U.S. Department of Justice

Office of the Deputy Attorney General

The Deputy Attorney General

Washington, D.C. 20530

March 30, 2011

MEMORANDUM FOR THE ASSOCIATE ATTORNEY GENERAL AND
THE ASSISTANT ATTORNEYS GENERAL FOR THE
CRIMINAL DIVISION
NATIONAL SECURITY DIVISION
CIVIL RIGHTS DIVISION
ANTITRUST DIVISION
ENVIRONMENTAL AND NATIONAL RESOURCES DIVISION
TAX DIVISION

DIRECTOR, FEDERAL BUREAU OF INVESTIGATION
ADMINISTRATOR, DRUG ENFORCEMENT ADMINISTRATION
DIRECTOR, UNITED STATES MARSHALS SERVICE
PRINCIPAL DEPUTY DIRECTOR, BUREAU OF ALCOHOL,
TOBACCO, FIREARMS AND EXPLOSIVES
DIRECTOR, BUREAU OF PRISONS

ALL UNITED STATES ATTORNEYS

FROM: James M. Cole
Deputy Attorney General

SUBJECT: Guidance on the Use, Preservation, and Disclosure of Electronic Communications in Federal Criminal Cases

This memorandum supplements the January 4, 2010 Guidance for Prosecutors Regarding Criminal Discovery issued by Deputy Attorney General David W. Ogden (Ogden Memo), particularly section 1.B.5, Substantive Case-Related Communications, and is to be read in conjunction therewith.[1] The guidance contained herein is directed to all Department of Justice personnel and to all law enforcement personnel participating as members of a prosecution team.[2]

[1] For guidance concerning cases involving national security information, *see* 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."

[2] "Prosecution team" members 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. USAM 9-5.001. The Ogden Memo provides additional guidance where state and local law enforcement has any involvement in a criminal case, stating:

I. Summary

This memorandum provides guidance for prosecution team members on the use and preservation of electronic communications ("e-communications"). The basic principles are simple. Prosecution team members should think about the content of any e-communication before sending it; use appropriate language; think about whether e-communication is appropriate to the circumstances, or whether an alternative form of communication is more appropriate; and determine in advance how to preserve potentially discoverable information.

II. The Relationship Between the Government's Legal Discovery Obligations, Department of Justice Discovery Policies, and This Guidance

The Government's discovery obligations in federal criminal cases are set forth in constitutional case law, particularly *Brady v. Maryland*, 373 U.S. 83 (1963), and *Giglio v. United States*, 405 U.S. 150 (1972); the Jencks Act (18 U.S.C. 3500); Federal Rules of Criminal Procedure 16 and 26.2; and applicable rules of professional conduct.

Specific Department of Justice disclosure policies entitled Disclosure of Exculpatory and Impeachment Information (*Brady* policy) and Potential Impeachment Information Concerning Law Enforcement Witnesses (*Giglio* policy) are set forth in the United States Attorneys' Manual (USAM) at Sections 9-5.001 and 9-5.100.

The purpose of this memorandum is to provide guidance to ensure that the Government meets its legal discovery obligations as applied to electronic communications.[3] As used in this guidance, the term "e-communications" includes emails, text messages, SMS (short message service), instant messages, voice mail, pin-to-pin communications, social networking sites, bulletin boards, blogs, and similar means of electronic communication. This memorandum also provides guidance on how e-communications should and should not be used during the investigation and prosecution of a federal criminal case. A failure to comply with the guidance

---

In such cases, prosecutors should consider (1) whether state or local agents are working on behalf of the prosecutor or are under the prosecutor's control; (2) the extent to which state and federal governments are part of a team, are participating in a joint investigation, or are sharing resources; and (3) whether the prosecutor has ready access to the evidence. Courts will generally evaluate the role of a state or local law enforcement agency on a case-by-case basis. Therefore, prosecutors should make sure they understand the law in their circuit and their office's practice regarding discovery in cases in which a state or local agency participated in the investigation or on a task force that conducted the investigation.

Prosecutors are encouraged to err on the side of inclusiveness when identifying the members of the prosecution team for discovery purposes. Carefully considered efforts to locate discoverable information are more likely to avoid future litigation over *Brady* and *Giglio* issues and avoid surprises at trial.

[3] This memorandum is solely intended to provide guidance to law enforcement personnel in order to attain compliance with the government's criminal discovery obligations with regard to electronic communications. It does not create any right in any person or entity, and it is not enforceable in any criminal or civil case. *United States v. Caceres*, 440 U.S. 741 (1979).

contained in this memorandum may result in delay, expense, and other consequences prejudicial to a prosecution, but it does not necessarily mean that there has been or will be a violation of a disclosure obligation.

III. Guidance for Achieving Full Compliance with the Government's Legal Discovery Obligations Relating to Electronic Communications

A. Benefits and Risks of E-communications

E-communications offer substantial benefits, including speed, sharing, and efficiency.

E-communications also present substantial risks. Because e-communications frequently are prepared and sent quickly and without supervisory review, they may not be as complete or accurate as more formal reports and may reflect a familiar or jovial tone. In court, defense counsel may try to use e-communications containing material inconsistencies, omissions, errors, incomplete statements, or jokes to impeach the credibility of a witness. Additionally, there is a risk that defense counsel will use poorly drafted e-communications between agents, witnesses, and/or prosecutors in court to create the false impression that they contain relevant or contradictory factual information. These risks can be particularly problematic in criminal prosecutions because, depending upon their content, e-communications may be discoverable under federal law.

Thus, prosecution team members should exercise the same care in generating case-related e-communications that they exercise when drafting more formal reports. All prosecution team members need to understand the risks of e-communications, the need to comply with agency rules regarding documentation and record-keeping during an investigation, the importance of careful and professional communication, and the obligation to preserve and produce such communications when appropriate.

B. Categories of E-communications

Case-related e-communications generally fall into four categories:

Substantive communications. "Substantive communications" include:

- factual information about investigative activity;
- factual information obtained during interviews or interactions with witnesses (including victims), potential witnesses, experts, informants, or cooperators;
- factual discussions related to the merits of evidence;

- factual information or opinions relating to the credibility or bias of witnesses, informants and potential witnesses;[4] and

- other factual information that is potentially discoverable under *Brady, Giglio*, Rule 16, or Rule 26.2 (Jencks Act).

Substantive communications or the information within them may be discoverable.

Logistical communications. "Logistical communications" include e-communications that contain travel information; identify dates, times and locations of hearings or meetings; transmit reports; etc. Generally, logistical communications are not discoverable.

Privileged or protected communications. "Privileged communications" include attorney-client privileged communications, attorney work product communications, and deliberative process privileged communications.[5] "Protected communications" are those covered by F.R.Crim.P. 16(a)(2).[6] Generally, these communications are not discoverable so long as any discoverable facts contained in them are disclosed in other materials produced in discovery.

---

[4] For example, if a prosecutor or agent opines that an informant will make a "bad" witness because the informant has made prior inconsistent statements, the opinion itself is core work product that need not be disclosed to the defense, but the prior inconsistent statements should be disclosed if the informant testifies at trial. *See generally,* Discovery BlueBook § 6.12.5, *Opinion or Reputation Evidence Regarding Veracity.*

[5] Pursuant to applicable law, a privilege may apply to communications:

a. between prosecutors on matters that require supervisory approval or legal advice, *e.g.*, prosecution memoranda, *Touhy* approval requests, *Giglio* requests, wire tap applications and reviews, and case strategy discussions;

b. between prosecutors or agency counsel and other prosecuting office personnel, agents, or other agency personnel on case-related matters, including but not limited to organization, tasks that need to be accomplished, research, and analysis;

c. between prosecutors and agency counsel or agency personnel (including agents) on legal issues relating to criminal cases, including, but not limited to, *Giglio* and *Touhy* requests; and

d. from the prosecutor or agency counsel to an agent, other agency personnel, or prosecuting office personnel giving legal advice or requesting investigation of certain matters in anticipation of litigation (*e.g.*, "to-do" list).

If warranted, the sender of a privileged e-communication is encouraged to place a "privileged communication" warning on the communication to flag its privileged nature.

[6] *See, generally,* Discovery BlueBook 3.8, *Information Not Subject to Disclosure by the Government – Rule 16(a)(2).*

Mixed Communications. A communication that contains a mix of the categories above may be partially discoverable and may need careful review by a prosecutor or review by a court before a final determination is made as to whether it should be disclosed in discovery.[7]

C. Using E-communications

The following guidance applies at all phases of a criminal case including investigation, trial preparation, trial, and after trial:

1. Prosecution team members should discuss and make sure they understand the e-communications and discovery policies and guidance applicable to their case.

2. Prosecution team members should only write and send e-communications that they would feel comfortable being displayed to the jury in court or in the media.

3. Prosecution team members should be particularly cautious in any e-communications with potential witnesses who are not law enforcement personnel, taking care to avoid substantive e-communications. Of course, any potentially discoverable information should be preserved, regardless of whether the communication is written or oral.

4. Substantive e-communications among prosecution team members should be avoided except when, to meet operational needs, they are the most effective means of communication. Examples include where prosecution team members are in different countries or time zones, or where other operational imperatives require such e-communications. Prosecution team members should consider whether a formal report would be a better way of ensuring accurate communication, clarifying a matter, or preserving potentially discoverable information. Again, potentially discoverable information should be preserved, regardless of whether the communication is written or oral.

5. Prosecution team members may use e-communications for logistical communications, for example, to schedule meetings with witnesses, agents, prosecutors, or other members of the prosecution team, or to transmit a formal report. However, prosecution team members should avoid including any substantive information in such e-communications.

---

[7] For e-communications containing information to be produced in discovery, a prosecutor may make appropriate redactions, summarize the substance of an e-communication in a letter rather than disclosing the e-communication itself, seek a protective order, or take other safeguarding measures.

6. E-communications, like formal reports, should state facts accurately and completely; be professional in tone; and avoid witticism, careless commentary, opinion, or over-familiarity. E-communications should maintain and accurately reflect an arms-length relationship with potential witnesses who are not law enforcement personnel, including victims and informants.

7. Prosecution team members ordinarily should not include information in an e-communication that must be incorporated into a formal agency report, especially with regard to witness interviews or other communications containing a witness's or agent's factual recitations. If for some reason substantive case-related information must be contained in an e-communication, prosecution team members should ensure that the information is accurate and is included in any formal report required by agency policies. Material inconsistencies between an e-communication and a formal report, or omissions, errors, or incomplete statements in e-communications, may be impeachment information and may be used in cross-examination in court proceedings.

8. Prosecution team members should limit the subject matter of any e-communication to a single case at a time to make it easier to segregate e-communications by case.

9. Prosecution team members should inform individuals not on the prosecution team but otherwise involved in the case, including victims, witnesses, and outside experts, that e-communications are a written record that might be disclosed to the defendant and used for impeachment in court like any other written record.

10. Prosecution team members must comply with any applicable policies governing e-communications and should not use personally-owned electronic communication devices, personal email accounts, social networking sites, or similar accounts to transmit or post case-related information.

11. Prosecution team members should not post case-related or sensitive agency information on a non-agency website or social networking site. Information posted on publically accessible websites or social networking sites may be used to impeach the author.

12. Prosecution team members should send e-communications only to those individuals who have a need to know the information contained in the communication.

13. Prosecution team members should employ practices that will preserve any potentially discoverable information contained in e-communications. Preservation of e-communications in certain messaging formats (e.g., text, SMS, instant, PIN, etc.) may present unique challenges.[8] At present, the approaches to preserving potentially discoverable information in e-communications may include: incorporating any potentially discoverable information into a comprehensive report, capturing the message in some format that can be made available to the prosecutor, or preserving the e-communication itself. These approaches may evolve as technology changes and technical capabilities change.

14. The sender should notify recipients of any restrictions on forwarding e-communications that the sender wants observed.

D. Preservation of E-communications

There are three steps to proper handling of e-communications in criminal cases: preservation,[9] review, and disclosure. The number of e-communications preserved and reviewed likely will be greater than the number ultimately produced as discovery.

1. Who is responsible for preserving e-communications?

Each potentially discoverable e-communication should be preserved by each member of the prosecution team who is either (a) the creator/sender/forwarder of the e-communication, or (b) a primary addressee (*i.e.*, in the "To" line). If no member of the prosecution team is a sender or primary addressee of a substantive e-communication (*e.g.*, if an agent is cc'd on an email by a witness to a third party), then each member of the prosecution team who is a secondary addressee (*i.e.*, a "cc" or "bcc" recipient) should preserve the email. Although in some instances this practice will lead to preserving multiple copies of the same e-communication, it will ensure preservation.

2. When should e-communications be preserved?

To ensure that e-communications are properly preserved, prosecution team members should move and/or copy potentially discoverable e-communications, together with any potentially discoverable attachments and threads of related e-communications, from the user's e-

---

[8] Each component should provide guidance to affected employees on how to preserve the various messaging formats (text, SMS, IM, PIN, etc.), or any other e-communication that may contain potentially discoverable information. Where an e-communication containing potentially discoverable information cannot be preserved electronically or printed, the agency's inability to do so should be documented so that the preservation approach can be explained in court.

[9] This guidance is concerned only with the Government's criminal discovery obligations. It is not intended to address the requirements of the Federal Records Act, 44 U.S.C. §§ 3101 *et seq.*

communication account[10] to a secure permanent or semi-permanent storage location associated with the investigation and prosecution, or print and place them with the criminal case file as soon as possible but not later than 10 days after the e-communication is sent or received. Prosecution team members should ensure that such preservation occurs before the agency computer system automatically deletes the e-communication because of storage limitations or retention policies. Designated network locations that are not subject to automatic deletion may be a secure storage location for potentially discoverable e-communications.

3. Which e-communications should be preserved for later review?

During an investigation it is difficult to know which e-communications may be discoverable if the case is charged. Therefore, members of the prosecution team should err on the side of preservation when deciding which e-communications to preserve for review.

The following e-communications should be preserved for later review and possible disclosure to the defendant:

- Substantive e-communications created or received in the course of an investigation and prosecution.
- All e-communications sent to or received from potential witnesses who are not law enforcement personnel regardless of content.
- E-communications that contain both potentially privileged and unprivileged substantive information.

As discussed below in section II.E.2, agents and their supervisors should work with prosecutors to identify all e-communications that are particularly sensitive and deserve careful consideration before any determination is made to provide them to the defendant as discovery.

4. Which e-communications do not need to be preserved for later review?

Logistical communications between prosecution team members, *e.g.,* scheduling meetings or assigning tasks, generally do not need to be preserved and made available to the prosecutor for review because they are not discoverable unless something in their content suggests they should be disclosed under *Brady*, *Giglio*, Jencks or Rule 16.

[10] With respect to emails, this includes the user's inbox, sent items, and deleted items.

5. How should e-communications be preserved?

When possible, e-communications should be preserved in their native electronic format to enable efficient discovery review. Otherwise, they should be printed and preserved.[11] E-communications that cannot be printed should be preserved in some other fashion, *e.g.*, a narrative report. For email, creation of electronic folders into which pertinent emails can be easily moved is the recommended method for preservation in native format.

6. How do parallel civil or administrative investigations/proceedings affect which e-communications should be preserved in a criminal case?

The best practices for parallel criminal, civil, and administrative proceedings vary from case to case. Be aware that civil proceedings may have different or broader preservation requirements; therefore, the prosecution team should consult with the lawyers handling the parallel proceedings for guidance on preserving e-communications in the early stages of parallel proceedings.

E. Reviewing and Producing Discoverable E-communications to the Defendant

1. Responsibilities of the Prosecutor

It is the prosecutor's responsibility to oversee the gathering, review and production of discovery.[12] In determining what will be disclosed in discovery, the prosecutor should ensure that each e-communication is evaluated, taking into consideration, among other things, what facts are reported, the author, whether the author will be a witness, whether it is inconsistent with other e-communications or formal reports, and whether it reflects bias, contains impeachment information, or contains any information (regardless of credibility or admissibility) that appears inconsistent with any element of the offense or the Government's theory of the case.

If the e-communication contains any particularly sensitive information (as described below), then the prosecutor should consider whether to file a motion for a protective order, seek supervisory approval to delay disclosure (in accordance with USAM § 9-5.001), make appropriate redactions, summarize the substance of an e-communication in a letter rather than disclosing the e-communication itself, or take other safeguarding measures.

---

[11] Agencies may require some e-communications to be printed to paper to comply with the Federal Records Act. Notwithstanding paper copies, preserving e-communications in native electronic format still is appropriate, when feasible, to facilitate electronic review and to preserve metadata that, in rare circumstances, may be discoverable.

[12] When dealing with voluminous e-communications, the prosecution team should discuss and plan for a substantial lead time to gather and review the materials.

2. Responsibilities of the Prosecution Team

It is the responsibility of each member of the prosecution team to make available to the prosecutor all potentially discoverable e-communications so that the prosecutor can review them to determine what should be produced in discovery. The discovery obligation continues throughout the case. *See* Fed.R. Crim. P. 16(c).

Prosecution team members who submit potentially discoverable e-communications to the prosecutor should identify e-communications that deserve especially careful scrutiny by the prosecutor. For example, prosecution team members should identify e-communications the disclosure of which could:

- affect the safety of any person,
- reveal sensitive investigative techniques,
- compromise the integrity of another investigation, or
- reveal national security information.