

No. 18-5933

---

**In the Supreme Court of the United States**

---

MARY WILKERSON · PETITIONER

v.

UNITED STATES OF AMERICA · RESPONDENT

---

*ON PETITION FOR A WRIT OF CERTIORARI  
TO THE ELEVENTH CIRCUIT COURT OF APPEALS*

---

APPENDICES

PETITION FOR RECONSIDERATION AND  
REHEARING OF  
MARY WILKERSON,  
In Forma Pauperis

---

# **APPENDIX A**

## **DISCOVERY POLICY MIDDLE DISTRICT OF GEORGIA OCTOBER 2010**

**PAGES 1-5, 7-8, 11, 19-20**

(Updated October 15, 2010)

**DISCOVERY POLICY  
MIDDLE DISTRICT OF GEORGIA  
OCTOBER 2010**

BACKGROUND

On January 4, 2010, Deputy Attorney General Ogden issued a memorandum entitled "Guidance for Prosecutors Regarding Criminal Discovery" ("DAG Ogden Criminal Discovery Guidance." That same date, he issued a memorandum directing that USAOs promulgate discovery policies governing several enumerated issues. This comprehensive discovery policy implements the directives of the Deputy Attorney General.<sup>1</sup>

GENERAL PRINCIPLES

First, the discovery obligations of federal prosecutors in the Middle District of Georgia are established by the Federal Rules of Criminal Procedure, 18 U.S.C. § 3500 (the Jencks Act), *Brady v. Maryland*, 373 U.S. 83 (1963), *Giglio v. United States*, 405 U.S. 150 (1972), and relevant case law, the Department of Justice's policy on the disclosure of exculpatory and impeachment information, the Standard Pretrial Order entered by the District Court after a defendant is arraigned, and the State Bar Rules governing professional conduct. We must comply with the authorities set forth above. Thus, the first principle in the discovery policy for this Office is "**obey all rules.**"

Second, as a general matter and allowing for the exercise of prosecutorial discretion and subject to the needs of individual cases, prosecutors in this District are required to provide discovery beyond what the rules, statutes, and case law mandate ("expansive discovery").

The decision in any particular case on whether, how much, and when to provide materials in excess of that which is required will rest with the prosecutor in a case. There may well be good reason for withholding something that does not have to be disclosed, such as the need to protect a witness or safeguard investigations of other people or other crimes committed by the defendant, or to preserve a legitimate

---

<sup>1</sup>The guidance is subject to legal precedent, court orders, and local rules. It provides prospective guidance only and is not intended to have the force of law or to create or confer any rights, privileges, or benefits. See *United States v. Caceres*, 440 U.S. 741 (1979). This discovery policy does not govern disclosure in cases involving terrorism and national security. Policy concerning these cases will be dependent on guidance currently being developed by the Department.

trial strategy. Keep in mind, however, that expansive discovery may facilitate plea negotiations or otherwise expedite litigation. In the long term, moreover, expansive discovery may foster or support our Office's reputation for candor and fair dealing.

Third, it is required that AUSAs in this District not refer to the office discovery policy as an "open file" policy. The concern about using the term "open file" is that it may be misleading and inexact because there are times that a file may contain attorney work product information and other non-discoverable information.<sup>2</sup>

Finally, cases involving national security, including terrorism, espionage, counterintelligence, and export enforcement, can present unique and difficult criminal discovery issues. The Department of Justice has developed special guidance for those cases, which is contained in Acting Deputy Attorney General Gary G. Grindler's September 29, 2010, memorandum, "Policy and Procedures Regarding the Government's Duty To Search for Discoverable Information in the Possession of the Intelligence Community or Military in Criminal Investigations." Prosecutors should consult that memorandum and their supervisors regarding discovery obligations relating to classified or other sensitive national security information. As a general rule, in those cases where the prosecutor, after conferring with other members of the prosecution team, has a specific reason to believe that one or more elements of the Intelligence Community (IC) possess discoverable material, he or she should consult NSD regarding whether to request a prudential search of the pertinent IC element(s). All prudential search requests and other discovery requests of the IC must be coordinated through NSD.

Although discovery issues relating to classified information are most likely to arise in national security cases, they may also arise in a variety of other criminal cases, including narcotics cases, human trafficking cases, money laundering cases, and organized crime cases. In particular, it is important to determine whether the prosecutor, or another member of the prosecution team, has specific reason to believe that one or more elements of the IC possess discoverable material in the following kinds of criminal cases:

- Those targeting corrupt or fraudulent practices by middle or upper officials of a foreign government;
- Those involving alleged violations of the Arms Export Control Act or the International Emergency Economic Powers Act;
- Those involving trading with the enemy, international terrorism, or significant international narcotics trafficking, especially if they involve foreign government or military personnel;
- Other significant cases involving international suspects and targets; and

---

<sup>2</sup> The decision to discontinue using the term "open file" policy is consistent with the direction given U.S. Attorney Offices from the Deputy Attorney general in his January 4, 2010, Memorandum, Guidance for Prosecutors Regarding Criminal Discovery. A copy of the memorandum is included in the training materials provided AUSAs for the April 2010 training.

- Cases in which one or more targets are, or have previously been, associated with an intelligence agency.

For these cases, or for any other case in which the prosecutors, case agents, or supervisors making actual decisions on an investigation or case have a specific reason to believe that an element of the IC possesses discoverable material, the prosecutor should consult with NSD regarding whether to make through NSD a request that the pertinent IC element conduct a prudential search. If neither the prosecutor, nor any other member of the prosecution team, has a reason to believe that an element of the IC possesses discoverable material, then a prudential search generally is not necessary.

### EXCULPATORY AND IMPEACHMENT MATERIAL

#### 1. BRADY AND GIGLIO

We have constitutional obligations, as set forth in *Brady v. Maryland*, 373 U.S. 83 (1963), and *Giglio v. United States*, 405 U.S. 150 (1972), and other case law, to disclose exculpatory and impeachment information when such information is material to guilt or punishment, **regardless of whether a defendant makes a request for such information**. Exculpatory and impeachment information is deemed material to a finding of guilt when there is a reasonable probability that effective use of that information will result in an acquittal. DOJ policy, however, demands broader disclosure. Prosecutors must take a broad view of materiality and err on the side of disclosure.

#### 2. DOJ POLICY

The Department of Justice has adopted a policy that requires us to go beyond even the strict requirements of *Brady* and *Giglio* and other relevant case law. Specifically:

1. Exculpatory information - information that is inconsistent with any element of the crime or which establishes a recognized affirmative defense, regardless of whether the prosecutor believes the information is admissible evidence or will make a difference between conviction or acquittal.
2. Impeachment information - information that either casts a substantial doubt on the accuracy of any evidence the prosecutor

intends to rely on to establish an element (including but not limited to witness testimony) or which might have a significant bearing on the admissibility of prosecution evidence. This is regardless of whether the prosecutor believes the information is admissible as evidence or will make a difference between conviction and acquittal.

3. Admissibility of the exculpatory or impeachment information - our disclosure requirement applies even when the information subject to disclosure is not itself admissible evidence.
4. Cumulative impact - if the cumulative impact of several pieces of information meets the disclosure requirements, disclose all of the information even if the pieces, considered separately, do not meet the requirements.

See United States Attorney's Manual Section 9-5.001. (A copy is included in the April 2010 training materials.)

### 3. THE "PROSECUTION TEAM" CONCEPT (WHO IS PART OF THE TEAM?)

In some cases, there may be Brady or Giglio material that an agent knows about but the AUSA does not. In 1995, the U.S. Supreme Court made clear that a defendant is entitled to the disclosure of *all* Brady and Giglio material known to *any member of the prosecution team*. See Kyles v. Whitley, 514 U.S. 419, 437-38 (1995). Thus, if any member of the prosecution team knows of any Brady or Giglio material, the AUSA will be held legally responsible for disclosing that evidence to the defendant, whether or not the AUSA actually knows about the evidence. That is, *the AUSA's ignorance of such evidence will not prevent a court from penalizing the government* by suppressing evidence, vacating a sentence, reversing a conviction, or recommending that the AUSA be professionally sanctioned.

*The prosecution team includes all "others acting on the government's behalf in the case."* Kyles, 514 U.S. at 437. At a minimum, this includes *all federal, state, and local law enforcement personnel directly involved in the investigation or prosecution of the federal criminal case*.

### 4. THE AUSA'S RESPONSIBILITIES UNDER *BRADY*

#### A. Communicating with the Case Agent

As noted above, Brady requires the prosecution to disclose to the defendant all *"evidence favorable to [him]" . . . where*

*the evidence is material . . . to guilt," that is, all evidence that could be used by the defendant to make his conviction less likely.*<sup>3</sup>

Although many criminal investigations do not uncover any Brady material, many do.

Ultimately, in any given case, it is the AUSA who decides, based on the AUSA's professional judgment, what evidence is covered by Brady and must, therefore, be disclosed to the defendant. Plainly, the AUSA is responsible for disclosing any Brady material that the AUSA is aware of.

But, as noted above, the Supreme Court has made clear that a defendant is entitled to the disclosure of all Brady material known to the government, *even Brady material "known only to police investigators and not to the prosecutor."* Kyles v. Whitley, 514 U.S. 419, 438 (1995). Thus,

*the individual prosecutor has a duty to learn* of any favorable evidence known to the others acting on the government's behalf in the case, including the police.

Id. at 437.

---

<sup>3</sup> Brady also requires the prosecution to disclose evidence favorable to the defendant concerning punishment.

- Evidence tending to show the absence of any element of the offense, or which is inconsistent with any element of the offense (e.g., evidence showing that an alleged interstate wire transfer was actually an intrastate wire transfer).<sup>5</sup>
- Evidence that either casts a substantive doubt upon the accuracy of evidence including but not limited to witness testimony the AUSA intends to rely on to prove an element of any crime charged, or which may have a significant bearing on the admissibility of prosecution's evidence.<sup>6</sup>
- Evidence tending to show the existence of an affirmative defense, such as entrapment or duress.
- Evidence tending to show the existence of past or present circumstances that might reduce the defendant's guideline range under the federal Sentencing Guidelines, support a request for a sentence at the low end of the guideline range or for a downward departure, or make inapplicable to the defendant a mandatory minimum sentence.

#### C. Looking for *Brady* Material

The government is required only to *disclose* the *Brady* material that the prosecution team knows about. *The prosecution team is not required to look for unknown Brady material.* That's the defendant's job. Indeed, in many cases there will be no *Brady* material for anyone to find.

### 5. THE AUSA'S RESPONSIBILITIES UNDER *GIGLIO*

#### A. Communicating with the Case Agent

The government's constitutional duty to disclose evidence favorable to the defendant includes "*evidence affecting [the] credibility of key government witnesses*" *Giglio v. United States*, 405 U.S. 150, 154 (1972). This duty exists with respect to

---

<sup>5</sup> The AUSA must disclose this information even if he/she does not believe such information will make the difference between conviction and acquittal for a charged crime. USAM § 9-5.001(c).

<sup>6</sup> USAM § 9-5.001(c).



key government witnesses at suppression hearings, trials, and sentencing hearings.

As with Brady material, an AUSA is constitutionally required to disclose all Giglio material that the AUSA *or any other member of the prosecution team* is aware of. The AUSA, consequently, "has a duty to learn of any [Giglio material] known to the others acting on the government's behalf in the case, including the police." Kyles v. Whitley, 514 U.S. 419, 437 (1995).

Accordingly, the AUSA *must* ask the case agent if he/she *or any other member of the prosecution team* knows of any Giglio material on any government witness. The office's mandatory Brady/Giglio form letter to case agents does this. A copy of this is included with the April 2010 training material. The AUSA should repeat this inquiry, orally, before all suppression hearings, trials, and sentencing hearings. Under Kyles, the AUSA is *required* to make these inquiries.

*The primary responsibility for getting Giglio material to the AUSA on civilian witnesses — i.e., government witnesses other than law enforcement witnesses — lies with the case agent. However, in all likelihood the Court will look to us if an issue arises.*

**NOTE:** The separate subject of Giglio material on *law enforcement* witnesses is discussed below. The acquisition by federal prosecutors of evidence that could be used to impeach law enforcement witnesses (particularly evidence of prior agent misconduct) and the disclosure of such evidence to defendants are sensitive matters that are governed by specific rules. Finally, two things should be kept in mind about potential Giglio material that comes to the AUSA's attention: First, the decision to disclose or not disclose impeachment evidence on a *civilian* government witness ultimately rests with the AUSA, and so evidence that is identified as Giglio material by the case agent and provided to the AUSA will not necessarily be disclosed to the court or the defendant. Second, evidence that *is* disclosed to the defendant will not necessarily be admissible at trial. The AUSA should make sure that the case agent understands both of these facts and the AUSA should consult with the Criminal Chief on all issues concerning Giglio matters.

## B. Examples of *Giglio* Material

To decide what evidence is covered by Giglio, one needs to know the ways in which a witness can be impeached. AUSAs should be especially alert to the existence of evidence relating to the first two forms of impeachment described below, namely, a witness's bias and a witness's prior misconduct involving dishonesty.

### 1. Bias

### C. *Giglio* Material on Law Enforcement Witnesses

#### 1. *Generally*

A law enforcement agent who is called as a witness knows (or certainly should know) whether there is anything that exists that could be used to impeach him. That simple fact taken together with the irrebuttable presumption, established in Kyles v. Whitley, that the AUSA knows everything that any member of the prosecution team knows (whether or not the AUSA has such actual knowledge) means that the AUSA will be held legally responsible for disclosing all Giglio material on law enforcement witnesses, even if the AUSA and the case agent have no idea that such material exists. Hence the AUSA absolutely must find out, one way or another, if there is any Giglio material on any employee of a law enforcement agency — whether federal, *state, or local* — who will or might be a witness at any suppression hearing, trial, or sentencing hearing. The two forms of impeachment that will come into play most often with law enforcement witnesses are bias and specific instances of misconduct involving dishonesty, which are discussed above.

#### 2. *The Attorney General's Giglio Policy*

In recognition of the tension that may arise between AUSAs and agents because of Giglio, the Attorney General issued a directive, dated December 9, 1996, entitled "*Policy Regarding the Disclosure to Prosecutors of Potential Impeachment Information Concerning Law Enforcement Agency Witnesses ('AG's Giglio Policy')*." This policy was amended on October 19, 2006, to conform to the Department's new policy regarding disclosure of exculpatory and impeachment evidence. (This is included as a separate attachment for the April 2010 training.) By its own terms, the AG's Giglio Policy governs only the DOJ law enforcement agencies (FBI, USMS, DEA, INS). But the Secretary of the Treasury has adopted the AG's Giglio Policy for the Treasury agencies as well. See United States Attorneys' Manual § 9-5.001.

There are three methods an AUSA can use to learn whether there is any potential Giglio material on a law enforcement witness.

**First**, the AUSA can ask the witness. In this regard, the AG's Giglio Policy provides:

It is expected that a prosecutor generally will be able to obtain all potential impeachment information directly from potential agency witnesses and/or affiants. Each investigative agency employee is **obligated to inform** prosecutors with whom they work of potential impeachment information as early as possible prior to providing a sworn statement or testimony in any criminal investigation or case.

have their own established procedures for retaining information about those witnesses. The agencies may keep multiple files containing different types of records or information. Thus, inquiries to agencies about informants should include a review of every kind of file that might contain information about the individual.

3. Evidence/information obtained via subpoena, search warrants, or other legal process. With respect to electronically-stored evidence, including e-mails, sufficient time must be allotted for a search of hard drives, disks and other storage hardware. These searches may take a long time, so they should be undertaken well before indictment.
4. Evidence/information gathered by civil or regulatory agencies in parallel investigations.
5. Substantive communications/correspondence including e-mails, text messages, and letters, between and among prosecutors, agents, witnesses, victims, victim-witness coordinators, etc.
6. Potential *Giglio* information about non-law enforcement witnesses (including declarants whose hearsay statements the government might seek to introduce at trial). Ask the case agent to run a criminal history report on all non-law enforcement witnesses.

#### C. Trial Preparation Interviews

When preparing a witness for a hearing or trial, be very aware of our continuing obligation to disclose information that might be exculpatory or have impeachment value. Thus, if a witness provides information that conflicts in material ways with information the witness has previously provided, or conflicts with material information provided by other witnesses, we should disclose that conflict to the defendant.

***PRACTICE TIP:*** *What is the standard? Measure any conflicting information provided by a witness against the standards set forth in the DOJ Policy, United States Attorney's Manual section 9-5.001.*

### 11. PREPARING DISCOVERY MATERIALS FOR AND MAKING THE DISCLOSURE

#### A. Bates Labeling/Electronic Storage of Materials (One Option)

##### 1. Bates labeling.

As documents are gathered during the course of an investigation, you should

make a complete and organized record of what has been gathered by the prosecution team. You should Bates label the documents. This process can be done very quickly with office software. **Do not Bates label original documents.** Scan the originals and Bates label the electronic version. The originals should be kept in the order and condition in which they were obtained.

***PRACTICE TIP:*** *It is recommended that you Bates label the documents in a way that will allow you to determine the source of the documents. (It is also recommended that you keep a record or log containing a description of the documents, the Bates numbers, the source of the documents, and how they were obtained). For example, in an investigation of John Doe, rather than simply Bates labeling all documents in numerical order with no reference to the source, you may wish to Bates label that bank's records as DOE.Bank ABC.0001 - 1000, or in a similar fashion. Documents obtained via search warrant might be labeled DOE.SW.0001-1000. You might use the initials "VP" to indicate voluntary production.*

*It is not necessary to include the target's name in the label, and you may ultimately choose to label documents in any manner that fits the needs of your particular case. Whatever system you use, however, please ensure that you have a record system that will allow you, as well as any person who might have to deal with the documents at a later time (including the Office's FOIA contact), to determine the source of the documents and how they were obtained. It is important that we be able to determine if records were obtained via the grand jury, in order to ensure that we comply with the secrecy requirements of Rule 6 of the Federal Rules of Criminal Procedure.*

## **2. Formatting.**

You may format the documents using either the .tif or the .pdf file format. You may also choose to use OCR (optical character recognition) for the documents. OCR will allow the documents to be searched for particular words or terms.

***PRACTICE TIP:*** *The recent trend, particularly in large, document-intensive cases, is to provide documents with OCR. The defense will in all likelihood ask the court for documents to be disclosed in a searchable format. Consult with a member of our litigation support staff or other trained office employee about using either Adobe, eScan-IT, or other software to use OCR on documents.*

## **B. Grand Jury Materials**

### **1. Handling grand jury materials.**

The Department of Justice has guidelines for obtaining and handling evidence pursuant to grand jury subpoena. See United States Attorney's Manual section 9-11.254; *Federal Grand Jury Practice Manual*, Chapter 6 (October 2008). Specific points to remember:

# **APPENDIX B**

**U. S. DEPARTMENT OF JUSTICE**

**CRIMINAL DIVISION**

**OCTOBER 2010**

**DISCOVERY POLICY**

**Page 1, 17, 18**



U.S. Department of Justice

Criminal Division


Office of the Assistant Attorney General

Washington, D.C. 20530

October 18, 2010

MEMORANDUM

TO: All Criminal Division Attorneys

FROM: Lanny A. Breuer   
Assistant Attorney General

SUBJECT: Criminal Division Policy Regarding Discovery Practices

INTRODUCTION

This policy is intended to provide guidance on the Criminal Division's discovery practices and rules related to disclosure.<sup>1</sup> It is designed to facilitate Criminal Division (CRM) Attorneys' compliance with disclosure obligations, to identify common discovery-related issues of which all CRM Attorneys should be aware, and to ensure that CRM Attorneys have adequate resources and guidance available to enable them to make appropriate disclosure decisions, either on their own or in consultation with the leadership of their section and the Division. In general, this policy encourages earlier and more liberal disclosure by Division prosecutors than either the Constitution or law requires. This policy is also intended to be sufficiently flexible to give attorneys discretion where permitted by law and to account for the fact that CRM Attorneys operate in jurisdictions throughout the nation that have different discovery rules and practices.

**Overview of the Policy**

The discovery obligations of CRM Attorneys are established by the Federal Rules of Criminal Procedure, 18 U.S.C. § 3500 (the Jencks Act), *Brady v. Maryland*, 373 U.S. 83 (1963), *Giglio v. United States*, 405 U.S. 150 (1972), relevant case law, the Department of Justice's policy on the disclosure of exculpatory and impeachment information, applicable Local Rules of Criminal Procedure, discovery orders entered in particular cases, and the rules governing professional conduct. All CRM Attorneys must comply with the authorities set forth above. In addition, as set forth more fully in this guidance, it is the policy of the Criminal Division to provide discovery beyond what the rules, statutes, and case law mandate. When faced with a close call as to whether certain information should be disclosed, CRM Attorneys should err on the side of

<sup>1</sup> This policy guidance is intended to satisfy the January 4, 2010 directive from the Deputy Attorney General to develop a discovery policy with which CRM prosecutors must also comply. See "Requirement for Office Discovery Policies in Criminal Matters," Memorandum dated January 4, 2010. The guidance, which is solely prospective, is for internal CRM use only and does not create any privileges, benefits, or rights, substantive or procedural, enforceable by any individual, party, or witness in any administrative, civil, or criminal matter.

- d. The investigative agency *must* keep track of the defense's *access* to all documents. It is recommended that the agent present the defense with a list of the bates numbers to which the defense is being given access and ask for a signature of the reviewing defense attorney.
2. Electronically Stored Information. CRM Attorneys should consider the disclosure of electronically stored information ("ESI") on a case-by-case basis, in consultation with the agents and the relevant USAO.
- a. If documents are in electronic form, the CRM Attorney should consider providing electronic copies on DVD.
  - b. For electronic evidence seized by warrant, CRM Attorneys should consider having a tech agent pull word processing documents, spreadsheets, databases, emails and other substantive files off of drives and provide that data on disc.
  - c. For an entire computer imaged pursuant to warrant, CRM Attorneys should consider making a forensic image available to the defense by allowing the defense to supply a blank hard drive onto which the tech agent would copy the forensic image. (As described below in paragraph (d)(i), there is an open question as to what portions of imaged computers to disclose to the defense if the warrant authorizes the government to review only limited files.)
  - d. CRM Attorneys must disclose ESI in accordance with the same discovery provisions governing disclosure of non-ESI, including Rules 16 and 26.2, *Brady*, and *Giglio*. Similarly, CRM Attorneys who know, or have reason to believe, that otherwise discoverable ESI includes child pornography, should provide counsel for the defendant a reasonable opportunity to inspect the contraband pursuant to 18 U.S.C. § 3509(m). If the otherwise discoverable ESI contains other forms of contraband, the CRM Attorneys should consider either providing the defendant with an opportunity to inspect the materials, or providing a copy of the materials to the defendant subject to a protective order.
    - i. In those cases where the complete contents of ESI have not been reviewed by the government, either because of limitations in the scope of a warrant or because of the volume of stored material, the CRM Attorney should consider whether there is a statutory or other prudential reason for not disclosing the unexamined ESI. If the CRM Attorney determines that non-disclosure is warranted, the attorney should notify defense counsel of the non-disclosure and the basis for the non-disclosure.
  - e. Be prepared to work with the defense to ensure it can review ESI. You may need to provide access to a terminal and/or technical assistance, especially if the defense lacks financial resources.

3. Large Volumes of Documents. When providing the defense with access to a large number of bankers boxes of documents, consider providing a general index of documents (e.g., "search records," "bank records," "phone records" will often suffice). Also, when dealing with massive amounts of data and a defense lacking resources, consider whether to provide the defense with "hot docs" or search terms. Consult with your supervisor before disclosing such work product.

**D. What to Disclose:** CRM Attorneys bear ultimate responsibility for disclosure decisions. Disclosure of records and physical objects collected as part of the investigation should be as broad as possible, in order to avoid situations where withheld records or objects are later determined to be relevant to the government's case in chief or to the preparation of the defense. That said, as noted above, the government's discovery policy is not "open file" discovery, and this term should never be used to describe it. CRM Attorneys should consult with any participating AUSAs before making disclosures.

1. Materials that must be disclosed:
  - a. *Brady*, Jencks, and *Giglio* materials.
  - b. All materials required by Fed. R. Crim. P. 16 and 26.2, including statements of the defendant under Rule 16(a)(1)(A) and (B).
  - c. Exculpatory and impeachment materials required by USAM § 9-5.001.
  - d. Additional materials or information required by any discovery order entered by the court.
2. Additional materials for which disclosure should be strongly considered, even where they do not fall into the categories described in paragraph 1 above, include:
  - a. Materials obtained pursuant to grand jury subpoena.
  - b. Documents provided voluntarily by potential witnesses, including cooperating defendants/targets.
  - c. Search warrant materials.
  - d. Other relevant materials collected in the course of the investigation.
3. What may be withheld (unless they contain *Brady* or *Giglio* material):
  - a. CRM Attorney notes (but see subsection 4 below).
  - b. Agent rough notes, where they are formalized in a final MOI (but see subsection 4 below).
  - c. Other materials subject to attorney/client, work product (not including witness MOIs), or deliberative process privileges (but see subsection 4 below).
  - d. Reports and grand jury transcripts of non-testifying witnesses, unless they are transcripts of employees of an organizational defendant, disclosure of which is governed by Fed. R. Crim. P. 16(a)(1)(C).
  - e. Other materials collected in the course of the investigation that are not arguably relevant to the case charged.



## **APPENDIX C**

### **Supreme Court**

### **Guidelines for the Submission of Documents to the Supreme Court's Electronic Filing System**

### **Rule 29.7**

**SUPREME COURT OF THE UNITED STATES  
OFFICE OF THE CLERK  
WASHINGTON, D.C. 20543**

---

**GUIDELINES FOR THE SUBMISSION OF DOCUMENTS TO  
THE SUPREME COURT'S ELECTRONIC FILING SYSTEM**

---

These guidelines govern the submission of documents to the electronic filing system at the Supreme Court of the United States. They are issued pursuant to Supreme Court Rule 29.7, and are effective beginning November 13, 2017.

**1. Electronic Submission Requirement.** Filings submitted by parties represented by counsel (with the exception of material addressed in paragraphs 7, 9 and 14 below) must be submitted through the Court's electronic filing system. This requirement is in addition to the existing requirements concerning the paper filing of documents with the Court. This requirement applies to all documents required or permitted to be presented to the Court or a Justice, unless otherwise directed by Court Rule, these Guidelines, or other communication from the Clerk's Office. Documents should be submitted through the electronic filing system contemporaneously with their filing pursuant to Rule 29.2, *i.e.*, at or near the time they are delivered to the Court, placed in the mail, delivered to a third-party carrier, etc.

Only the following types of letters to the Court should be submitted through the electronic filing system: (1) motions for an extension of time under Rule 30.4, and responses thereto; (2) notices under Rule 12.6 of a petitioner's view that a party below no longer has an interest in the outcome of a petition, and responses thereto; (3) amendments to corporate disclosure statements or party name changes; (4) substitutions of public officers under Rule 35.3; (5) renewed applications under

Rule 22.4; (6) waivers of the 14-day waiting period under Rule 15.5; (7) blanket consents to the filing of *amicus* briefs; and (8) letters that are submitted in response to a specific request from the Court. Any other letters or correspondence to the Court should be submitted in paper form only.

**2. Registration.** Before submitting documents through the electronic filing system, attorneys must register at <https://file.supremecourt.gov>. Only members of the Supreme Court Bar and attorneys appointed for a particular case under the federal Criminal Justice Act are eligible to register. As part of the registration process, an attorney will establish a username and password that will enable the attorney to submit documents through the system. Users must protect the security of their username and password, and must notify the Clerk's Office immediately upon learning that either has been compromised. Users also have a responsibility to keep contact information up-to-date; changes to contact information can be made through the "My Account" link on the electronic filing system home page.

**3. Notice of Appearance.** Attorneys are required to enter a notice of appearance in a case before submitting filings on behalf of a party or *amicus curiae* in that case. The submission of a case-initiating document (*e.g.*, a petition for a writ of certiorari, a jurisdictional statement, a petition for an extraordinary writ, or an application not connected to an existing case) will serve as a notice of appearance for the filer. But a filer seeking to submit any other filings in a case will be required to enter a notice of appearance in that case. The notice of appearance is created and submitted entirely through the system itself; no separate paper document need be submitted, and no PDF need be uploaded. While it is permissible for multiple attorneys to submit notices of appearance on behalf of the same party, the requirement that a party have a single counsel of record remains in effect. If an attorney no longer represents a party in this Court, the attorney should submit a withdrawal of appearance through the system. This withdrawal will also be entirely electronic; no paper document need be submitted, and no PDF need be uploaded.

**4. Format of Documents.** Documents submitted through the electronic filing system should be in the PDF/A format. Where possible, the electronic file should be created from a word processing document and should be text searchable. Where possible, the electronic version of a document with a signature (including

letters to the Court, certificates of compliance with word limitations under Rule 33(h), and proofs of service under Rule 29.5) should also be created from a word processing document and be text searchable; the version submitted through the electronic filing system need not contain a physical signature. Items included in an appendix to a filing may be scanned if a word-processing document is not available. A document submitted through the electronic filing system may contain hyperlinks to another part of the same document, or to an external source cited in the document.

**5. Maximum Size of Documents.** The maximum size of any single computer file that can be uploaded to the electronic filing system is 100MB. Documents larger than 100MB should be separated into multiple parts to allow each part to be under this limit.

**6. Viruses and Malware.** Before submitting any document through the electronic filing system, the filer should ensure that the document has been scanned for viruses and malware. The electronic filing system will also perform a scan for viruses and malware, and it will not accept a filing until the scan has determined that the entire document does not pose a risk of infection for the system. In most instances, the scan should be completed within 3-5 minutes of the time that a document has been uploaded. (Note that the "Summary" page for a filing will update automatically to reflect when the scan has been completed.)

**7. Documents Containing Sealed Material.** Documents containing material that is under seal, including documents filed under seal in lower courts and motions to file documents under seal in this Court, should *not* be submitted through the electronic filing system. Those documents (including redacted versions for the public record) should be submitted only in paper form. Such documents also should not be served upon other parties electronically. Filers are admonished to pay strict attention to the prohibition, since documents submitted through the electronic filing system may be posted publicly before personal review by Clerk's Office staff.

**8. Redaction of Personal Identifying Information.** Personal identifying information contained in filings must be redacted in keeping with the standards set forth in Rule 34.6. No motion is required to make redactions to conform with this rule. Nothing in the rule precludes a party from filing a motion

to redact additional information in appropriate circumstances. The responsibility to redact this information rests with counsel and the parties.

**9. Cases Governed by Fed. R. Civ. P. 5.2(c).** In cases governed below by Federal Rule of Civil Procedure 5.2(c), including immigration cases addressed in Federal Rule of Criminal Procedure 49.1(c), filings by the parties should not be submitted through the electronic filing system. *A cover letter provided along with the petition for a writ of certiorari, application for an extension of time to file a petition for a writ of certiorari, or other case-initiating document should clearly state that the case was governed by Rule 5.2(c).*

**10. Posting of Documents.** Electronic versions of all documents filed with the Court (except those containing sealed material or otherwise exempt from electronic posting) will be made available to the public without charge on the Supreme Court's website at <http://www.supremecourt.gov>.

(a) Filings that initiate a new case at the Supreme Court will be posted on the Court's website only after the Clerk's Office has received and reviewed the paper version of the filing, determined that it should be accepted for filing, and assigned a case number.

(b) Subsequent filings from represented parties that are submitted through the electronic filing system will be posted upon electronic submission to the system. Such filings will initially be noted on the docket as "Submitted." Once the Clerk's Office has received and reviewed the paper version of the document and determined that it should be accepted for filing, the docket will reflect that the document has been "Filed." If a document is not accepted for filing, the docket entry will reflect that it is "Not Accepted for Filing," and an electronic version of the document will no longer be accessible.

(c) Paper filings from parties not represented by counsel will be scanned by the Clerk's Office and posted on the Court's website once the Clerk's Office has reviewed the filing and determined that it should be accepted for filing.

**11. Service and Notification of Case Activity.** Registered users who have entered an appearance in a given case will receive automated email notification of all action in that case, including filings by other parties. This

notification does not constitute official service, and parties remain obligated to effect formal service as outlined in the Rules of the Court. The system will also have the ability to provide notification of case activity to email addresses of attorneys and other legal professionals actually working on the case.

**12. Changes to Filings.** Once a document is submitted through the electronic filing system, the filer will no longer have the ability to withdraw the electronic filing or make changes to it through the system. In the event that a filer needs to make a change to the document that was submitted, the filer should contact the Clerk's Office.

**13. Filing Fees.** Filers submitting through the electronic filing system will continue to pay filing fees, where applicable, by check. If a fee is required, the filing will not be docketed until the fee is received.

**14. Supreme Court Bar Matters.** Documents relating to membership in the Supreme Court Bar, including responses to rules to show cause why a member of the Court's Bar should not be disbarred, should not be submitted through the electronic filing system. Such documents should be submitted only on paper.

**15. Technical Problems.** A filer who is unable to submit documents through the system due to technical problems can contact the Clerk's Office for assistance at [efilingsupport@supremecourt.gov](mailto:efilingsupport@supremecourt.gov) or 202-479-5660. Clerk's Office personnel will be available to respond to telephone inquiries between 9:00 am and 5:00 pm on days that the Clerk's Office is open under Rule 1.3. In the event that a technical problem is discovered after working hours and the deadline to file is before the Clerk's Office reopens, the filing should be emailed to other parties and to [efilingsupport@supremecourt.gov](mailto:efilingsupport@supremecourt.gov). The inability to submit a document through the electronic filing system due to technical problems does not affect the timeliness of the filing, but the Clerk's Office generally will not docket filings from attorneys until they are submitted through the electronic filing system.

**Updated: November 20, 2017**

## APPENDIX D

U. S. DEPARTMENT OF JUSTICE

Memorandum of

Sally Q. Yates,

Deputy Attorney General

January 5, 2017



U.S. Department of Justice

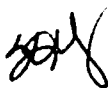
Office of the Deputy Attorney General

The Deputy Attorney General

Washington, D.C. 20530

January 5, 2017

MEMORANDUM FOR DEPARTMENT PROSECUTORS  
DEPARTMENT FORENSIC SCIENCE PERSONNEL

FROM: Sally Q. Yates   
Deputy Attorney General

SUBJECT: Supplemental Guidance for Prosecutors Regarding Criminal Discovery  
Involving Forensic Evidence and Experts

Forensic evidence is an essential tool in helping prosecutors ensure public safety and obtain justice for victims of crime. When introduced at trial, such evidence can be among the most powerful and persuasive evidence used to prove the government's case. Yet it is precisely for these reasons that prosecutors must exercise special care in how and when forensic evidence is used. Among other things, prosecutors must ensure that they satisfy their discovery obligations regarding forensic evidence and experts, so that defendants have a fair opportunity to understand the evidence that could be used against them.

In January 2010, then-Deputy Attorney General David Ogden issued a memorandum entitled *Guidance for Prosecutors Regarding Criminal Discovery* (the "Ogden Memo"), which provided general guidance on gathering, reviewing, and disclosing information to defendants.<sup>1</sup> Given that most prosecutors lack formal training in technical or scientific fields, the Department has since determined that it would be helpful to issue supplemental guidance that clarifies what a prosecutor is expected to disclose to defendants regarding forensic evidence or experts. Over the past year, a team of United States Attorneys, Department prosecutors, law enforcement personnel, and forensic scientists worked together to develop the below guidance, which serves as an addendum to the Ogden Memo.

All Department prosecutors should review this guidance before handling a case involving forensic evidence. In addition, any individuals involved in the practice of forensic science at the Department, especially those working at our law enforcement laboratories, should familiarize themselves with this guidance so that they can assist prosecutors when the government receives a request for discoverable material in a case. Thank you for your attention to this issue and for the work you do every day to further the proud mission of this Department.

---

<sup>1</sup> Memorandum from David W. Ogden, Deputy Attorney General, to Department Prosecutors, *Guidance for Prosecutors Regarding Criminal Discovery*, January 4, 2010, available at [http://dojnet.doj.gov/usao/eousa/olc/usabook/memo/ogden\\_memo.pdf](http://dojnet.doj.gov/usao/eousa/olc/usabook/memo/ogden_memo.pdf).



## SUPPLEMENTAL GUIDANCE FOR PROSECUTORS REGARDING CRIMINAL DISCOVERY INVOLVING FORENSIC EVIDENCE AND EXPERTS<sup>1</sup>

Forensic science covers a variety of fields, including such specialties as DNA testing, chemistry, and ballistics and impression analysis, among others. As a general guiding rule, and allowing for the facts and circumstances of individual cases, prosecutors should provide broad discovery relating to forensic science evidence as outlined here. Disclosure of information relating to forensic science evidence in discovery does not mean that the Department concedes the admissibility of that information, which may be litigated simultaneously with or subsequent to disclosure.

### The Duty to Disclose, Generally

The prosecution's duty to disclose is generally governed by Federal Rules of Criminal Procedure 16 and 26.2, the Jencks Act (18 U.S.C. §3500), *Brady v. Maryland*, 373 U.S. 83 (1963), and *Giglio v. United States*, 405 U.S. 150 (1972). In addition, §9-5.001 of the United States Attorney's Manual describes the Department's policy for disclosure of exculpatory and impeachment material.

Rule 16 of the Federal Rules of Criminal Procedure establishes three disclosure responsibilities for prosecutors that may be relevant to forensic evidence. First, under Fed. R. Crim. P. 16(a)(1)(F), the government must, upon request of the defense, turn over the results or reports of any scientific test or experiment (i) in the government's possession, custody or control, (ii) that an attorney for the government knows or through due diligence could know, and (iii) that would be material to preparing the defense or that the government intends to use at trial. Second, under Fed. R. Crim. P. 16(a)(1)(G), if requested by the defense, the government must provide a written summary of any expert testimony the government intends to use at trial. At a minimum, this summary must include the witness's opinions, the bases and reasons for those opinions, and the expert's qualifications. Third, under Fed. R. Crim. P. 16(a)(1)(E), if requested by the defense, the government must produce documents and items material to preparing the defense that are in the possession, custody, or control of the government. This may extend to records documenting the tests performed, the maintenance and reliability of tools used to perform those tests, and/or the methodologies employed in those tests.

Both the Jencks Act and *Brady/Giglio* may also come into play in relation to forensic evidence. For example, a written statement (report, email, memo) by a testifying forensic witness may be subject to disclosure under the Jencks Act if it relates to the subject matter of his or her testimony. Information providing the defense with an avenue for challenging test results may be *Brady/Giglio* information that must be disclosed. And, for forensic witnesses employed by the government, *Giglio* information must be gathered from the employing agency and reviewed for possible disclosure.

These are the minimum requirements, and the Department's discovery policies call for disclosure beyond these thresholds.

---

<sup>1</sup> This document is not intended to create, does not create, and may not be relied upon to create any rights, substantive or procedural, enforceable at law by any party in any matter civil or criminal.

## The Duty to Disclose in Cases with Forensic Evidence and Experts

The Department's policy to provide discovery over and above the minimum legal thresholds applies to cases with forensic evidence. Rule 16's disclosure requirements – disclosing the results of scientific tests (16(a)(1)(F)), the witness' written summary (16(a)(1)(G)), and documents and items material to preparing the defense (16(a)(1)(E)) – are often jointly satisfied when presenting expert forensic testimony, since disclosure of the test results, the bases for those results, and the expert's qualifications will often provide all the necessary information material to preparation of the defense. But, depending on the complexity of the forensic evidence, or where multiple forensic tests have been performed, the process can be complicated because it may require the prosecutor to work in tandem with various forensic scientists to identify and prepare additional relevant information for disclosure. Although prosecutors generally should consult with forensic experts to understand the tests or experiments conducted, responsibility for disclosure ultimately rests with the prosecutor assigned to the case.

In meeting obligations under Rule 16(a)(1)(E), (F), and (G), the Jencks Act, and *Brady/Giglio*, and to comply with the Department's policies of broad disclosure, the prosecutor should be attuned to the following four steps:

1. First, the prosecutor should obtain the forensic expert's laboratory report, which is a document that describes the scope of work assigned, the evidence tested, the method of examination or analysis used, and the conclusions drawn from the analyses conducted. Depending on the laboratory, the report may be in written or electronic format; the laboratory may routinely route the report to the prosecutor, or the prosecutor may need to affirmatively seek the report from the forensic expert or his or her laboratory. In most cases the best practice is to turn over the forensic expert's report to the defense if requested. This is so regardless of whether the government intends to use it at trial or whether the report is perceived to be material to the preparation of the defense. If the report contains personal information about a victim or witness, or other sensitive information, redaction may be appropriate and necessary. This may require court authorization if the forensic expert will testify, as the report likely will be considered a Jencks Act statement. (See the Additional Considerations section below.)
2. Second, the prosecutor should disclose to the defense, if requested, a written summary for any forensic expert the government intends to call as an expert at trial. This statement should summarize the analyses performed by the forensic expert and describe any conclusions reached. Although the written summary will vary in length depending on the number and complexity of the tests conducted, it should be sufficient to explain the basis and reasons for the expert's expected testimony. Oftentimes, an expert will provide this information in an "executive summary" or "synopsis" section at the beginning of a report or a "conclusion" section at the end. Prosecutors should be mindful to ensure that any separate summary provided pursuant to Rule 16(a) should be consistent with these sections of the report. Further, any changes to an expert's opinion that are made subsequent to the initial disclosure to the defense ordinarily should be made in writing and disclosed to the defense.

3. Third, if requested by the defense, the prosecutor should provide the defense with a copy of, or access to, the laboratory or forensic expert's "case file," either in electronic or hard-copy form. This information, which may be kept in an actual file or may be compiled by the forensic expert, normally will describe the facts or data considered by the forensic expert, include the underlying documentation of the examination or analysis performed, and contain the material necessary for another examiner to understand the expert's report. The exact material contained in a case file varies depending on the type of forensic analysis performed. It may include such items as a chain-of-custody log; photographs of physical evidence; analysts' worksheets or bench notes; a scope of work; an examination plan; and data, charts and graphs that illustrate the results of the tests conducted.

In some circumstances, the defense may seek laboratory policies and protocols. To the extent that a laboratory provides this information online, the prosecutor may simply share the web address with the defense. Otherwise, determinations regarding disclosure of this information should be made on a case-by-case basis in consultation with the forensic analysts involved, taking into account the particularity of the defense's request and how relevant the request appears to be to the anticipated defenses.

4. Fourth, the prosecutor should provide to the defense information on the expert's qualifications. Typically, this material will include such items as the expert's curriculum vitae, highlighting relevant education, training and publications, and a brief summary that describes the analyst's synopsis of experience in testifying as an expert at trial or by deposition. The prosecutor should gather potential *Giglio* information from the government agency that employs the forensic expert. If using an independent retained forensic expert, the prosecutor should disclose the level of compensation as potential *Giglio* information; the format of this disclosure is left to the discretion of the individual prosecuting office.

Disclosure should be made according to local rules but at least as soon as is reasonably practical and, of course, reasonably in advance of trial. It is important that the prosecutor leave sufficient time to obtain documents and prepare information ahead of disclosure. When requesting supporting documents from a laboratory's file regarding a forensic examination, the prosecutor should consult the guidelines set by the laboratory for the manner in which discovery requests should be made, and for the time required for them to process and deliver the materials to the prosecutor. Further, if multiple forensic teams have worked on a case, the prosecutor should build in sufficient time to consult with, and obtain relevant materials from, each relevant office or forensic expert.

### **Additional Considerations**

Certain situations call for special attention. These may include cases with classified information or when forensic reports reveal the identities of cooperating witnesses or undercover officers, or disclose pending covert investigations. In such cases, when redaction or a protective order may be necessary, prosecutors should ordinarily consult with supervisors.

Laboratory case files may include written communications, including electronic communication such as emails, between forensic experts or between forensic experts and prosecutors. Prosecutors should review this information themselves to determine which communications, if any, are protected and which information should be disclosed under *Brady/Giglio*, Jencks, or Rule 16. If the circumstances warrant (for example, where review of a case file indicates that tests in another case or communications outside the case file may be relevant), prosecutors should request to review additional materials outside the case file. At the outset of a case, prosecutors should ensure that they and all forensic analysts involved are familiar with and follow the Deputy Attorney General's memorandum entitled "Guidance on the Use, Preservation, and Disclosure of Electronic Communications in Federal Criminal Cases": [http://dojnet.doj.gov/usao/eousa/ole/usabook/memo/dag\\_ecom.pdf](http://dojnet.doj.gov/usao/eousa/ole/usabook/memo/dag_ecom.pdf).

Finally, when faced with questions about disclosure, prosecutors should consult with a supervisor, as the precise documents to disclose tend to evolve, based especially upon the practice of particular laboratories, the type and manner of documentation at the laboratory, and current rulings from the courts.

## **APPENDIX E**

### **9.5.001 Policy Regarding Disclosure of Exculpatory and Impeachment Information**

## 9-5.000 - ISSUES RELATED TO DISCOVERY, TRIALS, AND OTHER PROCEEDINGS

<u>9-5.001</u>	Policy Regarding Disclosure of Exculpatory and Impeachment Information
<u>9-5.002</u>	Criminal Discovery
<u>9-5.003</u>	Criminal Discovery Involving Forensic Evidence and Experts
<u>9-5.100</u>	Policy Regarding the Disclosure to Prosecutors of Potential Impeachment Information Concerning Law Enforcement Agency Witnesses ("Giglio Policy")
<u>9-5.110</u>	Testimony of FBI Laboratory Examiners
<u>9-5.150</u>	Authorization to Close Judicial Proceedings to Members of the Press and Public

### 9-5.001 - POLICY REGARDING DISCLOSURE OF EXCULPATORY AND IMPEACHMENT INFORMATION

- A. **Purpose.** Consistent with applicable federal statutes, rules, and case law, the policy set forth here is intended to promote regularity in disclosure practices, through the reasoned and guided exercise of prosecutorial judgment and discretion by attorneys for the government, with respect to the government's obligation both to disclose exculpatory and impeachment information to criminal defendants and to seek a just result in every case. The policy is intended to ensure timely disclosure of an appropriate scope of exculpatory and impeachment information so as to ensure that trials are fair. The policy, however, recognizes that other interests, such as witness security and national security, are also critically important, see JM 9-21.000, and that if disclosure prior to trial might jeopardize these interests, disclosure may be delayed or restricted (e.g. pursuant to the Classified Information Procedures Act). This policy is not a substitute for researching the legal issues that may arise in an individual case. Additionally, this policy does not alter or supersede the policy that requires prosecutors to disclose "substantial evidence that directly negates the guilt of a subject of the investigation" to the grand jury before seeking an indictment, see JM 9-11.233.
- B. **Constitutional obligation to ensure a fair trial and disclose material exculpatory and impeachment evidence.** Government disclosure of material exculpatory and impeachment evidence is part of the constitutional guarantee to a fair trial. *Brady v. Maryland*, 373 U.S. 83, 87 (1963); *Giglio v. United States*, 405 U.S. 150, 154 (1972). The law requires the disclosure of exculpatory and impeachment evidence when such evidence is material to guilt or punishment. *Brady*, 373 U.S. at 87; *Giglio*, 405 U.S. at 154. Because they are Constitutional obligations, *Brady* and *Giglio* evidence must be disclosed regardless of whether the defendant makes a request for exculpatory or impeachment evidence. *Kyles v. Whitley*, 514 U.S. 419, 432-33 (1995). Neither the Constitution nor this policy, however, creates a general discovery right for trial preparation or plea negotiations. *U.S. v. Ruiz*, 536 U.S. 622, 629 (2002); *Weatherford v. Bursey*, 429 U.S. 545, 559 (1977).
1. **Materiality and Admissibility.** Exculpatory and impeachment evidence is material to a finding of guilt—and thus the Constitution requires disclosure—when there is a reasonable probability that effective use of the evidence will result in an acquittal. *United States v. Bagley*, 475 U.S. 667, 676 (1985). Recognizing that it is sometimes difficult to assess the materiality of evidence before trial, prosecutors generally must take a broad view of materiality and err

on the side of disclosing exculpatory and impeaching evidence. *Kyles*, 514 U.S. at 439. While ordinarily, evidence that would not be admissible at trial need not be disclosed, this policy encourages prosecutors to err on the side of disclosure if admissibility is a close question.

2. **The prosecution team.** It is the obligation of federal prosecutors, in preparing for trial, to seek all exculpatory and impeachment information from all the members of the prosecution team. Members of the prosecution team include federal, state, and local law enforcement officers and other government officials participating in the investigation and prosecution of the criminal case against the defendant. *Kyles*, 514 U.S. at 437.

**C. Disclosure of exculpatory and impeachment information beyond that which is constitutionally and legally required.** Department policy recognizes that a fair trial will often include examination of relevant exculpatory or impeachment information that is significantly probative of the issues before the court but that may not, on its own, result in an acquittal or, as is often colloquially expressed, make the difference between guilt and innocence. As a result, this policy requires disclosure by prosecutors of information beyond that which is "material" to guilt as articulated in *Kyles v. Whitley*, 514 U.S. 419 (1995), and *Strickler v. Greene*, 527 U.S. 263, 280-81 (1999). The policy recognizes, however, that a trial should not involve the consideration of information which is irrelevant or not significantly probative of the issues before the court and should not involve spurious issues or arguments which serve to divert the trial process from examining the genuine issues. Information that goes only to such matters does not advance the purpose of a trial and thus is not subject to disclosure.

1. **Additional exculpatory information that must be disclosed.** A prosecutor must disclose information that is inconsistent with any element of any crime charged against the defendant or that establishes a recognized affirmative defense, regardless of whether the prosecutor believes such information will make the difference between conviction and acquittal of the defendant for a charged crime.
2. **Additional impeachment information that must be disclosed.** A prosecutor must disclose information that either casts a substantial doubt upon the accuracy of any evidence—including but not limited to witness testimony—the prosecutor intends to rely on to prove an element of any crime charged, or might have a significant bearing on the admissibility of prosecution evidence. This information must be disclosed regardless of whether it is likely to make the difference between conviction and acquittal of the defendant for a charged crime.
3. **Information.** Unlike the requirements of *Brady* and its progeny, which focus on evidence, the disclosure requirement of this section applies to information regardless of whether the information subject to disclosure would itself constitute admissible evidence.
4. **Cumulative impact of items of information.** While items of information viewed in isolation may not reasonably be seen as meeting the standards outlined in paragraphs 1 and 2 above, several items together can have such an effect. If this is the case, all such items must be disclosed.

**D. Timing of disclosure.** Due process requires that disclosure of exculpatory and impeachment evidence material to guilt or innocence be made in sufficient time to permit the defendant to make effective use of that information at trial. See, e.g. *Weatherford v. Bursey*, 429 U.S. 545, 559 (1997); *United States v. Farley*, 2 F.3d 645, 654 (6th Cir. 1993). In most cases, the disclosures required by the Constitution and this policy will be made in advance of trial.

1. **Exculpatory information.** Exculpatory information must be disclosed reasonably promptly after it is discovered. This policy recognizes that exculpatory information that includes classified or otherwise sensitive national security material may require certain protective measures that may cause disclosure to be delayed or restricted (e.g. pursuant to the Classified Information Procedures Act).

## **APPENDIX F**

**The Champion**

**National Association of Criminal Defense Lawyers**

**September/October 2018 Issue**

**“Unable to Bear the Weight of the ‘Document  
Dump’:**

**A Heavy Burden on the Individuals and an  
Increasing Threat to Due Process”**

**By**

**Drew Findling, President of NACDL**



THE National Association of Criminal Defense Lawyers®

# CHAMPION®

September/October 2018

NACDL.ORG

White Collar Crime





# FROM THE PRESIDENT

DREW FINDLING

## Unable to Bear the Weight of the 'Document Dump': A Heavy Burden on Individuals and an Increasing Threat to Due Process

Most of us have been part of the proverbial "document dump" by the government. We have experienced the feeling of dread as we are told to come pick up a hard drive (or several) rather than a disc or packet of discovery. Those hard drives often contain hundreds of gigabytes (GB) and sometimes several terabytes of documents and other media, resulting in millions upon millions of pages that we as defense attorneys are obligated to review. The mass production of discovery connotes a corporate investigation or white collar case, where often financial resources are available to properly parse through and analyze the evidence purported by the government. The reality is that in 2018, "document dumps" are no longer relegated to white collar and/or corporate cases. Increasingly, large quantities of discovery are turned over in a wide variety of matters involving individual defendants.

Why is this happening? Take a second and think about how much time you spend each day on your cellphone, tablet, and computer. Think about the volume of texts, emails, photos, and voicemails that are stored on your devices at any given time. It is a difficult number to quantify, and yet we are increasingly being asked to do just that as complete downloads of electronic devices are becoming common discovery items in all types of criminal cases. This is the reality of modern communication, and it is reshaping both the way cases are prosecuted and how we perform our roles as defense attorneys. What began as a major issue in white collar cases has now expanded to the point that almost any case can become burdened with gigabytes of electronic discovery.

The early 2000s saw a massive increase in the quantity of electronically stored information (ESI) being produced by the government in white collar cases. The courts recognized that the criminal discovery rules did not adequately address these new ESI issues. To address this, the Joint Electronic Technology Working Group was established in 1998 to create recommendations on managing ESI in federal criminal cases.<sup>1</sup> While these recommendations have helped to standardize production of ESI in federal cases, it has not addressed the hurdles individuals charged in these cases must overcome to defend themselves, nor has there been similar guidance provided at the state level, where substantial ESI production is becoming more common in a variety of cases. Both the financial and manpower costs of reviewing ESI are becoming a growing problem that continues to threaten the liberty of the accused across the nation.

The first problem presented by the increase in ESI production is the problem of how to find *Brady* material. In *United States v. Skilling*, the defendant argued that the sheer volume of material produced by the government (several hundred million pages) made it impossible to successfully identify favorable material contained within and thus the government was functionally suppressing those materials.<sup>2</sup> The court rejected that argument because the government

highlighted specific documents that it thought were potentially relevant to the defendant's case and provided indices to other documents. The court did provide, however, specific examples of government conduct that would be improper:

We do not hold that the use of a voluminous open file can never violate *Brady*. For instance, evidence that the government "padded" an open file with pointless or superfluous information to frustrate a defendant's review of the file might raise serious *Brady* issues. Creating a voluminous file that is unduly onerous to access might raise similar concerns. And it should go without saying that the government may not hide *Brady* material of which it is aware in a huge open file in the hope that the defendant will never find it. These scenarios would indicate that the government was acting in bad faith in performing its obligations under *Brady*.<sup>3</sup>

Cases like *Skilling* give us a basic framework to rely on in our push for the government to do more than simply turn over millions of pages of documents to meet its *Brady* obligation.

The goal of setting guidelines for ESI format production was to standardize production generated by a multitude of sources into a consistent format. The resulting recommendation, which is generally followed by the DOJ,<sup>4</sup> is that the party provide either the native file or a single image file of each page and an accompanying optical character recognition (OCR) file with the same name as the image file.<sup>5</sup> In theory,



Photo by Johnathon Kelsa @johnathonkelsa

Drew Findling is principal of The Findling Law Firm, which he founded after serving as an Assistant Public Defender in Fulton County, Georgia. He has tried federal and state criminal cases throughout the United States and has spoken in CLEs in over 40 states. He is a recipient of the Heeney Award, the NAACP's Civil and Human Rights Award, a commendation by the Legislative Black Caucus of Georgia, and GACDL's Indigent Defense Award.

### DREW FINDLING

Findling Law Firm  
Atlanta, Georgia  
404-460-4500

EMAIL [drew@findlinglawfirm.com](mailto:drew@findlinglawfirm.com)  
WEBSITE [www.findlinglawfirm.com](http://www.findlinglawfirm.com)  
TWITTER @drewfindling  
INSTAGRAM @drewfindling



this should create a searchable OCR file without formatting and an accompanying image file of the original. While the conversion to OCR may make each document individually searchable, this does little to combat the total size of documents that needs to be searched. Additional software is still required to make the discovery manageable, all at additional cost to the defendant. These programs are commonly utilized by firms that handle complex civil matters, where the field of ESI discovery management is far more developed but remains fairly unknown to the average criminal law practitioner.

The costs for file hosting and licensing required to efficiently review and process sizable ESI discovery can easily rival and sometimes far exceed that of any expert and creates a threshold defense issue. Unlike an expert whose billing will vary greatly from month to month, discovery vendor costs are consistent throughout the duration of the case. Average market rates for ESI hosting and software licensing range from \$100-\$150 per GB per month. For reference, e-discovery vendors estimate 3,000 documents per gigabyte based on DOJ production methods. For a 300,000-document production, which is small in a white collar case, the accused is looking at \$2,000-\$2,500 per month. It is not uncommon for cases to take from months to years before reaching trial, and during that time the client is incurring continually mounting costs to maintain access to discovery. Defendants are being required to spend thousands per month as additional legal fees just to be able to understand the strength of the evidence against them. And these costs will continue to accumulate for the duration of the case as the attorney is dependent on third-party licensing and file hosting for meaningful access to discovery.

Outside of the white collar context, substantial production of ESI has expanded to drug cases, gang cases, small conspiracies, and virtually every case that involves multiple defendants or unindicted co-conspirators. This ESI commonly manifests itself as extensive chat logs acquired from social media websites and computer/cell-phone downloads. For reference, Snapchat currently has over 300 million active users and 187 million daily active users.<sup>6</sup> Instagram has over 800 million active users and 500 million daily active users.<sup>7</sup> Facebook boasts an incredible 2.072 billion global active users and 1.66 billion global daily active users.<sup>8</sup> As more people utilize social media as a platform for communication, so too do law enforcement

agencies increasingly seek logs of communication from these platforms to investigate and bolster their cases. For example, it is unsurprising to see months of communication logs from Snapchat, Instagram, and Facebook in addition to traditional text message and phone communication logs in both state and federal drug cases. In a 2012 survey, over 80 percent of law enforcement officers interviewed had used social media to assist in investigations.<sup>9</sup>

Similarly, modern cellphones can have anywhere from 8 GB to 256 GB of storage. A common law enforcement practice is to obtain a warrant and perform a full download of any cellphone found on a defendant at the time of arrest and provide that in discovery. This functionally transforms what would have been in the early 2000s a case involving a few documents to a case in 2018 requiring an extensive ESI review. Stored text communications, social media communications, photographs, videos, and even recently visited websites could contain valuable exculpatory information.

As recently noted in NACDL's trial penalty report, there has been a continuing 50-year decline in the percentage of cases going to trial.<sup>10</sup> Substantial production of ESI compounds this problem by generating pretrial costs that the accused must absorb. It takes no great imagination to envision a defendant who, confronted with the monthly cost of reasonable access to discovery, would take a quick plea rather than undertaking those expenses to fight the case. In many cases these expenses are not only burdensome but also prohibitive, and they have constitutional implications. When individuals lack the resources to pay for meaningful access to discovery, their right to due process, right to confront witnesses, and right to meaningful assistance of counsel are all being substantially limited.

When Criminal Justice Act (CJA) and federal defender organization (FDO) attorneys represent indigent defendants in cases involving substantial ESI production, additional resources are available to help alleviate these costs through the Administrative Office (AO) of the United States Courts. The AO has Coordinating Discovery Attorneys on staff who can provide expertise and resources for handling ESI. However, this does not address the broad class of defendants who do not qualify for CJA and FDO services but also cannot afford the prohibitively expensive software licenses needed for meaningful access to discovery. The increased expenses for access to discovery and the additional time required to review the discovery make cases longer

and costlier. The accused must absorb the cost of review and consequences of pretrial release or pretrial incarceration while defense counsel sifts through the voluminous production in the case.

How can we avoid a public defender office having to dedicate its already limited resources to spending hours reviewing Snapchat logs and Facebook messages? How do we avoid solo practitioners having to turn down cases because they simply no longer have the time to review thousands of pages of Instagram communications between co-defendants? NACDL members must make a unified push, at both the state and federal levels, to force the government to share the costs and burdens generated by its voluminous ESI production.<sup>11</sup> We must argue that simply turning over a 64 GB cellphone download does not meet the requirements of *Brady* without additional direction.

In a recent case in South Carolina, my office, along with NACDL member Rauch Wise, was lucky enough to have a senior district court judge who would not tolerate the government's attempts to utilize large scale ESI production to overwhelm our client and hinder his resources.<sup>12</sup> In that case, we represented an individual charged with making a false statement in the context of a much larger FCPA investigation. The government produced over 600,000 documents (1.8 million pages), prompting the defense team to request additional time to review discovery and request that the court order the government lawyers to direct us to both the documents they planned to present in their case-in-chief and any *Brady* materials. The court relentlessly pushed lawyers for the government on why they provided so much discovery for a single count false statement case, and the court required them to state on the record how many documents would be used in their case-in-chief. When pressed, the government claimed it needed less than 20 documents to present its case. Without that additional intervention from the court, our client would have been spending thousands per month to third parties so that we could review hundreds of thousands of documents the government had no intention of using.

Prior to the court's intervention, we interviewed multiple e-discovery vendors and were given price quotes ranging from \$3,500 to \$6,000 per month to host the documents and provide us access to their proprietary software, which would have been necessary to make the documents searchable. Without that software we estimated it would take approximately 15,000



hours to complete review of all discovery provided. Thankfully, in South Carolina we had a judge who understood that the government should not be permitted to use ESI document dumps as a weapon against the accused. Document dumps undermine the defendant's due process rights by hiding *Brady* material and essentially reversing the roles for locating favorable material. In a time when less than three percent of federal cases go to trial,<sup>13</sup> and when there are incentives at both the state and federal levels for an accused to enter an early plea, we cannot allow the government to abuse the discovery process as an additional tactic to coerce accused individuals into guilty pleas because they lack the resources to handle ESI discovery.

## Notes

1. Dep't of Justice and 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* (2012), available at <http://www.fd.org/docs/litigation-support/final-esi-protocol.pdf>.

2. 554 F.3d 529 (5th Cir. 2009).

3. *Id.* at 577.

4. David W. Ogden, Guidance for Prosecutors Regarding Criminal Discovery 165 (2010), available at <https://www.justice.gov/usam/criminal-resource-manual-165-guidance-prosecutors-regarding-criminal-discovery>.

5. *Id.*

6. Salman Aslam, Snapchat by the Numbers: Stats, Demographics & Fun Facts (2018), available at <https://www.omnicoreagency.com/snapchat-statistics>.

7. *Id.*

8. *Id.*

9. Role of Social Media in Law Enforcement Significant and Growing (2012), available at <https://www.lexisnexis.com/en-us/about-us/media/press-release.page?id=1342623085481181>.

10. NAT'L ASS'N CRIM. DEFENSE LAWYERS, THE TRIAL PENALTY: THE SIXTH AMENDMENT RIGHT TO TRIAL ON THE VERGE OF EXTINCTION AND HOW TO SAVE IT (2018), available at [www.nacdl.org/trialpenaltyreport](http://www.nacdl.org/trialpenaltyreport).

11. NACDL, in a joint effort with the New York Council of Defense Lawyers (NYCDL), has proposed a new federal Rule 16.1 to address the increase in ESI in federal cases. The proposed rule would require counsel for both sides to meet within 14 days after arraignment to confer and try to agree on a timetable and procedures for pretrial disclosures under Rule 16.

12. *United States v. Charley Hill*, 8:17-CR-01187 (2018).

13. *Supra* note 10. ■

## NACDL® STAFF DIRECTORY

MEMBERSHIP HOTLINE 202-872-4001

Senior Resource Counsel	Vanessa Antoun	202-465-7663	vantoun@nacdl.org
Director of Events	Akvile Athanason	202-465-7630	aathanason@nacdl.org
Assistant to the Executive Director	Tatum A. Brooks	202-465-7657	tbrooks@nacdl.org
National Affairs Assistant	Shuli Carroll	202-465-7638	scarroll@nacdl.org
Grant Manager	Tom Chambers	202-465-7625	tchambers@nacdl.org
Senior Editor, The Champion®	Quintin M. Chatman	202-465-7633	qchatman@nacdl.org
Membership Director	Michael Connor	202-465-7654	mconnor@nacdl.org
Education Assistant	Cori Crisfield	202-465-7643	ccrisfield@nacdl.org
Resource Counsel	Jessica DaSilva	202-465-7646	jdasilva@nacdl.org
Senior Director of Public Affairs and Communications	Ivan Dominguez	202-465-7662	idominguez@nacdl.org
Junior Graphic Designer	Julian Giles	202-465-7655	jgiles@nacdl.org
Director of Public Defense Reform and Training	Bonnie Hoffman	202-465-7649	bhoffman@nacdl.org
Education & Research Associate Fourth Amendment Center	Wendy Lee	202-465-7652	wlee@nacdl.org
Associate Executive Director for Programs, Business Services, and Technology	Gerald Lippert	202-465-7636	glippert@nacdl.org
Senior Privacy and National Security Counsel	Jumana Musa	202-465-7658	jmusa@nacdl.org
Public Affairs & Communications Assistant	Ian Nawalinski	202-465-7624	inawalinski@nacdl.org
Associate Executive Director for Policy	Kyle O'Dowd	202-465-7626	kodowd@nacdl.org
Sales and Marketing Manager	Jason Hawthorne Petty	202-465-7637	jpetty@nacdl.org
Senior Litigation Counsel	Michael Price	202-465-7615	mprice@nacdl.org
Director of Advocacy	Monica L. Reid	202-465-7660	mreid@nacdl.org
Executive Director	Norman L. Reimer	202-465-7623	nreimer@nacdl.org
Graphics Assistant	Saira Rivera	202-465-7635	srivera@nacdl.org
Member Services Assistant	Nelle Sandridge	202-465-7639	nsandridge@nacdl.org
Senior Membership and Operations Associate	Viviana Sejas	202-465-7632	vsejas@nacdl.org
Information Services Manager	Doug Shaner	202-465-7648	dshaner@nacdl.org
Fourth Amendment Center Fellow	Zachary Simonetti	202-465-7659	zsimonetti@nacdl.org
Public Defense Reform and Training Counsel	Renee Spence	202-465-7651	rspence@nacdl.org
Associate Executive Director for Strategic Marketing	Jessica Stepan	202-465-7629	jstepan@nacdl.org
Manager — Multimedia Production & Sales	Koichi Take	202-465-7661	ktake@nacdl.org
Counsel for Special Projects and Foundation Manager	Daniel Weir	202-465-7640	dweir@nacdl.org
Art Director	Catherine Zlomek	202-465-7634	czlomek@nacdl.org

# APPENDIX G

## CRIMINAL E-DISCOVERY

### A Pocket Guide for Judges

Sean Broderick

Donna Lee Elm

Andrew Goldsmith

John Haried

Kiran Raj

Federal Judicial Center

2015

Pages 1-16

# CRIMINAL E-DISCOVERY

## *A Pocket Guide for Judges*

SEAN BRODERICK

*National Litigation Support Administrator  
Administrative Office of the U.S. Courts, Defender Services Office*

DONNA LEE ELM

*Federal Defender  
Middle District of Florida*

ANDREW GOLDSMITH

*Associate Deputy Attorney General & National Criminal Discovery Coordinator  
U.S. Department of Justice*

JOHN HARIED

*Co-Chair, eDiscovery Working Group — EOUSA  
U.S. Department of Justice*

KIRAN RAJ

*Senior Counsel to the Deputy Attorney General  
U.S. Department of Justice*

**Federal Judicial Center  
2015**

This Federal Judicial Center publication was undertaken in furtherance of the Center's statutory mission to develop educational materials for the judicial branch. While the Center regards the content as responsible and valuable, it does not reflect policy or recommendations of the Board of the Federal Judicial Center.

second printing

## Table of Contents

<b>I. Overview</b>	1
A. Lack of Criminal e-Discovery Guidance	1
B. Civil e-Discovery Rules and Practices Do Not Lend Themselves to Criminal e-Discovery	2
C. A Practitioner's Guide to Criminal e-Discovery	4
<b>II. Common Issues in Criminal e-Discovery</b>	5
A. Funding the Defendant's e-Discovery	5
B. Lack of ESI Experience, Knowledge, and Competency	10
C. Necessity of Litigation Support Assistance	11
D. The Workflow in Processing ESI	12
E. Varieties of Evidence-Review Software	13
F. Volume of e-Discovery	13
G. Form of Production — ESI Formats	14
H. Form of Production — Paper Formats	16
I. Disorganized and Redundant ESI	17
J. Providing Incarcerated Defendants Access to e-Discovery	17
K. Multiple Defendants	18
<b>III. Judicial Management of Criminal e-Discovery</b>	19
A. Managing Voluminous e-Discovery in Criminal Cases	19
B. Early Discussion of e-Discovery Issues	20
Ask About the Case	21
Advise About Expectations	21
Advise About Resources	22
Schedule Discovery Conferences	22
C. Subsequent Status of e-Discovery Issues	22
<b>IV. Conclusion</b>	23
<b>Appendix A: ESI Protocol Description</b>	25
<b>Appendix B: ESI Protocol</b>	35
<b>Appendix C: First Appearance e-Discovery Colloquy</b>	73
<b>Appendix D: Discovery Status Conference e-Discovery Colloquy</b>	81



## **I. Overview**

The rapid growth of digital technology and its spread into every facet of life are producing increasingly complex discovery issues in federal criminal cases. There are several advantages to electronically stored information (ESI, or e-discovery), including speed, efficiency, and quality of information. To ensure these benefits are realized, judges and lawyers working on federal criminal cases need guidance on how best to address e-discovery issues.

Judges can play a vital oversight role to ensure that e-discovery moves smoothly, trial deadlines are met, and the parties and courts are able to review and identify critical evidence. This pocket guide was developed to help judges manage complex e-discovery in criminal cases. A note of appreciation goes to Judge Xavier Rodriguez (W.D. Tex.), and Magistrate Judges Laurel Beeler (N.D. Cal.) and Jonathan W. Feldman (W.D.N.Y.), for their suggestions and advice, as well as to our fellow members of the Joint Electronic Technology Working Group, who improved this publication.

### **A. Lack of Criminal e-Discovery Guidance**

Although the Federal Rules of Criminal Procedure offer guidance on a number of topics, they offer little help to judges and litigants concerning how to conduct e-discovery. As the Sixth Circuit noted in *United States v. Warshak*, Rule 16 of the Federal Rules of Criminal Procedure is “entirely silent on the issue of the form that discovery must take; it contains no indication that documents must be organized or indexed.”<sup>1</sup> To be sure, Rule 16 provides a court the discretion to fashion discovery orders to serve the particular needs of a case, but it does not “specify the manner in which production is done.”<sup>2</sup>

---

1. 631 F.3d 266, 296 (6th Cir. 2010). In that case, the defendant argued that the “district court must order the government to produce electronic discovery in a particular fashion.” In rejecting this argument, the court noted that there is “a dearth of precedent suggesting that the district court was wrong” in allowing the government to produce discovery in an electronic format different from what the defendant sought. *Id.*

2. See Fed. Crim. Rules Handbook § IV (Arrest and Preparation for Trial) (Dec. 2012).

## *Criminal e-Discovery*

### **B. Civil e-Discovery Rules and Practices Do Not Lend Themselves to Criminal e-Discovery**

The rules governing civil and criminal discovery are fundamentally dissimilar due to the different public policies underlying criminal and civil litigation, constitutional requirements, and special ethical obligations of prosecutors and defense counsel. Consequently, courts have generally refrained from applying civil e-discovery rules to criminal discovery.<sup>3</sup>

An essential difference between civil and criminal discovery is breadth:

A criminal defendant is entitled to rather limited discovery, with no general right to obtain the statements of the Government's witnesses before they have testified. Fed. Rules Crim. Proc. 16(a)(2), 26.2. In a civil case, by contrast, a party is entitled as a general matter to discovery of any information sought if it appears "reasonably calculated to lead to the discovery of admissible evidence." Fed. Rule Civ. Proc. 26(b)(1).<sup>4</sup>

Federal Rule of Criminal Procedure 16 does not mandate any mechanisms or procedures for addressing e-discovery equivalent to those found in Federal Rules of Civil Procedure 26 and 34. Rule 16 includes "data" as a proper object of criminal discovery, but the rule does not address the mechanics of e-discovery.

Furthermore, the nature of the parties and proceedings differ in criminal cases. Unlike civil cases, where discovery is an adversarial process in which the government's discovery obligations are similar to any litigant's, the government has unique nonadversarial discovery obligations in criminal cases. As a representative of the sovereign, prosecutors are obliged to prosecute impartially and ensure that justice

---

3. The Sixth Circuit rejected the defendant's argument that the electronic discovery format standards of Federal Rule of Civil Procedure 34(b)(2)(E)(i) should apply to criminal cases. *Warshak*, 631 F.3d at 296. Nonetheless, two magistrate judges have turned to civil e-discovery rules for guidance because there is a void in the criminal rules regarding this issue. See *United States v. O'Keefe*, 537 F. Supp. 2d 14, 18-19 (D.D.C. 2008); *United States v. Briggs*, No. 10CR184S, 2011 WL 4017886, at \*8 (W.D.N.Y. Sept. 8, 2011).

4. *Degen v. United States*, 517 U.S. 820, 825-26 (1996).

## I. Overview

is done.<sup>5</sup> For example, the Due Process Clause imposes a “fundamental fairness” requirement on the government’s discovery, as expressed in the government’s *Brady* and *Giglio* obligations.<sup>6</sup> Additionally, speedy trial rights may be implicated when defendants have little time to come to grips with vast e-discovery.<sup>7</sup> Similarly, defendants are entitled to effective assistance of counsel at trial and during plea negotiations.<sup>8</sup> Defense counsel’s effectiveness may depend on whether he or she has reviewed and understands the e-discovery in time to enter into informed plea negotiations.<sup>9</sup> When the government provides e-discovery in a reasonably organized fashion, it can help the defense efficiently review discovery and can lead to more productive plea discussions, less litigation, and speedier resolution of a case.

Criminal investigations and third-party subpoenas by both the prosecution and defense often bring vast quantities of ESI to criminal e-discovery. Complex ESI cases usually require litigation support resources not typically found in criminal defense practices. Indigent defendants need adequate funding to obtain those resources.

---

5. ABA Model Rules of Professional Responsibility 3.8, comt. 1; *see also* *Berger v. United States*, 295 U.S. 78 (1935).

6. *See also* *United States v. Bagley*, 473 U.S. 667, 675 (1985) (withholding *Brady* evidence violates due process). The prosecutor’s *Brady* obligation is addressed in ABA Model Rule of Professional Conduct 3.8(d) (requiring prosecutors to “make timely disclosure to the defense of all evidence or information known to the prosecutor that tends to negate the guilt of the accused or mitigates the offense, and, in connection with sentencing, disclose to the defense and to the tribunal all unprivileged mitigating information known to the prosecutor, except when the prosecutor is relieved of this responsibility by a protective order of the tribunal.”).

7. *See* U.S. Const. amend. VI; 18 U.S.C. § 3161 (“Speedy Trial Act”).

8. *Lafler v. Cooper*, 132 S. Ct. 1376 (2012); *Missouri v. Frye*, 132 S. Ct. 1399 (2012).

9. Although lawyers need not review every document in a voluminous e-discovery production before entering into a plea bargain, they should review a reasonable and targeted portion of discovery so as to provide reasonably effective advice regarding resolution. Thus, depending upon the nature and complexity of the e-discovery, to conduct plea negotiations the defense may need to have e-discovery in a reasonably useable format, and have engaged in thoughtful e-discovery review.

## *Criminal e-Discovery*

### **C. A Practitioner's Guide to Criminal e-Discovery**

One attempt to provide comprehensive, national guidance is the ESI Protocol (see Appendices A & B), which was produced by a joint working group composed of the Department of Justice and representatives of the criminal defense bar.<sup>10</sup> The ESI Protocol is one approach for judges to use to encourage interparty cooperation and reduce the need for judicial intervention. Indeed, some federal district courts have begun integrating the ESI Protocol into their courtroom practices.<sup>11</sup>

The ESI Protocol draws on many sources, including case law, local rules, and seasoned defense and prosecution practitioners' experience. Its goal is to provide courts and litigants with best practices consisting of general principles, recommendations, and concrete strategies for improving efficiency, minimizing expense, increasing security, and decreasing frustration and litigation. Importantly, the ESI Protocol does not enlarge or diminish any party's substantive legal discovery obligations imposed by applicable federal statutes, rules, or case law.<sup>12</sup>

---

10. The Recommendations for Electronically Stored Information Discovery Production in Federal Criminal Cases (hereinafter "the ESI Protocol") was produced by the Joint Electronic Technology Working Group (JETWG), which comprises representatives of the Administrative Office of the U.S. Courts (AOUSC), Defender Services Office (DSO), the Department of Justice (DOJ), Federal Public and Community Defender Organizations (FPDOs and CDOs), private attorneys who accept Criminal Justice Act (CJA) appointments, and liaisons from the United States Judiciary and other AOUSC offices. The Federal Judicial Center does not endorse any specific discovery approach, including the ESI Protocol.

11. *See, e.g.*, Best Practices for Electronic Discovery in Criminal Cases: Western District of Washington (Mar. 21, 2013), available at <http://www.wawd.uscourts.gov/sites/wawd/files/32113BESTPRACTICESFORELECTRONIC.pdf>; Northern District of California, Criminal Justice Act, Capital and Non-Capital Criminal Representation (2001), available at <http://www.cand.uscourts.gov/pages/965> (linking to the ESI Protocol).

12. *See, e.g.*, *Brady v. Maryland*, 373 U.S. 83 (1963); *Giglio v. United States*, 405 U.S. 150 (1972); 18 U.S.C. § 3500 (the "Jencks Act"); and Federal Rules of Criminal Procedure 16 & 26.2.

## *II. Common Issues in Criminal e-Discovery*

The ESI Protocol will be familiar to most federal criminal practitioners. The Department of Justice trains its prosecutors to use the ESI Protocol in cases involving complex e-discovery. Most federal defenders and Criminal Justice Act (CJA) representatives receive similar training on the ESI Protocol.

## **II. Common Issues in Criminal e-Discovery**

Both prosecutors and defense attorneys struggle with the same e-discovery issues: large volume; a variety of sources and formats; hidden information (metadata and embedded data); differing formats for production; software and hardware limitations; and finding efficient, cost-effective ways to review ESI. Some challenges are unique to criminal practice, such as incarcerated defendants' access to e-discovery, while others are the same as those arising in civil practice. For many prosecutors and defense counsel, a lack of experience with ESI presents a significant challenge; but it is the lack of resources—money, personnel, training—that often overshadows all other problems. And even when resources are available, considerable time is often required to arrange for and execute the processing necessary to make ESI readily available.

For CJA counsel, the challenges of ESI may be especially daunting. Often, they are solo practitioners who lack the resources for sophisticated software tools. Because they are usually appointed post-indictment, they need to get up to speed on matters that the government may have spent many months or years investigating and preparing—while at the same time getting up to speed on how to manage electronic discovery. Besides training and software tools, they often may need experienced litigation support assistance, which can be provided pursuant to 18 U.S.C. § 3006A.

The following are e-discovery issues that judges may need to understand or address.

### **A. Funding the Defendant's e-Discovery**

There was a time when voluminous e-discovery cases were confined to white-collar prosecutions, and those defendants typically paid the costs

### *Criminal e-Discovery*

of their own defense. Today, even routine drug cases and bank robberies often involve extensive cell phone data or other ESI.<sup>13</sup> This has funding consequences for indigent defendants and the court.

When a case has complex e-discovery issues, the judge considering a CJA appointment may need to factor in the additional cost of reviewing, organizing, and working with e-discovery.<sup>14</sup> The Act is silent about when a defendant would be so destitute as to need appointed counsel, but the cost of working with complex e-discovery can itself exceed what many defendants can afford even if they are able to pay for counsel.<sup>15</sup>

Some CJA panels have formal tiers or informal lists of specialized lawyers for capital, financial, or immigration cases. Courts that take their CJA attorneys' skills into consideration can also consider creating

---

13. Smartphone data provides an example of the magnitude of e-discovery. Many smartphones hold sixteen to sixty-four gigabytes of data, not including storage cards (which can double that amount), and have cloud access to much more data. They contain emails, call history and contact information, calendars, text messages, GPS data, photographs, videos, internet history, and social media information, all of which can result in thousands of potentially relevant items of discovery. Multiple-defendant cases could dramatically increase that amount. Add to that the corresponding laptops, tablets, desktops, and surveillance data also readily accessible, and the amount of e-discovery can quickly exceed document-based paper discovery in a white-collar or corporate prosecution from fifteen years ago.

14. The court can ask the government to give it early notice if the case involves voluminous e-discovery.

15. The Criminal Justice Act can authorize payment of e-discovery review costs when the extent of those costs would render a defendant unable to pay for e-discovery review regardless of whether a defendant can otherwise afford retained counsel. 18 U.S.C. § 3006A(e)(1) allows retained counsel to apply for services to be paid through the CJA system. *See* Guide to Judiciary Policies and Procedures, Vol. VII, § 310.10.20, *available at* [http://www.uscourts.gov/rules-policies/judiciary-policies/cja-guidelines/chapter-3-ss-310-general#a310\\_10](http://www.uscourts.gov/rules-policies/judiciary-policies/cja-guidelines/chapter-3-ss-310-general#a310_10). If outside assistance is needed, the protocol for authorization and payment for investigative, expert, or other services in CJA-appointed cases is governed by Vol. VII, Chapter 3 of the Guide to Judiciary Policies and Procedures. *See* <http://www.uscourts.gov/FederalCourts/AppointmentOfCounsel/CJAGuidelinesForms/vol7PartA/vol7PartAChapter3.aspx>. If counsel anticipates that the costs will exceed the statutory maximum, advance approval should be obtained from the court and the chief judge of the circuit (or the active or senior circuit judge who has been delegated authority to approve excess compensation). *See* Vol. VII, § 310.20.20 for further information and a sample order, *available at* [http://www.uscourts.gov/rules-policies/judiciary-policies/cja-guidelines/chapter-3-ss-310-general#a310\\_20](http://www.uscourts.gov/rules-policies/judiciary-policies/cja-guidelines/chapter-3-ss-310-general#a310_20).

## *II. Common Issues in Criminal e-Discovery*

The court can ask for assistance from the NLST.<sup>23</sup>

- The DSO has three national coordinating discovery attorneys (CDAs) who are experts in e-discovery, have experience with CJA cases, and are knowledgeable about litigation technology. They work with CJA counsel and federal defenders in multidefendant cases to manage large volumes of e-discovery efficiently and cost-effectively to best fit the defendants' needs. The court can ask CJA counsel to request that the case be referred to a CDA through the National Litigation Support Team.<sup>24</sup>
- All circuits except the Fifth, Eleventh, and D.C. have case budgeting attorneys (CBAs) who work with judges and CJA panel attorneys to develop and review budgets for criminal "mega cases."<sup>25</sup> They assist in addressing attorney and paralegal time, as well as expert, investigative, and other costs, to ensure that critical defense needs are budgeted to optimize resources while fostering high-quality, cost-controlled represen-

---

FederalCourts/AppointmentOfCounsel/Viewer.aspx?doc=/uscourts/FederalCourts/AppointmentOfCounsel/vol7/Vol\_07.pdf.

23. The NLST can be contacted at (510) 637-3500. Further information about the NLST can be found on fd.org at <http://www.fd.org/navigation/litigation-support/subsections/who-is-the-national-litigation-support-team>.

24. Further information regarding CDAs can be found on the J-Net at <http://jnet.ao.dcn/court-services/cja-panel-attorneys-and-defenders/services-coordinating-discovery-attorneys-available-selected-federal-criminal-justice-act-cases> (not accessible to the public).

25. For CJA panel attorneys, "mega cases" are either: (a) federal capital prosecutions and capital habeas corpus cases, or (b) noncapital representations with the potential for extraordinary cost (attorney work expected to exceed 300 hours or total expenditures for attorneys and investigative, expert, and other service providers expected to exceed \$30,000 for an individual CJA defendant). This is distinguished from "mega budget cases," referring to federal and community defender office cases that will substantially impact their office budgets (by a 10% or \$500,000 increase or more), so that an additional budget is developed to fund just that one case. See *Case-Budgeting Techniques and Other Cost-Containment Policies* (June 30, 2014), available at <http://www.fd.org/docs/select-topics/cja/case-budgeting-techniques-and-other-cost-containment-strategies.pdf?sfvrsn=8>.

### *Criminal e-Discovery*

tation. In appropriate cases, the budgets may address litigation support costs, and the CBAs have working relationships with the NLST to consult on litigation support matters. Judges in a district without a CBA can contact the DSO for assistance.<sup>26</sup>

There are considerable funding consequences to voluminous e-discovery. The court should expect additional CJA costs in these cases, but managing e-discovery can be done thoughtfully and reasonably to mitigate costs.

#### **B. Lack of ESI Experience, Knowledge, and Competency**

Unfortunately, many criminal practitioners still do not have an adequate understanding of e-discovery issues and litigation technology. However, attorney competency ethics standards are evolving to require an adequate understanding of e-discovery and the technology needed to review it.<sup>27</sup> Lawyers who are unfamiliar with e-discovery can associate or consult with others who have the expertise.<sup>28</sup> Nonetheless, they remain responsible for e-discovery decisions and should be able to do the following, either themselves or in association or consultation with others:

- Implement procedures to preserve potentially discoverable electronic information.

---

26. Further information on case budgeting and case budgeting attorneys can be found on the J-Net at <http://jnet.ao.dcn/court-services/cja-panel-attorneys-and-defenders/case-budgeting> (not accessible to public). Judges who do not have a CBA in their circuit can contact the duty attorney for the Defender Services Office at (800) 788-9908.

27. 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 and Conduct, Formal Op. No. 2015-193 (2015). This development follows the 2012 American Bar Association amendment to its Model Rule 1.1, stating that lawyers need to "keep abreast of changes in the law and its practice, *including the benefits and risks associated with relevant technology.*" ABA Model Rules of Professional Conduct, Model Rule 1.1, comt. 8 (emphasis added).

28. If a CJA attorney needs to retain expert assistance, payment would have to be approved by the court.



### *Criminal e-Discovery*

analyzing, and presenting case data. Using both project management and technology, they ensure that e-discovery is handled in a cost-effective and time-efficient manner that allows for effective organization, easy retrieval, and quality client representation.

Just as judges should be mindful of attorney knowledge and experience in managing e-discovery, they should also be aware that even knowledgeable attorneys need skilled litigation support.

#### **D. The Workflow in Processing ESI**

ESI generally takes one of two possible forms: preprocessed (raw) or postprocessed. Some raw ESI is not ready to be reviewed electronically; it must be processed<sup>29</sup> into a digital file that can be loaded into document-review software. Similarly, paper records can be processed into electronic files like TIFFs with extracted text or searchable PDFs with the extracted text embedded in the file itself.

The workflow for processing ESI can be complicated. When ESI is in a proprietary format (for example, a Google Mail file), it cannot be reviewed with industry-standard tools; instead, review requires specialized hardware, software, and expertise to convert the data into a form that can be reviewed with standard tools.<sup>30</sup> Even if the discovery is produced in an optimal way,<sup>31</sup> defense counsel may still need expert assistance, such as litigation support personnel, paralegals, or database vendors, to convert e-discovery into a format they can use and to decide what processing, software, and expertise is needed to assess the ESI. Next, the ESI should be organized to facilitate finding informa-

---

29. See *supra* n. 20 for a definition of "processing."

30. Many state and federal law enforcement agencies have outdated computer systems, so the data in these outdated systems cannot be viewed with current industry-standard litigation support software. This is particularly common with audio and video files, necessitating conversion to industry-standard formats.

31. Parties should not be obstructionist and ought to produce discovery in a usable format if they reasonably can. According to the ESI Protocol, when a producing party elects to engage in processing ESI, the results of that processing (unless it contains work product) should be produced as discovery; this saves the receiving party the expense of replicating the work. ESI Protocol, Recommendations ¶ 6(d). That said, the ESI Protocol states that the government is not obligated to convert ESI into a format specified by the defense beyond what it would do for its own case preparation or discovery production.

## *II. Common Issues in Criminal e-Discovery*

tion. In voluminous e-discovery cases, parties must be able to rely on document-review software, which can be costly. Nonetheless, it saves money because it speeds up the review process and improves counsel's ability to find information. Such software affords counsel a variety of search strategies, including word searches, document searches, date searches, sender/recipient searches, concept searches, and predictive coding searches.<sup>32</sup>

### **E. Varieties of Evidence-Review Software**

There is a vast array of software tools for handling 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. There is frequently overlap between what various products can do. 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 evidence display in the courtroom. As a result, litigants have different collections of tools. That creates compatibility and conversion issues.

A meet-and-confer is an important stage in tackling those compatibility and conversion issues, particularly when the parties do not already have an established routine for exchanging discovery or when they face novel or difficult ESI issues. One goal of the meet-and-confer is to address technical issues so that the ESI produced in discovery is readable and usable. An important part of that process is the parties' discussion of production formats, volume, timing, and other issues.<sup>33</sup>

### **F. Volume of e-Discovery**

The great volume of e-discovery poses a serious challenge due to the variety of devices on which ESI can be created and stored, the ease of

---

32. Technology-assisted review (also called predictive coding) is a process for prioritizing or coding a collection of documents using a computerized system that harnesses human judgments of one or more subject matter expert(s) on a smaller set of documents, and then extrapolates those judgments to the remaining data.

33. See ESI Protocol, attached as Appendix B.

### *Criminal e-Discovery*

various forms of telecommunication (such as texting and social media), and the declining cost of storage. ESI can come from many custodians<sup>34</sup> or sources—mobile phones, smartphones, tablets, laptops, desktops, computer network servers, external ESI storage devices (such as flash drives or external hard drives), cloud storage, GPS tracking devices, social media. Because of this, the amount of ESI in criminal cases has grown exponentially, and this growth is expected to continue, significantly complicating management and review of evidence. For example, in 2011, court-appointed defense counsel in one multi-defendant case had to review discovery comprising 240,000 pages of documents on 19 DVDs and CD ROMs, 185 banker boxes of paper documents (approximately 460,000 pages), and 30 forensic images (that is, copies) of complete computers, servers, and thumb drives holding approximately 4.3 terabytes of data.<sup>35</sup> Additionally, the defendants gathered 750,000 pages of third-party information directly relevant to their defenses. Cases like this benefit substantially from sophisticated software and advanced review practices such as technology-assisted review.

It is important to recognize that complex ESI requiring technological assistance is not constrained to computer and white-collar fraud crimes. Vast amounts of ESI are found in small cases as well. Even relatively modest amounts of e-discovery, depending on format, can create obstacles to reviewing evidence. Moreover, simple cases of possession of drugs or guns, for example, can involve smartphones and computers containing gigabytes or even terabytes of data. Lawyers unaided by technology cannot review this much data.

#### **G. Form of Production—ESI Formats**

The format in which ESI is gathered affects how the data can be used. For example, text messages collected as text-only files can be searched for particular words or combinations of words. But if the metadata for those same text messages is also gathered, then thousands or millions of text messages can not only be searched for particular words, they

---

34. In e-discovery terms, “custodian” refers to the person whose data was collected.

35. Applying litigation support standard calculations, 4.3 terabytes of data is the equivalent of 215 million pages, or 86,000 banker boxes, of documents.

## *II. Common Issues in Criminal e-Discovery*

can also be sorted by date, custodian, and author or addressee, and software can plot who communicated with whom, how frequently, when, and where. Such information can have tremendous utility in criminal cases.

Lawyers need specialized litigation software to work with ESI in its many formats. For example, they need software to review ESI documents, which can be as basic as a PDF viewer or far more complex. Most document-review platforms allow parties to view many file types. The DOJ and most civil law firms have managed their own discovery materials with software programs and technical personnel for years. Criminal defense practitioners, especially those involved in indigent defense, are relative latecomers to this world. Most CJA panel attorneys do not have litigation support software that can view and organize TIF or native file productions. Similarly, most do not have tools to take advantage of a “load file,”<sup>36</sup> extracted metadata, or files in native or near-native ESI format.<sup>37</sup> It is only recently that federal defender offices gained that capability nationally. As a result, the DOJ may be able to produce discovery in a reasonably usable format, but CJA counsel may not be able to utilize the most robust litigation software available. To provide computer-challenged defense counsel with reasonably useable e-discovery, the U.S. Attorney’s Office typically provides e-discovery on disks that contain software for viewing, searching, and tagging documents. For more sophisticated defense counsel, the DOJ typically creates load files or otherwise configures its e-discovery productions in industry-standard formats. Of course, there are instances where typical practices do not work well, and those are proper subjects for a meet-and-confer.

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

---

36. A load file is a cross-reference file used to import images or data into databases. A data load file may contain Bates numbers, metadata, paths to native files, coded data, and extracted or OCR text. An image load file may contain document-boundary, image-type, and path information. Load files must be obtained and provided in software-specific formats to ensure they can be used by the receiving party.

37. A significant advantage to web-hosted document-review platforms for the CJA panel is that IT support is provided by the vendor, since most do not have in-house IT staff.

### *Criminal e-Discovery*

of the data. Attorneys who do not understand the various formats should consult with a litigation support or IT expert before receiving or processing their e-discovery.

#### **H. Form of Production—Paper Formats**

Some contemporary records and many historical records only exist on paper. Converting paper discovery to electronic formats makes it easier to duplicate, exchange, and search. But converting voluminous paper records takes time and money. Accurate document breaks (also known as document unitization<sup>38</sup>) too frequently are not captured when scanning paper records. When this happens, document unitization is lost, diminishing the utility of the resulting electronic files. Although the producing party is not obligated to reformat paper records into an electronic form,<sup>39</sup> in some cases both parties may save time and money by converting paper into electronic formats. Cost sharing may be an option if the parties agree that scanning serves both sides.

Scanning a paper record and making it searchable through optical character recognition (OCR) software is an improvement over leaving it in paper form, but it is not a perfect solution. Scanning can be prohibitively expensive. Moreover, OCR programs have established error rates, decreasing the accuracy and reliability of electronic searches of documents. That unreliability causes some attorneys to default to using their own eyes to search rather than scanning paper records for electronic review.

Today, some records custodians' systems still are configured to produce subpoenaed records in paper, even when they have the same data electronically. If a records custodian is willing to produce the information in an electronic format, the electronic version usually will yield more reliable searches.<sup>40</sup> However, what is efficient and afforda-

---

38. Document unitization is the process of determining where a document begins (its first page) and ends (its last page), with the goal of accurately describing what was a "unit" as it was received by the party or was kept in the ordinary course of business by the document's custodian.

39. See ESI Protocol, Principle 6.

40. There are several options for electronic formats. Sometimes the records custodian can produce the native-format version, for example, a Word document as a Word file as opposed to a paper document or a PDF. Sometimes the native format