Transcript of E-Discovery in Federal Criminal Investigations and Prosecutions Podcast

Part 2

John Besselman (JB) - Hi. I'm John Besselman, Assistant Division Chief for the Legal Division, back with Assistant Division Chief Bob Cauthen for Part 2 of our podcast on e-discovery in federal criminal investigations and prosecutions.

Bob Cauthen (BC) - In part 1 of our podcast we talked about the tremendous growth in the use of electronic data, electronic devices, and e-communications.

JB - And we talked about the benefits and risks in their use. We ended by mentioning that in March 2011, Deputy Attorney General James Cole issued the DOJ *Guidance on the Use, Preservation, and Disclosure of Electronic Communications in Federal Cases* on how e-communications should and should not be used during the investigation and prosecution of a federal criminal case and how to ensure that the government meets its discovery obligations. Let's take a detailed look at that guidance.

First, let's look at those to whom this guidance applies. They're called the "Prosecution Team." Who is a part of the "Prosecution Team?"

BC - It includes all DOJ personnel, federal, state, and local law enforcement, and other government officials participating in the investigation and prosecution of the criminal case.

JB - It's easy to understand how it includes federal officers, but why state and local officers?

BC - They are included because of the large number of cases prosecuted in federal court that come out of initial contacts between state and local officers and defendants. When identifying members of the team, prosecutors should err on the side of inclusion in a carefully considered effort to locate discoverable information.

JB - What are the "e-communications" covered by the guidance?

BC - As mentioned in Part 1 of this podcast, they include e-mail, text messages, instant messages, short message service – for example, tweeting – pin-to-pin, social networking sites, bulletin boards, and blogs.

JB - The guidance also breaks down e-communications into three categories – Substantive, Logistical, and Privileged. What are each of those?

BC - Substantive communications include those that contain
Factual information about investigative activity,
Factual information from interviews or interactions with victims, witnesses, potential witnesses, informants, cooperators, and experts,
Factual discussions about the merits of evidence, and
Factual information regarding the credibility or bias of witnesses.

JB - It's easy to see the theme. Substantive communications contain factual information about the case.

BC - Logistical communications include those that contain
Travel information,
Dates, times, locations of hearings or meetings, and those that
Transmit reports.
Generally, logistical communications are not discoverable.
And finally, there's
Privileged communications. Those include
Attorney-client privileged communications,
Attorney work product communications, and
Deliberative process communications, and
Protected communications, those covered by Federal Rule of Criminal Procedure 16(a)(2).
Generally, so long as any discoverable facts in them are disclosed in other materials, privileged and protected communications are not discoverable.

JB - The guidance gives some basic principles apply to drafting and using e-communications during and as part of an investigation and prosecution. What are they?

BC - First, think about whether e-communication is appropriate to the circumstances or whether an alternative form of communication, such as a formal report or telephone call, is a better choice.

Don't send substantive, case-related e-communications unless absolutely necessary and only to those with a need to know. For example, an e-mail may be appropriate when the recipient is in a time zone that makes coordinating a telephone call almost impossible. Texting may be the better choice when you're worried about being overheard. When you use e-communications, notify recipients of any restrictions on forwarding and sharing. Do not use personally-owned electronic devices, personal e-mail accounts, social networking sites to transmit case related information. Do not post case-related or sensitive agency information on a non-agency website or social networking site. Typically, logistical information is better suited for e-communications.

Secondly, think about the content of any e-communication before using it. You may expect it to remain private, but once you send it or post it you've lost all control over it. Those to whom you send it and your "friends" on your social media site can share it with anyone they want. We've all seen plenty of examples of e-mails and social media postings displayed in court and in

the media that are embarrassing and damaging. There's a question we've all been told to ask ourselves. Would you do it or say it in front of your mother? Or, put another way, how will this look in the newspaper, sound on TV, or while you're cross examined on the stand?

JB - The principle is simple. Be professional, especially with non-law enforcement personnel. When you do send substantive e-communications, write them like a formal report with accurate and complete facts. Avoid witticism, careless commentary, opinion, and over familiarity. They should reflect an arms-length relationship with non-law enforcement witnesses. And, limit e-communications to a single case. Also, tell non-prosecution team members that e-communications are a record and that they may be disclosed to the defense.

BC - Finally, figure out in advance how and where you are going to preserve potentially discoverable e-communications. Talk to the prosecutors about their policies, how you need to, and how you're going to handle e-communications. Figure out the plan; put the plan in place; and use the system from start to finish.

The goal is to reduce the amount of case related e-communications to just those that are appropriate. That reduces the time and costs of managing discovery to ensure full compliance. Remember and appreciate that the guiding point is that any potentially discoverable information and communication should be preserved and delivered to the prosecutor.

JB - Who is responsible for preserving it?

BC - The short answer to that question is every member of the "Prosecution Team." Each Prosecution Team member who is the creator, sender, forwarder, or the primary addressee - in the "To" line - of an e-communication is required to preserve it. If none of the above apply, for instance it's an e-mail from a witness to a 3rd party, then each Prosecution Team member who is a secondary recipient, in the "cc" or "bcc" line is required to preserve it. Admittedly, this will preserve multiple copies, but it will also ensure that every e-communication is preserved.

JB - What needs to be preserved?

BC - All potentially discoverable e-communications including attachments and threads of related e-communications. For e-mails that includes what's in your inbox, sent items, and deleted items.

JB - OK, what is meant by "All potentially discoverable e-communications?"

BC - It includes all substantive e-communications created or received during investigation and prosecution. It includes <u>all</u> e-communications sent to or received from non-law enforcement potential witnesses regardless of content. It also includes e-communications that contain both potentially privileged and unprivileged substantive information. If you're not sure, err on the side of preservation. Purely logistical e-communications need not be preserved.

JB - When should it be preserved?

BC - As soon as possible but no later than 10 days after the e-communication is sent or received. Make sure it's before your agency system automatically deletes because of storage limitations or retention policies.

JB - Where should it be preserved?

BC - You need to put it in secure permanent or semi-permanent storage associated with the particular investigation and prosecution. For e-mail create a specific folder to which they can be moved. Or, you can print and put in the criminal case file.

JB - How should it be preserved?

BC - E-communications should be preserved in their native e-format. Otherwise, they should be printed and preserved.

JB - 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.

Let the prosecutor know if there are e-communications that deserve especially careful scrutiny because disclosure could affect the safety of any person,
reveal sensitive investigative techniques,
compromise the integrity of another investigation, or
reveal national security information.

BC - The goal of the Deputy Attorney General's guidance is to reduce the volume of and establish a system to manage potentially discoverable e-communications. That reduces the time and costs of managing discovery and ensures full compliance with our ethical and legal discovery obligations.

JB - We've posted a copy of the guidance on the Legal Division website. You'll find it by clicking on the Downloads and Articles link, then clicking the Downloads link, and then the DOJ Guidance link.

Thank you from the Federal Law Enforcement Training Centers Legal Division for joining us for the discussion of this very important subject.

Then End