# The “Ins” and “Outs” of Electronic Information in Criminal Investigations and Actions

BNA - March 10, 2011

# Our Speakers

Sean Broderick

Andrew Goldsmith

Judge Herbert B. Dixon, Jr.

Ron Hedges

Ken Withers

Justin Murphy

# Key Topics for Discussion

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

# 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*, D.N.J., No. 09-932 (JLL) (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).
- The internal investigation conundrum
  - Preservation of data without tipping off subjects of investigation.

# 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 3d parties.

# Government Has Broad Investigative Authority

- Few options to challenge subpoenas
- *FTC v. Church & Dwight*, D.D.C., Misc. No. 10-149 (J. Facciola) (Oct. 29, 2010). Upheld FTC subpoena requesting significant sales and marketing data from multi-national company because federal agencies have broader powers during investigative stage – to collect information it deems relevant to the investigation – than it would during discovery.
  - "It cannot be true that in a globalized economy a federal agency may never investigate the activities of a foreign subsidiary of an American company merely because the agency's original grant of authority is the investigation of the economic activity that has had an impact on interstate commerce within the United States."

# Subpoenas – Discussions with Gov't

- Production of ESI
  - Similar to Civil Rule 26(f) conference: identify and avoid problems
  - Gather facts about IT systems first (with expert help)
  - Common issues for discussion
    - Form of production
    - Rolling production
    - Common limitations on production: dates, custodians, etc.
    - Filtering with search terms
    - Privilege and clawback agreements
  - Opportunity to influence Gov't thinking and gain insight into investigation theories and focus
  - Status in investigation

# Subpoenas - Discussions with Gov't (cont.)

- Consider negotiating preservation issues
  - Backup tapes
  - Scope of forensic copies of hard drives
  - Databases
  - Subpoena cut-off date
  - Key custodians

# ESI and Search Warrants

- The 18th century vs. the 21st century: Reconciling the "particularity" requirement with the reality of "intermingled data" and extraordinary volumes of data
- "First" search and seizure
  - Search: search the identified premises for hardware
  - Seizure: 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 – Case Studies

- *U.S. v. Comprehensive Drug Testing, Inc.*, 579 F.3d 989 (9th Cir. 2009) (en banc)
- Facts
  - Probable cause that at least 10 MLB players had obtained steroids from BALCO
  - Gov't agents executed warrants at testing lab seeking information about 10 named MLB players
  - During search, Gov't seized computer directory containing testing data for more than 100 other MLB players and participants in 13 other sports and businesses
  - Gov't obtained further warrant for 100 other MLB players who were listed as also having tested positive for steroids

# Search Warrants – Case Study (cont.)

- *En banc* panel reversed original panel ruling and established specific rules for warrants seeking ESI:
  - 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 – Case Study (cont.)

- *CDT* IV 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 Views

- *U.S. v. Mann*, 592 F.3d 779 (7th Cir. 2010)
  - Skeptical of rule requiring officers to always obtain pre-approval from magistrate judge to use the electronic tools necessary to conduct searches tailored to uncovering evidence that is responsive to a properly circumscribed warrant.
  - "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.

# Search Warrants – Other Views (cont.)

- *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 – Other Views (cont.)

- *U.S. v. Stabile*, 2011 WL 294036 (3d Cir. Feb. 1, 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 – Plain View

- Inconsistent application of “plain view” doctrine to digital evidence search warrants.
- Special treatment for computer search warrants or analogous to document containers such as filing cabinets?
- Supreme Court review?

# Fourth Amendment and Third Party Internet Service Providers (ISP)

- Stored Communications Act allows government compelled disclosure of e-mails from an ISP on a standard of less than probable cause.
- *U.S. v. Warshak*, 2010 WL 5071766 (6th Cir. Dec. 14, 2010) – to the extent the SCA permits the government to obtain such e-mails without a warrant, the SCA is unconstitutional. The government may not compel a commercial ISP to turn over the contents of a subscriber's e-mails without first obtaining a warrant based on probable cause.
  - E-mail is analogous to phone call or letter, ISP is the intermediary that makes e-mail communication possible, and ISP is functional equivalent of post office or telephone company. Subscriber enjoys reasonable expectation of privacy in contents of e-mails stored with, sent through, or received through a commercial ISP.

# Other Fourth Amendment Issues

- California Supreme Court (*People v. Diaz*, No. S166600, Jan. 3, 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 is unwilling to conclude that a cell-phone that is found in a defendant's clothing and on his person should not be considered an element of the 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).

# 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.
- *United States v. Sparks*, 2010 WL 4595522 (D. Mass. Nov. 10, 2010) (court rejecting defendant's *Maynard* "aggregate travels" argument).

# ESI in the Post-Indictment Stage

- Government obligations come into play
  - Production obligations
  - Preservation obligations
- Possible remedies
  - Dismissal for violation of Due Process
  - 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 Fed. R. Civ. P. into criminal cases.
    - form of production (Rule 34)
    - preservation "safe harbor" (Rule 37)
- *Warshak* declined to follow *O'Keefe* on form of production, noting that Rule 16 is silent on this issue.
- *U.S. v. Suarez*, D.N.J., No. 09-932 (JLL) (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. In determining sanctions, court relied on *Pension Committee* ).


21

# 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 did not violate obligation to disclose exculpatory evidence in their possession when they delivered hundreds of millions of pages of ESI and left it to defense attorneys to find what they wanted.
  - Gov't provided searchable electronic "open file", a set of "hot documents" and indices to "hot documents." No evidence of bad faith or that Gov't padded "open file" with superfluous information.
- Gov't reprimanded for massive "data dump." *SEC v. Collins*, 256 FRD 403 (S.D.N.Y. 2009)
  - Court found that SEC failed to follow common protocols for electronic document production and SEC's claim of work product over its organized set of documents rejected.
- *Warshak* – 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)
  - Gov't 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)


23

# Admissibility – Getting ESI Into Evidence

- Five hurdles to consider:
  - Whether the ESI is relevant (Rule 401)?
  - Whether it can be shown to be authentic (Rules 901 and 902)?
  - Whether it is hearsay (if offered for the substantive truth, Rules 801-807)?
  - Whether it is an original or a duplicate (Rules 1001-1008)?
  - Whether its probative value substantially outweighs the danger of the ESI's unfair prejudice against those it is used against (Rule 403)?

# 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).

# Juror Issues

- Jury Instructions
  - Proposed Texas Jury Instructions specifically address juror use of cell phones and other electronic devices, use of social networking, and use of internet while serving as juror.

# Juror Issues (cont.)

- Florida District Court of Appeals overturned a manslaughter conviction because one of the jurors used his iPhone to look up the word “prudent” and then shared his recollection with other jurors. The defendant claimed to have feared for his life so as to render his decision to shoot his neighbor during the argument “prudent,” a term used in both the closing arguments and in the jury instructions. *Tapanes v. State of Florida*, 43 So.3d 159 (Dist. Ct. App. Fla. 2010).

- In 2009 Judge William Zloch learned that a juror in a federal drug trial in Florida had been doing Internet research, in violation of the court's instructions. After questioning the other jurors, he learned that eight others had been doing Web research on the case. The judge had no choice but to declare a mistrial. “We were stunned,” said defense attorney Peter Raben, who was told by jurors that they had been headed toward acquittal before Zloch declared a mistrial. “It’s the first time modern technology struck us in that fashion, and it hit us right over the head.” Martha Neil, *A Shock for Judge Zloch: 9 Jurrors in 1 Trial Doing Web Research,* ABA Journal, Law News Now. (Mar.17 2009) *(*recounting *United States v. Hernandez* (S.D. Fla. 2009).

# For More Information, Please Contact:


| | |
|---|---|
| Sean Broderick | Sean_Broderick@fd.org |
| Judge Herbert Dixon | herbert.dixon@dcsc.gov |
| Andrew Goldsmith | andrew.goldsmith@usdoj.gov |
| Ron Hedges | r_hedges@live.com |
| Justin Murphy | justin.murphy@crowell.com |
| Ken Withers | kjw@sedonaconference.org |