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

Part 1

John Besselman (JB) - Hi. I'm John Besselman, Division Chief for the Legal Division.

Bob Cauthen (BC) - And I'm Bob Cauthen, Assistant Division Chief.

JB - In this 2 part podcast, we're going to talk about an emerging issue that's rapidly growing in scope and importance:
E-discovery in federal criminal investigations and prosecutions.

BC - Like it or not, embrace it or not, we live in a digital world with a proliferation of electronic devices, electronically stored information, or ESI as it's called, electronic communications, that's e-communications, and social media. John, I saw recently where it is estimated that over 90% of all new information is created and stored electronically. And we are certainly more likely to communicate by e-mail, text message, social media, instant messaging, short message service, and pin-to-pin than ever before.

It's easy to see that this digital world has had an enormous impact on criminal investigations and prosecutions. Criminals have gone digital, and so have officers and investigators. First of all, as criminal evidence, ESI – now we're talking phone calls, text messages, e-mails, internet use, and electronic data - has become a huge part of every kind of crime. Secondly, police and investigative reports and memoranda are increasingly digital in form. Agencies are issuing laptops, tablets, smart phones, and other electronic devices to their officers and investigators for use in conducting investigations, taking statements, and communicating with each other, informants, witnesses, and prosecutors. Officers and investigators are also increasingly using their personal electronic devices for official work purposes. Bring your own device programs and policies are being developed and implemented as we speak. Also, the clear trend in our courts is electronic filings for search and arrest warrants, affidavits, and court orders vice hard copy documents.

JB - There are several reasons why this is true now and will continue into the future. There are real benefits in the use of ESI and e-communications. For instance,
<u>Speed</u> – e-mail is certainly faster than snail-mail;

<u>It's Efficient</u> – ESI and e-communications create an instant record of the information that is mobile, requires very little physical storage space, and is easily converted into different forms. An enormous amount of data can be stored on a very small flash drive. And, then there's

<u>Ease of sharing</u> – huge amounts of information can be securely shared with an unlimited number of people. Think encryption. Think large "contacts lists," "reply to all," "and forward."

BC - But with those benefits come risks.

Speed is a benefit, but it's also a potential risk. Formal communications and documents take time to compose and can be reviewed and edited. E-communications are often hastily prepared, quickly sent, and may not be as complete as formal documents. Also, for e-communications, "sent" is almost the equivalent of "received" with no time for intervening clarification.

Misinterpretation is a potentially BIG problem. The language and style of e-communication is typically much more abbreviated and is markedly different than formal and face to face communication. And, maybe 80% of what is communicated during face to face conversations is through the human interaction – the tone, the inflection, the facial expressions, and the body language – not the actual words that are spoken. Context can be lost. What may actually be understood and taken as funny by the sender and receiver may not read that way at all to others. And, the words can take on completely different meanings when stripped of those human factors.

JB - Let's see if we can illustrate this danger.

Let's say you get an e-mail or text message with these words in it:

I - didn't - say - he - did - that.
What does it mean? Can that same sentence, those same words, mean completely different things?

What if it were spoken this way – **I** didn't say he did that.

BC - Or spoken this way – I **DIDN'T** say he did that. Or perhaps this way – I didn't **SAY** he did that.

JB - Or maybe this way – I didn't say **HE** did that. Or even this way – I didn't say he did **THAT**.

Arguably, those same words could reasonably carry 5, and possibly more, different meanings when you strip away the speaker's tone, inflection, facial expressions, and eliminate context.

BC - The sheer volume of ESI and e-communications and the potential problematic nature of e-communications present distinct challenges for law enforcement.

How do we take advantage of the technology while minimizing the risks?

How do we ensure full and complete compliance with discovery statutes, rules, and court orders? In other words, how do we create and maintain our own ESI, how do we seize and store ESI that is criminal evidence, and how do we create, capture, and store our case related e-communications so as to fully comply with our ethical and legal discovery obligations?

JB - For investigations, creating, obtaining, seizing, and maintaining ESI is primarily a function of case organization and management. There are numerous software systems that perform well, and agencies typically pick one that fits their kind of cases best. For prosecutions, there are a number of presentation software systems that perform well, and prosecution offices typically pick one that fits best.

BC - What we want to focus on for this podcast and part 2 is the creation, capture, storage, and disclosure of e-communications. It can be a huge, costly undertaking to find and assemble all of the case related e-communications. Yet, it's critical that all those deemed discoverable be turned over to the defense in full compliance with our obligations.

The guiding principle in all of this discussion is this: Any potentially discoverable information and communication should be preserved and delivered to the prosecutor. Period.

JB - The Department of Justice has given us some direction on this subject. In March 2011, Deputy Attorney General James Cole issued the DOJ *Guidance on the Use, Preservation, and Disclosure of Electronic Communications in Federal Cases.* The memorandum provides guidance on how e-communications should and should not be used during the investigation and prosecution of a federal criminal case and guidance to ensure that the government meets its discovery obligations. What I like about the memo is that it clearly describes the scope of the issue, defines terms, and sets out the responsibilities of all those involved in the investigation and prosecution of federal criminal cases.

BC - We'll take a detailed look at that guidance in Part 2 of this podcast. Join us there.