Mastering eLitigation: How to Organize the Collection, Review, and Production of Large Volumes of Data in Complex Investigations

Daniel V. Shapiro
Assistant United States Attorney
District of New Jersey

John Haried
Criminal eDiscovery Coordinator
Executive Office for United States Attorneys

I. Introduction

The explosion of digital information has increased the complexity of criminal litigation. Cases that used to have paper investigative reports and business records now have cell tower data, emails, text messages, Facebook chats, Instagram posts, surveillance videos, and more. The challenge of managing all of this digital information becomes even more pronounced in complex long-term investigations.

Complex investigations have unique challenges: large volumes of digital evidence, multiple agents and/or prosecutors during the life span of the case, and significant analysis conducted by the investigative team. Every investigation also requires a dual track. You must gather and preserve evidence in its original state so that it can ultimately be admitted into evidence at trial. At the same time, you must also analyze the collected evidence, which frequently requires the original evidence to be processed in some way to make it more easily reviewed and searched. It is crucial to have a strategy for managing your investigation at the outset of the case. This article will discuss strategies to help prosecutors deal with the large volumes of data involved in complex investigations. It will focus on (1) digital case folder organization, (2) the intake and review of evidence, and (3) tips to avoid the over-collection of digital evidence. We also suggest policies and procedures that will help prosecutors investigate complex cases more quickly, efficiently, and in a way that mitigates litigation risk down the road.

II. The Digital Case Folder

We urge you to keep your case files digitally. In complex investigations, paper files become unmanageable quickly and make it more difficult for multiple members of your team to work on the case at the same time. Every subpoena return, responsive search warrant record, and other documentary evidence and report should be stored on the computer network of the United States Attorney's Office (the "Digital Case Folder"). Evidence must be added to your Digital Case Folder on a rolling basis as it comes in. Your team cannot analyze evidence if you do not have a copy of it or it exists only on a CD or hard drive in your file cabinet. You should maintain physical copies of court documents with original signatures or certified court documents, but the rest of your file should be entirely digital. The original copy of a grand jury subpoena return or search warrant return should ultimately be maintained in accordance with the policies of your district. If a piece of evidence is too large to copy to the Digital Case

Folder or host in-house at the United States Attorney's Office, a plan must be made to store, process, and review the evidence. Options include using the Litigation Technology Service Center, an outside vendor, or working with the investigative agency to process and host the data.

Organize your Digital Case Folders in a logical and consistent way. We suggest that you name your Digital Case Folders using a consistent syntax that includes the USAO number in the folder name. Create a default folder structure to use for all of your cases (or all cases of a certain type) and start using it from the beginning of each case. A sample Digital Case Folder (with some example sub-folders) is set forth below:

Sample Digital Case Folder

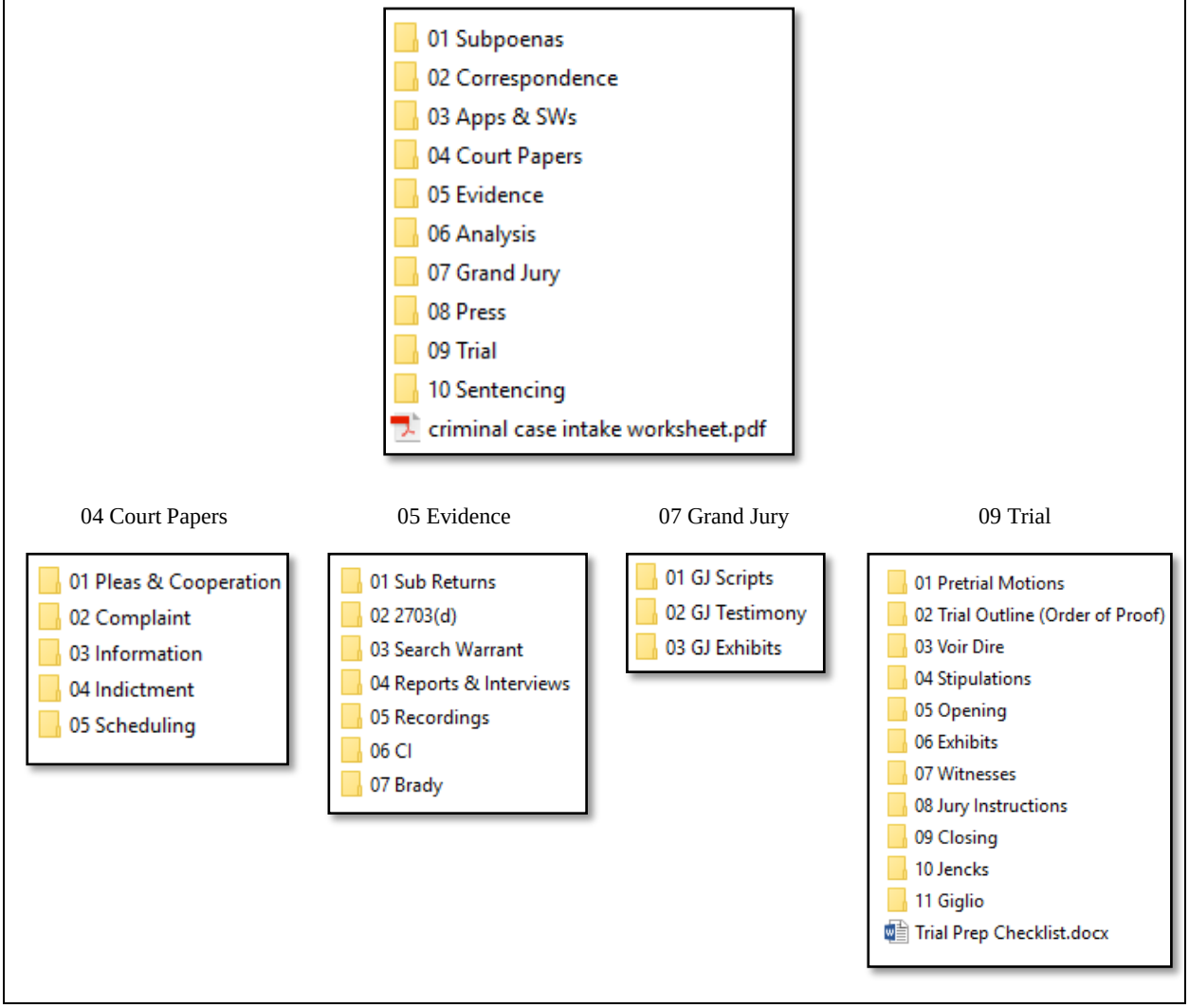

Table 1: Sample Digital Case Folder

Make sure that your Digital Case Folder resides at a location on the network where the rest of your team at your office will have access to it and where supervisors and successor prosecutors would expect to find it. This organization enables legal assistants, paralegals, analysts, and investigators to more effectively work on the case and ensures transitions that are more efficient when members leave and join the investigative team. It also aids in the production of discovery, as further discussed below.

If your district has adopted digital grand jury subpoenas, use them to avoid unnecessary printing and scanning. In cases involving hundreds of subpoenas, this will save a significant amount of time. If you need to restrict access to the Digital Case Folder, speak with your IT staff to limit access.

III. Evidence Intake and Analysis

Most complex investigations have at least five fundamental litigation needs:

1. A method for storing, organizing, and tracking incoming information.
2. A means of converting incoming information from its raw state—paper, native files, PDFs, subpoena returns, etc.—into an electronic format that your evidence review software can handle.
3. Efficient review of voluminous information using evidence review software.
4. A method for organizing the important facts, hot documents, key witnesses, critical investigative reports, and important transcripts that comprise the core of your investigation.
5. A record of what you produced to the opposing party as discovery.

Each of these five needs is addressed below.

A. Storing, Organizing, and Tracking Incoming Information

The starting point is knowing what you have. If you want to understand just how much trouble you can get into by failing to inventory what your investigation has collected, just read *United States v. Pedersen*[1] and *United States v. Toilolo*[2].

No prosecutor should assume the burden of managing and organizing a complex investigation without help. Fully employ and leverage the support staff of paralegals and legal assistants that work with you. Involve them in the organization of your case and the intake of evidence. For large cases, consider having subpoenas returnable to a paralegal at the United States Attorney's Office instead of directly to an investigative agency. The paralegal can then serve as the central point at which subpoenas are (1) received, (2) copied or scanned to the Digital Case Folder, (3) distributed to the investigative agency, and (4) provided to litigation support for processing to be loaded into a review platform.

To prepare for discovery obligations, you should keep a separate area of your Digital Case Folder for pristine copies of the grand jury subpoena returns and other evidence received in your case (for example, the "05 Evidence" subfolder discussed above). Any analysis of that evidence should be conducted on a review platform or using a copy of that evidence in another part of the Digital Case Folder. When it comes time to produce discovery in the case, you will already have a complete set of subpoena returns and other evidence to turn over.

Track your subpoenas using a numbering system that corresponds to the folders where you store the subpoena returns. First, number your subpoenas using the USAO number for the case and the subpoena number. Each page of your subpoena and any attachments should contain the USAO number and subpoena number so that when you receive back subpoena returns that do not reference any subpoena number, but include a business record certification, you will still be able to associate it with a case.

[1] United States v. Pedersen, No. 3:12-CR-00431-HA, 2014 WL 3871197 (D. Or. Aug. 6, 2014) (complex case with discovery from multiple law enforcement agencies. "[T]he government mishandled this case badly. It failed to fulfill its discovery obligations . . .").

[2] United States v. Toilolo, 666 F. App'x 618 (9th Cir. 2016) (government's handling of discovery was "sloppy, inexcusably tardy, and almost grossly negligent[;]" jury instructed on government's misconduct.).

Second, keep a "subpoena returns" folder in your Digital Case Folder organized with folders with the subpoena number and the entity that produced the records, i.e., 001-Citibank. Use leading zeros to ensure that the folders will sort properly, and if you think there may end up being more than 100 subpoenas in the case, use at least two leading zeros.

A successful intake log requires planning and dogged execution. Before your evidence starts coming in, plan what information you will log and who will be responsible for preparing the log. An intake log can be a simple spreadsheet:

Date Rec'd	Rec'd From	Rec'd By	Source / Obtained From	Description	Format
11/20/2014	IRS Agent Harold Crick	Jamaal Jones	GJ Sub #14-472	Wells Fargo records for account xxx-5810	paper
11/22/2014	DEA SA HSchrader	Jamaal Jones	DEA disk 14	Photos - search warrant executed at 124 S Main	.jpeg
11/28/2014	Google	Sally Smith	Google	2703(d) order for getrichnow@gmail.com	.pst

Table 2: Simple Intake Log

Adding a few columns can make a simple intake log more useful:

Label / ID	Quantity	Storage Location	Contains Contraband	Special Handling Instructions	General Notes
FBI thumb drive 14-209	1	FBI – evidence room	☑	Needs redaction of CI info	Emailed agent. Contains contraband CP.
Seagate 500 GB ex HD - #4857-MBD	1	USAO – media storage vault – bin #3429-C	☐	Surveillance video in a proprietary format	Need to convert for discovery.

Table 3: More Intricate Intake Log

We recommend using CaseMap or Excel for intake logs. Using those tools, you can easily sort and search information, add custom columns or hide columns as needed, create separate spreadsheets for main categories (grand jury subpoenas, search warrants, 2703 orders, etc.), and link each item to its supporting documents (subpoenas, law enforcement records, photos), etc. We do not recommend using Word because CaseMap and Excel offer features that are more robust and can readily handle more items.

B. Processing Raw Incoming Information

Once your evidence starts to come in, you need an organized approach to manage and review it. This frequently means using a software tool for efficient review of voluminous documents and other information, as well as software tools to help manage key information. If you are going to use document review software such as Eclipse SE, Relativity, or a similar software, then the incoming raw electronically stored information ("ESI") and paper records must be "processed" to make them usable by the review software. DOJ uses several software tools for processing, including eScanIT, LAW PreDiscovery, Nuix, and similar commercial products. During 2018, EOUSA will deploy Nuix to all United States Attorney Offices and provide training.

Processing software extracts metadata and text from raw ESI. For example, processing software extracts from a collection of emails their metadata—the date sent, sender, recipient, subject, and attachments, as well as the message's text content—and stages that information for loading into review software. That makes it possible for the document review software to give you fast and accurate search results, even from thousands or millions of records. The end product of processing software is a package of instructions—called a load file—that tells the computer what, how, and where to stage your data to make it possible for you to use the powerful features of Eclipse and Relativity.

1. Deduping

Processing software can streamline the review process of certain types of evidence by eliminating duplicative files (commonly called "deduplication" or "deduping"), but you should proceed with caution. For example, processing software can detect and segregate out exact duplicates of files. This can make your search more efficient when reviewing, say, 200,000 corporate emails; otherwise, your word search for "sales incentives" will return 10,000 copies of the same quarterly management motivation email sent to all employees. Similarly, processing software can perform "near-deduplication," which means culling out different file types with the exact same content, for example, the Word and PDF versions of the same document. Reducing the number of hits that are merely duplicates of each other makes your searches and review more efficient. Deduplication is most beneficial when you receive a production of email from a company that includes the email accounts of several employees and that may contain many copies of the same emails. It can also be useful to dedupe when an email provider produces both a preserved copy of an email account and the current contents of that account.

However, the burden in criminal cases to prove an individual defendant's knowledge and mens rea may make it important to know all of the accounts, devices, and locations where an important document was found. You should be aware that deduplication may end up removing copies of an important document from one set of evidence if another copy is found somewhere else in your deduped data (although they will remain in your pristine, original copy of the data). In addition, filter reviews sometimes require a filter attorney to turn over every document that hits on certain keywords to defense counsel. Deduplication may have removed additional copies of documents that hit on those keywords. For these reasons, we advise caution before deduping your entire investigative database or deduping across sources of documents, i.e., deduping multiple email accounts or electronic devices against each other.

2. De-NISTing

Processing software also can segregate out irrelevant files obtained from the search of an electronic device, such as the application files for computer programs like Microsoft Word or Excel, and the operating system files found on a computer. This process is called "de-NISTing." NIST is an acronym for the National Institute of Standards and Technology. NIST maintains the National Software Reference Library, which lists common computer applications. De-NISTing the files collected from a computer can eliminate files that are irrelevant and makes your searches faster. This process is best used when you are interested in reviewing the contents of devices, as opposed to conducting a forensic examination. (A forensic examination to show who controlled the electronic device would require access to operating system files and applications.)

3. Email Threading

"Email threading" is another means of simplifying your searches. An email collection typically includes many email chains consisting of the original message, many replies and responses, and forwarded versions. Processing software will identify the threads of related emails. Email threading puts email chains into chronological order and groups related emails together, thereby improving the speed, accuracy, and completeness of your review. In short, processing software can both cull your data set and focus your review on relevant information.

4. Optical Character Recognition (OCR)

When processing paper records to a digital file, processing software creates a static image of the record in a TIFF (Tagged Image File Format) or PDF, together with the paper document's text obtained by OCR (optical character recognition). This enables computerized word searching, quicker filter review, and easier storage and exchange. However, it is important to note that text obtained by OCR is roughly eighty to ninety percent accurate, which is poor compared to the 100 percent accuracy of text extracted

from ESI. Nonetheless, converting paper records to a digital format permits faster, more efficient, and more complete review compared to review by human eyes on paper.

5. Custodians

There are certain differences between civil and criminal litigation that must be kept in mind when processing data. Processing and document review tools are generally created with civil litigation in mind and not specifically for use in criminal cases. As a result, some of the terminology needs to be adjusted. When processing your evidence, litigation support staff may ask you about the "custodian" field. In a civil litigation where a company has produced voluminous documents, the custodian would likely be the individual to whom the files belong, or from whose office or electronic files the evidence was produced. The vast majority of evidence in a criminal case is not produced this way. We suggest that you typically have the custodian field relate back to the legal process that returned the evidence. For example, the custodian for the Citibank records produced in response to subpoena 001 would simply be 001-Citibank and would match the name of the folder containing those records. For devices obtained from a premises search warrant, the custodian would be the address of the searched premises, e.g., 123 Main Street. Electronic accounts can be organized by the name of the account, e.g., johnsmith@gmail.com. This will also assist you in determining where the evidence originated from when you are reviewing it in your document review platform.

6. Discovery Considerations

You must prepare to be flexible in how you will ultimately produce discovery. Criminal cases differ from civil cases because the judge and defense counsel are unknown until the later phases of an investigation, or until you charge the case. As a result, the preferences of the judge and defense counsel with respect to discovery are also unknown. Processing all of your data, without maintaining an organized complete set of your original data, could be a mistake when defense counsel ultimately asks you for copies of the original evidence you collected.

In addition, processed data is not identical to your original data. It may have been changed during processing and some information may have been removed. For example, depending on the settings used during processing, an email that has been processed may not contain the full detailed header information about all of the computer servers that the email passed through before it was ultimately delivered. If this is important information for your investigation, you should make sure the full email header is extracted during processing. In addition, during discovery you may want to make available copies of the original evidence you received.

C. Software Tools for Reviewing Evidence

At present, USAO litigation teams have two choices for evidence review: Eclipse SE or Relativity. Prosecutors in the other litigating components have different software options.

The document review tools available to United States Attorneys' Offices will help you efficiently execute critical tasks:

- View documents: You can view native files or processed images.
- Identify relevant documents and cull out irrelevant documents: You can cull documents by date range, source, topic, or other characteristics.
- Sort by characteristics: You can sort by date, author and recipient, document type, or other information.
- View, code, and tag: You can view documents (for example, business records, investigative reports), and tag documents (such as hot doc, the issue or witness they relate to, etc.).

- Sophisticated searching: You can search across the different documents in your collection—business records, reports, emails, transcripts, spreadsheets—to identify similar characteristics across data types, much like Westlaw allows you to search for terms and ideas across its information sources. You can also search within searches and by document tags.
- Highlight, annotate, and redact: You can record your value-added assessment of individual documents.
- Track and produce: You can track when and how documents were received and produced as discovery, and create discovery productions in various formats.

It is important to note that to get the most out of document review software, you should request that electronic information be provided to you in either (1) native format (with original metadata), so that it can be processed into a format that Eclipse SE or Relativity can handle, or (2) load files with associated text and TIFF images that can be loaded directly into Eclipse SE or Relativity. You should involve your litigation support technologist early so that they can assist you in navigating the best way to gather and process electronic information so that it is usable.

Eclipse SE allows you to manage your case within your USAO, with help from your litigation support technologist, paralegal, and systems manager. All of your data will be processed and hosted locally at your USAO. Your USAO's practices and procedures with respect to eDiscovery processing, loading, and productions will continue to govern how your case is supported. Access to Eclipse SE for case team members outside of your USAO requires producing a copy of the database with a stand-alone viewer. This production will be static and will not include any information added to the database after the stand-alone copy is created.

Relativity is a robust document review platform that can handle very large cases. Relativity offers advanced analytical searching tools, including concept searching and "find similar" searches, both of which can be more effective than searches for specific terms. It is web-based, meaning your documents reside on a centralized group of servers, and you can access and review them via a web portal. USAOs have access to Relativity through the Litigation Technology Service Center (LTSC), located in Columbia, South Carolina, which can host Relativity databases that are in the range of low single-digit terabytes in size. Data must be sent to the LTSC, where it is processed. Investigative agencies can be given access to the Relativity web portal to access the most up-to-date version of your data. Because the LTSC services all of the districts in the country, individual USAOs have less control over the priority and order in which data is processed. If you want to know whether the LTSC can host your case, talk with your litigation support technologist.

D. Software Tools for Developing Your Case: CaseMap

CaseMap is a digital trial notebook. It helps you organize what is important: the key facts, documents, witnesses, issues, questions, and legal research. CaseMap is a set of interconnected spreadsheets that hold just your key information about facts, people, documents, issues, questions, and legal research. Importantly, you add to the CaseMap file only what information you decide will serve your needs. It is completely customizable. CaseMap helps you create a list of hot documents that you can turn into an exhibit list; an outline of factual and legal issues for charging, motions practice, and trial; a log of subpoenas issued and returned; a file of key case law, statutes, and regulations; and a To-do list. Most importantly, CaseMap is not extra work. It is a more efficient way of capturing the work you are already doing in other ways. If you start putting your work product into CaseMap from the outset, then it is easy and efficient. That means using CaseMap to preserve your thinking about what is critical to building your case—your facts, witnesses, documents, other evidence, issues, and legal research.

CaseMap's fact spreadsheet: The chronology of important facts in your case should (1) refer back to the source evidence that proves the fact, and (2) record the legal process that you used to obtain the evidence. The chronology contains the facts that prove your case. The source documents are what you will use to prove your facts. The legal process used to obtain the evidence will lead you to witnesses that will lay the foundation for introducing the evidence at trial. In CaseMap, the items in the "source(s)" column, below, with the dotted underline are linked from this spreadsheet to the actual electronic file proving the fact.

Date & Time	Fact Text	Source(s)
Thu 02/14/1929 9:30 a.m. CT	Al Capone made a phone call about money from his home.	FBI0001923 - house photo
Thu 02/14/1929 11:40 a.m. CT	2 men dressed as Chicago Police enter 2122 North Clark Street along with 2 men in street	JonesP 302
Thu 02/14/1929 11:43 a.m. CT	Neighbors in vicinity of 2122 North Clark Street hear loud gun fire.	JonesP 302
Thu 02/14/1929 11:46 a.m. CT	Neighbors see 2 police with weapons drawn on 2 men in street clothes exit 2122 North	JonesP 302
Thu 02/14/1929 12:05 p.m. CT	Police and ambulances arrive at 2122 North Clark Street and find the bodies of 6 dead men	FBI0012003 FBI0012004
Wed 05/15/1929	The FBI conducted the search of Al Capone home in Chicago.	FBI0001999

Table 4: Example of an Electronic File

CaseMap's document/evidence spreadsheet: CaseMap gives you spreadsheets to organize information about documents and other evidence, and even links to the item itself, as shown in the "linked file" column:

Doc date	Description	Doc Summary	Source of Doc +	Linked File
Fri 10/31/1028	Johnny Welder's hand-written notes from 10/31/1928.	Johnny Welder's notes about job to cut Chicago Bank & Trust alarms with welding	Investigation	...\Johnny Weld
Thu 02/14/1929	Photo #1 of Valentine's Day Massacre victims' bodies	Shows bodies of Peter Gusenberg, Frank Gusenberg, Albert Weinshank, and Albert	Chicago PD	...\Photo - crim
Wed 04/10/1929	Line Sheet re recorded telephone call from Ronnie	Johnny Torres and Ronnie Garcia discuss an attempt to sell whisky.	Title 3 Wire Tap	...\Line sheet sa
Thu 06/20/1929	USFA Check # 628 to Joe Wimer for $1,360	Proceeds used by Al Capone to pay trigger men	GJ subpoena 29-111	...\Photo - USFA

Table 5: Example of the Linked File Column

CaseMap's witness/persons spreadsheet: CaseMap gives you a spreadsheet you can customize to organize information about your witnesses:

Full Name	Role In Case	Address	Phone Nu...	Email
Allison Becker	FBI tech who monitored intercepted phone calls.	FBI - Chicago	312.555.9999	cbecker@ic.fbi.gov
Joe Boggart	Lead agent for FBI.	FBI - Chicago	312.555.9999	JBoggart@ic.fbi.gov
Byron Bolton	Bolton claims he was involved in the massacre as a look-out,	Federal Witness Protection	Protected	
Al Capone	Mob boss for gang involved in loan sharking, gambling,	1 Lake Shore Drive, Chicago, IL	312.555.1111	ACapone@gmail.com

Table 6: Example of Customizable Spreadsheet

CaseMap gives you similar spreadsheets to organize your witness questions, legal research, and the issues in your case linked to your evidence. In addition, multiple members of your team can access and work in the CaseMap database at the same time.

E. Tracking the Discovery Produced

Finally, tracking what you produced helps you ensure you have complied with your discovery obligations and helps you prove that, in fact, you did produce the item that the opposing attorney claims he never received. Several software tools are effective for creating discovery production log: CaseMap, Eclipse SE, Excel, and others. Here are some types of information that help you know what you produced:

Vol. No.	Bates - Begin	Description	Sent to	Prod date	Notes
2	USB0001-00246	USBank records - acct #123456	Jim Bacon (def atty)	Wed 06/11/193(	Password = JON#002*DSC
3	FBI0090-0099	FBI crime scene photos	Anita Gonzales Jim Bacon Ian Nicholas	Tue 07/01/1930	Password = JON#003*DSC
2	LS_000008	Line Sheet re recorded telephone call	Ian Nichols (def atty)	Wed 06/11/1930	Password = JON#002*DSC
1	FBI0012741	Al Capone's FBI booking sheet	Anita Gonzales (def atty)	Fri 05/02/1930	Password = JON#001*DSC

Table 7: Example of Production Tracking

IV. Seized Electronic Devices

The review of electronic devices searched during an investigation is typically a multi-stage process: (1) seize the device, (2) search the device for material responsive to the search warrant, (3) search the responsive material for potential trial exhibits, and (4) establish the foundation necessary to introduce the potential trial exhibits into evidence at trial. The process of reviewing electronic devices is extremely time- and labor-intensive and should be taken into account when deciding how many electronic devices to seize. The fact that you have probable cause to search a device should not be the end of the

analysis. Don't seize a particular computer or cell phone without a substantial reason. You should conduct a cost-benefit analysis for every electronic device seized. Conducting a forensic review of a single electronic device can take months to complete.

Similarly, as your data grows in size and complexity it consumes more of your time, more of your agent's time, and more of your staff's time. Sensitive information—like personal identification information ("PII") and attorney-client privileged material—may require time-intensive review procedures, including filter team review. At both ends of your workflow—intake and discovery production—higher data volumes mean your litigation support technologist needs much more time for processing, organization, problem solving, and quality control. Just processing voluminous data can take days or weeks. Data storage space is limited, and moving large data sets can be difficult and time consuming. Collecting unnecessary data will gum up your case. Before collecting by seizure or subpoena, try to learn how much data exists, how it is maintained (file types, etc.), and ways to target important information and avoid unimportant information. If possible, create parameters for collections by date ranges, custodians, subject matter, particular transactions, etc. to streamline the amount of data collected.

Finally, many opposing parties and their attorneys simply do not have the technology, staff, and money to review voluminous discovery efficiently. Criminal defendants in pretrial detention and pro se parties have very limited resources. Hence, when you over-collect data, you may be handing the opposing party persuasive grounds to delay trial and drag out the pretrial phase.

V. Conclusion

Based on the tips and strategies in this article, we suggest the policies and procedures below to investigate complex cases more quickly and efficiently.

THE DIGITAL CASE FOLDER
1. Keep a digital copy of all of your investigative files on the network at the United States Attorney's Office. 2. Use standard naming conventions for each case that include the USAO number so others can locate the Digital Case Folder. 3. Use standard folder structures for the Digital Case Folder that are put in place at the beginning of the case.
EVIDENCE INTAKE & ANALYSIS
1. Assign paralegals to complex investigations early. Don't wait until the discovery or trial phase. 2. Use a system to manage and organize the intake of evidence into the Digital Case Folder and put it in place at the beginning of the investigation.

3. Involve Litigation Support early in your investigation.

4. Process data into an evidence review tool, such as Eclipse SE or Relativity, as you receive it.

5. Make sure you understand and discuss with support staff how you want your evidence to be processed before it happens. Discuss deduping, de-NISTing, email threading, and the types of data to extract.

6. Have a method in place to build a chronology for the case.

7. Track the discovery you produce.

AVOID OVER-COLLECTION

1. Even if you have probable cause, don't seize a particular computer or cell phone without a substantial reason.

2. Before collecting by seizure or subpoena, try to learn how much data exists, how it is maintained (file types, etc.), and ways to target important information and avoid unimportant information.

3. Create parameters for collections by date ranges, custodians, subject matter, particular transactions, etc.

ABOUT THE AUTHORS

❑ **Daniel V. Shapiro** is an Assistant United States Attorney in the Economic Crimes Unit and Computer Hacking and Intellectual Property Section of the United States Attorney's Office for the District of New Jersey. He also serves as the Criminal eDiscovery Coordinator for the District of New Jersey and as a member of EOUSA's Electronic Litigation Working Group.

❑ **John Haried** is the Criminal eDiscovery Coordinator for the Executive Office for United States Attorneys (EOUSA) in the Department of Justice. He is an Assistant United States Attorney in the District of Colorado. He is a member of EOUSA's Electronic Litigation Working Group. He is an instructor for the Office of Legal Education at the National Advocacy Center on electronic management of case information and discovery-related topics. He previously wrote for the U.S. Attorneys Bulletin: USAO Options for Managing Small, Medium, and Large Cases (2016); The New Criminal ESI Discovery Protocol (2012); Flying Cars and Web Glasses: How the Digital Revolution is Changing Law Enforcement (2011).