Originally published in Criminal Justice, Volume 30, Number 4, Winter 2016.

Federal Indigent Defense: How to Stop Worrying and Love the Digital Age

By Sean Broderick and Russell M. Aoki

Today, technology impacts every attorney defending an indigent client against a federal criminal prosecution. Public defenders and private court-appointed counsel increasingly need practical strategies to manage and review valuable evidence hidden like needles within the haystacks of discovery. No longer just a consideration for complex multiple-defendant cases, technology strategies must be considered and effectively employed to address government discovery productions even in "simple" single-defendant prosecutions.

Technology's impact is most felt in the realm of electronic discovery, referred to as "e-discovery" or "ESI" (electronically stored information). Lawyers in large firms with experienced e-discovery staff know how to develop and implement discovery management plans. They understand the importance of usable formats, software tools, and processes specifically designed for the digital age. But the challenges of ESI may be especially daunting for private court-appointed counsel, who are predominantly solo or small-firm lawyers with little exposure to complex e-discovery. Because nearly 90 percent of all defendants in federal criminal cases have court-appointed counsel (either an attorney from the local federal public or community defender office, or a private attorney who accepts Criminal Justice Act (CJA) appointments), it's vital for the integrity of the judicial system that counsel for indigent defendants adapt to the digital era. Broadly stated, the key to adequately addressing e-discovery challenges is understanding the technology and how to strategically use software and resources to efficiently review and manage e-discovery.

The days of paper investigative reports are long gone. Discovery productions now include e-discovery extracted from client computers and mobile devices. Agents look at social media sites like Facebook, Instagram, and Twitter to capture possible incriminating materials. Videos are common and include months of pole-camera recordings, business security videos, and even concealed camera footage. Add in government-created evidence using technology such as cell phone wiretaps, body wires, and GPS tracking devices, and it becomes clear technology is more than the form of discovery: it's the tool to gather evidence, the means to manage evidence, and frequently the evidence itself.

Although tempting, hitting the print button will not solve discovery management problems. Hard copies will not address the mixed-media discovery—the volume is too substantial to print, and critical information will not appear on the paper. Counsel for indigent defendants will lose out on the speed, efficiency, and quality of information that e-discovery can provide when done thoughtfully and produced in reasonably usable formats.

There are several critical issues indigent defense counsel must address to adequately manage and review e-discovery:

- Large volumes of information even in “small cases”;
- A variety of sources (from a multitude of digital devices and locations);
- Proprietary formats;
- Hidden information (metadata and embedded data);
- Differing formats for production; and
- Software and hardware limitations.

Regardless of the size of the firm and the availability of support staff, the challenges of technology and the management of e-discovery can be a time-consuming and distressing distraction, and are compounded by the ticking speedy-trial clock, impatient judges wanting to move the case along, and anxious in-custody clients seeking to review the materials that will be used to prosecute them. To meet these litigation demands and effectively represent their clients, defense counsel must leverage technology support tools for end-to-end discovery management. The solution to e-discovery’s challenges starts with making a plan then implementing it.

Make a Plan

Because public defenders and private court-appointed counsel are rarely appointed pre-indictment, they typically are not aware of specifics of the discovery such as volume and type. It can be particularly challenging to learn how to manage various forms of e-discovery while learning the case. The first step to making a plan is to meet and confer with the government about the nature and volume of e-discovery and the mechanics of producing it, specifically addressing the form of discovery production.

Historically, one of the challenges for all federal criminal practitioners has been the lack of established rules and procedures regarding how to manage e-discovery in criminal cases. Unlike the Federal Rules of Civil Procedure, the Federal Rules of Criminal Procedure are largely silent on how to conduct e-discovery and do not address the form of production. In the absence of rules, an excellent road map for managing post-indictment e-discovery is the *Recommendations for Electronically Stored Information (ESI) Discovery Production in Federal Criminal Cases* (http:// www.fd.org/docs/litigation-support/final-esi-protocol.pdf), also known as the ESI Protocol. This document was produced by the Joint Electronic Technology Working Group (JETWG) with representatives of the Administrative Office of the US Courts’ (AOUSC’s) Office of Defender Services (now called the Defender Services Office, or DSO), the Department of Justice (DOJ), federal public and community defender organizations, private attorneys who accept CJA appointments, and liaisons from the United States judiciary and other AOUSC offices.

Published in 2012 with the support and encouragement of then Deputy Attorney General James Cole on behalf of DOJ, the ESI Protocol outlines 10 principles for managing post-indictment e-discovery. The ESI Protocol is familiar to federal prosecutors, as DOJ trains them in the use of the ESI Protocol in cases involving complex e-discovery, as well as to many federal public defenders, community defenders, and CJA panel attorneys. The document sets forth a collaborative approach to ESI discovery involving mutual and interdependent responsibilities. The goal is to benefit all parties by making ESI discovery more efficient, secure, and less costly.

Considering the guidance of the ESI Protocol and each lawyer's ethical responsibilities, every criminal defense lawyer's analysis of how to strategize e-discovery management should begin with four fundamental principles.

Learn technology. Many criminal practitioners should increase their understanding of e-discovery issues and litigation technology. Without sufficient knowledge in the constantly changing world of technology, counsel may miss potentially beneficial evidence by making critical mistakes early in the case, such as inadvertently choosing production formats they cannot use or that will not help find the evidence they need. The wrong format could cause valuable metadata in electronic records to be missed because counsel was entrenched in printing their discovery. Ethics opinions and the interpretations of the Rules of Professional Conduct are evolving, requiring a lawyer to have an adequate understanding of e-discovery and technology needs. For example, the State Bar of California issued a formal ethics opinion on this subject in the summer of 2015. (*See* State Bar of Cal. Standing Comm. on Prof'l Responsibility & Conduct, Formal Op. 2015-193 (2015).) Though focused on civil litigation, some of the points explicitly mentioned are directly relevant to counsel for indigent clients in federal criminal cases: the ability to initially assess e-discovery needs and issues; identifying custodians of potentially relevant ESI; engaging in competent and meaningful meet-and-confer with opposing counsel concerning an e-discovery plan; and performing data searches. This development follows the 2012 American Bar Association amendment to its Model Rule 1.1, stating that lawyers must "keep abreast of changes in the law and its practice, *including the benefits and risks associated with relevant technology*." (Model Rules of Prof'l Conduct R. 1.1 cmt. 8 (emphasis added).) Lawyers unfamiliar with e-discovery are encouraged to associate or consult with others who have the expertise. Ultimately, however, lawyers remain responsible for e-discovery decisions whether made by staff or third-party vendors. By staying current with technology trends, lawyers can confidently oversee nonlawyer technical assistance.

With state bars emphasizing the ethical issues relating to technology competence, CLE sessions on e-discovery management have become prevalent. Local and national seminars offer educational opportunities from hour-long sessions to multiple-day in-person trainings. Most lawyers know of litigation support specialists, paralegals with experience working e-discovery, or technology consultants who can also give advice.

Develop an early discovery plan based on volume and format. The temptation to dive into a haystack of discovery can be powerful but often proves to be an inefficient strategy for review. Sketching out even a basic plan to address discovery helps to stay focused on the greater and immediate objective of discovery management. A discovery plan typically starts with assessing the volume of materials and the format in which ESI is gathered for production before addressing case-specific issues.

E-discovery volume poses a serious challenge due to the variety of devices on which ESI can be created and stored, the ease of various forms of telecommunication (such as texting and social media), and the declining cost of storage. ESI can come from many sources, such as mobile phones, smartphones, tablets, laptops, desktops, computer network servers, external ESI storage devices (e.g., flash drives or external hard drives), cloud storage, GPS tracking

devices, and social media. The growth of ESI in criminal cases is expected to continue, significantly complicating organization and review of evidence. The presence of e-discovery is not limited to computer and white-collar fraud cases. What once were "straightforward" gun or drug cases may now have smartphones and computers as evidence, with gigabytes or even terabytes of data on the device. Without technological assistance, attorneys cannot review so much data. The greater the volume, the greater the need to identify the necessary technology tools for management and review. The format in which ESI is gathered affects how the data can be used. E-mail messages collected as PDF or text-only files can be searched for particular words or combinations of words. It can be cumbersome to review, sort, and filter the information. But if in the process of collecting the e-mail messages, the metadata is also gathered and produced, then thousands or millions of messages can not only be searched for particular words, but they can also be sorted and filtered in a number of combinations, including by date, custodian, and author or addressee, and software can be utilized to visually demonstrate who communicated with whom and how frequently.

To benefit from the information available in e-discovery, attorneys must know what format the original data was in, what formatting options are available, and how those options affect their potential review of the data. Attorneys who do not understand the various formats should consult with a litigation support expert before receiving or processing their e-discovery.

Meet and confer with the government. The ESI Protocol promotes early conferences with the government to ensure discovery is produced in a usable format. An early meet-and-confer is a valuable opportunity, because voluminous e-discovery cases present difficult challenges for both prosecutors and defense counsel. Missteps at the outset are costly to unwind or correct, and waste time and money. To get the parties to address e-discovery issues early, the ESI Protocol recommends three steps: (1) at the outset, the parties should meet and confer about the nature, volume, and mechanics of producing e-discovery; (2) at the meet-and-confer, the parties should address what is being produced, a table of contents of the discovery, the forms of production, discovery volume, software and hardware limitations, inspection of seized hardware, and a reasonable schedule for producing and reviewing e-discovery; and (3) the producing party should transmit its e-discovery in sufficient time to permit reasonable management and review, and the receiving party should be proactive about testing the accessibility of the ESI when it is received.

Become familiar with litigation support tools. There are numerous software tools available for managing all of the stages of electronic discovery: preserving, collecting, and harvesting data; processing and/or converting ESI; searching and retrieving information; reviewing ESI; and presenting evidence. It can be daunting to determine what tools to use, especially since many can be used for similar tasks. Often, companies name the tasks differently in their computer program, or the program completes the task in a somewhat different way. At this point no single software tool does everything needed for e-discovery. Some tools specialize in processing raw ESI into formats that another tool can then use, while other tools specialize in a discrete function such as document review, strategic analysis, case organization, production of discovery, or trial presentation in the courtroom.

For the solo and small-firm lawyers, litigation software is necessary to work with ESI in its

many formats. Most document review programs allow parties to view hundreds of different file types. DOJ and most civil law firms have managed their own discovery materials with software programs and technical personnel for years. However, many private court-appointed attorneys do not have litigation support software that can view and organize TIFF or native-file productions. (TIFF is a common file format for storing images; "native" refers to a file produced in the format in which it was originally created.) Similarly, most do not have tools to take advantage of a "load file" (a cross-reference file used to import images or data into litigation support databases), extracted metadata, or files in native or near-native ESI format. DOJ may produce discovery in a reasonably usable format, but court-appointed counsel may not utilize the most robust litigation software available to take advantage of the form of production. An important strategy is for computer-challenged defense counsel to seek reasonably useable e-discovery. US attorney's offices can provide e-discovery on disks that contain software for viewing, searching, and tagging documents. For more sophisticated defense counsel, DOJ typically creates load files or otherwise configures its e-discovery productions in industry standard formats. There are instances where typical practices do not work well, such as cases that involve predominantly surveillance materials. Those instances are excellent topics for a meet-and-confer.

Implement Your Plan

Initial review of data. Upon receipt, the discovery should be cataloged by the date received and the contents produced. A second working copy should be made with the original put away for safekeeping. A review of the composition of the data will confirm the volume and format of the discovery to ensure the production is complete and no files became corrupt during the collection or copying process.

The discovery should also be reviewed to determine if documents have been provided in a searchable format, or if they will need to be made searchable prior to loading into a discovery management tool. PDFs in the production should be reviewed to determine if they comprise many documents combined into one PDF, and if so, whether they should be separated into single-document PDFs. The types of documents must also be determined to identify the best method for organizing the data. Defense counsel may want investigative reports to be gathered and prioritized for immediate production and review to address pretrial motions and possible detention issues. Forensic images of computers should be handled separately as they take longer to produce and could take weeks from the time of receipt to analyze. Analysis of forensic computer data requires specialized tools to view while in their forensic state or to unlock for application of keyword searches. Which keywords to use may depend on information revealed in documents such as the investigative reports.

Selection of discovery management tools. Discovery management tools need not be expensive or complicated. The most effective tools are the ones counsel will use. Common business software programs provide features that will allow discovery to be cataloged, searched, and sorted, and are already available in every law firm, big or small. Programs such as Word and Excel all include the ability to create charts and tables, add and search comments, and hyperlink discovery items. Excel includes the ability to filter large quantities of materials to smaller collections. Even loading all the documents into a folder and using Windows Explorer or Apple's Finder for simple keyword searches is an easy and effective method to

locate materials in a small collection of searchable documents. More sophisticated desktop programs provide cost-effective review. Programs like Adobe Acrobat Pro that are designed to create, edit, convert, encrypt, and publish PDF files are excellent tools for managing electronically scanned paper, and provide basic organization, search, and annotation features. Besides providing an easy-to-use PDF-based desktop tool, the program can add Bates numbers or separate documents by page or by bookmarks. CaseMap is another desktop software application specifically designed for case management and analysis of legal and factual issues. It connects case facts, legal issues, key players, and key documents. Defense counsel can store important case information of many file types and generate relational spreadsheets for ready access and analysis. Through searching and flexible filtering, CaseMap enables end users to see how any person, fact, document, or issue relates to other elements in the case. Besides being a database and useful for discovery analysis, it can also create trial notebooks and prepare reports focused on any combination of issues, witnesses, or cross-examination material. Stand-alone sophisticated desktop search engines such as dtSearch can apply sophisticated multiword searches with results ranked based on relevance to the inquiry. Counsel merely assembles the discovery into a folder and points the search engine to index the materials for search capability. The program provides great functionality in searching both electronic documents and paper documents subsequently scanned and converted to a text-searchable format, especially since it can search and retrieve information in many file types.

The next step up in both sophistication and cost are web-hosted document review platforms. They have powerful databases with sophisticated search capabilities and enormous data capacity. Most are linked to multiple servers and can provide complex keyword search strings against millions of documents. The cost can be expensive, but considering the attorney time that would otherwise be spent conducting linear page-by-page review, a web-hosted document review platform can reduce the cost of searching and reviewing huge volumes of discovery. An outside service frees counsel from ensuring the program works properly, is kept secure, and is properly maintained with program updates.

Typically, web-hosted document review platforms entail two major costs. The first is processing, which is the loading of the discovery. Processing includes removing computer and system files that contain no probative evidence and indexing the material to be searchable. The second cost is hosting. Hosting fees are typically charged per month and based on how many gigabytes of data are being hosted. Often associated with monthly hosting are user fees where each end user is assessed a monthly charge. Web-hosted document review platforms are well suited for multiple-defendant prosecutions, involving huge amounts of discovery and defense teams that include support staff, investigators, and experts. These platforms use a database and tools to capture, organize, analyze, and review e-discovery. They enable multiple individuals to access discovery and other case materials through a secure online portal, much like accessing bank account information online. The e-discovery can be searched, retrieved, viewed, and/or printed. Each individual can work collaboratively from his or her respective offices or any location that allows Internet access and privately code or comment on documents for only fellow team members. For multiple-defendant cases, the cost per defense team makes the expense worthwhile.

Selection of outside vendors. Many cases require technical assistance from vendors. The

services could vary from converting proprietary audio and video files into formats for PC and Apple Mac computers, making huge volumes of discovery searchable, or enlisting a web-based database company to process and host discovery.

The most effective way to obtain court funding is to comparison shop for services and prices. One service provider may claim potential costs of $10,000 for a particular service, yet another vendor may do the same work for under $1,000. The cost difference often depends on the skill and experience of the vendor. By obtaining three or four proposals, the court develops greater confidence that the service is cost-effective and a competitive price was obtained. Counsel gains a better sense of the options available, and is more likely to choose tools and services that fit specific needs for the case.

To assist in being able to compare proposals and to get better pricing in complex cases, consider using requests for proposal (RFPs). By developing an RFP, you will better understand the scope of work and increase the likelihood you will get what you want from the system and vendor selected. By providing a customized RFP to prospective vendors, you will be able to compare bids among vendors so that you are not comparing apples to oranges, as many employ different pricing models, charging differently for various services (or not telling you about hidden costs with their proposed solution). In the best-case scenario, the RFP identifies the features and functions counsel believes will help them efficiently and effectively review, search, organize, and analyze the voluminous discovery in a case, while at the same time reducing overall costs. For federal court-appointed lawyers, the National Litigation Support Team (NLST), which is part of the DSO, is available to help attorneys for indigent defendants struggling with extensive e-discovery and can assist in this process.

When planning, technology and outside assistance can come together. For illustrations of how thoughtful planning by counsel, use of appropriate technology, and outside assistance can help overcome e-discovery challenges and provide a solution, consider the following two example cases where counsel for indigent clients (one state, one federal) were able to assist their clients and turn e-discovery from a challenge into an asset.

Wiretap cases can be frustrating and time-consuming for defense counsel. Often they will receive unorganized collections of tens of thousands of captured telephone conversations and a similar amount of linesheets, which are documents memorializing each recorded call. In one recent multidefendant wiretap, the discovery included more than 20,000 recorded calls. Though the discovery was initially produced by the government in proprietary formats, after a meet-and-confer the government was willing to provide the discovery in industry standard formats (computer-generated CSV and PDF files). Defense counsel worked with an outside technology company to create sortable spreadsheets that used an automated process to extract linesheet information (the target number, date, time, duration, and number dialed), break up or "unitize" the multiple-document PDFs that were produced into PDFs each containing only a single recording session, then associate the information to the audio. Though the volume of wiretaps was over 20,000 calls, the work was completed in a few weeks. Using the sort and filter functions of the spreadsheet, counsel could then quickly locate pertinent calls by the target phone number, specific days, particular number dialed, or any combination of these criteria, and display the relevant linesheets hyperlinked to the associated audio. Such a review,

performed manually by counsel and/or paralegals, would have taken hundreds of hours and cost many times over the expense of the vendor's automated program.

In another recent case, defense counsel was presented with a hard drive of discovery that included not only the investigative reports, but also forensically preserved file folders. These folders had to be unlocked to process the data. Counsel forwarded the hard drive to a small technology company and requested a file-type report describing the various files found on the device: e-mail, PDFs, picture files, system files, etc. Besides the file-type report, counsel could obtain a file-path report that showed not only the file types, but also the folder path revealing where the materials were on the hard drive. From this report it was determined that most of the 386 gigabytes of data—primarily program and system files, or iTunes music files—were irrelevant. The file-path report revealed there were only three gigabytes of documents. The technology company then created a sortable, hyperlinked spreadsheet with three worksheets. The first contained documents, the second the audiovisual files, and the third the remaining discovery data. The cost was substantially less than other solutions that a large technology company may have charged for processing the discovery, and much, much less (and more effective) than if counsel had resorted to hitting "print" and attempting to review the materials with eyes on paper.

The solutions described above were case-dependent, and in many instances the solutions required for complex e-discovery cases will take more time and/or resources than described above. But they illustrate the possibilities that exist when counsel representing indigent clients obtain e-discovery in reasonably usable format, leverage the appropriate technology, and strategically use outside resources to efficiently manage e-discovery and better defend their clients.

Defendant's access to e-Discovery when incarcerated

Providing in-custody defendants meaningful access to e-discovery is a significant issue for criminal defense practitioners. As counsel for indigent defendants know, it is important to facilitate access for their defendants as they often can help locate critical evidence much more quickly than defense team members. Importantly, defendant access to e-discovery allows them to assist in their own defense, facilitates attorney-defendant communication, and improves overall advocacy on the defendant's behalf. In 2013, DOJ reported that in recent years 76 percent of federal court defendants were in pretrial custody. With much of the discovery and potential evidence starting in digital form, developing ways for defendants to review e-discovery in digital form is a priority for all involved in the criminal justice system.

There is no easy answer on how to make the many formats of ESI accessible in a facility. Few in-custody defendants are housed in Bureau of Prisons (BOP) pretrial detention facilities. The BOP operates only seven dedicated detention centers. This means most defendants are in one of the approximately 1,800 state, county, or private facilities nationwide—each with varying discovery review policies. Some do not allow discovery in even paper form. Some facilities lack funding to provide discovery computers, lack staff to maintain equipment and monitor its use, or disallow computers due to their concerns regarding security for their particular facility. Yet others are considering tablet devices, but those devices cannot handle the many file types

common with e-discovery.

Even if equipment were available to review more file types, many facilities do not allow executable files (files that load software applications) to be added to inmate-accessible computers. This causes problems when defendants attempt to view many of the common surveillance audio and video files provided in discovery that can only be viewed by using proprietary viewers. Another variation on this problem is a defendant's inability to view files that require an IPRO runtime viewer. DOJ commonly produces TIFF images (a frequent file format for large e-discovery cases) in this manner. However, the IPRO viewer's self-executing feature means it is not allowed in many detention facilities. The files must be converted into a format the facility will allow, which is a time-consuming task defense counsel rarely know how to perform.

In addition, some of the discovery provided consists of unsearchable PDF documents. This causes significant delay in reviewing the discovery, because even the best PDF viewers cannot search PDF documents if the materials are not first made searchable. Defendants are left linearly reviewing discovery page by page. When facilities do allow computers, tablets, or other devices, they often require the attorney to be present with the defendant while he or she reviews the e-discovery. With large amounts of e-discovery, this can become quite time-consuming and costly for the CJA panel system.

JETWG is studying the risks and benefits of allowing inmates access to computers for e-discovery review. It hopes to produce practical recommendations soon, but with the wide variance in facilities and their respective policies, solutions will be difficult to identify. One thing is clear: there is no one-size-fits-all solution to this dilemma. In the interim, counsel working on behalf of indigent defendants should look to work with their local court, prosecution, defenders, CJA panel attorneys or representatives, and detention facility to find a workable solution.

Conclusion

Managing e-discovery is a critical component of today's criminal defense work and appears at first blush to be a daunting subject for most court-appointed counsel. However, taking the time to learn the technology will add a new skill to representing indigent defendants. If counsel is not sure what to do, they should ask those with experience. It may start with their local federal public or community defender office, CJA panel rep, or support staff experienced with managing e-discovery. The ability to manage e-discovery is an expectation of clients, the courts, and even the state bar associations.