are similarly situated to the plaintiff." *In re Abilify*, at *3. In this case, neither plaintiffs nor their counsel took any action prior to 2013 that would have alerted defendant to the threat of litigation.

As for the FDA regulation and the Pharmacovigilance agreement, the court found that any duty to retain documents created by either did not apply to plaintiffs. The duty under the regulations applied to the FDA, and the duty under the agreement applies to the other party thereto. The only obligation owed to plaintiffs was "the duty to reasonably preserve documents once litigation [became] foreseeable." *In re Abilify*, at *6.

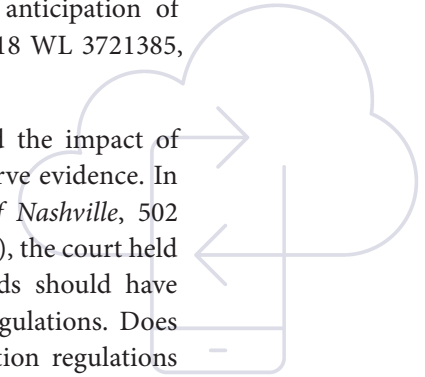
How would this case play out in Michigan? The Sixth Circuit Court of Appeals has not addressed the "industry-wide" theory, but a recent district court decision suggests that under circuit law, the outcome would be the same. In a products

liability action, the District Court for the Western District of Kentucky recently held that knowledge of substantially or reasonably similar incidents involving a defendant's products is not the same as knowledge of an alleged defect that would reasonably lead to anticipation of litigation. *Jackson v E-Z-GO*, 2018 WL 3721385, at *4 (WD Ky Aug 3, 2018).

The Sixth Circuit has addressed the impact of regulations on the duty to preserve evidence. In *Johnson v Metropolitan Gov't of Nashville*, 502 Fex Appx 523 (6CA Oct 18, 2012), the court held that deleted employment records should have been preserved under EEOC regulations. Does this mean that all record retention regulations create a duty to preserve evidence? Probably not. The EEOC regulations in the *Johnson* case have long been interpreted to inure to the benefit of employees in employment discrimination cases. See, e.g., *Hicks v Gates Rubber Co*, 833 F2d 1406 (10th Cir. 1987). As recognized by the *Abilify* court, the purpose behind the record retention regulation will determine if it creates a duty to preserve within the litigation context.

Finally, with respect to a contractual duty to preserve, no known cases within the Sixth Circuit address this issue. In a case where the litigant claiming the benefit of a contractual record retention obligation is not a party to the contract, presumably they would have to show intended third-party beneficiary status. Under Michigan state law, to be an intended third-party beneficiary, the contract must directly refer to the person or class of persons to be benefitted. The public at-large cannot qualify for intended third-party beneficiary status. *Johnson v Doodson Ins Brokerage, LLC*, 793 F.3d 674, 679 (6CA 2015). It would be a rare occurrence for a litigant to establish intended third-party beneficiary status.

Case law illustrates that the earlier in time the duty to preserve evidence is imposed, the greater the risk of spoliation. It makes sense to agree on a trigger date when possible. When not possible, assemble the evidence to establish the most favorable date for when litigation became "reasonably foreseeable."



technology

Utilizing Data Analytics to Improve Document Review

It's becoming harder to recall the time before computers, email, the Internet, smartphones and social media. The images are sepia toned ... rotary phones, handwritten letters, encyclopedias, "friending" someone by meeting them in person. Whether we long for those days or never experienced them, one thing is sure — they're not likely to return. However, technology isn't inherently good or bad — it's a tool. Used properly, it can help us be more effective and efficient. That's particularly true when it comes to litigation, especially discovery.

In the Information Age we live in, data is created every day in mind-blowing volume. 2.5 quintillion bytes per day according to one estimate (a quintillion is the number one followed by 18 zeros). To gain an appreciation for the immensity of this volume, consider that if it took one second to create one byte of data, it would take almost 80 billion years (six times the age of the universe) to create 2.5 quintillion bytes. This is happening every day... and the rate will only increase over time as more and more devices create data — from Fitbits to refrigerators.

Be they a Fortune 500 enterprise or a local "mom and pop," businesses create and store massive volumes of data. When litigation arises, all of this data becomes potentially discoverable. Sifting through this data manually just isn't possible.

"As corporate datasets have grown larger and larger, technology has endeavored to **keep evolving to meet increasing demand** for creative and efficient solutions to handle the immense volumes. Support professionals and attorneys involved in all aspects of litigation discovery must be up to date on all of the latest innovations in order to manage this demand."

ASHLEY TYLER
attorney
project manager



Special software tools and techniques have been developed to collect, cull, identify and produce the relevant information. Here are just a few that we routinely use to significantly reduce the time and expense of litigation discovery:

DE-DUPLICATING – In most organizations, more than one copy of an electronic record is stored in the system. A good example is email. An email sent company-wide can end up being stored in each email user's account. Not all copies of that email need to be reviewed and produced. We use eDiscovery software that can identify multiple copies of the same email — and keep track of who has received and kept the email, but only include one copy of the email in the review process.

DOMAIN PARSING – Like it or not, we all receive lots of junk email, even at work — some of it isn't junk, either. It's shopping — or hobby-related email or newsletters that come

continued on page 10

USED PROPERLY, IT CAN HELP US BE MORE EFFECTIVE AND EFFICIENT.

continued from page 9

from using our work email to conduct personal business. It is highly unlikely that emails from Amazon or ESPN or the local running club newsletter will contain relevant information. We use software that can identify every email domain, the “@companyname.com” portion of an email address, in a data collection. We then review those domain names and exclude all records from those that are unlikely to contain relevant information.

EMAIL THREADING – An email thread starts with the original email sent by the author. After that email is sent, it can be replied to and/or forwarded numerous times. We use eDiscovery software that can track these threads and identify which threads contain unique information. Only those threads that contain unique information, called “inclusive threads” will be included in the review process. As an example, assume an email has multiple replies, but all the replies fall within the same thread (each reply is added to the last reply in sequence). In this instance, only one email will be included in the review process because the earlier iterations of the email are redundant. Now assume someone in the thread forwarded the email to another recipient and that recipient replied back to the group. Two email threads would go into the review process: the email from the first example plus the forwarded email along with the reply.



“The “needle in the haystack” challenge in litigation is finding the most critical communications in the ever-increasing volume of business email. Data analytics, especially email threading, enables **experienced review teams to efficiently find the documents** litigators and clients need to evaluate litigation risk, respond to discovery requests, and prepare personnel to testify at depositions and trials.”



MYRA WILLIS
attorney
senior project manager

KEYWORD SEARCH – Not all documents maintained by an organization or individual will be relevant to every dispute. Keyword searches may be used to cull the universe of potentially relevant documents. To determine what words or phrases would most likely appear in documents relevant to the subject matter of the dispute, we interview the people in the organization most knowledgeable about the dispute — the “subject matter experts.” We develop a list of “keyword searches” from these interviews and import them into our eDiscovery software and have it identify the records containing those keywords and phrases. We then check to make sure the searches returned the records we would expect and fine-tune the searches as needed. Once comfortable with the keyword searches, only those documents containing the keywords are included in the review process.

DE-NISTING – NIST refers to the National Institute of Standards and Technology. NIST maintains a list of non-user created files such as executable files, that is, files used to execute

computer programs, Windows system and help files, and font files. These files exist on every computer and in every network, but typically have no evidentiary value. We use eDiscovery software that compares data collected for review against this list and remove those files from the review process beforehand.

TECHNOLOGY-ASSISTED REVIEW

(TAR) – TAR goes by other names, like Computer-Assisted Review, Machine-Assisted Review and, most notably, predictive coding. TAR refers to a process where a computer algorithm “learns” from coding decisions made by human subject matter experts — in this instance, the attorneys most knowledgeable about the case. The algorithm then applies that learning to make coding decisions in the larger review population. In the world of eDiscovery, this technology is only now becoming more prevalent as it becomes more accepted by courts. We have this technology available to us and can use it in multiple ways to reduce review costs depending on a client’s needs. It may be used as the exclusive way to identify relevant documents. It may be used to prioritize the documents most likely to be relevant for human review. Or, it may be used as a check against the coding done during human review. The more heavily the algorithm is relied upon, the less expensive the review process becomes.

There is no “typical case.” The amount of data reduction, and ultimately cost savings, that can be expected from the use of these techniques depends on the type and volume of data collected. However, we can give an example to provide some idea of how powerful these techniques can be.

Let’s assume a fairly simple case where data is collected from one computer with a 100 gigabyte hard drive. The hard drive is full, and all the data on the hard drive is collected. So, we start with 100 gigabytes of potentially relevant data. Here’s what we might expect to see using the techniques we’ve discussed.



Rather than reviewing 100 gigabytes of data, the review population is down to 5 gigabytes — a 95% reduction. The cost savings speak for themselves.

“Data analytics are a vital part of an efficient and defensible eDiscovery process. Coupled with a targeted collection performed at the direction of knowledgeable client staff and counsel, **the end result is a lean, high-relevance dataset.**”

ADAM CEFAI

attorney
litigation support manager



If you would like to see any of these data analytics techniques “in action,” we would be happy to provide a demonstration. Just contact us to arrange a date, time and place convenient for you.

USE IT IN MULTIPLE WAYS TO REDUCE THE COST OF REVIEW



Warner Norcross + Judd

These materials are for educational use only. This is not legal advice and does not create an attorney-client relationship.

401 EAST MICHIGAN AVENUE, SUITE 200, KALAMAZOO, MI 49007-5842

ADDRESS SERVICE REQUESTED

PRSR STD
U.S. Postage

PAID

Grand Rapids, MI
Permit # 564

Warner Discovery Center

Jay Yelton, Partner	jyelton@wnj.com
Myra Willis, Senior Project Manager	mwillis@wnj.com
Adam Cefai, Litigation Support Manager	acefai@wnj.com
Carrie Dearing, Staff Attorney	cdearing@wnj.com
Zach Nevenzel, Staff Attorney	znevenzel@wnj.com
Jeremy Nufer, Staff Attorney	jnufer@wnj.com
Bruce Olson, Staff Attorney	bolson@wnj.com
Todd Rooze, Staff Attorney	trooze@wnj.com
Kenneth Treece, Staff Attorney	ktreece@wnj.com
Ashley Tyler, Project Manager	atyler@wnj.com

The Warner Norcross + Judd Discovery Center offers wide-ranging eDiscovery and Data Analytic services. Our discovery professionals have 100+ years of combined expertise in discovery practice with a special emphasis on electronic data.

We are available to answer your questions regarding the discovery process and will work with you to develop a customized suite of services that fits your needs and your budget. Our services include:

Data Intake	Early Case Assessment
Data Processing	Project Management
Data Hosting	Discovery Dispute Mediation
Data Review	Discovery Management & Consulting
Data Production	
Data Analytics	