DEPARTMENT OF JUSTICE
JOURNAL OF FEDERAL LAW AND PRACTICE

Volume 68 May 2020 Number 3

United States
Department of Justice
Executive Office for
United States Attorneys
Washington, DC 20530

The Department of Justice Journal of Federal Law and Practice is published pursuant to 28 C.F.R. § 0.22(b).

The Department of Justice Journal of Federal Law and Practice is published by the Executive Office for United States Attorneys
Office of Legal Education
1620 Pendleton Street
Columbia, SC 29201

Cite as:
68 DOJ J. FED. L. & PRAC., no. 3, 2020.

Internet Address:
https://www.justice.gov/usao/resources/journal-of-federal-law-and-practice

Page Intentionally Left Blank

eLitigation

In This Issue

eLitigation

In This Issue

Foreword

Gregg N. Sofer
Counselor to the Attorney General
Office of the Attorney General

We are falling farther and farther behind. Litigating cases in a world dominated by cell phones, laptops, social media, encrypted apps, emails, and texts requires a robust capability to intake, process, analyze, organize, produce, and present in court electronic records, data, and communications. The failure to keep pace in this rapidly changing landscape is not without consequences. We have lost or settled virtuous cases because of electronic discovery problems. Many cases are not litigated efficiently, and that reduces our overall productivity. Rather than litigate cases on the merits, our opponents often try to gain a tactical advantage in court by focusing their efforts on the alleged failure of the government to turn over all discoverable materials or proficiently handle electronic evidence and exhibits in court. To fulfill the Department's mission, we must do better, and we will.

A constellation of changes in the quantity and variety of data, records, and electronic evidence collected in our criminal investigations and prosecutions, as well as in our civil practice, requires a new approach to all phases of civil and criminal litigation. Even relatively simple cases often require an analysis of vast electronic records. One cell phone can hold enough evidence to keep agents and prosecutors busy analyzing its contents for weeks or months. One incident can involve dozens of dash cam, body cam, and surveillance videos. Compounding the challenge is an increasingly multi-agency approach to investigating crime, combined with data centers where collections of reports and records are maintained in order to coordinate local, state, and federal efforts. It can be an enormous challenge to manage all of that electronic evidence across multiple agencies.

Increasingly, prosecutors are coming under scrutiny, and often criticism, from defense attorneys and judges who insist that discovery materials be provided in particular formats or with guides and indexes describing where certain materials are located. Criminal defense attorneys often accuse the government of purposely withholding materials or camouflaging critical records amongst a mountain of other discovery materials. Judges are appointing special

masters to manage discovery issues in complex cases, often dictating to the parties how discovery will be conducted. Rule 16.1 of the Federal Rules of Criminal Procedure, which became effective in December 2019, requires prosecutors to change their approach.

In this dynamic and complex environment, Department of Justice (Department) attorneys are, as they should be, held to highest standards of ethics and competency. The government is often viewed as having limitless resources and expertise to catalogue, analyze, process, and disclose discovery materials. And no Department attorney should expect leniency when the court adjudicates whether the government failed to comply with its statutory and constitutional discovery obligations. Many of our opponents are armed with advanced technology and the help of outside contractors. It is not unusual for Department lawyers to be so consumed by discovery issues that other key preparation suffers, and those that don't focus on discovery issues are exposing their cases—indeed their legal careers—to great jeopardy. Long gone are the days where prosecutors can ask their legal assistants to copy discovery provided by agents. Doing so in the current environment can be both reckless and ill-advised. After receiving comprehensive, mandatory professionalism training covering a host of complex discovery obligations, Department attorneys are often left asking, "I know what I have to do, but *how* am I supposed to do it?"

The answer is eLitigation competency. The Department is working hard to enhance its eLitigation capabilities. eLitigation is a term that describes an integrated approach to litigation that encompasses the employee skills, training, and associated best practices, as well as the technology-based tools, needed to handle the identification, collection, processing, review, analysis, production, and presentation of electronic evidence. While eLitigation includes the practice of producing electronic discovery (eDiscovery), it goes well beyond production and encompasses the entire lifecycle of electronic evidence. Developing eLitigation expertise is essential to succeeding in the increasingly complicated digital milieu. Every attorney and support staff member involved in the Department's litigation efforts must develop eLitigation skills and proficiencies to keep up—both with the changes we are experiencing now and those that will inevitably and exponentially increase with technological advances such as 5G technology. No office, component, support staff member, or attorney

can be left behind to fend for themselves. Everyone needs the proper suite of tools and relevant core competencies.

Our colleagues have written the articles in this issue to share their experiences and insights about how to succeed in managing electronic evidence. Their advice goes to the very heart of what each of us must learn in order to be successful litigators. The Department's mission remains the same. How we do it has changed. And the Department is changing to better support your hard work.

Page Intentionally Left Blank

Introduction

Christine Corndorf
eLitigation Coordinator
Executive Office for United States Attorneys

John Haried
Criminal eLitigation Coordinator
Executive Office for United States Attorneys

Susan Cooke
Litigation Technology Coordinator
Executive Office for United States Attorneys

Virginia Vance
Senior Litigation Counsel for Civil eDiscovery
Executive Office for United States Attorneys

Donna Miller
Document Management Systems Coordinator
Executive Office for United States Attorneys

The electronic evidence revolution has created new opportunities to litigate cases more effectively and efficiently, but to seize those opportunities, we must all embrace new business practices. As Gregg Sofer noted in his foreword to this issue, within the United States Attorneys' Offices (USAOs) community, these new practices are referred to as "eLitigation." eLitigation goes beyond eDiscovery; it also includes developing offices' structures, employees skills, and sound practices that appropriately incorporate technology-based tools and address the challenges created by growing volumes of digital case information.

eLitigation presents a unique challenge for USAOs and their Department of Justice (Department) counterparts because of our unique position in the legal community. Our practice is incredibly diverse: We investigate and prosecute a wide range of federal crimes, from complex cyber cases and white collar matters to drug and gun cases along with violent crimes; we defend the government against a variety of civil claims, from tort and contract to medical malpractice and employment matters; we also investigate and litigate affirmative civil matters on behalf of the United States, from civil rights suits and *qui tam* actions to environmental claims. Our cases vary in type, complexity, and size, but the eLitigation challenges remain the same: The identification, assessment, production, and presentation of

discoverable information from a variety of sources in a defensible manner.

These tasks are complicated by the vast array of electronic data types and formats the government, as investigator, prosecutor, or civil litigant, has legal access to but little control over—for example, evidence collected by state and local investigators, social media and electronic data provided by technology companies pursuant to search warrants, video and audio evidence captured in unique and sometimes proprietary formats by security systems, and bank records provided in unique and sometimes low-tech formats. Furthermore, because we face opposing counsel with varying levels of technological sophistication, we have to be agile enough to adapt our practices to ensure that our discovery obligations are met.

At the same time, Assistant United States Attorneys (AUSAs) and their Department colleagues are well positioned to take advantage of the opportunities created by effectively using federal rules and legal precedent, eLitigation tools, eLitigation best practices, empowered support staff, and dedicated AUSAs who support eLitigation workflows and best practices within USAOs. The articles in this issue discuss these important eLitigation issues and best practices, but they do not address *all* eLitigation issues. Rather, they focus on hot-button matters. By approaching the complexities of eLitigation from a framework of real-world experience and concrete scenarios, we hope that the articles in this issue can provide practical guidance.

Finally, there are many eLitigation experts within the Department who stand ready to help case teams as they confront difficult and novel questions, assess workflows, and employ best practices. The authors of the articles in this issue are a resource, as are the eDiscovery and eLitigation coordinators in the Department's litigating components. For USAOs, subject matter experts with the Office of Legal Programs at the Executive Office for United States Attorneys can assist USAO management and case teams with legal and technical guidance as they continue to improve their eLitigation practices. By leveraging this expertise and continuing the dialogue about eLitigation best practices and resources, together we can continue to develop our eLitigation competency.

Building a Successful eLitigation Practice and the Case for an AUSA Leading the Charge

Lisa Dunn
Assistant United States Attorney
Northern District of Texas
Dallas Criminal Division

Laura L. Hall
Assistant United States Attorney
Western District of Kentucky

I. What you can learn from our experiences

Over the past two years, our U.S. Attorney's Offices (USAOs)—the Northern District of Texas (NDTX) and the Western District of Kentucky (WDKY)—have increased overall productivity, improved the quality of our case work, avoided errors that used to plague us, and reduced everyone's stress. We did that by instituting better, standardized electronic litigation (eLitigation) practices. We are still pushing through the inevitable kinks and growing pains—it is a process. But our people are more confident.

Here are the critical gains we now enjoy. We manage our cases instead of our cases managing us. Our cases are better organized, which allows everyone to focus on the substantive issues of a case instead of wasting time trying to locate misplaced case material or learn a lawyer's or paralegal's idiosyncratic system. Our discovery productions are more complete and reliable, and if we are accused of a discovery error, we are able to defend ourselves better—we can either prove there was no error or prove that an error was an anomaly, not an egregious error warranting court sanctions. Standardized practices mean anyone—a lawyer, staffer, or agent—can come into a case, even at the last minute, and be effective because they know how the case is organized. We are using litigation software tools that improve our efficiency and effectiveness—Eclipse, Relativity, CaseMap, and Trial Director.

Each of us was charged with leading the revolution. We are experienced Assistant U.S. Attorneys (AUSAs). At the start, we were not strong on technology, but that did not matter. What mattered most were the skills we honed as AUSAs: our knowledge and

judgement about litigation, our ability to communicate and advocate, and our ability to be ambassadors both within the office and with external stakeholders, such as the court, opposing counsel, law enforcement agencies, and client agencies.

Your office can achieve the same gains. As AUSAs from two offices that have overhauled their eLitigation practices, we tell our stories here and share what we see as the imperatives behind installing an AUSA as the office's leader of eLitigation change.

II. A tale of two districts

"*It was the best of times, it was the worst of times, it was the age of wisdom, it was the age of foolishness . . . it was the spring of hope, it was the winter of despair . . . .*" [1]

Who knew that in 1859 Charles Dickens would so accurately describe what it means for a USAO to embark on building an eLitigation practice or that office morale during the process would be so akin to that during the French Revolution? Of course, that is a shameless over-exaggeration, but the opening lines of a *Tale of Two Cities* are an amusing yet appropriate backdrop for discussing our views on building a successful eLitigation practice in house and our perspectives as attorneys leading the charge in our respective USAOs. Indeed, it is an exciting prospect for an office to start this journey, but there are inevitable bumps along the way, which makes for both a good and not-always-so-good experience.

As we are well into what some call the *Digital Age*, more and more U.S. Attorneys are seeing the value and necessity of revamping their practices, policies, and office culture around eLitigation and discovery issues. Initially, some USAOs looked to systems managers or tech-savvy support staff to suggest changes. Recently, USAOs like ours have taken a different approach and turned, instead, to an experienced attorney to manage their office's eLitigation evolution. This model is used in many private law firms. Does it work? Well . . . we still have our heads (at least for now), and as this article's title suggests, we not only agree that it works, we also believe that an experienced AUSAs *must* lead the charge if a USAO wants to build a successful, comprehensive eLitigation program that extends well beyond the technical mechanics of processing and producing discovery.

---

[1] CHARLES DICKENS, A TALE OF TWO CITIES 1 (Dover Pub'ns, Inc.) (1859).

III. An awakening? Identifying the need for better eLitigation practices

Both of our offices were motivated to change because we had struggles:

NDTX. In 2017, we were well behind the times in terms of discovery management. It was catching up to us whether we realized it or not. Attorneys became anxious about discovery: Had agents turned over all of the case material? Had or hadn't we produced certain items to the defense? When did we produce them? Why didn't we produce them? AUSAs and staff became frustrated with the way agents provided investigative case materials to our office—materials that often required AUSAs and staff to wade through a sea of duplicates, try unsuccessfully to open files in non-standard formats, or make sense of a disorganized data dump. We had no uniform method for tracking our case materials from intake through discovery production. Few attorneys knew of document review tools like Eclipse and Relativity or how to use them. Those who did were not fans of either—so these tools were avoided. We lived in a world full of binders and printed paper. In the 21st century, we were still managing our case materials in the dark ages.

WDKY. Before 2018, the office had no standardized method for receiving investigative material, tracking and reviewing that material, and producing discovery. Rather, each AUSA used her own individualized methods to complete these tasks. While some methods were more successful than others, the lack of uniformity and standardized practices meant an overall lack of efficiency and unbalanced workloads among support staff. Also, we were concerned about whether our discovery productions were complete. Had we received everything from our agents? Had we fully complied with Rule 16 and the court's discovery orders? Was our district going to start seeing more motions claiming discovery violations like those that plagued other districts? If so, were we going to be able to successfully defend our discovery practices? And, like the NDTX, we were underutilizing available litigation software tools.

A. Northern District of Texas

The USAO for the NDTX serves an extra-large district with about 105 AUSAs serving 7 million residents over 96,000 square miles and 100 counties. About half of the AUSAs practice in the Dallas office, and the other half are spread among four satellite offices. For the last five years, NDTX has been one of the most productive USAOs in terms of criminal cases filed and defendants charged per AUSA—meaning we were all very busy, which exacerbated our risks around discovery management.

When Erin Nealy Cox, the U.S. Attorney for the Northern District of Texas, was appointed in November 2017, she quickly assessed the office's discovery practices and workflows. In January 2018, she constructed a plan for building a comprehensive, office-wide eLitigation practice, to include a stand-alone Litigation Technology Unit (LTU). Its mission: to facilitate office-wide discovery and case-management practices, to provide litigation support and consultation at every stage of litigation, and to work across divisions to set best practices to bridge the gap between the practice of law and technology.

Ms. Nealy Cox created an entirely new position to head the LTU—Senior Litigation Counsel for Litigation Support—dedicated to standing up the LTU and managing all aspects of eLitigation for the office. She selected me, Lisa Dunn, a criminal AUSA, to assume this new leadership position. Candidly, at the time I was not sure I was the right person for the job. I started my career in 1995 as an Assistant District Attorney in Oklahoma City. I became a federal prosecutor in 2001. Since then, along with trying a lot of cases (but not a lot of complex fraud cases), I have enjoyed a variety of experiences both outside the USAO, including at EOUSA in the General Counsel's Office, and in the USAO as the Ethics Advisor, the Professional Responsibility Officer, the Civil Rights Coordinator, the supervisor of one of our fraud sections, and the chief of the Criminal Division. At the time I was asked to become the Senior Litigation Counsel for Litigation Support, I was terrified and uncertain about what the new position would look like and how it would function in the office. The title "Litigation Technology Unit" intimidated me—I knew how to "litigate," but I was incredibly uncomfortable with the "technology" aspect. After all, I am an attorney, not a technical expert. And as I mentioned, most people in our USAO were unfamiliar and inexperienced with the processes and tools associated with good

eLitigation practices, and I was most certainly one of them. But now I can see how my experience as an AUSA enabled me to lead the eLitigation revolution in my USAO despite my technical shortcomings. More on that below.

B. Western District of Kentucky

The USAO for the WDKY serves a medium-sized district with approximately 80 staff members, half of whom are AUSAs. The district encompasses 53 counties, a population of more than 2.2 million, and two military installations. We prosecute a wide variety of criminal offenses, from petty offenses occurring at Fort Knox, Fort Campbell, and Mammoth Cave National Park, to district-wide offenses such as public corruption, child exploitation, civil rights violations, and elder fraud. Like other districts, our white collar crimes and health care fraud prosecutions are document intensive. Because primary north-south and east-west routes of the Interstate Highway System intersect in our district, we have a significant drug trafficking and money laundering caseload. With the drug crimes, gun crimes are as prevalent as they are in many other major U.S. cities. Top priorities of Russell M. Coleman, the U.S. Attorney for the Western District of Kentucky, include reducing the violent crime and narcotics trafficking plaguing the district. Mr. Coleman previously served as an FBI Special Agent.

Soon after being sworn in, U.S. Attorney Coleman recognized the challenges of prosecuting cases in the digital age. He embraced eLitigation change in the office. Under his leadership, we launched a Litigation Support Unit (LSU), and the office began using a uniform method to track and review investigative material, typically consisting of large volume and complex types of material. The office also began producing discovery in a uniform way. The office created a new position, LSU Attorney Coordinator, tasked with working with case teams to implement eLitigation changes and managing the day-to-day work of the LSU while meeting the litigation needs of the case teams. I, Laura Hall, was selected for this new position. When I started in the fall of 2017, I had no idea what I was getting into. I considered myself inexperienced with eLitigation. Although a bit embarrassing to admit, I had only been using an electronic calendar for a couple of years. I had been a prosecutor for 12 years in state court and more than 15 as an AUSA— more than 27 years in all. During my entire career, I never prosecuted document-intensive white collar offenses but rather handled cases involving drug and gun offenses, including reactive

cases. I was not aware of tools like Eclipse to help manage and review case material; the only "eclipse" I knew about was the August 2017 total solar eclipse that passed directly across our district. That said, I had always embraced technology in my personal life, and knew I could do the same professionally. And with so many experts and resources available in my office and throughout the USAO community, I had no trouble arming myself with the technological knowledge I needed to lead our LSU to success.

IV. Establishing a new order: centralization and standardization

USAOs that do not already have a well-established eLitigation practice, either through the use of a LTU, a LSU, or some other dedicated electronic litigation-centric unit/section must likely start from scratch, revamping current practices, in essence, sparking a "revolution" that demands broad sweeping change (to stick with our Dickens theme). In this section, we will describe the key changes our offices implemented. Understanding the scope of these changes will give context to the significant substantive work an eLitigation AUSA must perform.

A. Northern District of Texas

One of the key components to the eLitigation revolution in the NDTX was the establishment of the LTU. While describing how to create such a unit is outside of the scope of this article,[2] it is important to recognize its role and how it fits into the office. In the NDTX, the LTU, which is currently comprised of four Litigation Technology Specialists, serves our entire district (main office and four satellite offices). While it most heavily serves the Criminal Division, it is also a resource for the Civil Division. The LTU processes most of our case data; creates, loads, and administers Eclipse databases; pushes out discovery productions; and project-manages a small number of cases outsourced to the Litigation Technology Service Center (LTSC). Beyond case-specific projects, the LTU also trains staff and attorneys on all relevant litigation-support programs/software,

[2] For more information on how one district set up a Discovery Center, which is one type of LSU, see Bryan Schroder & Aunnie Steward, *Pioneering a Modern Discovery Process: District of Alaska's Discovery Center*, 66 DOJ J. FED. L. & PRAC., no. 5, 2018, at 51.

provides technical advice at discovery case meetings and conferences, and regularly troubleshoots for the support staff on a variety of litigation-support issues. I directly supervise the unit, meet with the team weekly, oversee its work, and prioritize the workflow. I report directly to the Managing AUSA (also known as the Executive AUSA in other districts), so the LTU sits outside of the litigating divisions' chain-of-command.

Another key component was establishing standardized practices for the LTU and the office as a whole. In developing the office's policies and protocols, I quickly recognized that they had to be stringent enough to be legally defensible without sacrificing the flexibility needed when the best-laid plans go wrong. For example, one of the first changes implemented in the NDTX was the adoption of standardized electronic file practices. I worked with the office's various divisions, both criminal and civil, to develop a uniform folder structure, and we moved all of our case files and case-related materials to the Cloud. This common folder structure kept our cases organized so that if a member of the case team was unavailable or the case was reassigned, newly assigned employees could easily locate case materials and work product. The common structure, however, was not so detailed and rigid that attorneys were not allowed the freedom to create their own subfolders per their particular organizational preferences or tailored to particular needs of a case. We also implemented for all criminal cases an intake and discovery production tracking system that required a designated USAO case team member (Discovery POC) to log all incoming and outgoing discovery for the case. While there is a default designee (who is the litigation support paralegal), AUSAs can designate whomever they wish as the Discovery POC, including themselves if they determine that is best for the case. One of the most important standard practices we set were baseline requirements for discovery productions in all cases: All productions must be searchable, trackable (for example, Bates numbered), indexed, and accompanied by a production letter. That said, as the Senior Litigation Counsel for Litigation Support, I retained the discretion to determine on a case-by-case basis when (and if) to diverge from these baseline requirements and how to implement the best "Plan B" for case teams in the event of unexpected time constraints or difficult, court-ordered discovery deadlines. Having an AUSA dedicated to making fast decisions about these issues gave attorneys the assurance that they could still meet court-mandated

deadlines even if, for reasons outside of their control, they could not strictly comply with NDTX policy. Instead, I stand ready to approve an exception to the rule as appropriate to keep teams in good stead with the court and safely moving forward in compliance with their discovery obligations.

Moreover, it was critically important to recognize that the scope of the changes necessary to build a successful eLitigation practice did not stop at our USAO's doors. It meant involving our law enforcement partners, opposing counsel, and even the court to achieve a legally defensible protocol that accounts for not only how the USAO manages discovery in house, but also how we receive case material from our agents and how we produce it. This 360-degree approach led to tremendous changes that enabled our internal policies to complement the efforts of our external counterparts, leading to less confusion and more transparency in the discovery process.

B. Western District of Kentucky

In the WDKY, one of the central components of our eLitigation change was establishing a unit dedicated to litigation support tasks—which we call the LSU. The LSU is separate from both the criminal and civil divisions, and its staff is supervised by the office's First Assistant United States Attorney. The LSU consists of a full-time AUSA as its coordinator and three staff members who process case material, build Eclipse databases, create discovery and other exports, and coordinate work with the LTSC in South Carolina. The LSU also performs tasks related to courtroom presentations, such as converting audio and video files and loading them onto iPads.

With the opening of the LSU, a radical but necessary change occurred in the way the criminal division received investigative case material, tracked and reviewed that material, and produced discovery. It shifted from each AUSA using his or her own individualized methods to a standardized framework for these tasks. The benefits are described below.

This framework includes a standardized process for tracking case material from the point it comes into the office, to if and when it is produced in discovery. This process includes using one case manifest per case, which is stored in the case's electronic file. The case manifest is an Excel spreadsheet with three parts: a collection log, a discovery index, and a production log. The information logged on the case manifest and contained in its three parts serve as proof that our

standardized practices were followed and can be used when defending against discovery violation motions.

When any criminal or civil case material is received, a designated WDKY staff member must enter its tracking information in the collection log of the case manifest. When the AUSA is ready for the material to be processed and loaded into either an Eclipse or Relativity review database, a case team member submits a work ticket to the LSU who performs this task. Case teams are required to use Eclipse or Relativity to more efficiently review, organize and redact material, and select material for upcoming discovery productions.[3] After the AUSA has selected discovery and completed redactions in the review database, a case team member submits a work ticket to the LSU who will create both an electronic export of the selected discovery and the discovery index of the case manifest. Lastly, when the discovery is transmitted to opposing counsel, the designated case team member enters the tracking information in the production log of the case manifest.

As in the NDTX, we see law enforcement as a vital partner, and we want to ensure that their evidence collection and organization methods complement our internal eLitigation efforts. As part of this effort, we created written guidelines for how we want investigators to organize and format the case materials they provide us. I provided training to investigators on our guidelines, and the office now requires investigators to follow the guidelines when providing materials.

Today, the WDKY would not choose to revert to our old ways—not the U.S. Attorney, not the lawyers, not the staff. Everyone is happier and more confident.

C. The benefits of centralization and standardization

If you are feeling overwhelmed by the prospect of building a standardized workflow from the ground up, do not be deterred. We have seen that the destination is very much worth the journey. Yes, it was overwhelming, and frustrating, and exhausting. But at the same time, it was very rewarding and invigorating. With the right AUSA

[3] If material is too large to store in a review database, as is often the case with computer or smart phone forensic examinations, a place holder is added to the review database, and the native material is stored in a central location. A place holder is also used for material that cannot be loaded into a review database, for instance when it can only be viewed using a proprietary player.

leading the charge, any USAO can get a formal, standardized eLitigation practice up and running. Then, once it is operational, seeing its success will have you questioning how you survived without one. In fact, U.S. Attorney Coleman often describes the WDKY's LSU and its associated standard practices as revolutionary.

Having *and following* a formal, standardized workflow to manage case material and discovery is essential to realizing several key benefits. First and foremost, it allows us to be better organized, which saves time and lowers stress. Better organization also allows us to improve our efficiency, which means more time can be spent on the substantive issues of a case instead of wasting time trying to locate misplaced case material. And naturally, more time spent on the substantive issues of a case ensures better case results. Ultimately, a standardized workflow enabled our offices to manage our cases instead of our cases managing us, moving us away from deadline driven discovery productions to quality driven discovery productions.

Having a standardized workflow also allows us to better defend ourselves in court against motions alleging discovery violations. If a discovery mistake were to happen in a case, being able to respond by describing a standardized workflow and offering proof that it was followed will more likely convince the court that the mistake was an anomaly and not a pattern likely to be repeated. Thus, the court will be more likely to rule in our favor and less likely to issue sanctions that could jeopardize our case.

Another benefit of a standardized workflow is more balanced workloads among USAO staff. Each case team member will know the exact task for which he or she is responsible for during the case's life, and the tasks can be equitably divided to optimize productivity. This standardization allows for interchangeability, and it eliminates the need for one AUSA or paralegal having to learn, or even worse, guess, another's idiosyncratic system. If one paralegal needs to cover for another in the middle of a case, or even one AUSA for another, it is accomplished seamlessly by using the standardized tracking logs to determine what case material has been received and what, if any, has been produced in discovery. In a criminal case, it is even helpful when a new agent takes over a case. The new case agent can see from the USAO's tracking log exactly what the previous case agent provided and can avoid bogging the case team down by providing duplicate material.

Standardized workflows incorporate software tools that further improve our efficiency and effectiveness. Tools like Eclipse, Relativity, CaseMap, and Trial Director are available to all USAOs. They are easy to use and should now be a part of our everyday practice. Consider their use as being akin to how we now Shepardize our case law. We no longer manually use Shepard's paper volumes to check case citations; instead, those tasks are automated by computer software, which saves a tremendous amount of time. It would be ludicrous to Shepardize a case now using those old books (assuming they are even still in libraries); it is an equally ludicrous proposition to not use the other software tools that enhance our efficiency and effectiveness as litigators.

V. Every revolution needs a strong, competent leader: the case for an eLitigation AUSA

Given the challenges of eLitigation and the amount of coordination and effort required to create and support eLitigation policies, workflows, and best practices, it is critically important to have an AUSA lead these efforts. But if you are thinking, "there is absolutely no way an AUSA can be taken off the line in my office" to perform this work, we urge you to reconsider. You will not be taking an AUSA off the line at all. To the contrary, you will be taking the substantial time and effort that all your AUSAs would otherwise inefficiently spend on electronic litigation issues and reassigning it to one AUSA who will do it better and faster. You will gain overall improved efficiency and effectiveness flowing from specialization and expertise that will more than make up for the fact that an AUSA has been reassigned to improve the handling of all your office's cases.

It reminds us of that parable about sharpening the saw: Two loggers are in the woods sawing down trees. One logger feverishly sawed and sawed, never stopping. The second logger stopped sawing at regular intervals, leaving the forest each time for a few minutes before returning. At the end of the week, the first logger had barely made a dent in his section, only cutting down a few trees despite not taking a single break. But the second logger had chopped down all of the trees in his section. The first logger was dumbfounded. He could not understand how the second logger cut down so many more trees despite taking so many regular breaks. When the first logger asked the second where he had disappeared to so regularly, the second

answered that he kept leaving to go sharpen his saw. By taking the time to maintain a sharp saw, the second logger was much more effective and efficient than the first. So when you pull an AUSA off the line to lead the office's eLitigation efforts, consider it to be sharpening your office's saw. Despite having one less AUSA assigned to individual cases, your office will be able to accomplish more across all of its cases because it will operate more effectively and efficiently.

"But," you may ask, "must it be an AUSA?" In our experience, the answer is a resounding, "Yes!" An experienced AUSA is best-positioned to achieve success because only an AUSA can fill the following indispensable roles.

The driver of change. Think about all of the decisions that have to be made to implement eLitigation changes in the office. For example, will the new protocols be mandatory for all case types or only for some? In which division, civil or criminal, or both? How will your staff be trained to follow the new protocols? What steps can be taken to best encourage staff to want to follow the new protocols? How will you transition to using the new protocols? Will the start date be based on the date a case is opened or the date case material arrives in your office? Will you require a portion of your protocols to be mandatory, for example, the logging and tracking of incoming material, while other portions are optional, for example, the use of a review database like Eclipse? How will you train your staff to use Eclipse considering any differences in experience levels? What permissions will you give your staff, and what standardized tags can be created so their use of Eclipse is optimized? Which network drive will you use to store the material going into Eclipse? If using the cloud, is your office willing to incur the related expense? When a case is closed, who will be responsible for deleting the Eclipse material from the designated drive, and when will the deletion occur? If you have staffed satellite offices separate from your main office, how will you successfully transfer data between office drives without it having a negative effect on your network? If you decide to establish a LSU, what system will you use to get and manage your LSU's work requests? Who will supervise your new LSU? Will your new LSU's staff, especially your unit's AUSA, need revised performance work plans?

Only an eLitigation AUSA can provide the judgement and insights necessary to guide the management team in answering these questions. An AUSA is able to talk to and learn from other AUSAs in similar positions throughout the USAO community, become adept at

technology-specific case issues, investigate the options available to your office based on its size and needs, weigh the pros and cons of the options, and make an informed recommendation to office leadership. An experienced AUSA is particularly well suited to do so because of their practical understanding of, and experience with, all steps in litigation. Better than an IT systems manager or technologist, an AUSA understands what the district's judges require and what challenges case teams face when dealing with investigators, agencies, and opposing counsel. Drawing on this understanding, an AUSA can tailor standard practices and workflows to accommodate what case teams really need to best accomplish the mission of the office.

Further, an AUSA dedicated to eLitigation issues can get in the weeds and *stay there* so office leadership and line AUSAs do not have to. The eLitigation AUSA can keep a constant eye on new and emerging trends in the field and emerging legal issues and help ensure that the USAO continues to move forward.

The Manager and Bridge Builder. Both of us oversee the operation of our LSUs. In this role, we prioritize and manage our unit's work, ensuring that case-related deadlines are timely met. Managing shifting priorities between cases is critical, and it requires an AUSA's judgment and authority. We have also been involved in hiring staff, designing and outfitting office space, acquiring equipment, and ensuring that litigation technology specialists are properly trained.

An AUSA brings an important perspective to this management role: They serve to bridge the thought process gap between litigation support personnel and the case AUSA who is—and should be—laser focused on cases. Quite simply, the litigation support brain and the case AUSA brain think differently because they have different training, experiences, and responsibilities.

Having an AUSA's thought process and constant presence in a LSU is the best way to ensure that the finished product fully meets the AUSA's needs every single time. It ensures that a case's technological-related problems are resolved to meet the AUSA's needs, led by the eLitigation AUSA. And it frees up the case AUSA to focus solely on the case's substantive issues while the eLitigation AUSA works though the case's technology issues in conjunction with litigation support personnel. In fact, the eLitigation AUSA can and should be a part of every single case early on in order to identify

potential technical problems related to litigation support and proactively work to solve those problems from the beginning.

Having had similar professional training and case experience, the eLitigation AUSA is a credible voice, a voice that speaks the same language as the case AUSA when discussing technology issues. When explained by a peer, the case AUSA is more likely to understand and accept the fact that litigation support personnel do not have "an easy button" to perform tasks and that some tasks take a certain amount of time to complete. This also allows litigation support personnel to feel, and actually be, supported. The eLitigation AUSA is better able to educate litigation support personnel about litigation-related issues. For example, when litigation support personnel are frustrated about having to process incoming case materials in a piecemeal fashion, the eLitigation AUSA can remind them that the case AUSA is not purposely trying to make a litigation support personnel's work more challenging. Instead, the case AUSA is receiving the material in a piecemeal fashion and may be equally frustrated.

Ultimately, instead of AUSAs and litigation support personnel existing on separate islands, the eLitigation AUSA can be the constant bridge between the two. Ideally, the eLitigation AUSA will equally have the backs of litigation support personnel and the case AUSA, all while ensuring the case AUSA's litigation needs are fully and timely met. That enables better communication, which results in a more harmonious and less contentious work environment, leading to increased productivity and improved morale.

The advocate. If there's one thing AUSAs know how to do, it is advocate. Without question, the eLitigation AUSA position requires full-time advocacy for the USAO's interests—even within the office—on a daily basis. eLitigation is ever-changing. For that reason, an eLitigation AUSA is constantly evaluating the USAO's needs and convincing someone to act—whether that is making the case for more litigation support personnel, encouraging an AUSA to use Eclipse, convincing a supervisory law enforcement agent to direct his forensics agents to use different processing tools for better compatibility with our processing software, and on and on. The eLitigation AUSA consistently engages, collaborates, negotiates, coordinates, and when appropriate, gently pushes the envelope with personnel in every office division and up to the highest ranks to advance and maintain each building block in an office's eLitigation practice.

The bottom line is that this role goes well beyond managing litigation support functions, which itself is a significant undertaking. It requires someone with an intimate understanding of the daily responsibilities and burdens of an AUSA and someone who can and will effectively advocate for the USAO from that perspective. Who better to lead this effort than an experienced AUSA?

The Ambassador. As we have emphasized, building a comprehensive eLitigation practice necessarily involves including our law enforcement partners and other outside stakeholders that directly impact the USAO's workflows. This effort requires frequently reaching out directly to agency leadership, the Federal Defender, and judges—a role uniquely suited to an experienced AUSA. In particular, when (1) forming guidelines for how agents provide case materials to the USAO for discovery; and (2) setting uniform standards for outgoing discovery productions in criminal and civil cases, an eLitigation AUSA's leadership is critical to success. These projects require frequent meetings with supervisory law enforcement agents and their chief division counsel, the Federal Defender and the chair of the Criminal Justice Act (CJA) panel attorneys, and magistrate judges, amongst others, to push for change, acknowledge their interests, explain the USAO's interests, and draft and formulate collaborative and effective guidelines and standards that will improve our overall work product and process. Simply put, such meetings and discussions, which are essential to a comprehensive eLitigation overhaul, can only be handled by an attorney, and most appropriately by an experienced attorney accustomed to negotiating and engaging with law enforcement representatives, opposing counsel, and judges.

The full-time, dedicated resource. But you may be thinking, do we really have to dedicate a *full-time* AUSA to this position? In our experience, the answer is, again, a resounding, "Yes!" We do not have regular dockets, nor could we work one properly if we did. This role, however, is legal work that heavily calls upon our AUSA expertise and requires our full-time attention. We make the other AUSAs much more efficient and productive. As eLitigation AUSAs, we directly oversee our LSU and their technical staff. We also serve as the central eLitigation trainer for AUSAs and staff; the primary case consultant for eLitigation legal and technical issues; the eLitigation advisor to USAO senior management; and our offices' liaison to Main Justice, outside agencies, and the court on all technical and legal eLitigation issues. We are responsible for keeping an eye on emerging eLitigation

issues and topics (and advising accordingly), creating go-bys, and consulting on legal briefs on eLitigation issues. Having served in this role for over two years, we can confirm that, to do it well, the amount of time and work involved in building and sustaining an eLitigation practice is easily a full-time job.

VI. Identifying the right eLitigation AUSA

Now that we have convinced you of the wisdom of creating the eLitigation AUSA position within your office, you must choose an AUSA for the position. What qualities must this person possess?

Litigation experience. The eLitigation AUSA should have a good deal of practical experience in litigation, in the courtroom, and in handling a variety of evidence types. Having sufficient practical case experience gives an eLitigation AUSA the background knowledge needed to see the big picture and know what strategies are workable for your particular office. With this experience, the AUSA will know what the desired end results are and can work backwards when developing protocols to reach the desired end. An inexperienced AUSA who has never seen "the end" is less likely to develop protocols that work for the end. Wisdom is required. Experienced AUSAs have the honed instincts and judgment from working cases to know when it's appropriate to break with standard practice if it becomes an impediment to satisfying a judge, fulfilling a legal obligation, or accomplishing the mission. A veteran AUSA who already has established credibility in the office may also find more success in making recommendations for change, as their peers may be more likely to trust and follow their lead. This established credibility allows the AUSA to get to yes quickly or push through the inevitable "no's," "can't do's," and other obstacles as changes are implemented.

Relationship builder. Building a new eLitigation practice for your office does not mean reinventing the wheel. Others in the USAO community are ready, willing, and able to help you. Finding success involves researching existing practices in other USAOs and figuring out what to borrow and what to ignore. An eLitigation AUSA proactively identifies and reaches out to people in other USAOs that are doing eLitigation right. Depending on the situation, networking on behalf of your USAO can be intimidating, and some perceive a solicitation for consultation or model processes as an admission of weakness. An effective eLitigation AUSA is willing and able to forge new connections with subject-matter experts occupying a variety of

positions in other USAOs, at EOUSA, and elsewhere. These connections are critical; they allow your office to benefit from other USAOs' successes and learn from their mistakes.

Positive problem solver. Having a cache of positive and valuable relationships outside of your office is only half of the equation. Relationships within your office are just as important, maybe even more so. An eLitigation AUSA who can adapt and positively solve a problem regardless of its source and type will likely be more successful. Being able to offer encouragement, optimism, support, and understanding when solving problems helps to ensure solutions are accepted even when everyone may not get exactly what they want.

Attention to detail. It is important for the eLitigation AUSA to be detail-oriented and have strong organizational skills. You certainly would not want to tap an AUSA who has a history of misplacing files with the task of building protocols designed to effectively track and manage everyone's case materials.

A willingness to learn key technical considerations and tools. All of the above being said, have you noticed that there was no mention of the AUSA being an expert in eLitigation or information technology? We did not overlook this trait; it is simply not as important as the others. We are living proof: As discussed above, neither of us brought technical expertise to the eLitigation AUSA position. But we each had a willingness to learn the technical aspects of our job, especially where legal considerations informed the technical choices that we had to make. These technical aspects can be learned; the instincts and experience of an AUSA that are critical to the big picture success of an eLitigation practice cannot be acquired by non-lawyers.

VII. Considerations for senior management

As we have noted, were it not for the vision and ongoing support of our U.S. Attorneys and the other senior leaders of our USAOs, we would not have been successful in our efforts. Their backing gave credibility to the process and the improvements we made. This is a critical lesson for other USAOs: The eLitigation AUSA *will not* succeed without ongoing support from senior management. This support takes a variety of forms, including:

Empowering the eLitigation AUSA to set policy for the office, and providing them with the tools to enforce it. The eLitigation leader can only be effective if they are empowered to set, implement,

and enforce eLitigation policy. This empowerment needs to be meaningful, and it also needs to be public—because unless you want every announcement, training, or decision to appear to come from someone else, people need to know that your eLitigation AUSA is in charge of eLitigation and all that it entails. Once the policy for the office has been set, you also need to have a unified plan to overcome recalcitrance and resistance. The message must be clear that everyone must follow the standard practice regardless of how exhaustively thought out the excuse not to do so may appear. It must be clear to everyone, including lower level supervisors tasked with ensuring compliance, that there are no exceptions. Instead, staff will be fully supported through the change with training and extra attention and help whenever needed. And if along the way a change in practice is suggested, then the suggested change must work well for the entire office in order for it to be implemented.

Making significant investments to properly equip, staff, and train personnel in sound eLitigation practices. Doing it right is expensive in terms of time and resources, and like any other transformation, you have to be willing to invest in the short term to reap the long-term returns on the investment.

Fully embracing the role of the eLitigation AUSA and understanding that it is a full-time job. Either sacrifice a front-line player or don't, but do not ask an AUSA to build the office's eLitigation practice and maintain a full case docket. You will set your AUSA up to fail on both accounts.

Setting realistic expectations on how quickly your office will move forward. Depending on the current state of your office's eLitigation practices and workflows, it will take time to get everything up and running, and after that, it will require near-constant reinforcement. Set small, attainable goals along the way and celebrate those successes. Don't set up your leader for failure by expecting an office-wide transformation overnight.

Recognizing there is no nirvana. As U.S. Attorney Nealy Cox repeatedly reminds everyone, there is no nirvana in eLitigation. No one will reach their happy place here (or find a unicorn). It doesn't exist. It will have to be satisfaction enough knowing that your office has established a solid eLitigation practice and a legally defensible workflow.

VIII. Final thoughts: pay it forward

Building an eLitigation practice from the ground up is no easy task, but it is attainable with a clear vision for your office, strong senior management support, and a little help from your friends like us who stand ready, willing, and available for questions, advice, encouragement, and anything else that may help other USAOs that are just starting their eLitigation revolution. With an experienced AUSA leading the charge—empowered and fully backed by senior leaders—your office will succeed in building for attorneys and staff a legally defensible workflow from intake through production to defend their convictions, protect their bar licenses, and ensure they get a better night's sleep. Finally, for those who may find themselves in our shoes, good luck, and don't forget as you work though these changes—try to hold on to your head!

About the Authors

Lisa Dunn is an Assistant U.S. Attorney for the Northern District of Texas, Dallas Criminal Division. Lisa is a graduate of the University of California, Berkeley and received her J.D. from Emory University in Atlanta, Georgia, in 1995. Lisa has been an AUSA with the Department of Justice since 2001, having started her tenure in the Western District of Oklahoma in Oklahoma City, Oklahoma. Before becoming an AUSA, Lisa was an Assistant District Attorney for five years at the Oklahoma County District Attorney's Office.

Laura L. Hall has been an Assistant U.S. Attorney in the Western District of Kentucky since May 2002. She is currently the Litigation Support Unit Attorney Coordinator. Previously, she was in the Criminal Division's Drugs and Violent Crimes section. AUSA Hall began her career as a prosecutor in February 1990 at the Commonwealth's Attorney's Office in Louisville, Kentucky. She is a 1989 graduate of the University of Louisville Brandeis School of Law.

Page Intentionally Left Blank

Don't Let Discovery Keep You Awake at Night: Best Practices for AUSAs

Donna Maddux
Assistant United States Attorney
District of Oregon

Susanne Luse
Assistant United States Attorney
District of Oregon

I. Introduction

Years ago, discovery looked different. Discovery felt different. Discovery was different. As little as a decade ago, someone delivered a stack of paper reports and related documents to you or your legal assistant. Those documents were copied or scanned and provided to opposing counsel. Discovery complete! Old-school discovery could be fairly simple and easy to manage.

Today, with the proliferation of digital evidence and other case information, things are far from simple and easy. Agencies often store reports and records in proprietary digital evidence management systems, and some agencies have complex IT systems that retain evidence in siloed locations. Search warrants sometimes result in the collection of voluminous electronically stored information (ESI) that is difficult to manage. Investigations can span years and cycle through any number of assigned agents and Assistant United States Attorneys (AUSAs). In these times, evidence collection, tracking, and production to a U.S. Attorney's Office (USAO) requires an organized system, a basic understanding of relevant digital platforms, robust communication between AUSAs and their support staff and agents/agencies, and a diligent criminal or civil litigation team.

The old-school model of trusting agencies to provide you with "everything" and delegating the oversight of discovery to support staff is no longer viable. Utilizing an outdated discovery management model in today's digital landscape can pose dire consequences for your case and your legal career. These concerns can keep you up at night.

This article will outline simple strategies that criminal and civil AUSAs can employ to ensure defensible collection and production processes. Better yet, when the eventual and nearly inevitable

discovery error occurs, adopting these practices will help you persuade the court and opposing counsel that you and your office acted in good faith and took reasonable steps to meet your obligations and close the potential gaps in the discovery process.

II. Criminal

A. Begin with the end in mind: discovery discussions early in the case

The first step to effectively managing ESI involves making strategic decisions regarding the amount and nature of materials you take in. In the past, agents may have been encouraged to seize and collect as much potentially relevant evidence as possible because the amount of evidence was relatively easy to manage. Today, AUSAs must push back on that concept. Over-collecting ESI can kill your case by making it impossible to manage. Consider a multi-site search warrant involving the seizure of multiple hard drives, servers, and cell phones—each of which contains voluminous ESI. Before seizing a large quantity of ESI, an AUSA must discuss the practical realities of the ESI with agents. Questions should include the following:

- Is there a less burdensome method for acquiring similar evidence?
- Do we really need the material to win our case?
- Are we unnecessarily creating grounds for the defendant to delay motions and trial?
- Who will store the ESI, and how accessible will it be to the case team?
- Will a document review tool be used, and will it be on the agency's system or the USAO's system?
- Who will conduct the forensic review and the search warrant Attachment B review?
- Are there possible filter issues and a filter plan in place?
- How long will this all take?
- Do the investigative agencies have the technology and staff resources to complete and manage the investigative review?
- How will the prosecution team manage this ESI for discovery?

AUSAs can and must lead these early discussions with case agents. It is our responsibility to educate agents regarding the perils and pitfalls of over-collection, including the burdens that over-collection creates in the life of each case.

B. The team approach to discovery: identify discovery team members

No one person is solely responsible for discovery outcomes in complex cases. Effective ESI management requires full participation from the entire investigative team. Early in the investigation, an AUSA must identify members of the discovery team for the case. In small cases with one or two agents, your investigative team is your discovery team. In large cases with multiple agencies and agents, your discovery team will be a smaller subset of your investigative team.

Discovery team members, in addition to an AUSA, should include:

- a discovery agent from each agency involved in the case (local, state, or federal);
- a legal support staffer or paralegal (if available); and
- the litigation support staffer (if available) who will help you manage your materials and oversee any case database.

An AUSA must serve as the leader or captain of the discovery team. It is the AUSA—not the agents—who bears the legal responsibility for complying with *Brady*[1] and *Giglio*[2] throughout the discovery process.

The AUSA is responsible for setting discovery team meetings, educating team members regarding discovery obligations, and communicating clear expectations and deadlines.

Exercising leadership of the discovery team will take time, energy, and effort, but it is time well spent. Only with front-end planning and organization can AUSAs later ensure that all discoverable material is collected, organized, assessed, and provided to the defense.

> *Discovery is only "extra work" if you don't do it right the first time. No one wants to do a four-month discovery audit after a case is charged. I know because we did one!*
> *—Lead Discovery Agent*

---

[1] Brady v. Maryland, 373 U.S. 83 (1963).
[2] Giglio v. United States, 405 U.S. 150 (1972).

Criminal AUSAs should work with the relevant investigative agencies to identify a primary discovery agent for each investigative agency assigned to the case. This primary discovery agent may or may not be the primary or lead investigative agent. If the primary investigative agent is deeply involved in ongoing investigative work or lacks the requisite organizational or technical skills for tracking and managing large amounts of evidence, a separate discovery agent may be necessary.

Because each assigned investigative agency generates unique and potentially discoverable materials, an agent from each agency should be included in discovery meetings. Some AUSAs may choose to run all records from supporting or secondary agencies through a primary agency. In those cases, the primary case discovery agent will serve as a funnel or pass-through for all investigative reports and will carry the sole responsibility of tracking those materials and ensuring the government satisfies its discovery obligations.

C. Use standardized practices

Alert agents early in the investigation about the importance of proper naming conventions for ESI. Using substantively meaningful and consistent naming conventions helps agents and prosecutors find key evidence, either when visually inspecting files by name or when using computer software for searches. Similarly, the naming convention may make it easier to use computer software to track both what the agent provided to the prosecutor and what the prosecutor elected to produce as discovery to the defendant.

For example, a naming convention for agents' reports could include date, report type, and interviewee: that is, 20180604_FBI302_JSmith. That format makes it easy to sort files chronologically, to find just the Jim Smith interviews, to distinguish between three different interviews of the same witness, and to separate FBI interviews (FD 302) from FBI physical surveillance reports (FD 1055) and DEA interviews (DEA 6). Effective naming conventions for bank records may include the bank, the last four digits of the account number, type of records, and the month or year of the records: for example, BOA_4354_checks_2018.

> *A comprehensive discovery table of contents substantially advances the administration of justice, facilitates cooperation from defendants, and greatly increases the likelihood of earlier settlement. Since the*

paradigm has shifted to the electronic production of discovery, not all defense counsel are equally adept at managing hundreds of thousands or millions of pages of electronic material. A consistent and usable discovery table of contents levels the field.
—Defense Counsel

Work with agents to establish a flexible approach that meets the needs of each case. Despite the need for flexibility, some standardized practices—such as naming conventions for files—work well for all cases.

D. Initial discovery planning meeting

Once the team is identified and the time is right, the AUSA should bring all members of the discovery team together for a face-to-face meeting. In complex criminal cases, this meeting should occur well before charging or takedown. The goal is to give the investigative team enough time to organize case materials and provide them to the AUSA and discovery team for review. Hopefully, the case team has time to review and identify key evidence and discoverable information in a systematic and organized fashion.

Ideally, when the case warrants it, the case team will have time to prepare the investigative materials for assessment in a document review tool like Eclipse or Relativity, utilize the review tool to efficiently search the database for discoverable materials, and Bates stamp those materials. This process is efficient and allows all members of the team to easily access and cross-reference relevant information. Rather than searching for a needle in the haystack of unorganized records, the AUSA can quickly and easily locate relevant documents and evidence through targeted database searches.

In the District of Oregon, for example, criminal discovery must be provided 14 days after the first appearance. If case materials are provided to your legal assistant or litigation support staff after charging, there may not be enough time to prepare the materials, perform the necessary quality assurance checks, and still provide discovery in a timely fashion.

Topics for the AUSA to discuss in the initial discovery planning meeting include:

- What is the role of the discovery agent? The discovery agent's primary task is to provide the AUSA with a full set of discovery, complete with a meaningful intake index that the discovery team

can use to keep track of cases materials and evidence from that agency. The AUSA must communicate this role clearly, define expectations, and offer guidance and support.

- What case management systems, if any, are your agents using? Do agents know how to extract records and indexes from their systems and produce them to the USAO for ready use? Some law enforcement agencies use electronic case management systems. Those systems operate very differently in terms of where and how case information is stored and how information is extracted from the system. For example, in some systems, reports and attachments may be stored in separate electronic locations. An agent may produce reports to the AUSA but unwittingly fail to extract and produce the associated attachments. If an AUSA is unfamiliar with these systems, the AUSA should go to the agent's desk and ask them to demonstrate how their system works.
- What is the complete universe of available electronic and physical case information? Encourage agents to provide electronic evidence in native or original format. Native items, including emails and images, include metadata. In some circumstances, this metadata is required to be disclosed under Rule 16,[3] *Brady*, or *Giglio*. Metadata may also provide the power behind your database searches by allowing you to quickly locate relevant dates, authors, or other information captured in the metadata.

> *A critical aspect of the AUSA–agent relationship is ensuring we are not ships passing in the night when it comes to collecting, organizing, and producing discovery. Often, we do not speak the same language. Some agencies have obscure, arcane names for the kinds of reports they generate. Most know what an FBI 302 or a DEA-6 is, but what about a DEA-7B? Until you understand the broad categories of materials the agencies create, it is difficult to know whether your agent is gathering all discoverable materials when you say,*

[3] FED. R. CRIM. P. 16.

"Bring me everything."
—AUSA

Under the leadership of the AUSA, during this initial meeting the discovery team should discuss the case history, develop a plan for deadlines, discuss the best format for the agent's index of case materials, and devise a workable process to take in material. Once the agents are fully informed and clear on the AUSA's expectations, they can begin the work of collecting and organizing case materials in preparation for the intake meeting.

Following a set process can reduce an agent's anxiety and stress about managing discovery. Documenting, for your recordkeeping and theirs, exactly what materials they provided to you and when makes a complex case more manageable in the long run. Time invested in the front end reduces time wasted later on. Many initially resistant agents in the District of Oregon are now believers in the wisdom of this approach.

During my 15 years as an agent, I've seen an increasing demand for getting discovery right. Those who get it wrong face harsh consequences. To be honest, I don't enjoy the administrative aspects of organizing discovery and compiling an index of my case materials, but I now know it's as essential as any work that we do as agents and prosecutors.
—Agent

E. Intake meeting

If you take one practice point away from this article, let it be this: Do not, under any circumstances, allow an agent to simply leave a CD on your desk as a means of providing you with complex discovery. This practice is fraught with peril. What could possibly go wrong? For starters:

- The agent provided you with records, but no index. You have no means to track exactly what records were provided to you. You have no means to perform a quality control check on your discovery production.
- The agent's index contains 100 items, but the disc only contains 98 items. This frequently occurs due to technical errors in copying.

- The disc is corrupted or somehow unusable in your system.
- The disc includes password-protected files but no passwords.

To counter these common problems, you can utilize a best practices approach to the discovery intake meeting that includes the following:

- All members of the discovery team are present. Each agent provides the AUSA with electronic records—disc, flash drive, or hard drive—for review. The meeting room is equipped with a laptop and monitor for group viewing. The AUSA opens each disc or drive, and the discovery agent talks about the scope and type of materials they provided.
- The AUSA spot tests for front-end quality assurance.
  - Make sure the number of items on the agent's index matches number of items in each sub-file. CaseMap or Excel spreadsheets are the best format for an agent's index.
  - Assess the agent's organization of case information (if the agency does not use a case management system that forces a particular format) and the agent's index. If there is a way to improve the organization, ask the agent to resubmit the information after reorganization.
  - There will be errors. Catching and discussing these errors helps agents understand the perils and pitfalls of electronic discovery.
- Create a system for tracking intake.
  - In the District of Oregon, some AUSAs provide agents with a discovery receipt form. This receipt identifies the intake date and the materials provided by the agent—for example, *On March 4th, Agent Smith provided four discs called Volumes 1–4.* Much later in the case, when trying to locate files or disputes arise about what was provided and when it was provided, these receipts, in conjunction with the agent's comprehensive index, can be invaluable.
  - Maintain a separate physical discovery file that includes discovery receipts and the original materials provided to the government.
  - If possible, save a copy of the materials and the agent's index to a cloud drive and maintain the unprocessed set.

- If the disc includes password-protected files, include the password in the agent's index under a notes column.
- Decide which items will be processed and which items are too large or unusual for processing. Do you have a year's worth of pole camera video? That amount cannot be processed by litigation support. Set this and other similar items aside to be copied or otherwise made available to the defense. Assign those items a single Bates stamp number for eventual tracking on your discovery table of contents.

> *Ensuring that your agents understand the stakes involved—and the bright lights that may someday shine on them and their agency if things are not properly produced—is fundamental to functioning as an effective prosecution team.*
> *—AUSA*

F. Post initial intake meeting

Discovery intake is not a one-time event. Cases continue to develop even after charging, and agents continue to generate potentially discoverable materials. Pre-trial, the discovery process may focus on agent emails or other statements. Rolling intake meetings, scheduled in advance in weekly or monthly intervals depending on need, should occur throughout the life of your case.

Do not allow agents to simply email you updated reports and expect they will make it into discovery. This practice is fraught with peril. Instead, adhere to the intake meeting and tracking practice throughout the life of the case. If you do, you and your agents will rest much easier when the judge asks, "Have you produced everything?" If your discovery team follows the process, you can safely answer, "Yes." The discovery process will become a tool to help you master your case, not a target-rich environment for killing your case.

> *When you handle discovery in a way that requires you to organize and create an index of case items, review, and have meetings with your prosecution team, it forces you to become a subject-matter expert on your case. As time consuming as complex discovery practice is, without organized discovery, you risk losing your case. If you start the organizational process early and continue to*

work together with your prosecution team, the chances of a successful outcome are much greater.
—Agent

G. Confer with defense counsel

Despite your best efforts to close the gaps and implement best practices, there will be discovery errors in every case. Your job is to minimize and mitigate errors. One way to identify and address discovery errors is by conferring with opposing counsel.[4] Sit down and discuss discovery with defense counsel in person when it will advance your aims and promote clear communication. Is defense counsel struggling with any file formats? Have they identified missing pages or poor quality scans? A world of potential issues can arise. Where necessary, document your efforts to clarify and address discovery issues. These practices will limit pre-trial discovery battles. If discovery battles do occur, you will be able to demonstrate to the court that you acted in good faith. Your professional reputation and the reputation of the office are on the line in every case.

III. Civil

A. Initial agency communications: know your agency client

Many years ago, a plaintiff's attorney was taking the deposition of a defendant–hospital's employee. Plaintiff's counsel tried to establish why a document the employee brought to her deposition was being presented for the first time, rather than during the initial disclosures. The employee calmly and rationally stated, "Because it was in my desk drawer." Counsel asked, "So why didn't you give it to the attorney before today?" The employee responded, "Because no one ever asked me for it."

In this age of technology, "documents" can be found in a wide variety of "drawers." It is up to AUSAs to educate themselves on the client agency's systems and available ESI—regardless of what or whose drawer they are stored in. Just as in criminal matters, this effort

---

[4] New Federal Rule of Criminal Procedure requires the parties to confer. *See* Thomas M. Woods, *Discovery Conferences Come to Criminal Practice: New Federal Rule of Criminal Procedure 16.1*, DOJ J. FED. L. & PRAC., no. 3, 2020, at 61 (discussing the origins and effects of Federal Rule of Criminal Procedure 16.1).

requires close communication and coordination with the agency defendants involved in your cases.

1. Identifying relevant information

Who AUSAs get their information from is critical to determining what information is available and where it is stored. Generally, agency counsel will be the main point of contact, but for various reasons, other points of contact may be better equipped to kick-start the process of identifying potentially relevant information.

For example, in some cases, agency counsel may be in the same situation as you, having limited knowledge of what particular ESI is available or where it can be found. This issue may occur because the agency has different types of information available to it, depending on the facility or office at issue—for example, specialized medical equipment. Simply asking agency counsel for all relevant materials will not always be sufficient. Thus, working with agency counsel, you must identify those points of contact that have in-depth knowledge of the potential data sources at issue.

Get to know the agency and the facility or office at issue. Learn what resources are available to you for your investigation and information gathering. Start these early conversations with a list of questions and continue to add to those questions as you learn more about the facts, whether during witness interviews or discussions with agency counsel or key employees, or even, unfortunately, during depositions. Throughout the case, revisit these questions and facts to ensure you have all the relevant information.

Gathering such information may involve asking agency counsel and other agency contacts questions such as:

- Who are the key custodians in the case—that is, the key agency employees most likely to have information relevant to the claims and defenses of the case?
- Is there an agency department—for example, a risk management department—that might have insight into the agency and facility/department/office's relevant evidence?
- Who manages the agency/department/office's IT? Is there more than one person who manages agency data—for example, do different IT specialists maintain email servers, share drives, databases, and other agency IT resources?

- Is there a centralized records department, or is each agency department/facility/office responsible for maintaining their own records?
- Do other agency offices, based on their functions—for example, the Freedom of Information Act (FOIA) office—have relevant information, records, or insight into where such ESI may be found?
- Do work-related files reside on a server, or is there unique ESI that resides on a custodian's computer?
- Does the agency still have information generated by former employees that may contain potentially relevant information?
- Does the agency issue cell phones? If so, what is the agency's policy on text messaging?
- Does the agency retain call logs or voicemails from agency phones that may contain relevant information?
- Are employees allowed to use any personal equipment for work purposes—for example, personal computers, cell phones, email accounts?
- Does the agency or facility have social media accounts or a website that may contain relevant information?
- What are the retention policies for the various types of relevant evidence identified by your conversations with the agency or facility?

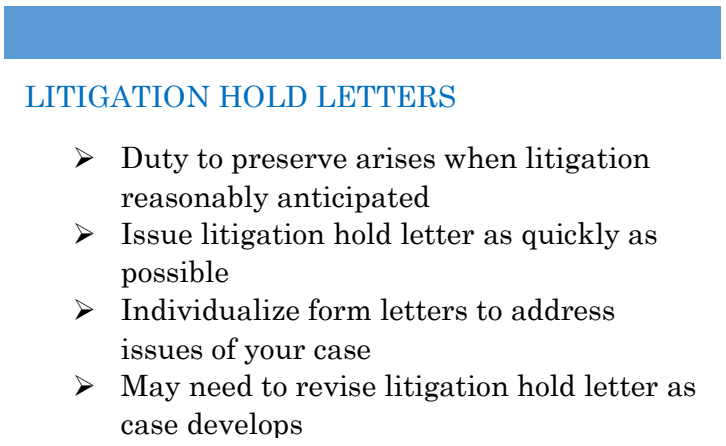
From a civil defensive case perspective, nothing can replace the efficiency and thoroughness of a face-to-face meeting at the agency, office, or facility at issue to sort through some of these key issues with agency counsel and key custodians. If possible, early in the case before discovery begins, have an in-person meeting with the stakeholders, including agency representatives and potential witnesses. By meeting face-to-face, you will feel less rushed, and they will feel more engaged in the process. When working in geographically large districts like Oregon, it can be difficult to visit the agency office or facility due to its distance from the United States Attorney's Office. In such situations, it may be helpful to combine these in-person visits with events in other cases—for example, a deposition in the same or neighboring city—making your time out of town more productive and efficient.

2. Preserving relevant information

Litigation hold letters and preservation issues should be a topic of very early conversations with the agency. These conversations may take place even before an in-person meeting can be arranged. In many cases, by the time an AUSA sends the litigation hold letter to agency counsel, the lawsuit has been filed, and the agency or its target component may have already anticipated the litigation and taken steps to ensure the preservation of relevant evidence. Litigation hold letters should be issued to agency counsel—in all cases—as soon as practical once the preservation obligation attaches. They should be designed to remind agencies of their preservation obligations and let them know what materials are likely to be deemed relevant. They should also explain the consequences of the failure to preserve potentially relevant materials.

Whenever possible, speak with agency counsel—along with a contact from the appropriate IT department(s) if you are unfamiliar with their system—*before* issuing a litigation hold. You should identify the relevant time period(s) at issue, understand what potentially relevant information is available, know the format of the potentially relevant information, and identify the location of the potentially relevant information to understand what information can and should be preserved. You should also know what retention policies are in place and who has access to the material. These conversations may start to answer the questions you have about the agency's sources of potentially relevant information and may allow you to further target your questions regarding relevant data that you have with key players as the case moves forward.

Initial form litigation hold letters may be appropriate at the outset to remind agencies of their duty to preserve as you work with agency counsel to identify the sources of potentially relevant information, but be specific if you know of particular key custodians and/or information that needs to be preserved because of its relevance to the litigation. The more specific you can be with your preservation requests, the more likely you will be able to avoid problems down the road. Once on notice, an agency can communicate with those holding the material to ensure proper retention.



Don't assume one litigation hold letter at the beginning of the case is sufficient. For example, subsequent to sending a form preservation instruction identifying potentially relevant materials and potential custodians, you may want to send a more robust preservation letter once you have consulted more thoroughly with agency counsel and IT and understand the identity of all key custodians and the most likely sources of potentially relevant information. In addition, you may need to update or amend preservation instructions under certain circumstances, such as (1) when you learn more about the case and additional claims; (2) defenses arise that bring additional relevant materials to the table; or (3) you learn more about where relevant information may be stored. For example, an agency may have a particular software program that retains certain relevant electronic records. You and agency counsel may not have been made aware of this potential data source during your initial inquiries. As a result, it may be necessary to address the preservation of these additional relevant materials with an amended litigation hold letter identifying the specific information that needs preservation.

Because the purpose of this article is to help you sleep at night, I am reluctant to give you the "fire and brimstone" speech. But you need to be aware of the ramifications for lost evidence. Rule 37(e) allows courts to sanction a party when (1) ESI is lost; (2) the lost ESI should have been preserved in anticipation of litigation; (3) a party failed to take reasonable steps to preserve the ESI; and (4) the ESI cannot be restored or replaced through additional discovery.[5]

Telling your teacher, "The dog ate my homework!" didn't keep you out of trouble in school. Similarly, telling the judge, "But your Honor! The agency doesn't have Smith's emails because she left the agency!" may not be excused—particularly if the employee left the agency after the litigation was filed. The potential sanctions imposed *are all bad*—think Arnold Schwarzenegger in *True Lies*—but increasingly so if the court finds the party acted with intent to deprive another party from using the information. In those situations, the sanctions may include an adverse inference to a jury, a dismissal, or a default judgment.

Courts expect parties to be familiar with eDiscovery issues. Courts may hold Department of Justice lawyers and government agencies to a higher standard when it comes to ensuring the proper preservation and disclosure of relevant information. So work with your agency clients to ensure you can approach discovery issues with confidence, knowing that you made appropriate identification and preservation efforts at the outset of the case.

This confidence will come from a well-documented process. Ideally, when working with agency counsel on source and preservation issues, both agency counsel and the AUSA (or designated support staff) should document the steps taken to identify potentially relevant custodians and sources of information, the steps taken to turn off automatic deletion policies that may apply to relevant information, and the steps taken to suspend the retention policies for relevant information. In addition, the agency and the AUSA should designate someone on the case team to track the litigation holds sent to key custodians, tracking such information as the date the hold was sent to a particular custodian, the date the custodian acknowledged the litigation hold, the dates of any litigation hold amendments and reminders that were sent to custodians, and the date the hold was lifted (if applicable). Documenting identification and preservation

[5] FED. R. CIV. P. 37(e).

efforts can help you sleep at night. It can also help you to prepare for the discovery phase of the case.

B. Rule 26(f) conference planning

The Rule 26(f)[6] conference can have a lasting effect on the life of your case and, quite frankly, on the quality of your life throughout the case. Make it count. Preparation will make your conference more valuable and, in ideal circumstances, discovery more manageable. Your planning meetings should involve agency counsel, agency IT, agency representatives responsible for collecting potentially relevant information, and litigation support personnel from the USAO, as appropriate.

Work with agency counsel and representatives to ensure you are prepared for the conference. Return to your list of questions you developed for your early meetings with agency counsel. Make sure you have answers to all of those questions. In addition, identify additional information that needs to be on hand for the Rule 26(f) conference and work with agency counsel and representatives to obtain that additional information. Develop a list of the discovery issues that need to be discussed at the conference, including potential issues with evidence collection and production: What materials are available for immediate disclosure? What is the anticipated scope of preservation and discovery? How much and what type of evidence is anticipated? Are there any issues relating to production, such as the timing of production or the format of production for ESI? Are there any known or potential problems with preserving relevant evidence? Are there any issues regarding privilege claims or protected information that need to be addressed? Finally, work with agency counsel, agency IT, and litigation support personnel to identify the costs associated with preserving or producing information—particularly if certain information is expensive to preserve and or collect and is of marginal relevance—and develop proposed options to address any issues you identify so that you are better equipped to negotiate with opposing counsel.

[6] FED. R. CIV. P. 26(f).

C. Rule 26(f) conference

As noted above, if there are any challenges relating to preservation or discovery, discuss those challenges with opposing counsel at the 26(f) conference. Do not wait! Addressing it with opposing counsel early avoids discovery surprises later in the case and, hopefully, will prevent the acrimony that develops when the issue unexpectedly arises in the middle of discovery. Alternative proposals regarding discovery can be discussed at the Rule 26(f) conference before counsel become entrenched in their views on the production of materials or the scope of discovery or preservation or other difficult discovery issues. By coming prepared to the Rule 26(f) conference, you can command more control over the discovery process, making reasonable proposals that you know the agency can meet. Agreements and compromises made early in the litigation help you avoid protracted and costly discovery battles and sanctions.

D. Communication and organization during discovery

So once you have ascertained and negotiated the initial scope of discovery and defined and identified the relevant evidence, then what?

THOUGHTFUL REQUESTS FOR DATA

- Carefully identify all relevant materials
- Revisit previous requests as case develops

Don't stop. Maintain effective communication during discovery with agency contacts and opposing counsel to ensure issues involving evidence collection and disclosure are anticipated and appropriately handled. In addition, make sure you have a system in place to manage the flow of information coming through your office.

1. Effective communication with agency contacts and opposing counsel

As discovery progresses, you should be revisiting your requests for information and perhaps supplement them to fit within the scope of ongoing discovery. There will be new issues that arise requiring you to

reevaluate what evidence may be available at the agency level and also what additional information you may need from third parties or opposing counsel.

With respect to agency counsel, continue to circle back to your agency contacts or IT specialists and explore whether there is any additional relevant evidence to gather as the case progresses and claims and defenses become more refined. Keep in mind that, as discovery progresses, you may also need to update the litigation hold if the evidence sought is not covered by the original litigation hold. Continuing to regularly touch base with agency counsel on collection and preservation issues, as well as strategies when propounding discovery, will ensure that attorney and client are on the same page.

With respect to opposing counsel, make sure you keep the lines of communication open. While some discovery disputes cannot be avoided, fostering cooperation between parties early in the discovery process may assist in resolving discovery issues during meet and confer sessions, thereby avoiding judicial involvement in these disputes.

2. Organizational tools tracking data flow

Over the course of the litigation, you will be gathering evidence from the agency, from opposing counsel, and from other sources. This information will need to be organized, reviewed, disclosed, and presented at trial. Given the volume of information flowing through your office, you need an effective system in place to track what you have requested from the agency or opposing party, what has been received, the status of your review, where the materials are located, and what you have disclosed or produced.

Depending upon the size of your case, using one or several logs to track evidence can be extremely helpful in managing evidence and your stress level. You can create simple tables created in Word or Excel to track important information about information received from opposing counsel or the client agency and information you produce to opposing counsel. For example, consider creating logs for collection to track the information received from the agency, including what was expected from a custodian or source and what was actually delivered to you so that you can identify any materials you may be missing from the agency. You can also add columns to these agency intake logs to track where the materials are stored in your office—for example, in a document review platform or CaseMap—and to indicate whether any materials from the data set were ultimately produced to opposing

counsel. Similarly, you can track productions to and from opposing counsel, including the date of the production, the bates range of the production, where the production resides within your office, and any other useful information regarding those productions such as custodians or sources included in the production, production passwords, and a link to any communication that accompanied the production. I have found that a simple Word table allows me to easily track information I have requested and disclosed. I always include a notes column that allows me to add notations for sources of additional information or updates regarding status reports, receipt of materials, review, or the identification of other potential sources of evidence. These tables have proven invaluable in the middle of trial when opposing counsel tries to argue they never received a particular piece of offered evidence. I have been able whip out a table, run through a search and identify the exact disclosure date it was provided. Voila!

IV. Conclusion

Evidence collection can be intimidating and stressful, but it doesn't have to be. Criminal and civil AUSAs can employ these communication and documentation strategies to ensure a defensible collection and production of evidence occurs. Some of the key points we hope stick with you long after our attempts at humor fade away are (1) educate yourself on evidence collection issues in your case; (2) organize meetings—preferably in-person meetings—with agents and agency representatives early in the case and as needed for the duration of a case, in order to address discovery planning and other discovery issues; and (3) create a system for tracking the receipt, review, and production of discovery that works for you and your case. If you employ these strategies for dealing with evidence collection, discovery won't keep you awake at night. If you're still awake, try a warm glass of milk.

About the Authors

Donna Maddux joined the District of Oregon as a fraud prosecutor in 2012 and serves as the district's Elder Justice Coordinator. She previously served as the chair of the District of Oregon's Discovery Work Group. Before becoming an Assistant U.S. Attorney, Donna worked in various fraud prosecution roles with the Oregon Department of Justice, including Medicaid Fraud and Tax Crimes. She is a 2002 graduate of the Lewis and Clark Law School in Portland.

Susanne Luse has been an Assistant U.S. Attorney with the District of Oregon, Civil Division, since 2015. Before joining the United States Attorney's Office, she was in private practice in Arizona, where she focused on defending medical malpractice and personal injury lawsuits. Susanne is a 2000 graduate of the University of Arizona James E. Rogers College of Law.

Unlocking Potential: Empowering Civil Support Staff as the Key to Success in the Electronic Discovery Process

Leah M. Wolfe
Assistant United States Attorney
Southern District of Ohio

Laura Hunt
Senior Litigation Counsel for eDiscovery
U.S. Department of Justice

Electronic discovery (eDiscovery) is the process by which electronically stored information (ESI) is preserved, identified, collected, reviewed, and produced in the context of an investigation or litigation. The majority of civil investigations and litigation now involve some form of eDiscovery.[1] The volume and complexity of ESI that may be relevant to an investigation or litigation can present a series of challenges for litigators. Support staff, including paralegals and legal assistants, possess a high level of administrative and analytical skill that can significantly contribute to avoiding the inherent pitfalls in the eDiscovery process. Those pitfalls include failing to produce certain information because of inadequate tracking between the client and the litigator, delaying implementation of the preservation obligation, or producing ESI in an incorrect format.

In order to maximize their contribution, support staff need to be equipped with an understanding of the way the process works and their role in its success. In other words, support staff need to know *why* they are doing each discovery-related task and *where* that task fits into the eDiscovery process. This insight requires knowledge of not only what civil rules apply to each stage of discovery, but also a keen awareness of the order in which the tasks must be completed and the extent to which each step is dependent upon and interrelated with other portions of the eDiscovery process.

---

[1] Betsy Barry et al., *The Big ESI: Going from Big to Better in E-Discovery*, 10 I/S: J.L. & POL'Y FOR INFO. SOC'Y 721, 723 (2015) ("In 1996, it was estimated that only 5% of discoverable information existed in electronic format. Today, this estimate has increased to over 90%.").

This article will (1) identify the key rules and concepts support staff must understand to maximize their participation in an effective eDiscovery practice; and (2) provide practical tips to improve the utilization of support staff in the management of the eDiscovery process.

I. Key rules and concepts essential to successfully navigating the electronic discovery process in civil matters

Discovery in the civil litigation context is governed by the Federal Rules of Civil Procedure, which permit the discovery of any information that is relevant, proportional to the needs of the case, and non-privileged.[2] Determining the proportional scope of discovery 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."[3]

In order to have such information to exchange and to comply with their obligations under both the common law and the federal rules, parties are required to preserve relevant information when there is reasonably anticipated or pending litigation. The consequences of failing to preserve relevant ESI are outlined in Rule 37(e).[4] One of the ways to avoid penalties under this rule and to comply with a party's common law duty to preserve relevant information is to implement a litigation hold once the duty to preserve is triggered.[5]

The litigation hold should include the issuance of a notice to individuals who have relevant information,[6] notifying those individuals that they are under an obligation to preserve that

---

[2] FED. R. CIV. P. 26(b)(1).
[3] *Id.*
[4] *See* FED. R. CIV. P. 37(e).
[5] *See generally* The Sedona Conference, *Commentary on Legal Holds, Second Edition: the Trigger & the Process*, 20 SEDONA CONF. J. 341 (2019).
[6] *See id.* at 257 n.29 (Individuals with relevant information are often referred to as "custodians.").

information and that they must not alter or delete the information.[7] The party subject to the preservation obligation should ensure that relevant information is preserved by suspending any deletion or other retention policy that could affect the availability of relevant information.[8]

Once litigation has commenced, parties have additional obligations under the federal rules to discuss and plan for discovery collaboratively.[9] Pursuant to Rule 26(f), the parties *must* meet and confer to discuss discovery at least 21 days before the court's scheduling conference or scheduling order deadline.[10]

At the Rule 26(f) conference, the parties must discuss the discovery timeline, including the exchange of initial disclosures[11] and the anticipated discovery completion date. Additionally, the parties must discuss any issues relating to ESI, including preservation concerns and form of production.

In addition to discussing ESI, the parties must discuss how privileged and sensitive information will be protected. With respect to privileged information, the parties must determine whether to agree to a clawback agreement under Federal Rule of Evidence (FRE) 502(d). This order is entered by the court and protects the responding party from waiving a privilege if privileged material is produced.[12] The parties may also determine whether to request a protective order

---

[7] *See* N.M. Oncology & Hematology Consultants, Ltd. v. Presbyterian Healthcare Servs., No. 1:12-cv-526, 2017 WL 3535293, at *5 (D.N.M. Aug. 16, 2017).

[8] *Id.*

[9] *See* FED. R. CIV. P. 1 advisory committee's note to 2015 amendments (noting that achievement of Rule 1's goal of a "just, speedy, and inexpensive determination of every action" requires "[e]ffective advocacy" which itself "depends upon cooperative and proportional use of procedure" (internal markings omitted)).

[10] FED. R. CIV. P. 26(f); FED. R. CIV. P. 16(b)(2) (timing of scheduling order).

[11] Initial disclosures are governed by FRCP 26(a)(1) and require that parties, unless exempted by FRCP 26(a)(1)(B), disclose to each other a list of witnesses and the category/location of documents that support claims, if plaintiff, or defenses, if defendant. Parties must also exchange a computation of damages, including supporting documentation, as well as any related insurance agreement. Initial disclosures must be exchanged within 14 days after the Rule 26(f) conference, unless another time is stipulated by the parties or ordered by the court. FED. R. CIV. P. 26(a)(1)(C).

[12] FED. R. EVID. 502(d).

entered pursuant to Rule 26(c). A protective order provides for the access, dissemination, and disposition of confidential information exchanged by the parties.[13] The entry of FRE 502(d) and protective orders are strongly encouraged to protect confidential and privileged government information.

Once discovery begins in earnest, the parties may obtain discoverable information through several different tools. These tools include interrogatories, written questions eliciting certain facts from the responding party;[14] requests for admission, written statements seeking the admission or denial of certain facts;[15] and depositions, a series of questions asked of a particular individual in order to elicit testimony.[16] Parties may also seek documents in discovery through a Rule 34 request for production of documents or from non-parties through a Rule 45 subpoena.[17]

Requests to produce documents can include a request for ESI, which is the primary form of relevant information in today's digitally focused environment.[18] Importantly, requests for ESI often specify the form in which the information should be produced, including which metadata fields must be turned over and how.[19] If the request does *not* specify a form for production (or if the parties did not agree on a form of production during the 26(f) process), the producing party may state the form it intends to use.[20] In short, ESI must be produced as it is "kept in the usual course of business"[21] and in the form in which "it is

---

[13] FED. R. CIV. P. 26(c).
[14] FED. R. CIV. P. 33.
[15] FED. R. CIV. P. 36.
[16] FED. R. CIV. P. 30.
[17] FED. R. CIV. P. 34, 45.
[18] Burke T. Ward et al., *Electronic Discovery: Rules for a Digital Age*, 18 B.U.J. SCI. & TECH. L. 150, 154 n.16 (2012) (estimating that over 92% of all information created is done so electronically); *see also* FED. R. CIV. P. 34 advisory committee note to 2006 amendments ("[A] Rule 34 request for production of 'documents' should be understood to encompass, and the response should include, electronically stored information[.]").
[19] FED. R. CIV. P. 34(b)(1)(C).
[20] FED. R. CIV. P. 34(b)(2)(D).
[21] FED. R. CIV. P. 34(b)(2)(E)(i).

ordinarily maintained"[22] or, if that is not feasible, then "in a reasonably usable form or forms."[23]

While these requirements may appear relatively straightforward in the abstract, a successful eDiscovery practice requires a significant amount of both technical skill and planning ability—making support staff a natural fit to oversee the process.

II. Incorporating support staff into the management of the electronic discovery process

Both litigators and support staff engage in project management on a daily basis without even realizing it. Project management is defined as "the structured application of skill, knowledge, tools and techniques to organize processes, activities and tasks" in order to reach "a desired outcome that efficiently meets a project or business need."[24]

So what are we as legal project managers actually managing? The most obvious "project" in the legal context is an individual case or matter, which the litigation team sees through from the preliminary stages through discovery, dispositive motions, settlement or trial, and appeal. What is sometimes less obvious is that, within each case—and within each stage of each case—individual sub-projects require management of their own.[25]

Discovery is one such subproject, and often, eDiscovery is another subproject (or series of subprojects) within that. Thus, "Application of project management to discovery projects is particularly appropriate given the abundance of repetitive and dependent tasks, the variety of people and organizations involved, and the need to find efficiencies that help better manage the timing and delivery of discovery projects."[26]

eDiscovery is frequently described in terms of the Electronic Discovery Reference Model (EDRM)—a conceptual workflow of

---

[22] FED. R. CIV. P. 34(b)(2)(E)(ii).
[23] *Id.*
[24] MICHAEL I. QUARTARARO ET AL., PROJECT MANAGEMENT IN ELECTRONIC DISCOVERY: AN INTRODUCTION TO CORE PRINCIPLES OF LEGAL PROJECT MANAGEMENT AND LEADERSHIP IN EDISCOVERY, at ch. 3 (2016).
[25] See *id.*
[26] *Id.* at ch.3.

eDiscovery stages and steps.[27] The EDRM suggests a general workflow for eDiscovery, starting with identification, moving to preservation and collection, then to processing and review, and finishing with production and presentation.[28] Merging project management concepts with the EDRM will result in "[a] well-designed e-discovery process" customized "to the specific case circumstances," featuring "iterative and adaptive procedures . . . that allow for learning and correction" as well as monitoring and quality control.[29]

Project management has five phases: initiating, planning, executing, monitoring and controlling, and closing.[30] These are not necessarily rigid categories, and in reality, most of us conceptualize the litigation lifecycle similarly. A case comes in, we plan and organize what we think we need for the case, we begin to execute that plan and litigate the case by issuing discovery requests or filing motions, we review the status of the case periodically to see if any adjustments to the plan are needed, and finally, we close the file out with a win (hopefully). What we may not consider are all the subprojects the litigation team must plan for, execute, and complete—often in a specific order and under tight deadlines—in order to reach that final stage.

The idea of applying project management concepts to litigation is not to impose artificial labels on what we already do, nor is the idea to add unnecessary steps to an already complex process.[31] Rather, the goal is to make sure we take the time to plan for each phase in the case and timely communicate those plans to all the personnel who are needed to make them happen—whether that be agency counsel or their IT staff, co-counsel, internal litigation support, opposing counsel or their litigation support, or even a judge. In short, project

---

[27] *EDRM Model*, ELECTRONIC DISCOVERY REFERENCE MODEL, https://www.edrm.net/resources/frameworks-and-standards/edrm-model/ (last visited Feb. 24, 2020).
[28] *Id.*
[29] The Sedona Conference, *The Sedona Conference Commentary on Achieving Quality in the E-Discovery Process*, 15 SEDONA CONF. J. 265, 270 (2014).
[30] QUARTARARO, *supra* note 24, at ch.4 fig. 3.
[31] *See* Mike Quartararo, *eDiscovery Project Management: Ask Forgiveness, Not Permission*, ABOVE THE L. (Dec. 11, 2018, 5:17 PM), https://abovethelaw.com/2018/12/ediscovery-project-management-ask-forgiveness-not-permission/.

management concepts are "aimed at adding value while reducing cost and effort."[32]

Support staff should play crucial roles at each phase of project management as it relates to the stages of an overall litigation plan and within the EDRM workflow. Nowhere is good project management more important than in eDiscovery.

A. What makes a good project manager also makes a good paralegal

Some insist that the "team leader" in eDiscovery must be an attorney,[33] and in fact, many of us assume that the lead attorney for litigation purposes is by default in charge of eDiscovery as well. But this sort of thinking ignores the skills and abilities that support staff can bring to the table, especially where the assigned lead attorney may well be the team member who is the least knowledgeable or comfortable with e-discovery and technology generally.[34] After all, "[p]roject management and eDiscovery are not subjects routinely taught in law school."[35]

Moreover, the traits that help people excel in legal support roles are the same qualities that create success in project management. For example, we all know that "[p]aralegals are skilled at keeping things organized and making sure tasks are completed on time."[36] Likewise, project managers should be knowledgeable, organized, well-written, well-spoken, confident, and decisive.[37] They should have "experience

---

[32] The Sedona Conference, *supra* note 29, at 270.
[33] *See id.* at 275.
[34] *See* Ari Kaplan, *Trends that Will Fuel the Influence and Impact of Paralegals and Paralegal Managers in 2019*, https://www.level2legal.com/news/paralegal-trends (last visited Jan. 8, 2020) (finding that one of the "most common challenges cited by paralegals . . . [was] lack of familiarity with discovery by the attorneys with whom they work"); *see also* CRAIG BALL, PROCESSING IN E-DISCOVERY, A PRIMER 4 (2019) ("Talk to lawyers about e-discovery processing and you'll likely get a blank stare suggesting no clue what you're talking about.").
[35] Jeane Thomas & Ben Hawksworth, *Lessons Learned, Master Mining: Three Views on EDD Project Management*, LAW FIRM INC., Mar./Apr. 2006, at 1.
[36] Barry Schwartz, *Paralegals in eDiscovery: Why They Should Be Involved from the Start*, NAT'L PARALEGAL REP., Spring 2018, at 3.
[37] *See* QUARTARARO, *supra* note 24, at ch.3.

with the various phases of e-discovery" while also understanding "both the substantive and strategic aspects of the litigation."[38]

Even more importantly, an eDiscovery project manager must know what they do *not* know—and crucially, what the *attorneys* on the team do not know.[39] And project managers must be able to explain and even persuade others on the litigation team to adopt the most efficient and defensible path forward and do so in a tactful way that considers the viewpoints of the entire case team.[40]

Sounds easy, right? Of course it doesn't—that's why lawyers never "should go it alone."[41] Involving support staff from the start is a key to eDiscovery success.[42]

B. How to use legal project management to empower support staff in the eDiscovery process

As mentioned above, discovery is a subproject within the overarching project of litigating a case, and eDiscovery is a subproject within discovery. While discussing the multitude of ways support staff can assist in each of the subprojects that make up successful eDiscovery is outside the scope of this article, the tips and practices below apply equally to both the eDiscovery subproject as a whole and to each discrete task within that subproject.

1. Initiating

There are important steps that support staff can take in the initiation phase of litigation, that is, when a complaint has just been received or filed or an investigation opened.

Support staff can ensure that a litigation hold is issued by the litigation team to the agency and that the agency issues a litigation hold to the relevant custodians. Support staff are key to tracking those litigation holds to make sure they reach the intended recipients

---

[38] The Sedona Conference, *supra* note 29, at 275 (Even Sedona recognizes that this is a big ask of an attorney, noting that a Team Leader who is also a lead attorney must also "balance his or her role in developing the facts of the case, interviewing witnesses, and related activities, with leadership of the team's e-discovery efforts.").

[39] *See* QUARTARARO, *supra* note 24, at ch. 3.

[40] *See id.*

[41] Thomas & Hawksworth, *supra* note 35.

[42] Schwartz, *supra* note 36.

and that documentation of the hold—for example, the date issued or custodian responses—is complete.

Support staff can also start to line up necessary resources, including alerting any internal litigation support staff who may be needed to process data or working with litigation support and contracting personnel to start the process of retaining a contractor. They can ensure tracking logs for incoming documents and productions are created and are ready to be completed; support staff can also locate and reach out to technical staff at the client agency to discuss the collection and subsequent transfer of data to the trial team. Starting these logistical processes early in the litigation helps things flow smoothly later when more projects are taking place simultaneously and attention may be more divided.

2. Planning

We have all been told that failing to plan is planning to fail, and those (perhaps overused) words hold true in eDiscovery. Not dedicating the time and energy to careful planning for eDiscovery almost guarantees the process will be anything but a success. Ideally, the litigation team will have a cohesive, well-thought-out plan for collection, processing, review, and production at the outset of the case; support staff should be involved in establishing each of these plans.

Additionally, support staff should be part of discussions about the timeline of the case, the makeup of the case team (including any need for outside litigation support and coordination of that support), and the goals of the client agency and the litigation team. Knowing that the agency is hoping for a quick settlement of a case rather than being willing to go to trial influences the whole litigation approach. The more they are involved in these important, preliminary discussions, the more support staff will understand the issues in the litigation and the various steps that need to be taken.

Support staff should also participate in meetings with the agency to determine possible sources and custodians of data. Involvement in these discussions helps support staff better know what to expect when documents are provided to the trial team, recognize when there may be missing information, and anticipate problematic data. Based on information gathered during these meetings, support staff can also be tasked with developing a draft preservation and collection plan for the AUSA and agency counsel. Likewise, participating in Rule 26(f) discussions and creating an initial draft of the Rule 26(f) report equip support staff with an understanding of what the parties have agreed

to and expect, again allowing them to quickly alert the litigation team if some aspect of discovery is starting to go off the rails.

Finally, "It is key for paralegals to be involved in creating" the document review database.[43] After all, if support staff are to take on a key role in using the database for document review and production, they need to have both input on how it is set up and an understanding of its parameters.

3. Executing

Once plans are in place and litigation really takes off, support staff can take the lead on tracking, troubleshooting, and documenting incoming and outgoing data. This may sound like mundane or even clerical work, but make no mistake—accurately tracking data is *crucial* to success (and everyone's sanity). Support staff are accustomed to tracking and are well-equipped to delve into the details and locate missing data, and frankly, they are generally better at it than attorneys, who may not be as focused on these types of details.

Another key benefit when support staff act in a project manager role for eDiscovery is having a person dedicated to ensuring consistency throughout each phase of the litigation.[44] This is especially important in cases with multiple productions because consistency in productions reduces duplication, increases efficiency, and eliminates an often fruitful source of tangential discovery disputes.

In eDiscovery, multiple projects and numerous steps within those projects are often happening at the same time. With careful tracking and an eye on the calendar and case plans, support staff can coordinate these steps, easing the mental load for the attorneys.

Support staff can also handle much of the day-to-day communications and inquiries about each of the discovery projects. For example, they can answer questions from opposing counsel concerning passwords and technical production issues. In addition, they can address technical issues with litigation support such as corrupted or missing data. Support staff can also handle routine status updates to the team; for example, they can inform the case team if processing is taking longer than expected or if a production is on track to meet a deadline. Finally, support staff can give reminders of upcoming deadlines or subprojects that need to begin.

---

[43] Schwartz, *supra* note 36, at 2.

[44] The Sedona Conference, *supra* note 29, at 275.

4. Monitoring and controlling

Quality control is a critical but often forgotten part of eDiscovery, at least in the sense that litigation teams often do not leave enough time or dedicate enough manpower to the task. When a project manager is on the job, however, their familiarity with the litigation, the data, and any past issues lessens the burden of quality control. Even better, support staff can ensure that quality control is an ongoing, iterative process that happens throughout document collection, processing, and review, such that it is not all put off to the end of discovery when deadlines are looming.[45]

For example, paralegals should routinely check incoming data from the agency and opposing counsel to make sure that it is usable, that it is the data that was expected or requested, and that nothing is missing. They should do the same for outgoing productions, as well as spot-checking for privilege issues or missed redactions or other endorsements. Support staff who have been involved throughout the litigation and understand the discovery plan are best equipped for these tasks.

In a project manager role, support staff are also more likely to spot the need to change litigation plans or to sound the alarm when a plan or deadline becomes unworkable. Support staff are best situated to keep an eye on progress (or the lack thereof) and adjust the workflow and timeline accordingly—for example, they can quickly recognize when missing passwords have caused delays in processing, when the team is behind the necessary pace to timely complete a large set of document review, or when the planned production will be too large to transmit using the agreed-upon method. Additionally, they can help manage the expectations of the attorneys involved—including opposing counsel—to eliminate unpleasant surprises if the process takes longer than expected.

5. Closing

In the closing phase of eDiscovery, support staff should do one final check to ensure that all tracking and documentation is complete, that all productions have been sent as expected, and that all incoming discovery has been received as promised.

And perhaps most importantly, support staff should take the winding down of the eDiscovery process as an opportunity to learn

---

[45] *See id.* at 284.

from any mistakes or issues that arose. Over time, this careful reflection results in the most elusive of assets: institutional knowledge, particularly an understanding of the common pitfalls associated with an agency or type of discovery and the ways to avoid them.

6. Real life

Implementing project management principles in civil litigation may feel like a daunting task that requires an impossible level of buy-in. But the beauty of using project management is that it can be as narrow or as broad as necessary; support staff can organize their tasks using these project management principles without imposing change on the rest of their unit or office. Even if they are the only member of the litigation team using these principles, they are still improving their work product and making their cases run more efficiently, benefitting the rest of the team.[46] The more project management principles are applied to litigation—and applied effectively—the more others in the office will see its value and begin to adopt these principles as well.

III. Conclusion

Support staff can and should take vital leadership positions in the management of the eDiscovery subproject and are truly essential to ensuring that the government meets its discovery obligations. Empowering support staff by ensuring they have a comprehensive understanding of the Federal Rules of Civil Procedure and the discovery process and, further, by including them in planning and strategizing conversations allows support staff to utilize project management principles to increase the efficiency and effectiveness of the litigation team.

[46] Quartararo, *supra* note 24, at ch.3.

About the Author

Leah Wolfe is an Assistant U.S. Attorney in the Civil Division of the USAO for the Southern District of Ohio, handling primarily defensive litigation with an emphasis on real property, medical malpractice, and employment cases. Recently, she has taught classes on discovery for civil support staff at the NAC. Leah previously worked as both a paralegal specialist and legal assistant in the USAO for eight years. She earned her J.D., *magna cum laude*, from Capital University Law School in 2015 and her B.A., *magna cum laude*, in History from the Honors Tutorial College at Ohio University. Leah's article, *The Perfect is the Enemy of the Good: The Case for Proportionality Rules Instead of Guidelines in Civil E-Discovery*, was published in Volume 42 of the Capital Law School Law Review.

Page Intentionally Left Blank

Discovery Conferences Come to Criminal Practice: New Federal Rule of Criminal Procedure 16.1

Thomas M. Woods
Assistant United States Attorney
Western District of Washington

I. Introduction

Our society increasingly collects and retains electronically stored information (ESI). As a result, simple cases increasingly involve complex discovery. A discovery packet for a typical identity theft case prosecuted in the 1990s might have contained nothing more than bank surveillance photographs, some paper bank records, case reports, and physical items seized from the defendant. For a case prosecuted today, those items typically would constitute a fraction of the overall discovery. For example, the discovery might include a forensic copy of the defendant's phone and other digital devices, iCloud and other remotely stored data, e-location information, text messages, and social media data.

In 2006, the Federal Rules of Civil Procedure were amended with new provisions that addressed challenges presented by the explosion of ESI.[1] As it became clear that ESI presented the same type of challenges in the criminal realm,[2] there were increasing calls to amend the Federal Rules of Criminal Procedure as well. In 2019, those calls were answered by the enactment of Federal Rule of Criminal Procedure 16.1.

Rule 16.1 represents a straightforward, albeit very important, approach to the problems and challenges of ESI. Rather than dictate the precise manner and means by which the parties must collect, organize, and produce ESI discovery, the Advisory Committee opted

---

[1] *See generally* Emily Burns et al., *E-Discovery: One Year of the Amended Federal Rules of Civil Procedure*, 64 N.Y.U. ANN. SURV. AM. L. 201, 201 (2008).

[2] *See generally* SEAN BRODERICK ET AL., FED. JUDICIAL CTR., CRIMINAL E-DISCOVERY: A POCKET GUIDE FOR JUDGES (2015).

for "something simple."[3] Under the rule, the parties must confer at the outset of the case about how discovery will be managed. If the parties cannot reach a consensus, either party can ask the court for a hearing to address the outstanding issues.

II. Origins of new criminal Rule 16.1

In March 2016, the New York Council of Defense Lawyers (NYCDL) proposed that the Advisory Committee on the Federal Rules of Criminal Procedure amend Rule 16 to create new discovery obligations in the context of complex cases.[4] The NYCDL complained that defense counsel routinely "receive enormous amounts of information at the outset of the discovery process, with relatively little guidance as to what might be relevant to the prosecution or defense of the charges contained in the indictment."[5] The NYCDL stated that it was increasingly common to receive "gigabytes of discovery" that might include "millions of pages of documentation and thousands of emails culled from the server of a client's employer."[6]

Under the NYCDL's proposal, the government would have been required to provide a discovery index that detailed, among other things, the source and location from which the items were acquired, the date and time of any recordings, and the names of any persons who appear on any recordings.[7] Also, the government would have been required to provide an early exhibit list and copies of the exhibits.[8] Finally, the government would have had to complete discovery within

---

[3] *See* Memorandum from Hon. Donald W. Malloy, Chair, Advisory Comm. on Criminal Rules, to Hon. David G. Campbell, Chair, Comm. on Criminal Rules of Practice and Procedure on Report of the Advisory Comm. on Criminal Rules 5 (May 19, 2017) [hereinafter Preliminary Report], https://www.uscourts.gov/sites/default/files/2017-06-cr_rules_committee_report_0.pdf.
[4] *See* Letter from Roland G. Riopelle, President, N.Y. Council of Def. Lawyers et al. to Hon. Donald W. Malloy, U.S. Dist. Judge on Proposed Amendments to Rule 16, at 1 (March 1, 2016), https://www.nacdl.org/getattachment/94e7a6b6-fd5a-4186-b771-5f9352b97da3/nacdl-comments-with-nycdl-to-judge-molloy-on-proposed-amendments-to-frcrp-rule-16-march-2016-.pdf.
[5] *Id.* at 2.
[6] *Id.*
[7] *Id.* at 5–6.
[8] *Id.* at 6.

six months of arraignment and certify to the court that discovery was in fact complete.[9]

The Rules Committee rejected the NYCDL's proposed measures, but it recognized that the increasing volume of ESI in criminal cases warranted a change in how prosecutors and defense counsel approach discovery at the outset of a case.[10] Specifically, the Committee felt that the concerns identified by the NYCDL "could be adequately addressed in most cases by an early discussion between counsel."[11] The Committee also felt that an early discussion between counsel would be productive in all cases, not simply complex ones involving a large volume of ESI.[12]

The Committee's work culminated in the drafting of Rule 16.1, which became effective December 1, 2019. The rule has two central requirements. First, the parties must confer within 14 days after arraignment about the timing and procedures for Rule 16 discovery.[13] Second, either party can, thereafter, request that the court hold a hearing to determine or modify the time, place, or manner of discovery.[14] The full text of Rule 16.1 states:

> A. Rule 16.1 Pretrial Discovery Conference; Request for Court Action
>
> (a) Discovery Conference. No later than 14 days after the arraignment, the attorney for the government and the defendant's attorney must confer and try to agree on a timetable and procedures for pretrial disclosure under Rule 16.
>
> (b) Request for Court Action. After the discovery conference, one or both parties may ask the court to

---

[9] *Id.* at 5.

[10] Preliminary Report, *supra* note 3, at 4–5.

[11] *See* Memorandum from Hon. Donald W. Malloy, Chair, Advisory Comm. to Hon. David G. Campbell, Chair, Comm. on Rules of Practice and Procedure on Report of the Advisory Comm. on Criminal Rules 2 (May 17, 2018) [hereinafter Final Report], https://www.uscourts.gov/sites/default/files/cr_report_0.pdf.

[12] *Id.*

[13] FED. R. CRIM. P. 16.1(a).

[14] FED. R. CRIM. P. 16.1(b).

> determine or modify the time, place, manner, or other aspects of disclosure to facilitate preparation for trial.[15]

The Committee specifically drafted Rule 16.1 with the intention that it be a freestanding rule, rather than part of Rule 16 itself. As the Committee explained, "Because [the rule] addresses activity that is to occur well in advance of discovery, shortly after arraignment, the Committee concluded it warrants a separate position in the rules."[16] The Committee also felt that a freestanding rule would draw more attention to the new requirements.[17]

III. What Rule 16.1 does and does not affect

The Advisory Committee Note and drafting history provide important guidance about how the rule operates in practice, which includes the following:

A. What does it mean to "confer" under the rule?

The Advisory Committee Note clarifies that the rule "states a general procedure that the parties can adapt to the circumstances."[18] Thus, "[s]imple cases may require only a brief informal conversation to settle the timing and procedures for discovery."[19] By contrast, "[a]greement may take more effort as case complexity and technological challenges increase."[20] Accordingly, in some cases, a brief phone call or an informal discussion at arraignment will suffice under the rule. In more complex cases, a formal meeting between counsel will often be appropriate.

The Committee also recognized that, in some cases, it is impractical to complete discussions under the rule within 14 days.[21] In these circumstances, a brief, informal discussion within the 14-day period, followed by a series of later discussions or meetings, would be appropriate.[22]

---

[15] FED. R. CRIM. P. 16.1.
[16] Final Report, *supra* note 11, at 2.
[17] *Id.*
[18] FED. R. CRIM. P. 16.1 advisory committee note to 2019 adoption.
[19] *Id.*
[20] *Id.*
[21] Final Report, *supra* note 11, at 2.
[22] *Id.*

B. Does the rule require the parties to cover any particular topics when they confer?

The rule directs that the parties "try to agree on a timetable and procedures for pretrial disclosure under Rule 16," but otherwise, it does not specify the specific topics that the parties are to discuss.[23] The Advisory Committee noted in its preliminary report that "[p]articipants did not support a rule that would attempt to . . . list the individual options that should be considered, such as providing [a discovery] index."[24]

C. Must the parties file a report with the court after the parties have conferred?

No. The Committee specifically considered and rejected a requirement that the parties file a joint discovery report after conferring under the rule.[25]

D. Does the rule apply to pro se defendants?

No. The Advisory Committee Note states that, for "practical reasons, the rule does not require attorneys for the government to confer with defendants who are not represented by counsel."[26] The Note cautions, however, that nothing in the rule "limit[s] existing judicial discretion to manage discovery in cases involving pro se defendants, and courts must ensure such defendants have full access to discovery."[27]

E. Does the rule authorize district courts to alter the timetable and procedural safeguards specified in other provisions of law regarding criminal discovery?

No. The initial draft of Rule 16.1 provided that the district court had the authority "to determine or modify the timing, manner, or other aspects of disclosure to facilitate preparation for trial."[28] The Department of Justice (Department) expressed concern that this language could be interpreted as authorizing a court to alter the

---

[23] FED. R. CRIM. P. 16.1(a).
[24] Preliminary Report, *supra* note 3, at 5.
[25] Final Report, *supra* note 11, at 7.
[26] *Id.* at 6.
[27] *Id.*
[28] *Id.* at 4 (emphasis omitted).

timetable or procedural safeguards specified in other provisions of law regarding criminal discovery.[29] For example, under the Jencks Act, the government need not produce a witness's statements until after the witness has testified on direct examination.[30] Although the government often produces such statements much earlier, courts lack the authority to compel the government to produce the statements earlier.[31] The Department's concern was whether Rule 16.1 could empower a court to alter this type of timetable.

The Advisory Committee clarified that Rule 16.1 does not provide courts with such authority. Specifically, the Committee included the following in the Advisory Committee Note: "[T]he rule does not . . . modify statutory safeguards provided in security and privacy laws such as the Jencks Act or the Classified Information Procedures Act . . . ."[32]

During the rule-making stage, the Department also expressed concern that Rule 16.1(b) could be read as authorizing expanded power for courts to order and manage discovery because the original language of Rule 16.1(b) differed slightly from existing Federal Rule of Criminal Procedure 16(d)(2)(A).[33] Under Rule 16(d)(2)(A), a court can order a party who fails to comply with Rule 16 "to permit the discovery or inspection; specify its time, place, and manner; and prescribe other just terms and conditions."[34] The original version of Rule 16.1 contained slightly different language—allowing a court to determine "the timing, manner, or other aspect of disclosure."[35] In response to the Department's concern, the Committee changed the wording of Rule 16.1 to track the wording of Rule 16(d)(2)(A). Thus, under the final version of Rule 16.1, a court is empowered to

---

[29] *Id.*

[30] *See* 18 U.S.C. § 3500(b).

[31] *See, e.g.*, United States v. Algie, 667 F.2d 569, 571–72 (6th Cir. 1982); United States v. Callahan, 534 F.2d 763, 765–66 (7th Cir. 1976); United States v. Spagnuolo, 515 F.2d 818, 821 (9th Cir. 1975); United States v. Sebastian, 497 F.2d 1267, 1270 (2d Cir. 1974).

[32] FED. R. CRIM. P. 16.1 advisory committee note to 2019 adoption; *see also* Final Report, *supra* note 11, at 5 ("[T]he new rule alters neither existing statutory safeguards for security and privacy, nor local rules or standing orders[.]").

[33] Final Report, *supra* note 11, at 4.

[34] FED. R. CRIM. P. 16(d)(2)(A).

[35] Final Report, *supra* note 11, at 4.

determine the "time, place, or manner, or other terms and conditions of disclosure.[36] The Committee also expressed its view that the language of Rule 16.1(b) was not intended to be materially different compared to the language of Rule 16(d)(2)(A).[37]

F. Does the rule prescribe the manner or form in which ESI discovery must be produced?

No. The Advisory Committee considered doing so, but it rejected this approach because "technology changes rapidly."[38] The Advisory Committee Note, however, advised that "counsel should be familiar with best practices" and specifically referenced the national ESI protocol published by the Joint Electronic Technology Working Group in 2012.[39] This group consisted of representatives from the Administrative Office of U.S. Courts' Office of Defender Services, the Department, Federal Defender Organizations, private attorneys who accept Criminal Justice Act appointments, and liaisons from the U.S. Judiciary. The protocol sets forth a number of recommendations as to how parties are to disclose and manage ESI discovery. For example, the protocol recommends that parties producing a large volume of ESI provide a table of contents that describes the general categories of information available as ESI discovery.[40] The protocol also includes recommendations regarding the format in which ESI is produced and how to produce ESI received from third parties.[41] The Advisory Committee heard that not all courts and practitioners were aware of the protocol and hoped to bring more attention to the

---

[36] FED. R. CRIM. P. 16.1(b).
[37] *See* Final Report, *supra* note 11, at 4.
[38] FED. R. CRIM. P. 16.1 advisory committee note to 2019 adoption.
[39] *Id.* A version of Recommendations for Electronically Stored Information (ESI) Discovery Production in Federal Criminal Cases, referred to as National ESI Protocol, is available at https://www.justice.gov/archives/dag/page/file/913236/download.
[40] DEP'T OF JUSTICE & ADMIN. OFFICE OF THE U.S. COURTS JOINT WORKING GRP. ON ELEC. TECH. IN THE CRIMINAL JUSTICE SYS., RECOMMENDATIONS FOR ELECTRONICALLY STORED INFORMATION (ESI) DISCOVERY PRODUCTION IN FEDERAL CRIMINAL CASES, STRATEGIES AND COMMENTARY ON ESI IN FEDERAL CRIMINAL CASES *Strategies* 2 (2012) [hereinafter National ESI Protocol].
[41] *Id.* at *Strategies* 2–4.

protocol by highlighting it in the Advisory Committee Note accompanying the rule.[42]

G. Is there a deadline by which the parties must request a hearing under Rule 16.1(b)?

No. The Committee's final report states: "The rule does not prescribe a time period for seeking judicial assistance."[43] Thus, a party can seek a hearing any time after the initial discussion under Rule 16.1(a) occurs.

H. Does Rule 16.1 displace local rules or standing orders that set forth additional requirements compared to what is required under the rule?

No. The Advisory Committee Note states that the rule does not "displace local rules or standing orders that supplement and are consistent with its requirements."[44] The Committee's final report also clarified that the district court retains "the authority to establish standards for the schedule and manner of discovery both in individual cases and through local rules and standing orders."[45] Also, the district court is not required to accept any agreement reached by the parties at the Rule 16.1 conference as to the timing or manner of discovery.[46]

I. Did the Advisory Committee intend that Rule 16.1 operate in a same or similar fashion as the procedure applicable under the civil rules?

No. Under Federal Rule of Civil Procedure 26(f), parties in a civil case must meet and address a number of specified topics.[47] The parties are, thereafter, required to file a written discovery plan to the court addressing those topics.[48] The Advisory Committee described Rule 16.1 as "bear[ing] some resemblance to Civil Rule 26(f), but . . . more narrowly focused than the Civil Rule."[49] Thus, cases and

---

[42] Preliminary Report, *supra* note 3, at 5; Final Report, *supra* note 11, at 3.
[43] Final Report, *supra* note 11, at 2.
[44] FED. R. CRIM. P. 16.1 advisory committee note to 2019 adoption.
[45] Final Report, *supra* note 11, at 3.
[46] *Id.*
[47] *See* FED. R. CIV. P. 26(f)(3).
[48] FED. R. CIV. P. 26(f)(2).
[49] Final Report, *supra* note 11, at 2.

authorities interpreting the parties' responsibilities under Rule 26(f) will not necessarily be pertinent to criminal cases concerning Rule 16.1.

IV. Conclusion

When the Advisory Committee started to grapple with how to address the challenges presented by ESI, "[a] surprising degree of consensus developed about what sort of rule was needed: something simple that puts the principal responsibility on the lawyers and encourages the use the ESI Protocol, which saves time and is cost-effective for the courts."[50] Rule 16.1 represents that consensus. Rather than overhaul the federal rules or detail how and when the government must produce and organize discovery, the Advisory Committee trusted that parties will largely be able to work through these issues on their own. By mandating early discussions between counsel at the outset of the case, the hope is that the need for a court hearing will prove to be the exception, not the rule.

About the Author

Thomas Woods is an Assistant U.S. Attorney for the Western District of Washington. He serves as the Office's Criminal Discovery Coordinator and is the Deputy Chief of the Terrorism and Violent Crimes Unit. He earned a B.A. in History and Political Science from the University of Wisconsin at Madison and a J.D. at New York University School of Law.

Mr. Woods recognizes with gratitude the contributions from Assistant U.S. Attorney Kristi O'Malley and John Haried, Criminal eDiscovery Coordinator for the Executive Office for U.S. Attorneys.

[50] Preliminary Report, *supra* note 3, at 5.

Page Intentionally Left Blank

Reaching Across the Courtroom: Working Groups that Work

Amy Harman Burkart
Assistant United States Attorney
District of Massachusetts

Timothy Watkins
Assistant Federal Defender
District of Massachusetts

I. Introduction

The impact of the digital age on the collection, management, exchange, and review of discovery in criminal cases cannot be overstated. The ubiquity of electronically stored information (ESI) has dramatically increased discovery volume, and as law enforcement investigations become increasingly data-driven, productions now include new and evolving data formats. The impact is already being felt in courtrooms, and it will continue to grow. We expect that soon many cases prosecuted and defended in federal court will hinge as much on reliable data management as they do on witness testimony. The new normal of data collection and discovery production demands new strategies to ensure that all stakeholders thoroughly understand and embrace the complexity of electronic systems and know how to properly handle, collect, track, review, process, manage, and produce ESI.

The Department of Justice (Department) has undertaken significant efforts internally to identify strategies and solutions to the challenges of ESI discovery for many years, and those efforts have grown into a comprehensive set of resources aimed at meeting eLitigation challenges. Likewise, the Administrative Office of the U.S. Courts Defender Services Office has significantly increased resources and training regarding these issues. But perhaps the most successful effort to date is a multiparty endeavor that has stood the test of time—the formation of the Joint Electronic Technology Working Group (JETWG) and its publications: *Recommendations for ESI Discovery in Federal Criminal Cases* (ESI Protocol),[1] Guidance for the

[1] DEP'T OF JUSTICE & ADMIN. OFFICE OF THE U.S. COURTS JOINT WORKING GRP. ON ELEC. TECH., RECOMMENDATIONS FOR ELECTRONICALLY STORED

Provision of ESI to Detainees (eDiscovery for Pretrial Detainees),[2] and *Criminal E-Discovery: A Pocket Guide for Judges*, (Pocket Guide).[3] These publications provide strategies and guidance and contain practical tips to address discovery issues surrounding ESI discovery. Together they provide a pathway to transforming discovery practices in the digital age.

Despite substantial efforts to publicize these guides and train stakeholders, the underlying principles championed by the ESI Protocol and the Pocket Guide are not consistently followed. At the same time, judicial concern about the quality of representation, as well as the rising costs related to defense discovery review, have increased. The promulgation of Rule 16.1 of the Federal Rules of Criminal Procedure, whose express purpose is to encourage better management of discovery productions by relying on the ESI Protocol's principles and best practices,[4] presents an opportunity to reexamine how to increase the adoption of the approach championed by the ESI Protocol and the Pocket Guide.

In our view, the best way to take advantage of this opportunity is to embrace the JETWG approach of stakeholder cooperation at the local level. While the creation of the ESI Protocol and the Pocket Guide at the national level was critical for obtaining the necessary expertise and authority, in order to most effectively implement the strategies, local practitioners must incorporate them. This is because discovery practices are, like politics, quintessentially local.

Efforts to address the challenge of effective ESI discovery management and review occurs against the background of local bench and bar culture, which in some cases is codified in local rules. Variations in caseload volume and type can also play a significant role in how and whether ESI challenges are addressed. The precise contours of effective practices will vary, sometimes widely, by district. Consequently, the defense attorneys and prosecutors working in the trenches are, along with the beneficence of a district's judicial officers,

---

INFORMATION (ESI) DISCOVERY PRODUCTION IN FEDERAL CRIMINAL CASES (2012).

[2] JOINT ELECTRONIC TECHNOLOGY WORKING GROUP, GUIDANCE FOR PROVISION OF ESI TO DETAINEES (2016).

[3] SEAN BRODERICK ET AL., CRIMINAL E-DISCOVERY: A POCKET GUIDE FOR JUDGES (2015).

[4] FED. R. CRIM. P. 16.1.

the ones who must determine how to apply the national strategies to their own practice.

We have sought to implement this change in our district through the formation of a local working group focused on finding common ground and practical solutions to the challenges of ESI discovery in our cases, guided by the ESI Protocol. We formed our working group informally several years ago, and recently, it has become more formal, and we added additional members. Overall, we have found the local working group to be a valuable resource and an agent for change. We posit that assembling institutional stakeholders into local, district-level working groups may be the single-best vehicle for addressing the systemic changes needed for ESI discovery practices.

II. A very brief history of local working groups

Our idea and subsequent efforts to create a local working group did not occur in a vacuum. Calls to establish local working groups to address novel discovery issues and generate best practices have been recurrent since the nascent appearance of ESI formats.[5] The most recent appeal for working groups was made in connection with

---

[5] *See, e.g.*, JOINT ADMINISTRATIVE OFFICE/DEPARTMENT OF JUSTICE WORKING GROUP ON ELECTRONIC DISCOVERY IN THE CRIMINAL JUSTICE SYSTEM 5 ("The judiciary should urge formation of local working groups in federal judicial districts that include federal prosecutors, defense lawyers, and judges to consider how best to address emerging uses of electronic data and technology that may impact criminal prosecutions in their district."); April 24, 2007 Joint Memorandum from Hon. John Gleeson and Hon. Paul Cassell (Chairs of the Judicial Conference Defender Services Committee and Criminal Law Committee, respectively) to Chief Judges of the District Courts, *Protocol for a Local Working Group On Electronic Technology in the Criminal Justice System* (Apr. 24, 2007) (available through the Administrative Office for U.S. Courts' archive) ("The [JETWG] recognize[s] that local working groups provide an effective means for addressing technological issues in criminal proceedings. We encourage you to consider forming them in your districts."); John McEnany & Donna Lee Elm, *Delivering E-Discovery to Federal Pretrial Detainees*, CRIM. JUST., at 49 (Summer 2017) (advocating for creation of local committee comprised of representatives of defense, prosecution, U.S. Marshals Service detention facilities, and potentially judges to address detainee discovery access).

JETWG's publication of *eDiscovery for Pretrial Detainees*.[6] Those calls for local working groups, however, have gone unheeded. An informal survey of Federal Defender Organizations (FDO), U.S. Attorney Offices (USAOs), and judges across the country uncovered just a smattering of informal working groups functioning in an ad hoc manner. Only one district, the Western District of Washington, established a structured group to systematically address emerging issues. At the same time, FDO offices in numerous districts voiced enthusiasm for developing local working groups to discuss and develop more routinized practices in cases featuring ESI. Similarly, judges grappling with ESI-specific issues triggering delay, rising defense costs, and sometimes ineffective representation have expressed their desire for insight into the changing demands on practitioners.

III. Forming a working group

A. The District of Massachusetts's working group

The authors, an Assistant U.S. Attorney and an Assistant Federal Defender, both of whom have substantial experience litigating large and complex ESI-intensive cases, independently recognized significant areas for improvement in discovery production, management, and review in the District of Massachusetts. Massachusetts is well suited to benefit from consistent delivery and management of ESI discovery: Our Federal Defender Office handles roughly 50% of all indigent appointments and is proactive in sponsoring training programs for the defense bar, while the USAO features a healthy mix of different types of cases, including complex economic and health care fraud prosecutions and multi-defendant violent gang prosecutions.

Joined by the district's Criminal Justice Act (CJA) panel representative and the First Circuit's Case Budgeting Attorney,[7] we began identifying strategies—predominantly focusing on technical competence training for CJA panel members and targeted training on specific areas of concern for USAO staff—to mitigate recurring issues.

---

[6] *See* GUIDANCE FOR THE PROVISION OF ESI TO DETAINEES, *supra*, note 2.

[7] The Case Budgeting Attorney provides assistance and guidance in complex federal criminal cases where ESI discovery tends to play a large role, by coordinating with CJA attorneys and judges within the First Circuit. The Case Budgeting Attorney has a wide range of knowledge in ESI discovery matters and advises whether CJA attorneys' requests are efficient and cost-effective.

In addition, the authors jointly developed a day-long seminar, which featured mandatory attendance by USAO personnel and CJA panelists at the district's smallest division in Springfield, Massachusetts.

The seminar highlighted the difficulties in managing discovery faced by practitioners on both sides, which in turn, precipitated a frank discussion of areas where improvements could be made. The Springfield training session was in many ways a proof-of-concept event. While we conducted "defense only" and "prosecution only" sessions at the end of each day, the majority of the training was conducted jointly with the presiding magistrate and district court judges in attendance for the final sessions, which we believe was a first for our district. The joint presentation sent a powerful message. While there are obviously areas in which we disagree, the shared insight into the challenges faced by each side were invaluable, and we were able to identify a number of practical areas of common ground.

These more informal efforts eventually ripened into a proposal to the district's trial judges for establishing a structured working group chaired by a magistrate judge with an expressed interest in learning about ESI discovery management issues. The response was overwhelmingly enthusiastic, and the District of Massachusetts ESI working group began bi-monthly meetings in June 2019.

B. Suggestions for forming local working groups in other districts

An effective working group requires input from a variety of stakeholders. Moreover, the members representing each stakeholder point of view must be leaders capable of garnering support outside of the room for the decisions made inside the room. In short, each stakeholder must be ready and able to "buy in," to turn recommendations into practice, and have the authority in their offices to train on any practice changes. All members of the group must have a baseline level of knowledge in working on large-scale ESI matters, the use of technology, and of course, a willingness to work with and learn from other stakeholders.

Fundamentally, a working group requires the participation of (1) a representative from the USAO; (2) a representative from the FDO; and (3) the CJA district panel representative. The necessity of these members is self-evident. Beyond that, however, based on our recent experience with a more formal group, we believe a member or

members from the judiciary are essential participants. Ideally, this participation would entail two or more judges who have a good working knowledge of technology issues, with one of the judges chairing the group. These members are necessary to promote the iterative nature of developing best practices for fellow judges district wide, informing and educating judges, and communicating feedback to the working group. In our working group, we have a magistrate court judge and a district court judge participating in and invested in the success of the group. We have also found that, as a practical matter, having judicial involvement keeps the working group moving forward and on task.

There are a number of other potential members of an effective working group:

- **The CJA Case Budgeting Attorney/CJA Supervising Attorney.** We have included the First Circuit Case Budgeting Attorney since the informal formation of our group, and his involvement has been valuable for a number of reasons. Many ESI solutions are expensive, and determining whether a CJA attorney's request is efficient and necessary requires a knowledge of the ESI protocols. We understand that, in other districts, there may be CJA supervising attorneys who fill the role that our Case Budgeting Attorney fills. Regardless of the structure, including the person that reviews and understands the funds requests that CJA attorneys are submitting in that district is useful. Our Case Budgeting Attorney provides the group with insight into the types of services that are needed, and he provides feedback about a better way forward to CJA attorneys seeking coverage for inefficient solutions.
- **A subject-matter expert or consultant on specific ESI issues.** This potential member is on as as-needed basis and can be waived if other members of the working group have significant technological competence.
- **A supervisory deputy from the U.S. Marshals Service (USMS).** This is helpful if detainee access issues are addressed.
- **A representative from the clerk's office.** This potential member helps organize and document meetings and shares insight into the impact of discovery issues on scheduling and other court matters.

IV. Identifying goals and scope

The first task of our working group was to identify and prioritize goals. There was unanimity that training was of paramount importance. Judges and CJA defense bar representatives reported particularly strong interests in training events focusing on ESI issues. The working group continues to discuss the most efficient methods to reach all stakeholders, with the currently preferred method being a two-stage training: (1) a presentation by the authors to the district's judges followed by (2) a presentation to a joint prosecutor/defense attorney assembly. Other issues currently under consideration by the working group include the following:

- The best practices to ensure implementation of Rule 16.1 of the Federal Rules of Criminal Procedure's "confer" provision, including insuring that parties meaningfully communicate about and resolve issues as identified in the ESI Protocol;
- Discovery disclosure logistics, including volume, timing, form, and scope of table of contents;
- The necessity or advisability of technical competence standards for attorneys regularly practicing in federal court;
- Challenges to detainee access to complex and voluminous discovery, including where protective orders may complicate access; and
- CJA access to, and funding for, technical assistance.

V. Key challenges and benefits of a working group

A. Challenges

The most significant challenges to starting a working group are working through the two issues identified above: finding the right people to form the group and defining the scope of what the group will handle.

Identifying appropriate representatives from each stakeholder is crucial to success. The natural instigating institutional actors will be senior level Assistant Federal Defenders and Assistant U.S. Attorneys from within the district with significant experience in large-volume ESI matters, both in handling the matters personally and in assisting or supervising colleagues with their own matters. Those personnel,

unfortunately, are also the most likely to have the least amount of discretionary time to devote to the work and the logistics of such a group. Nevertheless, experience and a certain level of seniority is required in order for the working group member to have the ability to speak for, and convey decisions back to, their respective constituents. Identifying potential participants with the ability and interest to strike this balance can be challenging.

Similarly, identifying a member of the defense bar/CJA panel who has the authority within the group, the experience and expertise to be a contributing member, and the bandwidth to participate in the group is difficult. While we were able to secure the participation of the CJA District Panel Representative, she struggles—as do we—with carving out sufficient time to devote to carrying out the tasks generated by the working group.

It is also vitally important to identify the appropriate non-courtroom attorney members of the Working Group. As noted above, the Working Group is strengthened by adding a member or members of the Judiciary, the Clerk's Office, the USMS, and the Budgeting Attorney. But it is the prosecutor and the defense attorneys that are closest to the intricate ins and outs of discovery practice and the real-life challenges of putting together and analyzing large-scale productions. There are many ideas that inevitably emerge in discussing eLitigation issues that sound reasonable in concept but are entirely unworkable in reality. The ESI Protocol and the other JETWEG documents have always encouraged putting the specifics of decision making in any particular case on the parties closest to that case—the attorneys prosecuting and defending it. We think the best working groups will take the same approach: Incorporating the perspectives and leadership of all members but expecting that most of the specific mechanics will be best understood by the litigating attorneys. Thus, once again, it is essential to identify the right people—those with the subject-matter interest and skills, as well as a collaborative attitude and an ability to know when it is wise to get involved in specifics and when it is wise to defer to others. In our group, we have been extraordinarily lucky to have other members, including the judiciary, that strike this delicate balance.

Identifying the scope of the working group is another critical challenge. As noted above, projects worth tackling abound. But with limited time, prioritizing the goals of the group and developing a concrete set of tasks and projects that advance those goals is paramount. This issue has remained the tallest hurdle for us—there

is much good work to be done, but each of the participants is juggling multiple commitments. We continue to work to define the priority goals and develop realistic steps we can take to advance those goals.

B. Benefits

We have found that the primary benefit of a working group is in getting everyone around the table to share concerns, information, and perspectives. Discussing our respective challenges with ESI discovery often reveals that different stakeholders are dealing with the same problem—the prosecutor's dilemma in obtaining readily usable social media material from providers becomes the defense attorney's headache in comprehensively reviewing it, which then winds up with a presiding judge grappling with a delay in setting trial dates and assessing what defense discovery review costs are reasonable.

At times, there is a sense that the problems are the "fault" of one of the other stakeholders—and it may well be the case that there are situations that are caused or exacerbated by the action or inaction of another stakeholder—we generally agree to table whether such occasions are warranted by the circumstances. But there are many times where we realize that we are both dealing with a problem that is caused not by any individual actor or institution but rather by a changing world—for example, a sharp increase in the volume of data available from a source as electronic data storage becomes cheaper, a proprietary format used by a third party that no stakeholder is able to use effectively, etc.

Specifically, simply developing and convening the working group has resulted in greater insight and a respect for

- the government's challenges in collecting data in "the wild"—as it exists in a variety of formats—and grappling with how to process that data for discovery production;
- defense attorneys' difficulties in obtaining technical competence and assistance where necessary; and
- judges' limitations in dealing with discovery disputes engendered by ESI, avoiding delay, and providing funding where supported.

As we become more aware of the challenges faced by each stakeholder, we work together to identify solutions, even to issues that are not "our" issues. For instance, the working group as a whole, including the budgeting attorney, the magistrate judge, as well as ourselves, have brainstormed ways to obtain better technical

paralegal support for defense attorneys on the CJA list. This is an issue that has continued to challenge the CJA panel, and working together to solve it will ultimately benefit the system as a whole. The collaborative discussion around this problem is the type of problem-solving approach that we hope to bring to additional challenges we address as a working group.

VI. Conclusion

Just as the success of JETWG's effort on a national level depended on the involvement of all stakeholders, the most effective implementation of the policies on a local level will require participation from all stakeholders. The amendment of Rule 16.1 to require a "confer" component with explicit reference to the ESI Protocols[8] provides an opportunity for districts to evaluate their compliance with the strategies and approaches outlined in the protocol and consider whether forming a local working group would further the adoption of the ESI Protocols. Based on our experience in the District of Massachusetts, our recommendation is for other districts to form such a group and have those groups define the scope and goals to suit the needs and meet the challenges of their local practice.

About the Authors

Timothy Watkins has been an Assistant Federal Defender in the District of Massachusetts for the last two decades, defending the gamut of federal criminal matters, including large fraud and terrorism cases. In 2018–2019, he was detailed to the Administrative Office of the U.S. Courts as a Director's Leadership Program Resident, where he examined court practices nationwide managing the challenges of criminal case discovery in the electronic age.

Amy Harman Burkart is the Chief of the Cybercrime Unit in the District of Massachusetts. From 2018–2020 she was the Co-Chair of the eLitigation Working Group.

[8] FED. R. CRIM P. 16.1 advisory committee's note to 2019 adoption.

Rule 26 Proportionality: Have the 2015 Amendments Brought Common Sense to the Preservation Obligation?

Sarah Himmelhoch
Senior Litigation Counsel for E-Discovery
Environment and Natural Resources Division

Neeli Ben-David
Deputy Chief, Civil Division
Northern District of Georgia

Since the turn of this century, the obligation to preserve evidence—particularly electronic documents and data—has been the subject of great attention and debate. This article explores the question of whether the 2015 amendments to the Federal Rules of Civil Procedure achieved the stated goal of "address[ing] the serious problems resulting from the continued exponential growth in the volume of such information."[1]

Unfortunately, a clear and simple answer to this question has not yet emerged. The case law interpreting the amended rules demonstrates that the determination as to whether to impose sanctions for the loss of electronic evidence remains highly case specific and, therefore, difficult to extrapolate. As the conclusion of this article demonstrates, however, the 2015 amendments and emerging case law do provide some insight to practitioners seeking to bring balance and reason to preservation efforts.

I. Background

The prohibition against destroying evidence, or spoliation, can be traced to Roman law, which included Justinian's maxim "*omnia praesumuntur contra spoliatorem*" or "all things are presumed against

[1] FED. R. CIV. P. 37(e) advisory committee's note to 2015 amendment.

the wrongdoer."[2] Early English and American common law adopted this doctrine.[3]

The preservation of evidence became a focus of many courts as electronic evidence made the destruction and alteration of evidence harder in some respects and easier in others. The profusion of electronic data, the ease with which that data can be altered, and the existence of multiple copies of most data on backup tapes or servers introduced new challenges to preserving evidence. This issue reached prominence in federal civil litigation early in this century, particularly in light of the attention given to the decisions in *Zubulake v. UBS Warburg LLC*.[4]

In *Zubulake*, a female equities trader specializing in Asian securities sued her former employer for gender discrimination.[5] In the court's own words,

> Fully aware of their common law duty to preserve relevant evidence, UBS's in-house attorneys gave oral instructions in August 2001—immediately after Zubulake filed her EEOC charge—instructing employees not to destroy or delete material potentially relevant to Zubulake's claims, and in fact to segregate such material into separate files for the lawyers' eventual review. This warning pertained to both electronic and hard-copy files, but did *not* specifically pertain to so-called "backup tapes," maintained by UBS's information technology personnel.[6]

Despite these and later instructions, the defendant deleted certain relevant emails from the active servers—meaning the only copies of these emails could be found in the less accessible backup media.[7] When the court ordered the defendants to restore the backup tapes to recover the missing emails, the defendant discovered some of the

---

[2] Kevin Eng, *Spoliation of Electronic Evidence*, 5 B.U.J. SCI. & TECH. L. 13 (1999).

[3] *See, e.g.*, *The Pizarro*, 15 U.S. 227 (1817); *Pomeroy v. Benton*, 77 Mo. 64 (1882).

[4] 229 F.R.D. 422 (S.D.N.Y. 2004).

[5] *Id.* at 424–25.

[6] *Id.* at 425 (footnotes omitted).

[7] *Id.* at 426.

tapes had been destroyed.[8] It also became clear that the defendant failed to produce some relevant emails retrieved from the backup media.[9]

On these facts, the *Zubulake* court held that the defendant had acted willfully in deleting relevant information.[10] Accordingly, the court ordered that the jury would be given an adverse inference instruction—directing them to infer that the lost evidence would have been favorable to the plaintiff.[11]

The strong language in the *Zubulake* opinion, the severe sanctions imposed, and the emphasis on counsel's duty with respect to implementing and monitoring compliance with a litigation hold garnered wide attention in legal circles. As one commentator stated:

> That 2004 ruling, nicknamed *Zubulake V* because it was the fifth of five pretrial decisions, became a landmark in many respects. It helped propel the e-discovery industry into the stratosphere, turning it into one worth billions, while setting up litigation rules that are still being fought over 10 years later.[12]

In the years following the *Zubulake* decision, escalating concern regarding the expense and burden of preserving electronic evidence—particularly in light of risk-adverse counsel's strict instructions issued for fear of violating their duty to impose and monitor litigation holds—led to calls for clarity and reason in the rules regarding the preservation of electronic evidence.[13]

---

[8] *Id.* at 427.
[9] *See id.* at 426–27.
[10] *Id.* at 436.
[11] *Id.* at 436–37.
[12] Victor Li, *Looking Back on Zubulake, 10 Years Later*, A.B.A. J. (Sept. 1, 2014), http://www.abajournal.com/magazine/article/looking_back_on_zubulake_10_years_later.
[13] *See, e.g.*, FED. R. CIV. P. 37(e) advisory committee's note to 2015 amendments ("These developments have caused litigants to expend excessive effort and money on preservation in order to avoid the risk of severe sanctions if a court finds they did not do enough.").

II. The 2015 amendments

In 2015, the Federal Rules of Civil Procedure were revised to address the practical challenges posed by the discovery of electronically stored information (ESI), including the huge amounts of potentially available ESI even in relatively small cases.[14] One of the most significant changes was the refinement of what is "discoverable" under Rule 26 to include the requirement that the discovery be proportional to the needs of the case (prior to the 2015 amendments, the proportionality factors were contained elsewhere in Rule 26). It is no longer enough for the materials to be relevant; the request for such materials must also be proportional to the needs of the case in order to fall within the Rule 26 definition of discoverable. As Chief Justice Roberts argued in his 2015 annual report, the amended Rule 26(b)(1) "crystalizes the concept of reasonable limits on discovery through increased reliance on the common-sense concept of proportionality."[15]

Courts are required to consider the following factors when determining whether materials are discoverable:

- "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."[16]

To ensure that the proportionality requirement was fully incorporated into the discovery process, the revised rules also raised the standard for imposing case-dispositive sanctions for the spoliation of electronic evidence (for example, adverse inference, dismissal, default judgment) to situations where the court finds an "intent to deprive another party of the information's use in litigation."[17]

---

[14] *Id.*

[15] 2015 YEAR-END REPORT ON THE FEDERAL JUDICIARY 6, https://www.supremecourt.gov/publicinfo/year-end/2015year-endreport.pdf.

[16] FED. R. CIV. P. 26(b)(1) (cleaned up).

[17] *See* FED. R. CIV. P. 37(e)(2).

Reading the revised Rule 26 and Rule 37 together, practitioners and courts alike hoped that they would reduce not only the discovery burden caused by the large amounts of available ESI, but also the preservation burden.[18]

III. Decisions under the 2015 amendments

Despite the high expectations of all involved, litigation under the amended Rule 37(e) has revealed that the question of whether dispositive sanctions should be imposed for the loss of electronic information remains highly fact specific. There are, nonetheless, some indications that the amendments have begun to focus the courts on the proportionality factors and to clarify the necessary intent under the amended rule. Practitioners can expect the continued refinement of these analyses will bring greater certainty with regard to the appropriate scope of preservation efforts in future cases and prevent some costly preservation practices from continuing.

A. Sometimes, the more things change, the more they stay the same

Importantly, Rule 37(e) has not eliminated the need for, or the actual imposition of, case-dispositive sanctions when material evidence has been spoliated. For example, in *Small v. University Medical Center*, the court issued sanctions, including an adverse inference instruction, against defendant University Medical Center (UMC) for failing to preserve several categories of ESI.[19] While UMC's preservation failings were systemic, the court found those breakdowns stemmed in large part from UMC's failure to conduct effective interviews of its employees.[20] Custodians possessing relevant

---

[18] *See, e.g.*, 2015 YEAR-END REPORT ON THE FEDERAL JUDICIARY, *supra* note 15, at 9 ("The 2015 civil rules amendments are a major stride toward a better federal court system. But they will achieve the goal of Rule 1—'the just, speedy, and inexpensive determination of every action and proceeding'—only if the entire legal community, including the bench, bar, and legal academy, step up to the challenge of making real change."); *Significant Changes Made To The Federal Rules Of Civil Procedure*, BENNETT, BIGELOW & LEEDOM, P.S., https://www.bbllaw.com/significant-changes-made-to-federal-rules-civil-procedure/ (last visited Feb. 18, 2020).

[19] No. 2:13-cv-0298-APG-PAL, 2018 WL 3795238, at *70–*71 (D. Nev. Aug. 9, 2018).

[20] *See id.* at *19–*20.

information were not interviewed until after the court appointed a special master to investigate UMC's discovery shortcomings—20 months after the litigation began. Once conducted, the interviews were deemed insufficient by both the special master and the court.[21]

Similarly, in *EPAC Technologies, Inc. v. HarperCollins Christian Publishing, Inc.*, the defendant allowed the destruction of over 750,000 emails and their attachments despite a relatively timely initial legal hold notice.[22] The court found that the evidence loss resulted from a litigation hold notice comprised solely of unhelpful boilerplate.[23] The defendant compounded the flaws in the litigation hold notice by improperly distributing the litigation hold and allowing the recipients to ignore the notice.[24]

The court found that the evidence did not support a finding of an intent to deprive the opposing party of access to the evidence. Nonetheless, the court found that the defendant made only "halfhearted attempts . . . to impose a litigation hold" and that the defendant's counsel failed to provide "sufficient guidance" or monitoring of compliance.[25] Recognizing that Rule 37(e) "plainly separates negligence and even gross negligence from the intent to prevent the use of evidence in litigation,"[26] the court did find prejudice resulting from the loss of the emails.[27]

Notably, this case also involved the loss of physical evidence. Rule 37(e), by its plain language, does not apply to the loss of paper or physical items as opposed to ESI. Thus, while the court concluded that it could not apply case-dispositive sanctions under Rule 37(e), it could do so under the common law.[28] In the end, the court stated it would

> instruct the jury that [the defendant] had a duty to preserve evidence relevant to this litigation; that it breached that duty by negligently allowing the books in its control to be sold, lost, or destroyed; and that the

---

[21] *See id.*
[22] No. 3:12-cv-00463, 2018 WL 1542040, at *6–*8, *17 (M.D. Tenn. Mar. 29, 2018).
[23] *Id.* at *7.
[24] *Id.*
[25] *Id.* at *18.
[26] *Id.*
[27] *Id.*
[28] *See id.* at *19.

> jury may infer that, if available, the books would support EPAC's claims and be adverse to Thomas Nelson's arguments.[29]

The court in *Nutrition Distribution LLC v. PEP Research* also imposed an adverse inference instruction against defendants for their failure to preserve relevant social media posts from Facebook and Twitter.[30] In that case, the defendants apparently destroyed the posts after the duty to preserve attached, with one of the defendants defiantly testifying at his deposition, "I have the right to do whatever I want to do with my Facebook account, regardless of a lawsuit or not. If I wanted to—if I want to delete every single post on my Facebook page, I have the right to do so."[31] That testimony, taken together with the defendants' failure to produce the requested social media posts, convinced the court that the defendants destroyed the relevant evidence with an intent to deprive the plaintiff of its use in the litigation.[32]

There is one final case demonstrating that some aspects of preservation disputes have not changed under the amended Rules of Civil Procedure. In *Gordon v. Almanza*, the defendant failed to preserve his cell phone containing data relevant to the accident that gave rise to the lawsuit.[33] The judge denied the plaintiff's request for an adverse inference, concluding that, although the defendant was unable to produce ESI from his cell phone, there was no prejudice because the plaintiff could still obtain all the data relevant to the issue of whether the defendant was on his cell phone at the time of the accident.[34]

Interestingly, although the judge essentially analyzed the case under Rule 37(e)(1), he reached his decision by determining whether he had the inherent authority to issue sanctions.[35] In other words, some courts do not wish to deviate from their inherent authority, even though the amended rule seems to account for all relevant factors for determining sanctions.

---

[29] *Id.* at *22.
[30] 16-cv-2328-WQH (BLM), 2018 WL 3769162, at *1 (S.D. Cal. Dec. 4, 2018).
[31] *Id.* at *16.
[32] *Id.* at *18.
[33] No. 16-CV-00603, 2018 WL 2085223, at *1 (S.D. Iowa Mar. 5, 2018).
[34] *Id.* at *2–*3.
[35] *Id.* at *1.

B. Overall, however, the times they are changing

Notwithstanding the continued imposition of severe sanctions in some cases, the post-2015 case law does indicate nascent changes in the approach to spoliation disputes; specifically, a move from the imposition of case-dispositive sanctions to measures sufficient to cure any prejudice that resulted from the spoliation.

For instance, in *GN Netcom, Inc. v. Plantronics*, after the lawsuit was filed, a former employee of the defendant wrote to his team, "please be careful about competitive statements like what was said below. I would suggest everyone immediately delete this message."[36] He repeated similar instructions when he received other emails that would be adverse if used as evidence in the lawsuit.[37] The same employee also deleted more than 40% of his own emails.[38] Other executives encouraged their employees to use code words to hide the challenged conduct.[39] The trial court held an evidentiary hearing on the spoliation. The court denied the plaintiffs' request for a default judgment but, instead, awarded a five million dollar fee against the defendant, instructed the jury on the spoliation, and allowed the plaintiff's counsel to comment about the spoliation during trial.[40]

Lest one think this case demonstrates continuity with pre-2015 case law, it is important to note that the judge still drew a line and denied the plaintiff's request for a dispositive sanction.[41] Arguably, the moderating influence of Rule 37(e) contributed to the court's calibration of the appropriate sanction to the prejudice caused by the spoliation.

A decision out of the Western District of New York, *Moody v. CSX Transportation, Inc.*, provides a similar example of the moderating influence of Rule 37(e).[42] *Moody* involved the loss of ESI from an event recorder in a locomotive.[43] ESI relevant to a personal injury accident had been downloaded from the recorder to a laptop.[44] The laptop

---

[36] 930 F.3d 76, 80 (3d Cir. 2019).
[37] *Id.*
[38] *Id.*
[39] *Id.*
[40] *See id.* at 81.
[41] *See id.* at 82–83.
[42] 271 F. Supp. 3d 410, 432 (W.D.N.Y. 2017).
[43] *See id.* at 415.
[44] *Id.* at 422.

crashed a year or more after the downloading, and the laptop was recycled or destroyed thereafter.[45] Moreover, the lost ESI was supposed to have been uploaded to a central repository but could not be accessed.[46] The court imposed an adverse-inference instruction against the defendants to address the "evidentiary gap caused by [the] defendants' loss of such material evidence."[47] Among other things, the court found that "the defendants' explanation for the loss of the data strains credulity" and that "[t]he proposition that a sophisticated railroad transportation corporation such as CSX could be involved in a serious accident in which an individual lost a limb and thereafter fail for four years to review critical data relating to how that accident occurred is unfathomable."[48] In other words, the defendants acted unreasonably in destroying or recycling the laptop and in failing to confirm that the ESI had been uploaded successfully, pursuant to an established corporate procedure.

Like the *Plantronics* court, however, the court refused to dismiss the case. The court emphasized that "[c]ourts must be wary of issuing case-dispositive sanctions; such sanctions should be imposed only in extreme circumstances, usually after consideration of alternative, less drastic sanctions."[49] In the court's view, the adverse inference was appropriately calibrated to the harm caused by the spoliation.

Further indications of the influence of Rule 37(e) come from *ML Healthcare Services, LLC v. Publix Super Markets, Inc.*, which focused on the interplay between proportionality and preservation.[50] In this slip and fall personal injury case, the plaintiff sent the defendant several demands for preservation and production of video of the incident.[51] Although the defendant did preserve one hour of video—that hour reflecting the 30 minutes before and after the accident—it allowed the automatic erasure of the remaining video of that day.[52] The plaintiff moved for "a ruling precluding [the d]efendant's witnesses from testifying that the aisle had been cleaned or inspected

---

[45] *Id.* at 423.
[46] *Id.* at 422–23.
[47] *Id.* at 432.
[48] *Id.* at 426–27.
[49] *Id.* at 432 (quoting Arista Records LLC v. Usenet.com, Inc., 633 F. Supp. 2d 124, 141 (S.D.N.Y. 2009)).
[50] 881 F.3d 1293 (11th Cir. 2018).
[51] *Id.* at 1307.
[52] *Id.*

prior to [the p]laintiff's fall."[53] The Eleventh Circuit upheld the trial court's refusal to impose sanctions, finding that the defendant's preservation of the excerpt of video

> Fulfill[ed] the request of [the p]laintiff's first two preservation letters. As to [the p]laintiff's subsequent preservation letters, the requests in those letters encompassed all video media from every camera at the store for a period of thirty-five days—totaling 840 hours of video per camera, assuming the cameras run for 24 hours a day. [The d]efendant might reasonably, and in good faith, have concluded that it did not have to comply with such a broad and far-reaching request.[54]

The appellate court emphasized that the plaintiff had not tailored its preservation demand to the need she had articulated—going right to the core of the concept of whether the preservation obligation was proportional to the needs of the case.[55]

Rule 37(e) has also clearly affected how courts analyze the question of the spoliator's fault or intent. For instance, in *Schmalz v. Village of North Riverside*, the defendants failed to preserve cell phones containing vital text messages after there was a litigation hold.[56] While the court awarded attorney's fees regarding the discovery of the text messages, it felt that the plaintiff's request for an adverse inference was too severe because the plaintiff failed to demonstrate that the defendant acted with an intent to deprive the other party of the ESI.[57] In a departure from some pre-2015 cases, the court stated:

> [The p]laintiff cites to several out of circuit cases for the proposition that intent and bad faith can be demonstrated by failing to take reasonable steps to preserve ESI. In these cases, however, the courts identified other factors in addition to failing to take

---

[53] *Id.*
[54] *Id.* at 1308.
[55] *See id.* at 1308–09.
[56] No. 13 C 8012, 2018 WL 1704109, at *2 (N.D. Ill. Mar. 23, 2018).
[57] *See id.* at *5.

> reasonable steps to preserve ESI to support a finding of intent.[58]

The Northern District of Illinois is not alone in recognizing that the intent requirement of the amended Rule 37(e) is greater than what was previously required to impose severe spoliation sanctions. In *Lokai Holdings LLC v. Twin Tiger USA LLC*, the court declined to find intentional spoliation where intent was not established by "clear and convincing evidence."[59] In this case, the defendants were subject to a cease-and-desist letter prior to litigation. Notwithstanding the notice of anticipated litigation, the defendant continued to manually delete old emails to stay within their provider's storage limit.[60] After receiving minimal email production during discovery, the plaintiff sought dispositive sanctions and claimed the defendants intentionally destroyed key emails.[61]

The court refused to impose the "severe sanction" of an adverse inference because the defendant provided a credible explanation for its actions that was not driven by an intent to deprive the plaintiff of the ESI:

> [T]here is no basis to conclude whether Defendants even engaged in selective deletion, much less whether they did so with an intent to deprive. While a court may infer that a party acted with an intent to deprive on the basis of circumstantial evidence, here, the presented evidence is capable of more than one interpretation, and this Court will not make a finding of intent to deprive on the basis of suspicion alone.[62]

Using the principles of Rule 37(e)(1), because the court found the plaintiff was prejudiced, the court awarded a curative sanction—

---

[58] *Id.* (emphasis omitted). *Compare* Housing Rights Ctr. v. Sterling, No. CV 03-859 DSF, 2005 WL 3320739, at *2, *8 (C.D. Cal. Mar. 2, 2005) (imposing sanctions for destruction of documents after acknowledging that there was no litigation hold in place).

[59] No. 15cv9363 (ALC) (DF), 2018 WL 1512055, at *1 (S.D.N.Y. Mar. 12, 2018).

[60] *See id.* at *2.

[61] *See id.* at *3–*4.

[62] *Id.* at *16 (citing Moody v. CSX Transp., 271 F. Supp. 3d 410, 431–32 (W.D.N.Y. 2017)).

payment of the plaintiff's fees and costs and precluding the defendant from mentioning the lost emails at trial.[63]

The District of Colorado undertook a similar analysis in *Mueller v. Swift*, in which a radio DJ claimed pop star Taylor Swift falsely accused him of sexual misconduct, resulting in his firing.[64] At the time of his termination, the DJ recorded his calls with his employer. Swift requested them in discovery.[65] The DJ turned over the files to his attorney, but not before editing them to delete everything that was not important.[66] He had retained unedited versions of the files on his laptop, but at some point after he provided the edited files to his attorney, "coffee was spilled on the keyboard of [the DJ's] laptop, damaging it."[67] Therefore the defendant, Taylor Swift, asked the court "to give the jury an adverse inference instruction at trial, to direct the jury 'that the entirety of the June 3, 2013 audio recording would have been unfavorable to Plaintiff.'"[68]

Applying Tenth Circuit precedent and Rule 37(e), the court held that such an inference is only warranted if there is sufficient proof the evidence was lost or deleted in bad faith.[69] Though the court found that the DJ was "unjustifiably careless in his handling of evidence that he had a clear duty to preserve," the court declined to find bad faith.[70] The court, therefore, denied Swift's request for an adverse inference but allowed her to cross-examine the plaintiff about the record of spoliation in front of the jury.[71]

Similarly, in *Shaffer v. Gaither*, the defendant filed a motion to dismiss, seeking dismissal "as a sanction for [the] plaintiff's failure to preserve electronically stored data, to wit, sexually suggestive text messages allegedly sent by plaintiff to a married third-party paramour, which defendant contends are critical to his defense."[72] It

---

[63] *See id.* at *17.
[64] No. 15-cv-1974-WJM-KLM, 2017 WL 3058027, at *1 (D. Colo. July 19, 2017).
[65] *Id.* at *1.
[66] *See id.*
[67] *Id.* at *2.
[68] *Id.* at *2.
[69] *Id.* (citing Turner v. Pub. Serv. Co., 563 F.3d 1136 (10th Cir. 2009)).
[70] *Id.* at *5.
[71] *Id.*
[72] No. 5:14-cv-00106-MOC-DSC, 2016 WL 6594126, at *1 (W.D.N.C. Sept. 1, 2016).

was undisputed that the text messages had been lost when the plaintiff's phone was dropped, damaged, and turned in for a replacement.[73] The court concluded this occurred well after a duty to preserve the messages had already arisen:

> The problem in this case is not that the phone was destroyed, but that the texts were not preserved well before May 2014. . . .
>
> Likewise, plaintiff and her counsel failed to take reasonable steps to preserve those texts as they apparently resided only on plaintiff's phone. Once it is clear that a litigant has ESI that is relevant to reasonably anticipated litigation, steps should be taken to preserve that material, such as printing out the texts, making an electronic copy of such texts, cloning the phone, or even taking possession of the phone and instructing the client to simply get another one. At this point, the court cannot conclude that plaintiff acted with an intent to deprive defendant of the ESI under Rule 37(e)(2); thus, spoliation does not yet come into play. Instead, the court's task is to craft an Order that cures the prejudice resulting from the loss.[74]

Because the primary source of the text messages was gone, and the messages could not be recovered from the carriers, the only avenues left to the defendant were to seek the recipients' copies through a third-party subpoena and to question the two of them about the contents of the communications.[75] The court denied the defendant's request for dismissal but allowed the presentation of evidence about the loss, and the court reserved the right to add a spoliation jury instruction after hearing the evidence—and to reconsider dismissal if evidence of intentionality was uncovered.[76]

One other sign of change resulting from the amendment of Rule 37(e) comes from *Henson v. Turn, Inc.*[77] In that case, the court evaluated the question of proportionality by weighing the plaintiffs' privacy concerns against the defendant's interest in obtaining the

---

[73] *Id.*
[74] *Id.* at *2.
[75] *See id.*
[76] *Id.* at *3.
[77] No. 15-cv-01497-JSW (LB), 2018 WL 5281629 (N.D. Cal. Oct. 22, 2018).

complete web browsing history on the plaintiffs' mobile devices.[78] The defendant sought to image the plaintiffs' mobile devices in an effort to ferret out aspects of their claims that the defendant improperly used enhanced internet tracking technology.[79] The court reasoned, however, that if the defendant were allowed to image the devices, it would be able to explore sensitive details about the plaintiffs' private lives that were not relevant to the claims or defenses.[80] Privacy considerations militated against such discovery, leading the court to determine that the requested discovery was both irrelevant and disproportionate to the needs of the case.[81]

The decision in *Henson* represents a departure from the traditional determination of burdens under a proportionality analysis that focused on the cost of discovery. Rather, *Henson* relied on nonmonetary factors, such as privacy, to evaluate the nature and extent of discovery burdens. This factor is particularly relevant when discovery is sought from smartphones and other internet-enabled devices. This change in focus reflects the introduction of all of the proportionality factors into the inquiry regarding the scope of discovery—and therefore, the scope of the preservation obligation.

IV. Conclusion and practice pointers

An exploration of the case law interpreting amended Rule 37(e) reveals that the question of the appropriate sanction remains very case specific and, therefore, it is difficult to make overarching pronouncements regarding the effect of the amended rules. The cases decided in the five years since the rules were amended, however, suggest that courts are trending toward more tightly correlating the importance of the evidence and the degree of prejudice with the particular sanctions imposed.

In light of this apparent trend, practitioners should have increased confidence in drawing reasonable boundaries when advising clients regarding the scope of preservation. Such confidence should be accompanied by some best practices. Most importantly, when working with a client to put a litigation hold in place, practitioners should gather information regarding the burden associated with the various

---

[78] *See id.* at *5.
[79] *See id.* at *4.
[80] *See id.* at *7.
[81] *See id.*

possibilities for the scope of the hold. Such information should be as specific as possible, including addressing the person-hours, the volume of data, the available storage options, the difficulty in preserving the accessibility of the ESI, and any issues with the format of ESI. When drawing the final boundaries of the hold, practitioners should make records of their reasoning, especially when choosing to exclude certain categories of information from the hold based on the burden associated with those preservation efforts.

Practitioners should address these measures with opposing counsel early on but no later than the 26(f) conference. For example, discuss who the key custodians are and the size of their email accounts. Identify ESI that is burdensome to preserve while also being of marginal usefulness. Common issues discussed at Rule 26(f) conferences include, among other things, the preservation of relevant information and ESI (for example, ephemeral data, text messages, self-deleting messages, and disaster recovery systems), the relevant metadata for the needs of the case that must be preserved, and other case-specific preservation challenges.

The final, and in some respects most important, lesson for practitioners facing challenges related to the scope and burdens of preservation is to recognize that if the parties cannot agree as to a reasonable scope of the litigation hold, Rule 16 provides that the first pretrial hearing after the Rule 26(f) conference should address issues related to preservation. Accordingly, if the parties cannot agree, practitioners should seek guidance from the court at the earliest opportunity.

Practitioners should also continue to recognize the need to not only issue the litigation hold notice, but also supervise and confirm the client's implementation of the hold. These efforts will require a plan that identifies the nature of the information to be protected, the methods that will be used to preserve the information, and any necessary steps to keep the data accessible. Enterprises involved in litigation should seek to develop a defensible process for preserving relevant electronic information. Such a process is characterized by various steps, including the need to notify key players and other data sources with relevant ESI of the requirement to preserve that information. In addition, in many cases, a critical step to ensuring relevant materials are preserved may be to conduct fulsome custodian interviews. Doing so will enable counsel to obtain a better understanding of the nature and extent of unique, relevant

information in the client's possession, custody, or control and the steps needed to preserve that information.

The case law since the 2015 amendments also advises practitioners to be cautious when allowing custodians to be responsible for collecting and preserving data themselves. This caution should be especially heightened when the custodians might be implicated in allegations of misconduct or improper behavior. Practitioners should take steps to supervise preservation efforts by personnel when they are being instructed to preserve and self-collect.

Further, practitioners are wise to take extra caution to ensure that relevant social media posts within the possession, custody, or control of the party are preserved for litigation. Like data from messaging applications and other smartphone apps, social media content is dynamic and can be easily modified or destroyed. Litigants in the current legal environment should have an updated litigation readiness program with questionnaires that spotlight different social media platforms and smartphone apps (particularly those used for messaging) that may contain relevant information. Promptly issuing a litigation hold instruction, together with a relevant source checklist and appropriate follow up measures, can help avoid a sanctions disaster like the kind that befell defendants in *Nutrition Distribution.*

With these practical steps and a continued focus on the enumerated proportionality factors, it is probable that, with time, the amendments to Rule 37(e) will bring common sense to the obligation to preserve evidence that may be relevant to pending or anticipated litigation.

About the Authors

Sarah Himmelhoch is the Senior Litigation Counsel for discovery for the Environment and Natural Resources Division. She entered the Division as an Honors Attorney 27 years ago, and since then, she has handled complex environmental civil litigation, which often involves substantial discovery and preservation obligations.

Neeli Ben-David is the Deputy Chief, Health Care Fraud Coordinator, and eDiscovery Coordinator for the Civil Division of the U.S. Attorney's Office for the Northern District of Georgia. She began serving as an Assistant U.S. Attorney in 2004, during which time she has both defended the United States in litigation and represented the United States in fraud investigations and *qui tam* actions under the False Claims Act.

Smart Collection When Using a Search Warrant to Seize Voluminous Electronic Evidence: Have a Strategy and a Plan

Larry J. Wszalek
Chief
Tax Divison

If you are a federal prosecutor, collecting large volumes of electronic evidence is a fact of life. It cannot be avoided, but you need to have a strategy and a plan that puts you in control instead of the evidence controlling you.

In the vast majority of cases, the forensic analysis of a hard drive (or other digital device) takes too long to perform during the execution of a search warrant. Agents typically remove storage media for off-site analysis to determine if the information falls within the scope of the warrant. So too, the Stored Communications Act (SCA) permits investigators to obtain "the contents of any wire or electronic communication . . . held or maintained" by a provider of remote computing services as long as the warrant comports with the Federal Rules of Criminal Procedure.[1] Federal Rule of Criminal Procedure 41(e)(2)(B) permits over-collection as part of a two-step process generally referred to as "seizure first, search second."[2]

> **(B) Warrant Seeking Electronically Stored Information.** A warrant under Rule 41(e)(2)(A) may authorize the seizure of electronic storage media or the seizure or copying of electronically stored information. Unless otherwise specified, the warrant authorizes a later review of the media or information consistent with the warrant. The time for executing the warrant in Rule 41(e)(2)(A) and (f)(1)(A) refers to the seizure or on-site copying of the media or information, and not to any later off-site copying or review.

Courts have also conceded "that over-seizing is an inherent part of the electronic search process and proceed on the assumption that,

---

[1] 18 U.S.C. § 2703(b).
[2] *See e.g.,* United States v. Flores, 802 F.3d 1028 (9th Cir. 2015); United States v. Evers, 669 F.3d 645 (6th Cir. 2012).

when it comes to the seizure of electronic records, this will be far more common than in the days of paper records."[3] Given the enormous amount of data that computers can store and the infinite places within a computer that electronic evidence might be located, the Fourth Amendment's "reasonableness" analysis focuses less on "what" a particular warrant permitted the government agents to search (for example, a computer or a hard drive) and more on "how" the agents carried out the search.[4] Thus, the law justifies the over-collection of ESI.

Courts have wrestled with finding the right balance, however, between law enforcement's interest in collecting relevant evidence in a criminal investigation and the privacy interests implicated in the over-collection of ESI. The government's seizure and retention of ESI gives it "possession of a vast trove of personal information about the person to whom the drive belongs, much of which may be entirely irrelevant to the criminal investigation that led to the seizure."[5] For prosecutors, collecting voluminous ESI can feel overwhelming. It is also fraught with legal hazards compounded by the uneven development of case law in this area. Below are tips to help prosecutors navigate the ESI minefields around search warrants.

A. Avoid facially overbroad warrants

A prosecutor should not endorse a poorly drafted search warrant. The best practice is for an affiant to include in the warrant or by attachment (1) a sufficiently particular description of what is to be

---

[3] United States v. Comprehensive Drug Testing, Inc. 621 F.3d 1162, 1177 (9th Cir. 2010).

[4] United States v. Loera, 923 F.3d 907, 916–17 (10th Cir. 2019); *see also Evers*, 669 F.3d at 652 ("The federal courts are in agreement that a warrant authorizing the seizure of a defendant's home computer equipment and digital media for a subsequent off-site electronic search is not unreasonable or overbroad, as long as the probable-cause showing in the warrant application and affidavit demonstrate a 'sufficient chance of finding some needles in the computer haystack.'" (quoting United States v. Upham, 168 F.3d 532, 535 (1st Cir. 1999))).

[5] United States v. Ganias, 824 F.3d 199, 217 (2d Cir. 2016).

seized and incorporate the affidavit;[6] (2) a list of the charged crimes;[7] (3) a description of the digital device to be searched; (4) a designation tying the information to be seized to the specified crimes;[8] and (5) a temporal limitation on the information to be seized.[9] Attention to these details will help avoid a facially defective warrant.

B. Monitor the pace of review

A prosecutor should insist that the seizing agency establish a scope-of-review protocol to ensure timely compliance with the Fourth Amendment's reasonableness requirements. Some U.S. Attorney's Offices (USAOs) have self-imposed deadlines, such as 120 days or 18 days (with the possibility of extensions) to complete this in-scope analysis. If so, the deadline may be included in the search warrant or warrant affidavit.

> B. During its review of the information received from Provider under this warrant, law enforcement will segregate the information into two groups: (i) information that is responsive to the warrant and that the government may therefore seize; and (ii) information that is not responsive to the warrant. This review will be performed within a reasonable amount of time not to exceed 180 days from the date of execution of the warrant. If the government needs additional time to conduct this review, it may seek an extension of the time period from the Court.

Search warrants without self-imposed deadlines are subject to the Fourth Amendment's "reasonableness" requirement.[10] There is no established upper limit as to when the government must complete its in-scope review of ESI. Several variables, including the storage capacity of the media, encryption or electronic booby traps, and

---

[6] *See* United States v. McGrew, 122 F.3d 847, 850 (9th Cir. 1997); United States v. Dale, 991 F.2d 819, 848 (D. D.C. 1993).
[7] *See In re* 650 Fifth Avenue & Related Properties, 830 F.3d 66, 99 (2d Cir. 2016).
[8] *See* United States v. Christie, 717 F.3d 1156, 1165 (10th Cir. 2013).
[9] *See* United States v. Wey, 256 F. Supp.3d 355 (S.D.N.Y. 2017); *In re* [REDACTED] @gmail.com, 62 F.Supp.3d 1100, 1104 (N.D. Cal. 2014).
[10] United States v. Ganias, 755 F.3d 125, 136 (2d Cir. 2014).

computer-lab workload influence the duration of a forensic analysis.[11] Courts conduct a "case-by-case factual analysis because what may be appropriate under one set of facts and circumstances may not be so under another."[12]

C. Be prepared to defend the review protocol in court

Because the law sanctions collecting entire ESI storage devices, which means seizing large volumes of ESI, courts have trained their attention on "how" the government searches ESI, specifically evaluating the manner in which ESI is reviewed for reasonableness under the Fourth Amendment.[13] There are no definitive procedural rules or laws governing the review of ESI. Rather, Rule 41 delegates search execution details to judicial regulation.[14] Prosecutors should, however, take steps to safeguard against general searches in violation of the Fourth Amendment.

Two basic themes govern. First, where possible, prosecutors should help develop a sound search protocol before seizing ESI by way of the search warrant. Courts are understandably critical when large volumes of ESI are collected and no review is done.[15]

---

[11] *See* FED. R. CRIM. P. 41(e)(2)(B) advisory committee notes to 2009 amendments.

[12] United States v. Metter, 860 F. Supp. 2d 205, 212, 215 (E.D.N.Y. 2012) (government's more than 15-month "retention of all imaged electronic documents, including personal emails, without any review whatsoever to determine not only their relevance to this case, but also to determine whether any recognized legal privileges attached to them, is unreasonable and disturbing"). *But see* United States v. Jarman, 847 F.3d 259, 267 (5th Cir. 2017) (upholding 23-month long review of electronic evidence); United States v. Mendlowitz, No. 17-CR-248, 2019 WL 1017533, at *12 (S.D.N.Y., Mar. 2, 2019) (upholding 18-month long review of electronic evidence).

[13] *See* United States v. Loera, 923 F.3d 907, 917 (10th Cir. 2019) (Fourth Amendment analysis focuses primarily on "how" the agents carried out the search of ESI.).

[14] *See* FED. R. CRIM. P. 41 advisory committee notes to 2009 amendment.

[15] *See, e.g.*, *Metter*, 860 F. Supp. 2d at 215 ("The parties have not provided the Court with any authority, nor has the Court found any, indicating that the government may seize and image electronic data and then retain that data with no plans whatsoever to *begin* review of the data to determine whether any irrelevant, personal information was improperly seized. The

Second, prosecutors should ensure that the search protocol is reasonably executed. Ideally, law enforcement agents will timely complete their review of ESI for information responsive to the warrant's Attachment B description of items to be seized and separate the in-scope ESI from the out-of-scope information. This timely review minimizes the risk of "a general, exploratory rummaging in a person's belongings."[16] Courts frown on long-term, rolling review of ESI that continually expands the search terms to include out-of-scope materials made relevant only by the intervening investigation.[17]

That said, there may be situations in which a rolling review of ESI is justified. For example, agents executing a warrant may gain a better understanding of the illegal conduct at issue in the warrant and additional targeted searches are a reasonable method for locating additional documents responsive to the warrant.[18] This is so, especially in the context of email search warrants, because the names on the accounts are generally not indicative of the actual user, and additional sweeps through the original data are required to determine if the ESI should be reclassified as "responsive" or "non-responsive."[19] Prosecutors should ensure that a rolling review of ESI does not stray into out-of-scope ESI. Other protocol considerations include the following measures.

---

government's blatant disregard for its responsibility in this case is unacceptable and unreasonable.").

[16] Coolidge v. New Hampshire, 403 U.S. 443, 467 (1971).

[17] *See, e.g.,* United States v. Wey, 256 F. Supp.3d 355, 375 (S.D.N.Y. 2017) (new search terms and names added 15 months after execution of the warrant based on information gleaned from search warrant evidence itself were not in the original "Items to be Seized" and were unknown to the affiant making later searches "unreasonable").

[18] *See* United States v. Lustyik, No. 2:12-cr-645-TC, 2014 WL 1494019, at *5 (D. Utah Apr. 16, 2014) (citing United States v. Burgess, 576 F.3d 1078, 1091 (10th Cir. 2009) (observing that the process of developing in-scope search methods is "dynamic").

[19] United States v. Matter of Search of Info. Associated With Fifteen Email Addresses Stored at Premises Owned, No. 2:17-CM-3152-WC, 2017 WL 4322826 (M.D. Ala. Sept. 28, 2017).

1. Search protocol in the warrant or affidavit

Prosecutors should consider whether to include a written search protocol in the warrant or affidavit. Generally, an affiant is not required to include in the search warrant or warrant affidavit a protocol for reviewing ESI.[20]

Some courts have strongly encouraged including a protocol in the warrant or affidavit, however, to help ensure that the seizure of ESI does not exceed the bounds supported by probable cause.[21] Other courts specifically mandate affiants include specific protocols in the search warrant affidavit.[22] Prosecutors should consider including a search protocol in the affidavit to the extent it will help satisfy the Fourth Amendment's requirement that the things to be seized be "particularly describ[ed]."[23] In addition, a prosecutor may want to include protocol details in the warrant to satisfy the court's concerns that investigators will only search for in-scope ESI and, thereafter, seek a secondary search warrant for out-of-scope ESI.[24]

---

[20] *See, e.g.*, United States v. Richards, 659 F.3d 527, 538 (6th Cir. 2011) ("[G]iven the unique problem encountered in computer searches, and the practical difficulties inherent in implementing universal search methodologies, the majority of federal courts have eschewed the use of a specific search protocol and, instead, have employed the Fourth Amendment's bedrock principle of reasonableness on a case-by-case basis."); United States v. Khanani, 502 F.3d 1281, 1290 (11th Cir. 2007) (rejecting argument that "the lack of a written 'search protocol' required the district court to suppress all evidence agents seized as a result of the search of the defendants' computers"); United States v. Brooks, 427 F.3d 1246, 1251 (10th Cir. 2005) ("This court has never required warrants to contain a particularized computer search strategy.").

[21] *See, e.g.,* United States v. Comprehensive Drug Testing, Inc. 621 F.3d 1162, 1179 (9th Cir. 2010) ("[T]he warrant application should normally include, or the issuing judicial officer should insert, a protocol for preventing agents involved in the investigation from examining or retaining any data other than that for which probable cause is shown.").

[22] *See*, Matter of the Search of Black iPhone 4, 27 F.Supp.3d 74, 80 (D. D.C. 2014) ("The government must specify what will occur [with out-of-scope data]—although it is admonished that any response other than 'the information will be returned or, if copies, destroyed' within a prompt period of time will likely find any revised application denied.").

[23] U.S. CONST. AMEND. IV.

[24] *See, e.g.,* United States v. Loera, 923 F.3d 907, 922–23 (10th Cir. 2019) (agent's "second look" at child pornography images on CDs seized by search

2. Retain or return out-of-scope ESI

Prosecutors should devise a protocol for handling out-of-scope ESI. It is not uncommon to return paper documents and digital devices that have been successfully imaged. For example, in *United States v. Manafort*, the court ordered the government to return any paper records that fell outside the warrant and confer with counsel as to whether any digital devices could be returned.[25] As for imaged devices, the court found no constitutional problem with the government's retention of images created during the execution of a search warrant given the need to authenticate exhibits at a later date.[26] Courts have been reluctant to require the deletion of out-of-scope ESI for other reasons, including *Brady* concerns and data corruption.[27]

But some courts will mandate a defined protocol for the return of property before authorizing issuance of the search warrant.[28]

3. Manage out-of-scope, third party ESI

A prosecutor must manage all ESI belonging to third parties unrelated to the criminal investigation. Courts demand adherence to an orderly protocol that protects the privacy interests of unrelated third parties. In *United States v. Comprehensive Drug Testing, Inc.*, the government obtained a search warrant for test results maintained by Comprehensive Drug Testing, Inc., of 10 major league baseball

---

warrant issued for "computer fraud" evidence was unreasonable because it was directed at uncovering evidence of child pornography thereby exceeding the scope of the first warrant); United States v. Nasher-Alneam, 399 F. Supp. 3d 579, 589–90 (S.D. W. Va. 2019) (Second search of ESI obtained by search warrant in Title 21 investigation for health care billing fraud 15 months after records were seized exceeded scope of search warrant.).

[25] 314 F. Supp. 3d 258 (D.D.C. 2018).

[26] *Id.* at. 272.

[27] *See* United States v. Matter of Search of Info. Associated with Fifteen Email Addresses, No. 2:17-CM-3152-WC, 2017 WL 4322826, at *9–*10 (M.D. Ala. Sept. 28, 2017).

[28] *See* Matter of the Search of Black iPhone 4, 27 F. Supp. 3d 74, 80 (D.D.C. 2014) ("The government must specify what will occur [with out-of-scope ESI]—although it is admonished that any response other than 'the information will be returned or, if copies, destroyed' within a prompt period of time will likely find any revised application denied.").

players believed to have tested positive for banned substances.[29] When the warrant was executed, the government seized and reviewed the drug testing records for hundreds of players in Major League Baseball and a great many other people.[30] The Ninth Circuit, sitting en banc, found that, although the government made a strong case for over-collecting ESI when executing the warrant, it ignored search warrant protocol that required computer personnel to screen and segregate responsive data.[31] The protocol also provided for a return of the out-of-scope ESI "within a reasonable period of time not to exceed 60 days from the date of the seizure unless further authorization [was] obtained from the Court."[32] The Ninth Circuit affirmed the lower court's finding that the case agent "demonstrated a callous disregard for the rights of those persons whose records were seized and searched outside the warrant."[33]

4. Potentially privileged information requires special attention

A prosecutor seeking a search warrant to obtain ESI from a lawyer or law firm must design a rigorous search (filter) protocol to protect the sanctity of the attorney–client privilege. Even then, it is not unheard of for a court to replace a government filter team with a special master to accomplish this objective. For example, in *Cohen v. United States*, the court appointed a special master to undertake a filter review of ESI and other materials seized from the office of Michael Cohen, a New York City lawyer, despite a rigorous filter protocol established by the government.[34] At an adversarial proceeding conducted by the district court, the government articulated a filter protocol that included (1) filter agents executing the search warrants rather than investigative agents; (2) forensic teams that immediately imaged digital devices; (3) the creation of a database platform onto which imaged ESI could be placed and shared with counsel within approximately 30 days; (4) the creation and production of separate load files to accommodate counsels' review of ESI; and (5)

---

[29] 621 F.3d 1162 (9th Cir. 2010).
[30] *Id.* at 1166.
[31] *Id.* at 1168.
[32] *Id.* at 1169.
[33] *Id.* at 1169–70.
[34] Order of Appointment, *In re* Search Warrants Executed on April 9, 2018, No. 1:18-mj-03161 (S.D.N.Y. Apr. 13, 2018), ECF No. 30.

a prohibition against the filter team releasing potentially privileged ESI to the investigation team without attorney consent or a court order.[35] The government eventually stipulated to the appointment of a special master to conduct a privilege review.[36] The case illustrates, however, the necessary planning and preparation the government must do in standing up and executing a robust filter protocol when seizing voluminous ESI from a lawyer or law firm.

Recently, in *In re Search Warrant Issued June 13, 2019*, the Fourth Circuit Court of Appeals considered the government's filter protocol for electronic evidence seized from a law firm.[37] Agents conducted a six-hour search of the law firm's offices and "electronically copied and seized the contents of Lawyer *A*'s iPhone and computer."[38] The Fourth Circuit rejected a magistrate-authorized filter protocol that defined members of the filter team to include lawyers and administrative staff from the USAO, as well as agents from the Internal Revenue Service and forensic examiners:

> [T]he magistrate judge erred in assigning judicial functions to the Filter Team, approving the Filter Team and its Protocol in *ex parte* proceedings without first ascertaining what had been seized in the Law Firm search, and disregarding the foundational principles that serve to protect attorney–client relationships. In these circumstances, we are satisfied that the magistrate judge (or an appointed special master)—rather than the Filter Team—must perform the privilege review of the seized materials.[39]

While the Fourth Circuit's holding in *In re Search Warrant Issued June 13, 2019* was based on facts specific to that case, all prosecutors must be cognizant of department policy related to searching the premises, electronic storage devices, and

---

[35] Letter, *In re* Search Warrants Executed on April 9, 2019, No. 1:18-mj-03161 (S.D.N.Y. Apr. 13, 2018), ECF No. 16; Transcript, *In re* Search Warrants Executed on April 9, 2019, No. 1:18-mj-03161 (S.D.N.Y. Apr. 13, 2018), ECF No. 104.
[36] Letter, *In re* Search Warrants Executed on April 9, 2018, No. 1:18-mj-03161 (S.D.N.Y. April 13, 2018), ECF No. 28.
[37] 942 F.3d 159 (4th Cir. 2019).
[38] *Id.* at 166.
[39] *Id.* at 181.

emails of an attorney. First, a prosecutor must consult with the Policy and Statutory Enforcement Unit (PSEU) in the Office of Enforcement Operations (OEO) before seeking judicial authorization for the search warrant. PSEU offers a template of instructions regarding (1) filter team membership; (2) procedures for the search of a physical location; and (3) procedures related to the filter team.[40] Second, the prosecution team and the filter team should consult with their Professional Responsibilities Officer (PRO) and the Professional Responsibility Advisory Office (PRAO) on issues related to professional responsibility. PRAO can provide guidance on circumstances that warrant use of a filter team, the creation and adequacy of a filter team, and alternatives and complements to a filter team, such as a magistrate judge or special master. It can also provide guidance on the use of new matter teams when circumstances may require contact with a represented party.

Prosecutors who are overseeing search warrant applications for evidence from an attorney must be aware of both their local procedures and practices as well as Department policy and recognize that some courts may view privilege determinations solely as a judicial function that cannot be delegated to an executive branch filter team. Consultation and authorization from local supervisors and department agencies, including PSEU and PRAO, is crucial for ensuring full compliance with legal and ethical obligations when conducting searches of locations and items that belong to an attorney.

D. Conclusion

There is no silver bullet or magic pill that will singularly cure all ills associated with the lawful collection of voluminous ESI in a criminal investigation and prosecution. Collecting large volumes of ESI is a fact of life, and it is here to stay. Prosecutors must learn to manage the complexities of handling voluminous ESI by (1) devising and coordinating sound strategies at the front end of an investigation; (2) endorsing well-drafted search warrants that comport with the dictates of the Fourth Amendment and protections afforded common law privileges; and (3) ensuring the search protocol is reasonably executed to collect only in-scope, non-privileged ESI in a timely and reliable

[40] *See* JUSTICE MANUAL § 9-13.420.

manner. A prosecutor cannot do this alone. It takes a team of professionals working towards a common goal who are organized, well-informed, and committed to advancing the interests of criminal law enforcement while at the same time rigorously adhering to the privacy interests and privileges of those affected by the over-collection of ESI.

About the Author

Larry J. Wszalek is the Chief of the Tax Division's Western Criminal Enforcement Section. He began his career in 1990 as an Assistant U.S. Attorney for the Western District of Wisconsin and joined the Tax Division as a Trial Attorney in 2001. Mr. Wszalek was named section Chief in 2014. He received a Bachelor of Arts degree from the University of Texas (Austin) and a J.D. from the University of Wisconsin (Madison).

Page Intentionally Left Blank

Judges' Treatment of Federal Rules of Evidence 902(13) and 902(14)

Andrew Schupanitz
Trial Attorney, San Francisco Office
Antitrust Division

Jacklin Chou Lem
Assistant Chief, San Francisco Office
Antitrust Division

New Federal Rules of Evidence 902(13)[1] and 902(14)[2] have been regularly used by parties since they came into effect on December 1, 2017. Though there have been few published opinions regarding the new rules, we conclude that they are functioning as intended: Parties are either stipulating to the authenticity of electronic evidence, or courts are accepting certifications under Rules 902(13) and 902(14) in a straightforward manner without protracted challenges or litigation from adversarial parties.

This article analyzes the district court opinions and orders issued in the two years following enactment of the new rules. It begins with a brief overview of the new rules, as well as some preliminary observations regarding the few opinions that have been published. Next, we look at Confrontation Clause challenges to Rule 902(13) certifications in criminal cases, building on the work of a February 2019 article published in this journal by Michael L. Levy and John M. Haried.[3] We also examine how the new rules have been used in

---

[1] FED. R. EVID. 902(13) ("A record generated by an electronic process or system that produces an accurate result, as shown by a certification of a qualified person that complies with the certification requirements of Rule 902(11) or (12). The proponent must also meet the notice requirements of Rule 902(11).").

[2] FED. R. EVID. 902(14) ("Data copied from an electronic device, storage medium, or file, if authenticated by a process of digital identification, as shown by a certification of a qualified person that complies with the certification requirements of Rule 902(11) or (12). The proponent must also meet the notice requirements of Rule 902(11).").

[3] Michael L. Levy & John M. Haried, *Practical Considerations When Using New Evidence Rule 902(13) to Self-Authenticate Electronically Generated*

conjunction with Rule 902(11) (self-authenticating business records)[4] and the business records exception to the rule against hearsay under Rule 803(6),[5] specifically with regard to email evidence. Finally, at the end of this article, we offer an appendix summarizing selected court decisions that may be useful to practitioners seeking authentication of electronic evidence under Rule 902(13) or 902(14).

I. Introduction to the rules

Rules 902(13) and 902(14) provide for the self-authentication of two categories of electronic evidence via certification, rather than through live witness testimony: (1) records generated by an electronic process or system; and (2) data copied from an electronic device, storage medium, or file. Specifically, electronic evidence is self-authenticating under Rule 902(13) where it is certified by a qualified person as "[a] record generated by an electronic process or system that produces an accurate result."[6] Electronic evidence is self-authenticating under Rule 902(14) if it is certified by a qualified person as "[d]ata copied from an electronic device, storage medium, or file, if authenticated by

---

Evidence in Criminal Cases, 67 DOJ J. FED. L. & PRAC., no. 1, 2019, at 81, 88–93; *see also* John M. Haried, *Two New Self-Authentication Rules That Make It Easier to Admit Electronic Evidence*, U.S. ATT'YS BULL., no.1, 2018, at 127, 133–34 n.1.

[4] FED. R. EVID. 902(11) ("The original or a copy of a domestic record that meets the requirements of Rule 803(6)(A)–(C), as shown by a certification of the custodian or another qualified person that complies with a federal statute or a rule prescribed by the Supreme Court. Before the trial or hearing, the proponent must give an adverse party reasonable written notice of the intent to offer the record—and must make the record and certification available for inspection—so that the party has a fair opportunity to challenge them.").

[5] FED. R. EVID. 803(6) ("A record of an act, event, condition, opinion, or diagnosis if: (A) the record was made at or near the time by—or from information transmitted by—someone with knowledge; (B) the record was kept in the course of a regularly conducted activity of a business, organization, occupation, or calling, whether or not for profit; (C) making the record was a regular practice of that activity; (D) all these conditions are shown by the testimony of the custodian or another qualified witness, or by a certification that complies with Rule 902(11) or (12) or with a statute permitting certification; and (E) the opponent does not show that the source of information or the method or circumstances of preparation indicate a lack of trustworthiness.").

[6] FED. R. EVID. 902(13).

a process of digital identification."[7] In the words of the Advisory Committee on the new rules, they were enacted because "the expense and inconvenience of producing a witness to authenticate an item of electronic evidence is often unnecessary."[8]

Before the new rules were implemented, an adversary could hamstring the presentation of electronic evidence by simply refusing to stipulate to its authenticity: "It is often the case that a party goes to the expense of producing an authentication witness, and then the adversary either stipulates to authenticity before the witness is called or fails to challenge the authentication testimony once it is presented."[9] An illustrative example from 2013 involves a case in which the government sought to admit screen captures from the Wayback Machine, an online internet archiving system. The court found the screen captures were not business records under Rule 902(11), and the evidence could only be authenticated by a live witness—in this case, a custodian from archive.org located in San Francisco. The courthouse was in Maryland. After dragging its feet for weeks, the defense stipulated to authenticity just as the archive.org witness was about to depart from San Francisco.[10] New Rules 902(13) and 902(14) save time and money by helping parties avoid this sort of gamesmanship. Instead, the new rules provide litigants with a notice-and-object mechanism that helps resolve authenticity objections well in advance of trial.

The language of Rule 902(13) mirrors that of Rule 901(b)(9), which provides for authenticity to be established by "[e]vidence describing a process or system and showing that it produces an accurate result."[11] Just as Rule 902(11) allows a party to establish the requirements of Rule 803(6)(A)–(C) by certification, Rule 902(13) allows a party to meet the authenticity foundation requirements of Rule 901(b)(9) through a certification, rather than through live testimony.[12]

---

[7] FED. R. EVID. 902(14).

[8] FED. R. EVID. 902(13), 902(14) advisory committee's note to 2017 amendment.

[9] *Id.*

[10] Haried, *supra* note 3, at 127; *cf.* Tompkins v. 23andMe, Inc., 2014 WL 2903752, at *1 n.1 (N.D. Cal. June 25, 2014) (taking judicial notice of an Archive.org version of 23andMe's website).

[11] FED. R. EVID. 901(b)(9).

[12] FED. R. EVID. 902(13) advisory committee's note to 2017 amendment ("The Rule specifically allows the authenticity foundation that satisfies Rule

Rule 902(14) does not require a certification that the process or system used "produces an accurate result," and as such, it is even more straightforward. Many types of electronic evidence offered at trial are a forensic copies of the original—for example, texts copied from a defendant's cell phone or emails produced from a company's server. Rule 902(14) allows parties to quickly establish authenticity by verifying that the copy matches the original according to commonly accepted standards. This is ordinarily done using "hash values."[13] A hash value is a unique hexadecimal identifier that is algorithmically determined based on the contents and characteristics of the electronic file or drive. Even small changes in a file or drive will change the hash value, so a certification that the hash value for the copy is identical to that of the original reliably demonstrates that they are identical. Though comparing hash values is standard practice today, the language of the rule is broad enough to accommodate other methods of verification—both now and in response to new technologies that may be developed in the future.[14]

II. Few adversary challenges?

Despite the fact that Rules 902(13) and 902(14) have been in effect for over two years, and parties started making use of their provisions even before December 2017,[15] courts have issued only a handful of published opinions regarding the new rules. One could take this as evidence that Rules 902(13) and 902(14) have not been widely used by litigants. But electronic evidence is ubiquitous, and it would be

---

901(b)(9) to be established by a certification rather than the testimony of a live witness.").

[13] *See* FED. R. EVID. 902(14), advisory committee's note to 2017 amendment ("This amendment allows self-authentication by a certification of a qualified person that she checked the hash value of the proffered item and that it was identical to the original.").

[14] *Id.* ("The rule is flexible enough to allow certifications through processes other than comparison of hash value, including by other reliable means of identification provided by future technology.").

[15] In one case, the court even allowed authentication via a Rule 902(13) certification for a trial that concluded before December 1, 2017. *See* United States v. Adams, No. 15-cr-00580, 2019 U.S. Dist. LEXIS 9558, at *35–*36 (E.D. Pa. Jan. 16, 2019) (overruling defendant's argument that the court abused its discretion in allowing Rule 902(13) authentication in a trial that concluded before Rule 902(13) took effect).

unusual for parties not to take advantage of rules that would save them both time and money. Moreover, even a cursory search on legal databases like Lexis or Westlaw turn up hundreds of filings citing to the new rules. Parties appear to be using the new rules, even if opinions interpreting them are few and far between.

A sounder interpretation of this paucity of opinions is that the rules are functioning exactly as intended: Adversaries are either stipulating to the authenticity of electronic evidence, or courts are accepting certifications under Rules 902(13) and 902(14) in a straightforward manner without challenges or protracted litigation. By removing the requirement of a live authentication witness for vast categories of electronic evidence—as well as the leverage that such a requirement conferred on opposing parties—the new rules have shifted the balance of power between parties on issues of authentication. They have eliminated the incentives for an opposing party to raise purely formal objections to authenticity or to refuse a stipulation.[16] In short, the results suggest that Rules 902(13) and 902(14) have discouraged the type of gamesmanship highlighted by the Advisory Committee before their enactment[17] and that less time and fewer resources are being spent authenticating electronic evidence. To take just one example, screen captures of the Wayback Machine—the same evidence cited above to illustrate the gamesmanship of defendants and the hassle of arranging for authentication witness testimony before the enactment of the new rules[18]—are self-authenticating under Rule 902(13).[19]

---

[16] An illustrative example of the newfound leverage held by parties seeking authentication under the new rules can be found in *United States v. Shafi*. Before trial, the government proposed stipulations on the authenticity of a number of categories of electronic evidence, which the defendant refused. Prosecutors filed a motion in limine seeking not to authenticate the evidence, but merely to inform the court that it *would* seek authentication under Rule 902 if the defendant continued to refuse a stipulation: "To the extent that the defendant continues to decline any stipulations for authentication purposes, the United States moves in limine to apprise the Court that it may authenticate its exhibits pursuant to Federal Rule of Evidence 902." United States' Motions in Limine at 7, United States v. Shafi, 252 F. Supp. 3d 787 (N.D. Cal. 2018) (No. 15-cr-00582-WHO-1), ECF No. 225.

[17] *See* note 9, *supra*.

[18] *See* note 3, *supra*.

[19] *See* United States v. Bondars, No. 1:16-cr-228, 2018 WL 9755074, at *2 (E.D. Va. Aug. 20, 2018).

Additionally, even where adversaries have disputed self-authentication under the new rules, their objections have, in many cases, already been explicitly dispensed with by the Advisory Committee, thus allowing courts to quickly and easily overrule them. In *United States v. Adams* for example, the defendant argued in a motion for a new trial that the court had improperly admitted evidence under Rules 801 and 902(13) because the certification failed to comply with "the certification requirements of Rule 902(11) or (12),"[20] as required by the text of Rule 902(13).[21] The defendant's argument, in other words, was that Rule 902(13) requires self-authenticating evidence to be certified as generated by an electronic process or system that produces an accurate result *and also* as a business record that meets the requirements of Rule 803(6)(A)–(C). As the *Adams* court pointed out, the defendant's argument ignored the explicit instructions of the Advisory Committee Notes to the rule: "The reference to the 'certification requirements of Rule 902(11) or (12)' is only to the procedural requirements for a valid certification. There is no intent to require, or permit, a certification under this Rule to prove the requirements of Rule 803(6)."[22]

Even ignoring the Advisory Committee's clear instructions, the defendant's argument in *Adams* is illogical on its face since it would render Rule 902(13) entirely pointless—a rerun of Rule 902(11) but

---

[20] FED. R. EVID. 902(13).

[21] United States v. Adams, No. 15-cr-00580-JLS, 2019 U.S. Dist. LEXIS 9558, at *35 (E.D. Pa. Jan. 16, 2019).

[22] FED. R. EVID. 902(13), advisory committee's note to 2017 amendment. *See Adams*, 2019 U.S. Dist. LEXIS 9558, at *40. This is certainly not the only example of a defendant attempting to transform the Rule 902(11) certification requirements referenced in Rules 902(13) and 902(14) into a requirement that the certification comply with the substantive terms of the business record exception to the hearsay rule under Rule 803(6). *See, e.g.*, Defendant's Motion to Suppress at 2, United States v. Stone, No. 1:19-CR-00018-ABJ, 2020 WL 1892360 (D.D.C. April 16, 2020), ECF No. 100 ("Federal Rule of Evidence 902(14) permits authentication through a 'process of digital identification by a qualified person' as long as it complies with Rule 902(11). That Rule requires compliance with the business records exception of hearsay."); *cf.* FED. R. EVID. 902(14) advisory committee's note to 2017 amendment ("There is no intent to require, or permit, a certification under this Rule to prove the requirements of Rule 803(6). Rule 902(14) is solely limited to authentication, and any attempt to satisfy a hearsay exception must be made independently.").

with the burden of an additional certification requirement. This argument contradicts the intent of the new rules to make authenticating electronic evidence faster, easier, and more flexible. A similar example can be found in a recent civil opinion, *Rosado-Mangual v. Xerox Corp.*[23] There, Xerox moved for summary judgment.[24] The plaintiffs objected to Xerox's use of a number of exhibits, including a record of trainings by one of the plaintiffs.[25] Though this plaintiff admitted the document was his training record during a deposition, the plaintiffs claimed that Xerox failed to properly authenticate the document as a record created by computer software under Rule 901(b)(9) or 903(13).[26] In overruling the plaintiffs' objection, the court first observed that a computer printout of a training record is "not the result of a process or system used to produce a result, but merely printouts of preexisting records that happened to be stored on a computer."[27] More importantly, the document had already been properly authenticated by a qualified witness during a deposition.[28] Even if authenticating the document under Rule 902(13) was appropriate, the court noted, "[A]s stated in the 2017 Advisory Committee Notes to Fed. R. Evid. 902(13), nothing in the rules was intended to limit a party from establishing the authentication of electronic evidence on any ground provided in the Rules of Evidence."[29]

Rules 902(13) and (14) were intended to make authentication easier and expand options for presenting self-authenticating evidence. We can infer from cases like *Adams* and *Rosado-Mangual* that courts will accordingly reject attempts to artificially constrain or narrow the means of authenticating electronic evidence offered by the new

---

[23] Rosado-Mangual v. Xerox Corp., No. 15-CV-3035-PAD, 2019 WL 7247776, at *28–*29 (D.P.R. Dec. 27, 2019).
[24] *Id.* at *1.
[25] *Id.* at *29.
[26] *Id.*
[27] *Id.* (quoting United States v. Meienberg, 263 F.3d 1177, 1181 (10th Cir. 2001)).
[28] *Id.*
[29] *Id.*; *see also* FED. R. EVID. 902(13) advisory committee's note to 2017 amendment ("Nothing in the amendment is intended to limit a party from establishing authenticity of electronic evidence on any ground provided in these Rules, including through judicial notice where appropriate.").

rules—particularly where such attempts directly contradict the intent and express instructions of the Advisory Committee.

III. Confrontation Clause challenges in criminal cases

Another area where defendants have sought—unsuccessfully— to challenge authentication under Rules 902(13) and (14) is by arguing that reliance on a certification violates the Confrontation Clause under *Crawford v. Washington*.[30] The Sixth Amendment states that "in all criminal prosecutions, the accused shall enjoy the right . . . to be confronted with the witnesses against him."[31] Generally, that right is exercised by cross-examining witnesses who offer testimonial evidence against a defendant. To frame the Confrontation Clause analysis with respect to authenticity certifications, it is helpful to understand the Supreme Court's decisions in *Melendez-Dias v. Massachusetts* and *Bullcoming v. New Mexico*.[32]

In *Melendez-Diaz v. Massachusetts*,[33] the trial court admitted a lab report attesting that evidence seized from the defendant contained cocaine. The Supreme Court held that the trial court's admission of the lab report violated the Confrontation Clause and that it should have required the lab analyst to testify about the presence of the drug in person.[34] In so ruling, the Court acknowledged a narrow exception to the Confrontation Clause regarding documents that are prepared for use at trial: "A clerk could by affidavit *authenticate* or provide a copy of an otherwise admissible record, but could not do what the analysts did here: *create* a record for the sole purpose of providing evidence against a defendant."[35] A clerk can certify the correctness of a copy of a preexisting record, and such a certification would not present any issues under *Crawford* if presented to the jury. But where a clerk attempts "to furnish, as evidence for the trial of a lawsuit, his

---

[30] 541 U.S. 36 (2004).

[31] U.S. CONST. amend. VI.

[32] For a useful overview of Confrontation Clause issues under *Melendez-Diaz* and the new rules, see Hon. Paul W. Grimm et al., *Authenticating Digital Evidence*, 69 BAYLOR L. REV. 1, 38–53 (2017).

[33] 557 U.S. 305 (2009).

[34] *Id.* at 357.

[35] *Id.* at 322–23 (emphasis in original).

interpretation of what the record contains or shows, or to *certify to its substance or effect*,"[36] the certificate violates the Confrontation Clause.

The Supreme Court's subsequent decision in *Bullcoming v. New Mexico*[37] helps to further illustrate the difference between constitutionally permissible authentication of a machine-produced result and assertions that interpret or explain those results in violation of the Confrontation Clause. In *Bullcoming*, the government offered the certificate of a lab analyst who performed a gas chromatography test through the testimony of a second analyst who was familiar with the testing procedure but did not sign the certificate and had no knowledge of the specific test that had been performed and certified in that case.[38] Rejecting the argument that the analyst who performed the test and signed the certificate was merely transcribing machine-generated results, the Court noted that the certificate included statements that the sample seals were intact and broken in the lab and that the testing followed procedures set by the lab.[39] Like the analyst's statement in *Melendez-Diaz* that the machine-generated results of lab testing indicated the presence of cocaine, the analyst's statements in *Bullcoming* that the testing had followed set procedures and the sample was unaltered went beyond authenticating a machine-generated result.[40]

As noted by Levy and Haried, courts following the reasoning of this "*Melendez-Diaz* carve-out" have regularly held that offering a business record certification from the record custodian does not violate the Confrontation Clause.[41] Their February 2019 article predicted that the *Melendez-Diaz* carve-out would easily resolve any Confrontation Clause challenges to Rule 902(14). They also explained how Rule 902(13)'s language regarding a "process or system that produces an accurate result"[42] could present Confrontation Clause pitfalls,

---

[36] *Id.* at 322 (emphasis added).
[37] 564 U.S. 647 (2011).
[38] *Id.* at 657.
[39] *Id.* at 653.
[40] *See* Levy & Haried, *supra* note 3, at 91 ("In *Melendez-Diaz* and in *Bullcoming*, the certificates contained assertions that interpreted, explained, or added context to machine-generated facts. The problematic assertions were the statements of the witnesses about their activities and interpretations of machine-generated information.").
[41] *Id.* at 89 n.37 (gathering cases).
[42] FED. R. EVID. 902(13).

particularly where the certification is overly detailed: "It is not the amount of detail showing authenticity that is the problem. Rather, the risk is that a prosecutor drafts an out-of-court statement that goes beyond authentication and attempts to interpret or explain the machine-generated record."[43] The surest way to avoid interpreting or explaining in a Rule 902(13) certification—and thus minimize potential Confrontation Clause challenges—is to track the language of the rule.[44]

Two published cases have addressed Confrontation Clause issues with Rule 902(13) certifications. In both cases, the courts found no issue with the certifications. In *United States v. Forty-Febres*,[45] the defendants were charged with two counts of carjacking under 18 U.S.C. § 2119. To prove the "interstate nexus" of the stolen vehicles, the government sought the admission of vehicle registration records from the Puerto Rico Department of Transportation's (DOTP) electronic database.[46] The registration records were accompanied by a Rule 902(11) certification signed by a DOTP employee, and the government sought to admit them as self-authenticating business records.[47] In the alternative, the government argued that the records were self-authenticating under Rule 902(13) because the certification noted that they were generated from the DOTP's electronic database (the David Plus System).[48] Citing *Melendez-Diaz*, the court found that the registration records were properly certified as authentic copies of domestic records under Rule 902(11) and as copies of an accurate search result of an electronic database under Rule 902(13)[49] and presented no Confrontation Clause issues.[50] Similarly, in

---

[43] Levy & Haried, *supra* note 3, at 92.

[44] *Id.* at 91 ("When the certification simply tracks the language of the rule (the 'process or system that produces an accurate result'), there should not be a Confrontation Clause problem when offering the certificate to the jury.").

[45] No. 16-330 (ADC), 2018 WL 2182653 (D.P.R. May 11, 2018).

[46] *Id.* at *2.

[47] *Id.*

[48] *Id.*

[49] *Id.*

[50] *Id.* at *2–*3. The defendant in *Forty-Febres* did not challenge the certification on Confrontation Clause grounds. Instead, he argued that the use of the registration records to prove an element of the carjacking charges required the presence of a sponsoring witness to testify to the interstate nexus—an argument for which the court found "no support." *Id.* at *3.

United States v. Adams,[51] the defendant argued in his motion for a new trial that the court erred in accepting the government's Rule 902(13) certification, depriving him of an opportunity to confront a qualifying witness.[52] The court found no issue under *Crawford* and rejected the Confrontation Clause challenge.[53]

Although a Confrontation Clause challenge under Rule 902(13) is a "new" issue given the relative newness of the rule itself, courts have confronted Confrontation Clause challenges under Rule 902 more broadly for years, and district and appellate courts have "uniformly" found under *Melendez-Diaz* that Rule 902(11) and (12) certifications do not violate the right to confrontation.[54] There is no reason for courts to treat certifications under the new rules any differently. The cool reception and brief treatment of Confrontation Clauses challenges in *Forty-Febres* and *Adams* suggests a similar approach to Rule 902(13); going forward, we can expect judicial skepticism with respect to Confrontation Clause challenges to Rules 902(13) and 902(14). Indeed, the Advisory Committee on Evidence Rules explicitly considered and rejected the possibility of Confrontation Clause issues arising from certifications under the new rules:

> The Committee was satisfied that there would be no constitutional issue, because the Supreme Court has stated in *Melendez-Diaz v. Massachusetts* that even when a certificate is prepared for litigation, the admission of that certificate is consistent with the right to confrontation if it does nothing more than authenticate another document or item of evidence. That is all that these certificates would be doing under the Rule 902(13) and (14) proposals.[55]

Given the scant number of opinions addressing Confrontation Clause challenges under Rule 902(13) and the seeming ease with which such challenges were overruled in *Forty-Febres* and *Adams*, it seems that

---

[51] No. 15-cr-00580-JLS, 2019 U.S. Dist. LEXIS 9558 (E.D. Pa. Jan. 16, 2019).
[52] *Id.* at *24.
[53] It should be noted that both *Melendez-Diaz* and *Adams* are on appeal to their respective circuit courts.
[54] Meeting Minutes, Jud. Conf. Advisory Comm. on the Fed. Rules of Evidence, at 8–9 (Apr. 17, 2015), https://www.uscourts.gov/sites/default/files/2015-04-evidence-minutes_0.pdf.
[55] *Id.* at 8.

both courts and (most) defendants are following the Advisory Committee's prediction.[56]

IV. Interaction with Rules 902(11) and 803(6): the email challenge

The cases and filings addressing Rules 902(13) and 902(14) reveal one striking trend above all others: a tendency by parties seeking authentication under the new rules to combine certifications under Rule 902(13) or (14) with a certification of business records under Rule 902(11). An illustrative example comes from *United States v. Razo-Quiroz*,[57] where the government sought the pretrial authentication of a number of categories of evidence certified by seven different custodians.[58] A number of the certifications offered by the government attested to authenticity under both Rule 902(11) and Rule 902(13). AT&T call records, for example, were certified in the following way:

> a. All records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of AT&T, and they were made by AT&T as a regular practice; and

---

[56] For practitioners encountering Confrontation Clause challenges to Rules 902(13) and 902(14) certifications and looking for useful citations and caselaw, see Government's Motion in Limine to Authenticate Records Pursuant to the Self-Authentication Provisions of Federal Rules of Evidence 902(11), 902(13), and 902(14), United States v. Aloba, No. CR 18-0083(B)-RGK (C.D. Cal. July 2, 2019), ECF No. 94.

[57] No. 1:19-cr-00015-DAD-BAM, 2019 WL 3035556, at *13 (E.D. Cal. July 11, 2019). The case is currently on appeal to the Ninth Circuit.

[58] The court offered no findings on the self-authentication of the various categories of evidence in its opinion, but merely instructed the parties to meet and confer, encouraging them "to reach agreement so as to avoid the unnecessary appearance of custodian of records witnesses at trial where there is no legitimate dispute as to the authenticity and admissibility of records." *Id.* at 13 n.17.

b. Such records were generated by AT&T's electronic process or system that produces an accurate result, to wit:

1. The records were copied from electronic device(s), storage medium(s), or file(s) in the custody of AT&T in a manner to ensure that they are true duplicates of the original records; and

2. The process or system is regularly verified by AT&T, and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.[59]

A Rule 902(11) certification, in addition to attesting to the authenticity of the evidence, qualifies it for admission as a business record and an exception to the rule against hearsay.[60] Because the relevant provisions of Rules 803(6) and 902(11) are virtually identical, a certification that satisfies the terms of Rule 902(11) will also satisfy the terms of the hearsay exception under Rule 803(6). In the words of one court, determining authenticity and admissibility under the two rules "go hand in hand."[61] One necessarily implies the other. By contrast, Rules 902(13) and (14) offer no such path around the hearsay

---

[59] Notice of Motion and Motion for Pretrial Hearing to Authenticate Recordings, Phone Extractions, Facebook Material and Transcripts and Notice of Intent to Offer Certified Domestic Records of Regularly Conducted Business Activity and Request for Order Authorizing Admissibility, Ex. A at 6, United States v. Razo-Quiroz, No. 1:19-cr-00015-DAD-BAM (E.D. Cal. April 17, 2019), ECF No. 287.

[60] FED. R. EVID. 803(6).

[61] United States v. Kahre, 610 F. Supp. 2d 1261, 1263 (D. Nev. 2009) (citing 5 Federal Evidence § 9:40 (3d ed.)); *see also* In re Vee Vinhnee, 336 B.R. 437, 444 (B.A.P. 9th Cir. 2005) ("Ordinarily, because the business record foundation commonly covers the [authenticity] ground, the authenticity analysis is merged into the business record analysis without formal focus on the question."); Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 572 (D. Md. May 4, 2007) ("Because the elements for both rules are essentially identical, they frequently are analyzed together when Rule 902(11) is the proffered means by which a party seek to admit a business record.").

rule, and the Advisory Committee Notes to the rules explicitly disclaim one: "Rule 902(13) is solely limited to authentication, and any attempt to satisfy a hearsay exception must be made independently . . . . The opponent remains free to object to admissibility of the proffered item on other grounds—including hearsay."[62]

One category of electronic evidence for which a dual 902(11) and 902(13) certification strategy may offer real advantages is emails, text messages, and other forms of electronic communications.[63] This strategy may be particularly useful if the evidence at issue contains a mixture of data generated from machines or other business-like processes (such as date and time stamps and logs of activity) and user-generated content like the body of an email or text message. As discussed below, even if a court is inclined to reject user-generated content as a business record, a practitioner may consider authenticating an email or text by arguing that parts of the email are business records under 902(11) and other parts, such as the words or symbols appearing in the record, are the product of a system or process under 902(13) that produces an accurate result of the users' input into the communication system.

Courts have sometimes been skeptical of treating emails as business records. The Ninth Circuit, for example, has held that email is not the sort of "systematic business activity" contemplated by Rule 803(6).[64] As a result, courts confronted with Rule 902(11) certifications for email evidence or other forms of electronic messaging have encountered substantially more difficulty with the "hand in hand" analysis under Rules 902(11) and 803(6). Courts have resolved the issue in a variety of ways: (1) simply accepting the certification under Rule 902(11) and finding the emails and their substantive content

---

[62] FED. R. EVID. 902(13) advisory committee's note to 2017 amendment.

[63] This would also include things like Facebook Messenger and other application-based chats, but we use "email" throughout this section for simplicity.

[64] Monotype Corp. PLC v. Int'l Typeface Corp., 43 F.3d 443, 450 (9th Cir. 1994) (finding that emails did not qualify as business records under Rule 803(6) because email "is far less of a systematic business activity than a monthly inventory printout. E-mail is an ongoing electronic message and retrieval system whereas an electronic inventory recording system is a regular, systematic function of a bookkeeper prepared in the course of business.").

authentic and admissible as business records under Rule 803(6); (2) finding the emails authentic and admissible only as to the limited facts that emails were exchanged by particular accounts at particular times on particular dates—essentially limiting admission to the email header and metadata—but requiring additional evidence to authenticate and admit the underlying substantive content; or (3) rejecting the Rule 902(11) certification altogether.

An example of the first approach can be found in *United States v. Way*.[65] In *Way*, the government filed a notice of intent to admit email evidence from several Google, Yahoo, and Hotmail accounts as business records under Rules 803(6), 902(11), and 902(13).[66] The court found the certifications submitted by the companies adequate to authenticate the emails under 902(11) and qualify them for admission under the business record exception of Rule 803(6).[67] In focusing on the business records certification as sufficient, the court appears to have completely ignored Rule 902(13) as an alternative basis for authentication.

A second approach that courts have taken is to accept the authentication and admissibility of certain limited aspects of the email evidence without finding the substantive *content* admissible as a business record under Rule 803(6). In *United States v. Browne*, for example, the Third Circuit concluded that Facebook chat logs were not records of regularly conducted activity under Rule 803(6), despite a Rule 902(11) certification from Facebook.[68] The court observed that portions of the chat logs could be properly authenticated and admitted as business records, but not their substantive content:

> If the Government here had sought to authenticate only the timestamps on the Facebook chats, the fact that the chats took place between particular Facebook accounts, and similarly technical information verified by Facebook "in the course of a regularly conducted

---

[65] No. 1:14-cr-00101-DAD-BAM-1, 2018 WL 2470944 (E.D. Cal. June 1, 2018).
[66] *Id.* at *1.
[67] *Id.* at *2; *see also* United States v. Gal, 606 F.App'x. 868, 874–75 (9th Cir. 2015) (finding no error in the district court's admission of emails pursuant to Rules 902(11) and 803(6) where the affiant did not certify that the defendant sent the emails, but only that Yahoo made a record of emails as they were sent or received from various addresses).
[68] United States v. Browne, 834 F.3d 403, 433–36 (3d Cir. 2016).

> activity," the records might be more readily analogized to bank records or phone records conventionally authenticated and admitted under Rules 902(11) and 803(6).[69]

Taken as a whole, however, the chat logs were not business records because Facebook did not rely on or verify the substantive content of the chats in the course of its business and had not verified the underlying content of the chat logs. The court reasoned that allowing the government to admit the contents of the chats by way of a Rule 902(11) certification from a third party "would mean that all electronic information whose storage or transmission could be verified by a third-party service provider would be exempt from the hearsay rules—a novel proposition indeed."[70] Similarly, in *United States v. Ayelotan*, the Fifth Circuit found that transmittal data for Google and Yahoo accounts that was accompanied by a Rule 902(11) certification from those companies was admissible under Rule 803(6), but the substantive content of the emails was only admissible under a different exception to the hearsay rule.[71]

A dual certification may be useful in cases where courts take this second approach of distinguishing between transmittal data for emails and the substantive content of the messages. For example, in *United States v. Edwards*, the court granted that Google, Blue Host, and eBay could certify as self-authenticating "only the limited facts that communications generally took place between particular accounts, at particular times, on particular dates" and held that a Rule 902(11) certificate "will not suffice for the government to authenticate any online communication's substantive content."[72] Because the authentication and admissibility of the Rule 902(11) certificate was limited to the transmittal data of the communications, the government would have to independently authenticate and provide a hearsay exclusion or exception to admit the substantive content of the communications.[73]

---

[69] *Id.* at 411.
[70] *Id.*
[71] United States v. Ayelotan, 917 F.3d 394, 402 (5th Cir. 2019).
[72] United States v. Edwards, No 16-20070-01/02-CM, 2019 WL 5196614, at *11 (D. Kan. Oct. 15, 2019).
[73] *Id.*

One can imagine that a number of these substantive communications would be admissible in a criminal case as non-hearsay—for example, as the defendant's own statements under Rule 801(d)(2)(A) or coconspirator statements under Rule 801(d)(2)(E).[74] Unlike a certificate of authenticity under Rule 902(11), the scope of a Rule 902(13) or (14) certificate is not strictly limited to whatever portions of the evidence qualify as a business record under Rule 803(6). A Rule 902(13) certification of the communications in *Edwards* would arguably extend to both the transmittal data of the communications and the underlying substantive content. A dual certification using both Rule 902(11) and Rule 902(13) or (14) would thus allow the government to authenticate and admit both the transmittal data certified under Rule 902(11) and, subject to a hearsay exception or non-hearsay argument, the substantive content of the messages under Rules 902(13) or (14).

A third approach can be found in *United States v. Safavian*.[75] In *Safavian*, the government submitted a Rule 902(11) certification of authenticity covering 467,747 emails produced by the law firm Greenberg Traurig, LLP. The government did not seek the admission of any of the Greenberg Traurig emails under Rule 803(6) and, instead, offered a number of other hearsay exceptions and non-hearsay arguments for their admission. Because the government was not offering the emails as business records under Rule 803(6), the court rejected authentication via the certification: "Because Rule 902(11) was intended as a means of authenticating *only* that evidence which is being offered under the business records exception to the hearsay rule, the Court will not accept the proffered Rule 902(11) certification . . . ."[76]

The new Rules 902(13) and (14) may also be useful in cases where courts take this third approach to Rule 902(11). In *Safavian*, though the court went on to find the contested emails authentic under Rule 901 based on their "distinctive characteristics" and comparison to already-authenticated emails,[77] a dual certification under Rules 902(11) and 902(13) or (14) would have obviated the need to analyze and compare individual emails. Where courts are inclined to follow

---

[74] *See Ayelotan*, 917 F.3d at 402.
[75] 435 F. Supp. 2d 36 (D.D.C. 2006).
[76] *Id.* at 39 (emphasis in original).
[77] *Id.* at 40–41.

Safavian in allowing self-authentication under Rule 902(11) for *only* those emails that are being admitted through Rule 803(6), a dual certification may be particularly useful given the uncertainty of whether an email can qualify as a business record under Rule 803(6).

Given the varying approaches taken by courts to certain categories of evidence under Rule 902(11), practitioners should give careful thought to how the new Rules 902(13) and (14) can be used in tandem with Rule 902(11) to maximize the chances of authenticating and admitting electronic evidence and minimizing uncertainty.

V. Conclusion

New Rules 902(13) and 902(14) were implemented to avoid the time and expense of calling a custodial witness to testify to the authentication of electronic evidence for which there is no dispute as to its authenticity. The handful of published opinions issued since the rules took effect on December 1, 2017, seem to indicate that the rules are working as intended. Challenges to self-authentication under the new rules—whether based on an expansive reading of the Rule 902(11) certification requirements included in the new rules or the Confrontation Clause—have fared poorly. We can infer from this that defendants are either stipulating to authenticity under the new rules, or courts are dispatching with objections in summary form without much in the way of published opinions.

Finally, the trend of dual certifications of electronic evidence, using both Rule 902(11) and Rule 902(13) or (14) to certify authenticity, offers potential advantages to practitioners seeking authentication and admission of email and other electronic communications evidence.

VI. Appendix: relevant cases

This appendix compiles selected cases addressing authentication under 902(13) and 902(14). Generally, the summaries below highlight the kind of evidence sought to be admitted, the identity of the declarant who provided the certification, and the content of the certification itself. The cases are listed in chronological order.

***La Force v. GoSmith, Inc.*, No. 17-cv-05101-YGR, 2017 WL 9938681 (N.D. Cal., Dec. 12, 2017).** In opposition to a motion to compel arbitration, a civil plaintiff argued that he never entered into an arbitration agreement with the defendant company, GoSmith (an online home improvement marketplace). In support of his motion, the plaintiff offered as evidence screenshots of a GoSmith registration

page, which he argued did not require him to agree to any arbitration terms. The district court refused to admit the screenshots. Although the plaintiff offered a declaration from his counsel stating the date, device, and browser used to obtain the screenshots, counsel failed to explain the process used to retrieve the images or to verify that he retrieved them. The court found counsel's declaration to be insufficient to meet the requirements of 902(13).

***United States v. Forty-Febres*,** No. 16-330, 2018 WL 2182653 (D.P.R. May 11, 2018)**.** To prove the interstate nexus element of a carjacking offense under 18 U.S.C. § 2119, the government sought to admit vehicle registration records showing that carjacked vehicles originated from Japan. The district court granted the government's motion in limine, finding that registration records from the Puerto Rico Department of Transportation's (DOT) electronic database were business records under 902(11) and copies of an accurate search result of an electronic database under 902(13). Certifications were made by a DOT investigator who, among other things, stated that the records were original or duplicate copies of original records in the department's electronic vehicle registration database.

***United States v. Nicolescu*, No. 1:16-cr-00224, ECF 60, 70 (N.D. Ohio, May 31, 2018).** The district court granted the government's motion in limine to admit records from service providers such as Google, Yahoo, and Facebook based on 902(11) and 902(13) certifications. A certification under 902(13) by a Google records custodian stated that documents produced in response to a search warrant were true duplicates of original records generated by Google's electronic process or system that produces an accurate result and that the accuracy of Google's electronic process and system is regularly verified by Google. The certification also included list of hash values corresponding to each document produced. The district court also granted the government's motion in limine to authenticate digital hard drive images as accurate copies of electronic devices. In support of its motion, the government offered 902(14) certifications from FBI forensic examiners who explained what software was used to make the images and that hash values were obtained to confirm that each image was an exact duplicate of the original.

***United States v. Bondars*, No. 1:16-cr-228, 2018 WL 9755074 (E.D. Va. Aug. 20, 2018).** The district court granted the government's motion in limine to admit screen shots of the Internet Archive's Wayback Machine based on a certification from an Internet Archive

office manager that met the requirements of 902(13). The certification (see ECF docket number 148-1, p. 10) explained that the Internet Archive is a website that provides access to a digital library of Internet sites; that the Wayback Machine uses a crawler to surf the Web and automatically store copies of web files, preserving the files as they exist at the point of capture; and that the screen shots produced by the Archive were true and accurate copies of printouts of the Archive's records.

***United States v. Adams,* No. 15-cr-00580, 2019 U.S. Dist. LEXIS 9558 (E.D. Pa. Jan. 16, 2019).** In a motion for new trial, the defendant argued that the district court abused its discretion by permitting the government to admit, using Rule 902(13) certification, evidence of text messages recovered from the defendant's cell phone. The certification was made by a Bureau of Alcohol, Tobacco, Firearms and Explosives special agent who was also a "Digital Media Collection Specialist." The special agent stated that Cellebrite software generates a file of extracted data which is then used to generate a report of the data and that he routinely determines the accuracy of such reports by comparing the report to the data on the device from where it came. The district court rejected the defendant's arguments that the court abused its discretion in admitting text messages.

***Rosado-Mangual v. Xerox Corp.*, No. 15-cv-3035, 2019 WL 7247776 (D.P.R. Dec. 27, 2019).** In a wrongful termination lawsuit, defendant Xerox moved for summary judgment. In opposing the motion, the plaintiff challenged Xerox's use of an exhibit showing a record of trainings the plaintiff took while at Xerox. The plaintiff argued that, because the records were created by computer software, Xerox had to use either 901(b)(9) or 902(13) to authenticate the records. The district court rejected this argument, noting that Xerox had properly authenticated the records under alternative methods (such as through circumstantial evidence and distinctive characteristics under 901(b)(4)), and as stated in the Advisory Committee Notes to 902(13), nothing in the rules was intended to limit a party from establishing authentication of electronic records on any ground provided in the rules.

About the Authors

Andrew Schupanitz is a Trial Attorney in the Antitrust Division's San Francisco Office. He has been with the Division since 2016.

Jacklin Chou Lem is an Assistant Chief in the Antitrust Division's San Francisco Office. She has been with the Division since 2008.

Page Intentionally Left Blank

Data Processing Explained: What Case Teams Should Know

Carrie Kitchen
Legal Administrative Specialist
Eastern District of Kentucky

Long gone are the days of cases involving just paper records and a few computer files. No longer is Electronically Stored Information (ESI) something only a case team[1] handling a large fraud case has to consider. Today, even the smallest case may have multiple types of ESI in addition to paper documents that must be managed and reviewed.

"Electronically Stored Information or ESI is information that is stored electronically on enumerable types of media regardless of the original format in which it was created."[2] ESI is everywhere in our cases. Files found on cell phones, tablets, digital cameras, and computers are considered ESI. ESI also includes items stored on external media, such as CDs, DVDs, external hard drives, and cloud storage.

The size of individual electronic files varies widely, as does the volume of ESI in individual cases. Case teams should know that when it comes to ESI, looks can be deceiving—assumptions cannot be made about the volume of ESI based solely on the size of the electronic device. For example, a USB drive may appear small, but it can contain a substantial volume of files. A LexisNexis fact sheet conservatively estimates that a 1 GB storage device may hold the equivalent of 64,782 pages of Microsoft Word files (.doc, .docx) and 100,099 pages of emails (.msg) if each email contained 1.5 pages.[3]

Further, it is unlikely that evidence on a storage device will be one file type. For example, a combination of business files, such as Word documents; Excel files (.csv, .xls, .xlsx); pictures (.jpg, .png); and audio and video files (.mp3, .avi), is commonplace. These examples are given to inform a case team that, in receiving six external devices containing

---

[1] As used in this article, "case team" refers to the attorneys, agents, and legal support assigned to a matter.

[2] *ESI/Electronically Stored Information*, *Glossary*, ELEC. DISCOVERY REFERENCE MODEL, https://www.edrm.net/glossary/esi-electronically-stored-information/ (last visited Mar. 20, 2020).

[3] LEXISNEXIS, DISCOVERY SERVICES FACT SHEET (2007).

many GBs of data, along with a couple of cell phones and a few email boxes, the amount of data could be enormous.

Because every case now has the potential to feature these large volumes of ESI, a case team finds itself facing decisions concerning ESI before collection even begins. Yet, it is difficult for a case team to make informed decisions on topics such as deduplication, numbering, or handling special formats when they do not understand what happens when they send both ESI and paper documents to litigation support personnel for processing. Case team members may have little understanding of how decisions made during processing may impact their case in the future, including the efficiency of their evidence review and their options for producing discovery when the time comes. Moreover, if a case team has little understanding of the time and resources that litigation support specialists invest in processing, how do they ensure their decisions will not cause delays when it is time to review or when production deadlines must be met?

This article is meant as a resource for case teams on evidence processing. It starts with an overview of the technical steps involved in processing paper documents and more complex ESI. It then explains several of the choices that must be made during processing and how case teams can help ensure sound choices are made, including planning for and assessing evidence before processing even begins. Additionally, this article seeks to encourage enhanced communication between the case team and litigation support specialists when discussing ESI, processing, and the associated technical terms.

I. Processing workflows

Processing refers to the process of converting data into formats more suitable for loading into review platforms, analysis, and production. What happens when paper documents and ESI are handed over to litigation support specialists for processing? It is likely that litigation support personnel will have to employ different methods and different software tools to process those materials. The method and tool will vary depending on the complexity of the materials and the needs of the case team. The time required to complete each processing step will also vary with the volume and complexity of the files and processing choices the team makes. No two cases are alike, and no two cases require the same steps to process evidentiary materials. Nonetheless,

below are simplified descriptions of the steps involved in processing paper and ESI.

A. Simple method: paper to ESI

The simplest processing workflow is for paper documents. In this workflow, a scanner and basic processing software convert paper into an electronic file. First, the scanner and software create an image of the document. Once that image is created, the processing software converts the words on the image to text, making it searchable. This process is called OCR (Optical Character Recognition). Redactions or tracking numbers are sometimes applied, and then, the image is exported to a file, such as a PDF.

Each of these steps takes varying amounts of time to complete, with image creation and OCR typically taking the longest. Case teams need to be aware that performing just these simple steps on large or complex evidence sets can take the processing software weeks. Moreover, the case team's choices also affect the project time frame. For example, if a case team insists that every document seized is processed without considering its relevance, it will add time that litigation support personnel need to finish the project.

Through these steps, the processing software has created three electronic layers for each document. Each layer contains different information. First, the image layer is like a photocopy of the original document; it is fixed in place, analogous to a photograph. You cannot search this layer. The second layer contains the text created by OCR, making the document searchable. The third layer is created if any annotations, such as redactions or highlights, are applied by the case team during review.

An important word of caution regarding OCR: it is not 100% accurate. During the OCR process, the software is simply looking at the image's pixels. A pixel is the smallest unit that makes up texts and images on a digital display.[4] During OCR, the software examines those pixels to determine whether they collectively match a number or a letter. In other words, OCR is the computer's best guess as to what word or number a collection of pixels is creating. Importantly, handwritten documents will not be searchable even after performing

[4] *Pixel*, *Dictionary*, TECHOPEDIA, https://www.techopedia.com/definition/24012/pixel (last updated July 26, 2016).

OCR. This is because the processing software cannot "read" handwriting.

Case teams should also understand that there are many factors that impact the accuracy of OCR. These factors include the quality and condition of the paper the document was printed on, any dirt or smudges on the document, and the lightness or darkness of the print on the page of the document. Further, the accuracy of OCR varies from program to program, and no program is 100% accurate. In fact, even under the *best* of conditions, OCR will only be approximately 80 to 85% accurate, and it is often significantly less accurate than that.[5]

For these reasons, case teams should exercise caution when performing electronic searches of scanned documents that were OCR'd. For example, case teams may miss valuable evidence if they rely solely on electronic searches of documents containing a substantial number of handwritten notes or aged documents with faint print.

II. Complex method: ESI

The more complex processing method involves ESI. Processing ESI requires sophisticated software due to the complexity associated with different ESI file types. Particularly complex ESI requires unique handling and, for this reason, is typically processed by those with a specialized knowledge of defensible electronic processing methods, such as litigation support specialists.

Though processing ESI involves some of the same steps as processing paper, there are some notable differences. In simplest terms, processing ESI involves the following: First, ESI is imported into processing software, which extracts the file's metadata.[6] Second, the software extracts the text of the file.[7] Third, an image of the file is created. Fourth, OCR is performed on documents that have no extractable text. Fifth, Bates numbers or other custom annotations can be applied if requested by the case team. Finally, a digital copy of the document is exported to a PDF or other format. This is a very simplified workflow for ESI, and the above steps will not always be performed in that order. Further, each step will be followed by quality

---

[5] *OCR, Definitions*, ELEC. DISCOVERY REFERENCE MODEL, https://www.edrm.net/glossary/ocr/#note-8225-1 (last visited Apr. 14, 2020).

[6] *See infra* Section II.A.

[7] *See infra* Section II.B.

control to ensure that the best possible output is being achieved. There are some issues that cannot be identified until processing begins, such as corrupted files. Litigation support personnel will be able to identify these issues and, in consultation with the case team, make decisions on how to best resolve the issues.

All forms of processing ESI require more than the simple steps outlined above and may be confusing to those who do not specialize in the field of litigation support. Below is a more detailed discussion of some of the considerations at each step.

A. Metadata

During the first step of processing ESI, metadata is extracted from each file. Metadata is sometimes referred to as "data about data." Every piece of ESI has metadata, which is information about the file itself. Examples of metadata include file name, file size, creation and modification dates, and the name of the file's owner.[8] This information can be very useful to a case team, but it can only be viewed and leveraged if the ESI is properly processed.

To illustrate this point, let's take email as an example. Email has both visible and hidden metadata. Visible email metadata includes the date sent, subject, sender, recipient, and whether there were any attachments to the email. By processing the email with specialized software, the case team will also be able to see the hidden metadata, including, for example, if the email was blind copied to someone, the IP address of the sender, and the metadata associated with any attachments to that email.

Because metadata may have evidentiary value, it may need to be preserved and protected from alteration. Indeed, courts have held that there is an obligation to preserve some metadata and that opposing

[8] *See, e.g.*, Zubulake v. UBS Warburg, LLC, 220 F.R.D 212 (2003); *The Sedona Principles, Third Edition: Best Practices, Recommendations & Principles for Addressing Electronic Document Production*, 19 SEDONA CONFERENCE J. 1, 171 cmt. 12(a) (2018).

parties may have the right to receive it.[9] Failing to preserve relevant metadata can lead to spoliation[10] sanctions.[11]

Case teams should be aware that inadvertently altering metadata is easy. For example, metadata can be altered by opening a file outside of a review platform. This will cause the computer to overwrite certain information, such as the date the file was last accessed, and in doing so, that metadata is changed forever. One of the most effective ways to protect against altering metadata is to use tools designed for that purpose, such as processing software. Case teams should rely on their litigation support personnel to complete this processing using specialized software.

B. Extracted text

During the second step of processing ESI, the software extracts the text from certain files. Extracted text and OCR are often confused by case teams. While OCR is the computer's best guess at what words the image's pixels create, extracted text is the actual text contained in a document. Processing software extracts the text directly from the file, making extracted text the closest to 100% accurate that can be achieved in processing.

Nonetheless, a few words of caution to case teams about extracted text: First, as previously discussed, evidence received at a United States Attorney's Office (USAO) will most likely have a mix of file types, and not all of them will contain text that can be extracted. Examples of these files include pictures that contain words or even non-searchable PDF files—that is, PDF files that do not contain a text layer. OCR will need to be performed on files lacking extracted text to make them searchable (a separate step), and as discussed above, OCR has its limitations. Second, electronic searches of files with extracted text are not fool-proof. For example, if a word is misspelled in the

---

[9] *See, e.g.*, Zubulake v. UBS Warburg, LLC, 220 F.R.D 212 (2003); *The Sedona Principles, Third Edition: Best Practices, Recommendations & Principles for Addressing Electronic Document Production*, 19 SEDONA CONFERENCE J. 1, 170 cmt. 12(a) (2018).

[10] Defined as destruction or alteration that destroys its value as evidence in a legal proceeding, see https://definitions.uslegal.com/s/spoliation/ (last visited Apr. 14, 2020).

[11] *See, e.g.*, *Leidig v. BuzzFeed, Inc.*, No. 16 Civ. 542 (S.D.N.Y. Dec. 19, 2017) (imposing spoliation sanctions where metadata not preserved).

document, it will be misspelled in the extracted text, meaning that electronic searches will not locate the term.

C. Imaging, endorsements, export

The next step in processing ESI involves the creation of an image for each file. Sometimes, this stage is called *TIFFing* because one image type that processing software creates is a TIFF file. This stage involves the software opening each file individually in the program it was created in, such as Word, and printing that file. The image is not printed to paper, but to an electronic image such as PDF, JPEG, or TIFF. Case teams have choices here, some of which can affect how quickly the project will be completed. A team should think about if they really need every file TIFFed. Perhaps they can skip TIFFing files they do not need to review. Some file types, like audio or video recordings, are not amenable to TIFFing. Excel spreadsheets, for example, are usually not TIFFed as choosing to do so will result in delays and a lot of blank pages in your review database. By way of another example, a case team choosing to have all their imaging done in color versus black and white could see an increased amount of time for processing and larger file sizes.

The remaining processing workflow is the same as for processing paper: a layer for endorsing, text files for searching, and the creation of a digital document for review.

Some case teams may choose at this point to simply endorse Bates numbers on the documents and export for production. The majority of cases will be assigned a review number (different from a Bates number in that this number is not burned onto the image) and exported to a review platform for analysis.

D. Special formats

What happens when the evidence contains Cellebrite extraction and phone reports, documents containing linked files, or audio and video files? These files are special formats that may require different handling; the case team should consult with litigation support specialists before processing. Litigation support personnel will provide advice on how to proceed with the files, including whether to process them at all. For example, Cellebrite extractions are not usually processed. These files arrive ready for case team review. Running them through processing software may actually break the files apart in such a way as to render them less useable to the case team.

Files, like Cellebrite extractions, that are not processed should be given an electronic "placeholder" in the document review tool so that the case team is aware of the file and its location and knows how to review it. These special format files will be duplicated for discovery purposes and provided to opposing counsel in the same format they were received by the USAO.

III. Considerations for case teams before processing

Now that you have an understanding of the processing steps outlined above, we will dive into how a case team should approach these steps and the decisions that accompany them. But first, a note on communication: As you know, throughout the life of a case, maintaining good communication between the case team and litigation support specialists is key, but it is not always easy. One impediment to good communication is terminology that may be unfamiliar to all members of the team or differing definitions for that terminology. Processing terms can be technical in nature, which can be intimidating to legal staff and attorneys. But these concepts are important, because they can affect the quality of the discovery, as discussed further below. It is worth taking the time to ask questions and get on the same page with litigation support staff before decisions are made.

A. Before processing, plan, assess, and communicate

Where to start when approaching discovery decisions? Start before collection even begins by having a case team meeting with your litigation support specialist to develop a plan for how evidentiary materials will be managed. Planning is necessary for every case, but it is particularly important for cases that involve complex or voluminous evidence, are high profile, or are expected to be highly contentious. Having an early case team meeting prior to receiving evidentiary materials that includes both legal and litigation support personnel serves many purposes.

First, it can be used to create a roadmap for the flow of evidentiary materials from original custodians, to agents and/or to the USAO, and to litigation support specialists. As part of this workflow, the team should define expectations, delineate each team member's roles and responsibilities, set out lines of communication, and establish deadlines for providing evidentiary materials. This way, everyone—

from agents to litigation support personnel—start on the same page. Importantly, an early meeting also helps create a team atmosphere, which will likely facilitate good communication throughout the life of the case.

The case team can also use this early moment to brainstorm about the quantities and types of ESI they expect to collect, as well as the key custodians, relevant dates of activity, and email addresses that may help fine tune a team's plan for searches or subpoenas. This approach may help save valuable time later by streamlining the approach to a case, which may result in less time collecting, processing, and reviewing files that have limited value to the case. Early brainstorming about the quantities and types of expected materials will also help the case team build a timeline that appropriately accounts for potentially voluminous and complex discovery. Litigation support personnel can be particularly valuable in helping build a realistic timeline, as they can draw on their extensive experience with processing and producing evidence sets of varying sizes and complexity.

Including litigation support personnel in the planning phase can also help ensure that their resources are available when the case team needs them. Most litigation support personnel support multiple case teams at a time—sometimes even supporting the entire office and branch office(s)—and they have limited hours and equipment to do so. Planning ahead is the best way to have their resources ready to devote to the team's discovery and will help eliminate most urgent requests, thereby avoiding tension, frustration, or a breakdown in communication. For example, if a case team has not included litigation support personnel in the planning from the onset of case assignment, it is possible that the first notice litigation support receives of a large ESI processing project is when it is submitted for processing. This may require litigation support to stop work on other projects to free up resources and personnel or to compromise quality control checks. Last minute projects are often the projects that have the most mistakes simply because there was no time to address issues found during quality control. Not having the time to address issues is often what leads to discovery disputes. Including litigation support personnel in the planning from the beginning of the case will inform them that a large project is on the horizon and allows for effective preparation, ensuring adequate resources and time are available for the project.

The planning phase is also a good time for case teams to consider whether a filter team is needed. If so, case teams should consider whether they want litigation support specialists to apply a set of search terms to the materials to screen out potentially privileged material before the materials are loaded to the case team's review platform. Developing a filter review plan before collection even begins will save time and reduce risk later.

Once the receipt of evidentiary materials begins, but before those materials are processed, there are additional steps case teams should take. First, the case team should inventory all evidence for tracking purposes. Then, the case team should focus on assessing the evidence they have received. How voluminous are the materials? Are they organized? Did the case team receive everything they expected in the formats they requested? Are materials obviously missing? Were passwords provided for encrypted media?

The case team should also evaluate the potential evidentiary value of the materials to decide whether office resources should be invested in processing them; for example, in criminal matters and affirmative civil investigations, voluminous records that, on their face, have limited value to the case may not need to be processed. The case team should also assess whether there are special considerations, such as a short time frame, that may impact how processing proceeds; for example, case teams in need of quick turnaround may opt to prioritize certain materials to process first. Case teams should assess the volume and complexity of the materials to determine whether outside resources—such as a litigation support vendor—are needed.

Litigation support personnel should be included and consulted on these types of questions so that their expertise is leveraged. For example, litigation support specialists can assist with assessing whether evidence needs processing or whether it has been delivered already processed in the form of load files. (Load files contain preprocessed materials that are loaded directly into a review platform.) Litigation support specialists can also offer ideas on how technology in their toolbox can assist in identifying the most important evidence within the volumes collected, including by using key word or custodian searches to narrow in quickly. Not including litigation support personnel in these discussions may result in the case team having to review and comprehend the entire universe of data collected or the inability of litigation support to dedicate resources and time to meet deadlines.

Now, a case team is ready to begin preparing evidence for processing. The case team should consider the organization of their data prior to submitting the materials to litigation support for processing. Think about how to organize the materials to make a review flow smoothly. Consider having files grouped by search terms, custodians, domains, or document type. Consider prioritizing key custodians and having their data processed and loaded into a review platform first, which will allow for fruitful review from the beginning. Again, consult with litigation support specialists on file organization strategies and to ensure that relevant metadata is not inadvertently altered during the organization process.

B. Before processing: making sound processing choices

There are certain choices that must be made during processing. Case teams should be involved in making those choices; they may impact the case later. For example, choices made during processing may impact the efficiency of the evidence review or even legal issues in the case. These choices need to be discussed before processing starts. As examples, case teams should meet with litigation support specialists to determine whether ESI should be deNISTED and deduplicated and which time zone to use for processing. Each of these concepts—and their impact on case teams—is described in turn.

First, what is DeNISTing, and what does it mean for the case team? DeNISTing is using processing software to remove program files and other files that do not have user generated content. These files are sometimes referred to as standard system files that keep the computer programs running. The National Institute of Standards and Technology (NIST) compiles a list of these files through the National Software Reference Library.[12] In most cases, these files are not evidence and do not need to be processed or reviewed by the case team.

Deduplicating data during processing may similarly enhance the efficiency of the case team's review because it may reduce the amount of material the case team ultimately needs to review. During

---

[12] *EDRM Processing Standards Guide, Version 1*, *Resources*, ELEC. DISCOVERY REFERENCE MODEL, https://www.edrm.net/resources/frameworks-and-standards/edrm-model/edrm-stages-standards/edrm-processing-standards-guide-version-1/ (last visited Feb. 2, 2020).

processing, the software identifies files that are identical copies. It does so by comparing the hash values of the documents. The hash value is like the DNA of a document—each file has a unique hash value. If the hash values of two documents are identical, the processing software will identify these documents as duplicates.

Before processing, the case team should consult with litigation support specialists to decide how they want to treat duplicates. One approach is to do nothing and leave all duplicates in the data set for case team review. Another option is to have the processing software identify duplicates during processing and leave them out entirely. This will result in no duplicates in the review set and no record of the duplicates should the case team need them down the road. A safer approach involves processing all files and having the software identify and remove duplicates in such a way that the case team will know of their existence and where they resided in the evidence set. With this approach, the case team may choose to either have the duplicate documents replaced with placeholders that provide information about the duplicate file or have the duplicate documents excluded from the review set but with information about the duplicates identified in a report generated by the processing software or in a field in the review database. Deduplication describes the process by which identical copies of a document are identified and removed after the document's first appearance in the data set.[13]

A litigation support specialist can guide case teams through the pros and cons of each approach in light of the facts of the case and goals of the evidence review. The approach selected will likely impact the pace of the review. As an illustration, let's say an evidence set is comprised of 100 documents; the processing software identifies 80 as unique and 20 as duplicates. Without deduplication, the case team will have 100 documents to review. If the case team chooses to deduplicate and replace duplicates with placeholders, they will still have 100 documents to click through in their database: 80 unique documents and 20 placeholders for the duplicates. If the case team chooses to deduplicate and exclude the duplicates, they will review only the 80 unique documents. This does not mean, however, that the case team loses access to information about the duplicates. That information can

[13] *Deduplication*, *Glossary*, ELEC. DISCOVERY REFERENCE MODEL, https://www.edrm.net/glossary/deduplication/ (last visited Jan. 16, 2020).

be captured in a field in the review database or in a report generated by the processing software.

Case teams interested in deduplication have an additional choice to make: Do they want to deduplicate vertically or horizontally? Vertical deduplication means deduplicating within the ESI belonging to one custodian.[14] For example, a case team receives the contents from *Suspect A's* hard drive. With vertical deduplication, the files on *Suspect A*'s hard drive are compared against each other to look for duplicates. If the hard drive contains multiple identical copies of the same document, the processing software will flag those files as duplicates.

Horizontal deduplication (also referred to as global deduplication) means deduplicating across multiple custodians.[15] In this example, *Suspect A*'s hard drive would be compared against *Suspect B*'s and *Suspect C*'s hard drives. The processing software will compare documents contained on all three hard drives to identify duplicates.

It should be noted that deduplication can only be done on ESI and should be performed by processing software. It is virtually impossible to deduplicate paper documents, and case teams should not rely on themselves to identify true duplicates. While deduplicating files clearly has some benefits, it may not be the right fit for all cases. It is incumbent upon case teams and litigation support staff to communicate about the pros and cons of deduplication for each case. Ultimately, the decision of whether or not to employ this feature is for the attorney to make.

Finally, case teams should give consideration to the concept of time zone normalization—the process by which dates and times are made consistent. This concept must be discussed at the beginning of the case, prior to any processing. Unless instructed to do otherwise, processing software will process ESI and metadata with the time zone of the location of the processing computer. For example, if emails are processed in the Eastern Time Zone, the default will be that the emails will display dates and times in the Eastern Time Zone, even if those emails originated on a computer in the Pacific Time Zone. As a

---

[14] *Vertical Deduplication*, *Glossary*, ELEC. DISCOVERY REFERENCE MODEL, https://www.edrm.net/glossary/vertical-deduplication/ (last visited Jan. 16, 2020).

[15] *Global Deduplication*, *Glossary*, ELEC. DISCOVERY REFERENCE MODEL, https://www.edrm.net/glossary/global-deduplication/ (last visited Jan. 16, 2020).

result, it will look as though emails were sent, or files were created, three hours later than they actually were. Litigation support specialists can correct this issue by adjusting the time zone for processing purposes, but only if they are made aware that ESI was generated in a different time zone.

Put another way, case teams have these choices for time zones: first, allow the software to decide based on the time zone the computer is set to; second, process each custodian's data in that custodian's known time zone (assuming the case team knows the proper zone); or third, use a single time zone for all processing. As with deduplication, decisions around time zone normalization may have legal implications. For this reason, the case team's attorneys should make the final decision about its use. No matter which option is chosen, the time zone used for processing should be communicated to opposing counsel when the ESI is produced in discovery.

A word of warning: Adjusting the time zone does not guarantee the day and time appearing on an image is correct. In today's world, it is difficult to know where someone was physically located when they created a file or sent an email. People can create computer files and emails from their phones while on vacation, in their office, or attending a conference across the country. An email processed using the Eastern Time Zone where the person is known to live may not display the correct day and time if, for example, that person actually sent it from a European vacation. For this reason, many legal teams have moved away from adjusting time zones for different batches of evidence and, instead, select a consistent time zone for all evidence processed in the case.

A final note regarding processing choices: While it is best to make these choices before processing begins, they should be revisited throughout the life of a case. The process is fluid. What was decided today may not be relevant tomorrow as a case changes and evolves.

IV. Conclusion

Decisions on evidence processing can be intimidating, as it is an area that case team members may not feel comfortable discussing. Hopefully with the knowledge gained from this article, it is a little less intimidating. Know too that litigation support personnel stand ready to provide resources and answers. The earlier litigation support specialists are included, the sooner they can help guide the case team through important decisions about evidence processing, review, and

production. With an understanding of the issues in the case and the case team's goals, they can help ensure that the most relevant evidentiary materials are processed and loaded into a review platform first. Litigation support specialists can also assist with creating a plan to organize evidentiary and discovery materials and with selecting a production format for use throughout the case. Ultimately, good communication between the case team and litigation support personnel will lead to a more efficient and effective process in preparing materials for discovery.

About the Author

Carrie Kitchen is a Legal Administrative Specialist in the Eastern District of Kentucky in Lexington, Kentucky. In her position, she processes and produces all discovery for the District's main office as part of a Litigation Support Unit staffed with three other litigation support technicians. She graduated from Morehead State University in 2000 with a degree in paralegal studies.

Special thanks to Christine Corndorf, Gina Alires, and Donna Miller.

Page Intentionally Left Blank

Effective Document Review Techniques in Eclipse and Relativity

Joseph P. Derrig
Assistant United States Attorney
Eastern District of Washington

Hetal J. Doshi
Assistant United States Attorney
District of Colorado

I. Introduction

A trial attorney's job is to tell a truthful, compelling story to a judge, jury, or mediator. Somewhere along the way, the ability to present a compelling story has gotten lost among a tsunami of electronic files. We increasingly spend more time searching through meaningless data than piecing together the truth and presenting the story of our cases. We have attempted to manage this data tsunami, first with notes and sticky flags, then with manually created electronic databases, and we have now moved to technology that lets us pull in files and auto-creates an electronic database for us from fields of metadata. The review tools we have now allow us to learn exponentially more in less time, assuming we use the tools correctly and efficiently.

Two popular review tools are Eclipse SE and Relativity. Eclipse SE is a desktop or in-house file review tool that can be managed by local office personnel who load data into, and generate productions from, Eclipse databases. Eclipse can readily handle hundreds of thousands of files, and since it is locally controlled, it allows greater flexibility on set-up and design, as well as control over the timing of file loading and production. It also has robust tagging and searching functionality, including through the use of search terms and metadata filtering. Overall, Eclipse is well-suited for most cases. It does not, however, allow for web access, nor does its in-house version have analytics.[1]

Comparatively, Relativity is a web-based file review tool that is likely supported outside of your office. If Relativity is supported by a

[1] IPRO, the owners of the `Eclipse SE` software, also have software called `Eclipse` that is web-based and allows for analytics. References in this article to `Eclipse` refer solely to the `Eclipse SE` software.

single processing center outside of your office, case team members have to build in additional time to account for transferring data remotely, and it may have to wait in the queue of requests from other offices served by that processing center. Relativity has the same tagging and searching functionality as Eclipse plus advanced analytics designed for sifting through very large or complex data sets, including email threading, near duplicate analysis, clustering, and concept searching. Additionally, because it is web-based, the database can be accessed and worked on by case team members in disperse geographical locations.[2]

This article will discuss how to use these tools effectively as well as some common features of these review tools and how they are useful in practice.

II. Building a usable database

Your ability to use document review tools to search the files gathered is only as good as the database created. Creating a usable database takes some technical knowledge and understanding of the files you are likely to collect, as well as time, thought, and planning. In order to make sure your review tool has the best fielded data[3] possible, the files collected have to be managed correctly from intake through processing before being loaded into the review tool. The planning and administration of the database is critically important to the successful use of these tools.

Whether it is a big case with the potential for big challenges or a small case, it is necessary to start the conversation on how the case team[4] will collect, manage, and review files at the earliest

---

[2] When selecting a review tool, case team members should consider whether the number of individuals reviewing files in the case will be geographically disperse and whether the volume as well as type of files would require the use of analytics. If so, a web-based review tool is likely a better selection.

[3] Fielded data is a combination of the document's relevant metadata along with other helpful information typically gathered when the document is collected, such as the document's custodian, the document category, the file location (for example, file path), the date of collection and/or production, the document's control number and/or bates number, and other information that is helpful to the reviewer.

[4] The case team includes all attorneys and support staff, including litigation support professionals, who will work on a matter. In cases where litigation support assistance is only required on occasion, litigation support staff

opportunity. The case team needs to think about what types of files are expected in the case, the ability to collect those files, the volume of those files, what type of metadata is important, how the case team would like to sort and review those files, as well as how discovery will be produced.[5] Thinking about and discussing these issues early is essential to building the best database for your particular case and its team. While it is inevitable that the case or investigation will have unanticipated twists that necessitate refining your document review protocol[6] and/or the structure you establish, it is much easier to manage those changes with a strong, comprehensive structure on the front end.

For example, let's assume you are assigned to defend single-plaintiff employment discrimination case. The case team is wholly within your office, the types of files collected is limited to five custodian's emails (.pst), medical records (.pdf), a small number of other Microsoft Office files (for example, .docx), and some photos (.jpeg). Further, assume your client's information technology folks have already preserved the relevant witnesses' electronically stored information (ESI) in native format via a forensic software tool such as EnCase. Based on your assessment of the data expected, you believe you will only need to search by typical types of metadata, such as date created, last saved, date sent, and so forth. Creating a database with Eclipse and using it for review and production would be the best choice for this type of case.

Comparatively, if you are working on a multidistrict fraud case with multiple defendants, vast amounts of files, a large number of different file types, and with case team members all over the United States, it may make more sense to use a more robust tool to create a database in Relativity for your review. Relativity may be the ideal review tool for this type of case because it can be accessed by trusted users both

---

should still be brought in at key points in the litigation to ensure the technical aspects of collection, processing, review, and production are adequately assessed.

[5] If you have files from individuals or entities with a special status (for example, grand jury, confidential sources, whistleblowers, etc.), safeguards will need to be put into place to ensure appropriate protections are in place when you make productions.

[6] For example, "a plan outlining the approach to reviewing evidence and documents within in a review tool, including defining relevant fields and the named tags utilized in the database."

inside and outside your office. That said, the case team's schedule may need to take into account the time it takes to transfer, load, and produce from an off-site centralized litigation technology center.

The take away is that you don't need to select the biggest chainsaw in the hardware store to cut down a sapling, and you definitely shouldn't if you are inexperienced. While the biggest chainsaw could do the job, you are going to expend more energy than necessary and, if inexperienced, more likely to seriously injury yourself with a small mistake. Don't seriously injury to your case; select the right tool and always have someone knowledgeable handling or instructing on proper use.

A. Collection

When working to collect files (that is, evidence), it is important to understand the following: What form(s) of files are likely to be collected (for example, .pst files, Microsoft Office files); how those files will be preserved or maintained, that is, does it preserve the underlying metadata; how those files will be collected, that is, with or without the underlying metadata; and an idea of the volume of the files that will be collected. Additionally, subpoenas should specify the format of production, including specifications describing the metadata that should be included. The same is true for materials procured through a search warrant or obtained via a release.[7] If `raw electronic files` (that is, ESI that has not been processed)[8] will be sent to the case team, the case team must build time into their case management plan for the data to be processed, as review of the data

[7] Prosecutors must also consider whether a filter review, privilege review, or taint team is necessary. A taint team is a collection of government lawyers and/or investigators separate from a primary litigation team created to shield the primary litigation team from exposure to material that it should not receive under the rules of professional conduct or other law.

[8] `Processing`, for the purposes of this article, describes the automated process by which electronic evidence is imported into a software program designed to extract a file's metadata and text so that the evidence can be loaded into, and analyzed in, a review tool like Eclipse or Relativity. Processing may also include the creation of a static .tiff, or other file type, image of the file.

cannot start until the data has been processed and placed into a document review tool.[9]

If your agent, agency, client, or other entity will provide PDFs (that is, converted electronic documents or scanned paper documents where the underlying metadata is not relevant to the document), it is important to ensure that the PDF files provided are searchable (through the Optical Character Recognition "OCR" process) and organized. Organization in folders by custodian, file type, date range, or useful identifiers can be captured by using processing tools that extract file paths so that the PDFs, when processed within your office, retain their organizational structure when placed into the review platform.

It is also important to remember that the process of converting paper documents into PDFs—scanning—needs to be precise and thoughtfully organized. If the your agent, agency, client, or other entity will provide scanned paper files, attorneys must understand how the they scanned the paper files and ensure that the process achieved the goal of legal scanning—that is, to have the digital version of the documents mimic the hard copy in sufficient quality so that one can understand how the paper documents were organized. This process, known as `document unitization`, allows case teams to understand the paper file organization, for example, which pages were grouped together with a staple or paper clip, which documents were grouped into a folder or grouped together as a main document followed by exhibits, and which folders were in a filing cabinet drawer. This information may be captured by the use of a robust scanning tool that will generate an index or load file. The index or load file will allow the case team to load the scanned documents into a document review tool and see the document breaks, folder breaks, and attachments.

If your office will ultimately process whatever files it receives, whether it is electronic data, scanned PDFs, or paper documents that still require scanning, it is important to bring litigation support

---

[9] If the agency, client, or opposing counsel will process the data so that it can be easily ingested and analyzed within a document review tool, it is important to discuss how the files will be processed, whether and what metadata fields will captured by any processing software, and the format in which the data will be delivered. Production specifications are often used to detail what metadata fields should be captured and the appropriate format of the processed data.

expertise to bear, regardless of how active they will be on the case team as the case moves forward. The case team and litigation support should agree on a processing plan that outlines how the data is to be processed and whether processing decisions will be different based on the types of data at issue. Getting such an agreement in place at the start of a case will save everyone time in the long run.

B. Processing

A large collection of files is almost never capable of being processed without flaws. Regardless of who you are collecting files from, inevitably, encrypted files, corrupt files, unrecognized file formats, or other types of files will require additional processing in order to effectively review them. Many files, such as audio files, require special tools or treatment to enable effective searching and review. Most processing tools are capable of generating exception reports that can identify issues with files that, if possible, should be addressed for accurate processing. It is important that the case team develop thoughtful quality control procedures, including a plan to resolve issues identified on exception reports, during processing.

Case teams must also consider whether DeNISTing, time zone normalization, deduplication, near-deduplication, or other techniques are necessary to help create a manageable, usable database.[10] When faced with large data sets, case teams should determine whether all data must be processed and loaded to the document review tool and then reviewed. For example, marketing emails and emails sent well outside the relevant date range can be filtered out during processing, such that only a smaller set must be reviewed. Agreed-upon search terms could also be applied to large data sets, with only records containing `hits` loaded to the review platform. Be sure to document these choices so that you have a record of them later.[11] The larger and

---

[10] The Sedona Conference Glossary is a good resource to consult if case team members are unfamiliar with any of these terms. The Sedona Conference (https://thesedonaconference.org) is a nonprofit, 501(c)(3) research and educational institute well known for, among other things, its thoughtful, balanced, and free publications, such as the Sedona Conference® Glossary, which can be downloaded from its website.

[11] In making a decision to load only documents that `hit` upon search terms to the database, attorneys are advised to create or request, and then assess, `hit reports` with opposing counsel. It is rare that an attorney's first set of

more complex the case and files become, the greater care and knowledge the case team must have to address the implications of various processing choices.

- [T]he bottom line: *The most sophisticated MRI scanner won't save those who don't survive the trip to the hospital.* It's more important to have triage that gets people to the hospital alive than the best-equipped emergency room. Collection and processing are the EMTs of e-discovery. If we don't pay close attention to quality, completeness and process *before* review, review won't save us.[12]

Attorneys must work closely with the case team's litigation support personnel and/or their litigation technology center to ensure quality processing before beginning review.

III. Setting up a document review protocol

Case teams are frequently excited and anxious to get started on reviewing evidence, so there can be pressure to start right away without a well-conceived plan. Litigation support staff should encourage case teams to invest time thinking through some issues and questions before beginning the review. It is worthwhile to have a team meeting to properly plan how the review will proceed and to document those choices so there is a baseline against which future refinements to the protocol are recorded and tracked. The team should consider:

- Whether a filter team already reviewed files collected, and if not, is one needed before review by the case team begins? Or in a civil case, will the case team need to review documents collected from an agency for privilege before production?
- Which records will need to be reviewed?
- Will linear or non-linear review be used?

---

suggested search terms is appropriately scoped, as quirks of how the entity or individual at issue communicates may refine the suggested search terms.

[12] CRAIG BALL, PROCESSING IN E-DISCOVERY: A PRIMER 32 (2019) (emphasis in original). Professor Ball's primer on processing contains a more detailed overview of processing and should be mandatory reading for attorneys before using review tools.

- What tags will be used, and how will they be used?
- Will there be a comments field to track why a particular document is `hot` or merited a different tag of interest?
- Will you use a needs-further-review field, and if so, how will you define those files so as not to necessitate a wholesale second review?

- Who will be doing the review and how will batches be divided up?
- Is redaction needed, and who will do it?

The answers to these questions will help you and your case team develop a battle plan to conquer the review. Like most battle plans, however, they rarely survive first contact with the enemy. The case team should re-evaluate the document review protocol shortly after the review begins to ensure it achieves the desired outcome.

At bottom, a review protocol can be brief, defining the metadata and fielded data headers, the names of the tags, and the appropriate uses for such tags. A more comprehensive review protocol might outline the allegations and elements of the crimes, claims, or defenses, provide specific examples of documents that would receive specific coding tags, and provide additional detail on the process by which questions regarding what tags should apply to a document can be quickly resolved. Regardless of the format selected, this review protocol should be updated by the case team lead so that all members of the case team have the most up to date instructions on how to review and analyze documents within the review tool.

IV. Common features of review tools

A. Basic search

Basic searching or `quick searching` is rarely effective on its own, but it still has some use. The basic search allows reviewers to search the files using syntaxes common in other methods of search. The searcher, however, must understand that it is not like using Google or Westlaw. The search will not automatically decide to produce results including `pooling` or `pools` when the search was simply for `pool`. The basic search will not return results for typos in files or return results for concepts similar to those searched for. The basic search, thus, has a limited application when using larger imperfect data sets.

In Eclipse and Relativity, a basic search can use AND, OR, AND NOT, OR NOT, quotes to search for exact phrases, wild cards to search for unknown characters or numbers, and proximity searches.[13] While a quick search or basic search may be sufficient to quickly identify files you already know exist in a small data set, it is rarely effective in culling larger, unknown datasets.

B. Advanced search

The advanced search functionality allows the user to build a search without memorizing a complex search syntax. This functionality makes it easier to narrow down the results of searches by allowing the case team more flexibility to develop complex searches. Advanced searches allow a number of different options for winnowing files in the database for review, including searching by document type, author, custodian, as well as allowing the use of fuzzy searching,[14] all in a single search.

For example, if the case team needs to search for all un-reviewed Microsoft Word documents by a specific author, from a specific custodian, that contain a keyword to include any common misspellings of that word, it can do so quickly. In Eclipse, the case team can simply select the advanced button and build out their search, selecting the type of search, fields to search, the search operator or search value (depending on the type of search selected), the terms to search within those fields, and the connectors (for example, AND, OR) between each search phrase developed during the advanced search.

The same advanced search capability is available in Relativity. In Relativity, the case team can use the filter functionality, also discussed *infra*, to identify the documents in the active file set.[15] Then, the user can, similar to Microsoft Excel, simply filter the data set by

---

[13] The Ipro's website contains manuals, explanations, and short videos showing how tasks in Eclipse SE: https://iprotech.com/. Similar content for using Relativity can be found on its website: https://www.relativity.com/.

[14] Fuzzy searches uses wild-card characters for one or more of the characters in the search term selected. For example, a search for free may return results for tree or fret. With some review tools, you are able to set the level of fuzziness, with the higher level potentially returning more words are

[15] The active view screen depicts all documents in Relativity for that assigned workspace. That is, this screen, and any searching through the filter process, queries against every record in the workspace without limitation as to date, file type, or custodian.

the custodian,[16] the type of file, and/or the relevant time range. Once that universe is identified, the user can hone in on the documents of interest by entering search terms, to include searches using `AND` or `OR` operators, into the search terms field at the top of the active file view screen. While robust in its scope, this search capability in Relativity is useful in the early stages of a review project when the case team is still becoming familiar with the way that custodians communicated about particular issues.

Once the case team is comfortable with its search terms and understands how the authors of the documents at issue communicated, it may be prudent to use the search panel on the `Documents` list in Relativity for a conditional search or to refine saved searches. To start a complex query, select `Search Condition` on the search panel and select the conditions to be applied in the search. So, for example, the case team could select a `File Extension` to identify only Microsoft Excel documents[17] and then layer extra search conditions one at a time, like excluding certain custodians, adding specific time ranges, excluding attachments, and including specific search terms to include common shorthand or misspellings of those search terms. Relativity's ability to layer conditions allows the case team to tinker with which condition most precisely generates the data set that the team is most interested in without starting the entire search all over again. These searches are then saved by Relativity and are available for further refinement throughout the team's investigation or review efforts.

---

[16] Another helpful option in the `filter` function for Relativity is the ability to do a multi-custodian search by selecting `Advanced` in the Custodian field. This will allow a user to quickly identify a set of limited documents from the entire universe of documents in the Relativity workspace that depict how the occasions on which two or more custodians may have communicated with each other. Such a functionality is particularly helpful to efficiently isolate proof of knowledge or the existence of a business relationship such that one party would have communicate key information to another.

[17] Relativity also allows the user to helpfully exclude certain types of data from searches. For example, on the search panel, once the user selects `Add Condition`, there is an option to select `is not` to cull out all file types the case team is not interested in at that moment. So if the case team is focused on email correspondence only, this functionality is useful in removing the `noise` of search results in the form of Microsoft Excel files.

C. Saving search results

After expending all that time thinking about and creating the perfect `Advanced` search, you don't want to lose it, and you want other case team members to have the benefit of that search. For example, in Eclipse, simply visit the Search Results heading under the Case Folders tab in Eclipse, right click to save the search, and ensure that you choose `Public` and name the search so that the rest of your team can locate and access your search under the `Searches` case folder. Saving searches can be useful to identify documents that the case team should prioritize in review, identify potential documents to use in interviews or depositions, and to keep a record of what searches have been completed.

D. Filtering and tallying

This function filters out all records except those fitting the criteria you select from a list. For example, you can filter on the database's `Document Type` field to review only Outlook emails or Excel spreadsheets or filter on the `custodian` field to review only those documents from Jane Doe. This narrowing happens without having to click through all the records in the database, and you can filter or tally multiple times to quickly identify, for example, all outlook files sent by a particular email address on a particular date. The Tally feature can be an efficient way to quickly winnow down search results when searches will generally concern fielded data.

E. Sorting

After you winnow your review through searches, you can use the sort function to, for example, review emails chronologically. Any field or column with dates, numbers, or alphabetical information can be sorted by the document review tools. Basic sorting allows you to click on the field header, and it will sort that column in either ascending or descending order. More advanced sorts are possible too: You can sort the records first by name and second by date so that you can review all the records pertaining to a person in chronological order. Sorting chronologically can be useful to keep track of the order of events and to find out exactly who knew what on the date in question.

F. Tagging

One of the greatest organizational features is the ability to create tags for whatever categories you choose. Tags are just checkboxes used to identify different categories of documents during your review. More than one tag can be applied to a document, and a tag category can have child categories, so when you check the child tag the document is also tagged with the parent. To illustrate, if the case team wants to create a tag for privilege, it may want to identify the various types of privilege that may be applicable in the case. A tag palette[18] can be set up with the parent tag as `privilege`, and the child tags underneath including `attorney-client`, `work-product`, etc. If the child tag `attorney-client` is checked, the document would be tagged as `privileged` and `attorney-client` with a single click. Multiple parent tags and child tags can be applied to any file.

Using the advanced search function discussed above, the case team can search for all documents tagged `privileged`, or more specifically, search only for documents tagged `A/C`. This process can be used for multiple scenarios. You might have a parent tag for `responsive` and child tags for different requests for production. You may want a parent tag for `trial exhibit`, with child tags for witness *X* or `impeachment only`. You may also have a parent tag for a crime with elements as a child. In this way, the tags in the database become another way to search the database records to locate what you need based on the results of the case team's review of records.

When setting up tags, the case team should make sure you put thought into what the tags and groupings should be and set rules for the review team about when the various tags will be used and what they indicate. Using a dozen well-defined tags is more useful in the end than setting up too many. Also, when pulling documents for a particular purpose, be mindful of circumstances where a tag was added midstream through the review process. This is why it is important to reduce your document review protocol to writing and to add refinements—along with the date on which they were implemented—to that protocol. Memorializing mid-stream tag changes allows reviewers to then only run searches and other filtering

[18] Tag palettes—that is, those check boxes the case team can select—can be set up by the administrator when the case is created. Tags can also be created by case team members assuming they have the proper permissions.

mechanisms on documents reviewed before the date of the tag change to identify other relevant documents.

Finally, the case team should consider inserting a free text box into the review panel to allow team members to identify certain key words or concepts that explain the relevance or import of a document. In large-scale review efforts, such text boxes can also be useful to conduct searches later for a particular deal of interest or shorthand for fraud. As with the tagging structure, the case team should define early what concepts or terms should be used in such a text box to avoid having the text simply be additional `noise`.

G. Mass tagging

Tags can be applied individually, but they can also be applied in bulk; so if you have used the search function to identify a key word in the case and used the tally function to limit those results to only emails sent by Jane Doe, you can tag all of them with her name with a few clicks, rather than marking each individually.

Mass tagging, particularly in large data sets, can have really expansive implications, especially when the mass tagging is incorrect or there is a bulk effort to remove a tag across many documents. Think through who you want to have the ability to mass tag or remove tags in bulk before granting such permissions.

H. Redacting and other annotations

Annotations allow you to mark up a document during review. Options include redacting, circling, highlighting, and electronic sticky notes. These actions are visible to the case team while using the review tool. When the documents are produced, however, the case team can decide which annotations it wants to *burn in* to the production. Typically, litigation support staff is asked to produce the files with redactions but without any other annotations for production to opposing counsel.

V. Conclusion

In most of the Department of Justice's (Department) cases, whether civil or criminal, data is ubiquitous. In 2011, an IBM study showed that 90% of the world's data—that is, evidence—had been created in the prior two years.[19] This makes sense as we as individuals continue to add mediums to communicate and those new vehicles of communication create ever-expanding universes of potentially relevant materials. The days in which a prosecutor is able to review ten banker's boxes of documents in support of an insider trading prosecution are over. Now, that prosecutor and her team have to mine through email, text messages, encrypted messaging platforms, social media accounts, and more to find that one coded tip. Getting to that key piece of evidence, that game-changer that will draw a gasp from a jury, is rarely, if ever, attained in today's data environment by simply slogging through every piece of evidence in a linear manner. Rather, the tools described herein provide case teams with an arsenal to whittle away at the noise quickly to most effectively litigate every aspect of a case. Whether it's confronting a witness in a deposition with proof that he knew about a fraudulent scheme despite his protestations or showing a jury an insider trading tip exchanged via Instagram, the review tools described herein will allow case teams to effectively turn the tide on the data tsunami that grows exponentially every day. Effectively using these tools allow Department attorneys and staff to affirmatively leverage data in support of the United States, rather than manage data to survive litigation.

[19] *IBM STUDY: Digital Era Transforming CMO's Agenda, Revealing Gap In Readiness*, IBM (Oct. 11, 2011), https://newsroom.ibm.com/2011-10-11-IBM-Study-Digital-Era-Transforming-CMOs-Agenda-Revealing-Gap-in-Readiness.

About the Authors

Joseph P. Derrig is an Assistant U.S. Attorney in the Eastern District of Washington. Prior to joining the United States Attorney's Office, he worked in private practice and also served in the United States Air Force. Mr. Derrig is currently the electronic discovery coordinator in the Eastern District of Washington and serves as a lawyer representative to the Ninth Circuit. He has also taught classes on e-discovery for the Office of Legal Education at the National Advocacy Center.

Hetal J. Doshi is an Assistant U.S. Attorney in the District of Colorado, where she prosecutes an array of white collar crimes to include complex securities and investment frauds, especially those involving cryptocurrency as well health care fraud and public corruption. She investigated multiple global financial institutions for their roles in the 2008 global financial crisis as part of the Department's Financial Fraud Enforcement Task Force. The resolutions of those investigations are amongst the largest civil penalties in the Department's history. In coordination with the Antitrust Division, she serves as the District of Colorado's Procurement Collusion Strike Force Coordinator and routinely delivers presentations on the use of cryptocurrency to facilitate frauds and money laundering. Prior to joining the Department, she was in private practice, where she worked on complex commercial litigation matters and white collar defense.

Page Intentionally Left Blank

Note from the Editor-in-Chief

These times, they are a-changin'.[1] It used to be that discovery was turned over to the opposing party in a manila envelope or even on a single CD-ROM disc. But those were the good old days. Today, with the ever-advancing technology, delivery methods are not only different, but the discovery itself has a new look: A lot of it is digital, and it's a lot more voluminous in the average case. eLitigation is at the forefront of modern practice, and no attorney wants to be left behind in the past. This issue represents some of the most forward-thinking and creative ideas on this burgeoning topic. I know that it will become your "go to" resource.

Hats off to all the esteemed authors and the discovery experts from the Executive Office for United States Attorneys who helped make this issue possible, especially Andrew Goldsmith, John Haried, Virginia Vance, Susan Cooke, Donna Miller, and Christine Corndorf. And thanks, as always, to the great Office of Legal Education Publications Team—Managing Editor Addison Gantt, Associate Editors Gurbani Saini and Phil Schneider, and our law clerks—who put together this highly technical issue. They make proper citation form of even obscure sources look easy.

Good luck in all your eLitigation endeavors both in and out of court!

Chris Fisanick
Columbia, South Carolina
May 2020

[1] BOB DYLAN, *These Times They are a-Changin'*, on THESE TIMES THEY ARE A-CHANGIN' (Columbia Records 1964).