E-Discovery Seminar for Federal Judges

Electronic Discovery in the Criminal Context

July 1, 2011

Key Topics for Discussion

- ESI in Investigations
- ESI and Search Warrants
- ESI in the Post-Indictment Stage
- Admissibility

Subpoenas – Duty to Preserve

- The duty to preserve can come before the subpoena
  - Civil: Whenever litigation is reasonably anticipated, threatened or pending . . .
  - Criminal: Essentially the same standard. See, *e.g.*, 18 U.S.C. § 1519 (SOX obstruction provision: ". . . in contemplation of . . .")
  - Government has a duty to preserve all material exculpatory evidence. *U.S. v. Branch*, 537 F.3d 582 (6th Cir. 2008); *U.S. v. Suarez*, 2010 WL 4226524 (D.N.J. Oct. 19, 2010) (adverse inference sanction levied against federal prosecutors for the deletion of text messages between FBI agents and cooperating witness in course of investigation).
- Direct and collateral consequences for failing to preserve
- Understand your own ESI first

Potential Obstruction of Justice Crimes

- Spoliation may be potential crime in and of itself ***and*** be used to prove consciousness of guilt for underlying crimes.
- Sarbanes-Oxley offenses – destroying or altering documents, emails, or other ESI may be a crime, even if no official "investigation" is pending or imminent.
  - 18 USC § 1519: *In Re: GJ Investigation*, 445 F.3d 266 (3rd Cir. 2006) (target destroyed emails after receipt of GJ subpoena); *U.S. v. Ganier*, 468 F.3d 920 (6th Cir. 2006) (target-CEO deleted files from his laptop and desktop PC and another employee's PC after learning of GJ investigation).
  - 18 USC § 1512(c).
- 18 USC § 1503: *U.S. v. Lundwall*, 1 F. Supp.2d 249 (SDNY 1998) (prosecution where defendants allegedly withheld & destroyed docs sought during discovery in civil case).
- Criminal referrals for civil litigants, including third parties.

Subpoenas – Discussions with Government

- Production of ESI
  - Similar to Civil Rule 26(f) conference: identify and avoid problems
  - Common issues for discussion
    - Form of production
    - Rolling production
    - Common limitations on preservation and production: dates, custodians, etc.
    - Filtering with search terms
    - Databases
    - Privilege and clawback agreements
  - Opportunity to influence Government thinking and gain insight into investigation theories and focus
  - Document all steps you take/discussions with Government
  - Status in investigation may impact negotiation.

ESI and Search Warrants

- The 18th century vs. the 21st century: Reconciling the "particularity" requirement with the reality of "intermingled data", extraordinary volumes of data, the plain view doctrine, and the role of the judiciary
- "First" search and seizure
  - Search: search the identified premises for hardware
  - Seizure: (over) seize the hardware (or copy its contents)
  - Constrained by the usual legal rules? Of course.
- "Second" search and seizure
  - Search: search the hardware or copy
  - Seizure: seize whatever data you want
  - Constrained by the usual legal rules? It depends . . .

Search Warrants – CDT

- *U.S. v. Comprehensive Drug Testing, Inc.*, 579 F.3d 989 (9th Cir. 2009) (en banc):
  - Magistrate Judges should insist that the government waive reliance upon the plain view doctrine in digital evidence cases.
  - Segregation of non-responsive materials must be done by specialized personnel who are walled off from the case agents, or an independent third party.
  - Warrants must disclose the actual risks of destruction of information, as well as prior efforts to seize that information in other judicial fora.
  - The government's search protocol must be designed to uncover only the information for which it has probable cause, and only that information may be examined by the case agents.
  - The government must destroy or return non-responsive data, keeping the issuing Magistrate Judge informed about when it has done so and what it has kept.

Search Warrants – Amended CDT Opinion

- *CDT* Amended Opinion (September 13, 2010):
  - Explicit restrictions on search warrants demoted to suggested guidance in concurring opinion.
  - Amended opinion instead adheres to prior ruling in *U.S. v. Tamura*, 694 F.2d 591 (9th Cir. 1982). Two-step process:
    1. Where officers come across relevant documents so intermingled with irrelevant documents that they cannot feasibly be sorted at the site, large scale removal of materials can be justified.
    2. A Magistrate Judge should then approve the conditions and limitations on a further search through those documents. The "essential safeguard required is that wholesale removal must be monitored by the judgment of a neutral, detached magistrate."
  - These guidelines offer "the government a safe harbor, while protecting the people's right to privacy and property in their papers and effects. District and magistrate judges must exercise their independent judgment in every case, but heeding this guidance will significantly increase the likelihood that the searches and seizures of electronic storage that they authorize will be deemed reasonable and lawful."

Search Warrants – Other Decisions

- *U.S. v. Mann*, 592 F.3d 779 (7th Cir. 2010)
  - "We are inclined to find more common ground with the dissent's position [in *CDT*] that jettisoning the plain view doctrine entirely in digital evidence cases is an efficient but overbroad approach."
  - Permit case law surrounding application of plain view to computer searches to develop through normal course of fact-based adjudication.
- *U.S. v. Stabile*, 633 F.3d 219(3d Cir. 2011)
  - "[P]lain view doctrine applies to seizures of evidence during searches of computer files, but the exact confines of the doctrine will vary from case to case in a common-sense, fact-intensive matter."
  - Search of video files upheld, as even if items were not in plain view, the independent source and inevitable discovery doctrines applied to file contents.

Search Warrants – Different View

- *U.S. v. Williams*, 592 F.3d 511 (4th Cir. 2010)
  - Warrant impliedly authorized officers to open each file on computer to view its contents, at least cursorily, to determine whether file fell within the scope of warrant's authorization. To be effective, search can't be limited to reviewing only file designation or labeling as they can easily be manipulated.
  - Once you accept that a computer search must, by implication, authorize at least a cursory review of each file on the computer, the plain view criteria is met.
  - Sheer amount of information contained on a computer does not distinguish the authorized search of the computer from an analogous search of a file cabinet containing a large number of documents.

Search Warrants – Plain View Doctrine

- Inconsistent application of “plain view” doctrine to digital evidence search warrants – if you have to click around, is it still in plain view?
- Special treatment for computer search warrants or analogous to document containers such as filing cabinets?
- With intermingled data and extraordinary data volumes, is “computer” still describing place to be searched with particularity? Does it need to be described virtually?
- Supreme Court review?

Other Fourth Amendment Issues

- California Supreme Court (*People v. Diaz*, 244 P.3d 501(Cal. 2011)) has found that the Fourth Amendment does not require law enforcement to get a warrant before searching text messages stored on cell phones in the possession of arrestees. Courts around country are divided on this.
- *U.S. v. Hill*, 2011 WL 90130 (N.D. Cal. Jan. 10, 2011) (court unwilling to conclude that cell-phone found in defendant's clothing and on his person should not be considered an element of person's clothing and should not be treated any differently than a wallet taken from a defendant's person).
- Search warrant of defendant's Facebook account upheld where defendant's best friend logged into his own Facebook account and informed police that defendant had recently communicated through Facebook network. *State v. Gurney*, 2010 Me. Super. LEXIS 96 (July 12, 2010).
- *Smallwood v. State*, 36 Fla. L. Weekly D911 (Fla. 1st DCA, Apr 29, 2011) ("were we free to do so, we would find, given the advancement of technology with regard to cell phones and other similar portable electronic devices, officers may only search cell phones incident to arrest if it is reasonable to believe evidence relevant to the crime of arrest might be found on the phone").

Other Fourth Amendment Issues (cont.)

GPS tracking devices

- *U.S. v. Pineda-Moreno*, 591 F.3d 1212 (9th Cir. 2010).
  - Officers installed tracking devices on vehicle parked in front of defendant's home without warrant.
  - Warrantless tracking upheld as defendant could not claim reasonable expectation of privacy in his driveway, even if portion of driveway was located within curtilage of home.
- *U.S. v. Maynard*, 615 F.3d 544 (D.C. Cir. 2010).
  - Tracking device used to track defendant's movements 24 hours a day for one month did constitute search because it revealed private information through patterns of behavior and search unreasonable because individuals have reasonable expectation of privacy in aggregate total of their movements over period of one month.

ESI in the Post-Indictment Stage

- Government obligations come into play
  - Preservation obligations
  - Production obligations
  - *Brady* obligations
- Influence of civil principles
- Possible remedies
  - Dismissal for due process violation
  - Adverse inference
  - Evidence/testimony stricken

Post-Indictment Discovery – Importing Civil Rules

- *U.S. v. O'Keefe*, 537 F. Supp. 2d 14 (D.D.C. 2008)
  - Importing Civil Rules into criminal cases.
    - Form of production (Rule 34)
    - Meet and confer (Rule 26(f))
- *U.S. v. Warshak*, 631 F.3d 266 (6th 2010) (finding that defendant's claims that voluminous data was unsearchable and disorganized were unfounded, and declined to follow *O'Keefe* on form of production, noting that Rule 16 is silent on this issue).
- *Suarez* (adverse inference sanction levied against federal prosecutors for the deletion of text messages between FBI agents and cooperating witness in course of investigation. In determining sanctions, court relied on *Pension Committee*).
- Court protocols requiring "26(f)" conference.

15

Post-Indictment Discovery – Productions

- No *Brady* violation for "open file" production of massive volume of ESI. *U.S. v. Skilling*, 554 F.3d 529, (5th Cir. 2009)
  - Gov't provided searchable electronic "open file", a set of "hot documents" and indices to "hot documents." No evidence of bad faith or that Government padded "open file" with superfluous information.
- *U.S. v. Salyer*, 2010 WL 3036444 (E.D. Cal. 2010) ("the government cannot meet its *Brady* obligations by providing [the defendant] with access to 600,000 documents and then claiming that she should have been able to find the exculpatory information in the haystack. Or, as the undersigned put it in the initial order: '[A]t some point (long since passed in this case) a duty to disclose may be unfulfilled by disclosing too much; at some point, 'disclosure,' in order to be meaningful, requires 'identification' as well'").
- *Warshak* – Criminal Rule 16 contains no indication that documents must be organized or indexed. No *Brady* violation where defendants' motion practice demonstrated they could navigate the discovery.
  - "[I]t would not be prejudicial if the defendants were denied the chance to excavate in a mine that contained no ore."

Post-Indictment Discovery - Dismissal

- Dismissal in *U.S. v. Graham*, 2008 WL 2098044 (S.D. Ohio May 16, 2008)
  - Government turned over vast amounts of discovery in criminal tax case; approx 1.5 million documents and other media. Gov't slow to produce materials and often tainted and/or incomplete.
  - Discovery volume unmanageable for Defendant.
  - Numerous trial delays resulted in dismissal for Speedy Trial Act violation.
  - Court noted: "discovery could have and should have been handled differently."
- *U.S. v. Qadri*, 2010 WL 933752 (D. Haw. March 9, 2010) (denying motion to dismiss indictment based on prosecutor's e-discovery delays)

17

Admissibility – Case Studies

- *U.S. v. Yeley-Davis*, No. 10-8000, 10th Cir. (Jan. 20, 2011) (cell phone records from wireless provider are business records, not testimonial in nature, and do not implicate 6th Amendment confrontation clause).
- *U.S. v. Dobbs*, No. 09-5025, 10th Cir. (Jan. 5, 2011) (presence of child pornography in defendant's computer cache directory insufficient evidence to satisfy knowledge element of offense).
- *State v. Thompson*, 2010 ND 10 (N.D. 2010) (threatening text messages sent to victim admissible to show defendant's state of mind the day of the attack; evidence from victim of his knowledge of defendant's cell phone number and defendant's signature on text messages sufficient to authenticate text messages).
- *People v. Fielding*, No. C06022 (Cal. App., June 18, 2010) (incriminating MySpace messages sent by defendant authenticated by victim who testified he believed defendant had sent them; inconsistencies and conflicting inferences regarding authenticity goes to weight of evidence, not its authenticity).
- *Coleman-Fuller v. State*, No. 1913 (Md. Ct. Spec. App., May 27, 2010) (police officer's testimony regarding cell phone records used to establish defendant's location at the time of a murder deemed inadmissible, as officer's "training" in functions of cell phone towers and tracking insufficient where officer was not qualified as expert).