

Electronic Discovery and Evidence in Criminal Actions



BNA Audioconference
September 23, 2009

Ron Hedges
Hon. Herbert B. Dixon, Jr.
Stephen M. Byers
Andrew D. Goldsmith

Key Topics for Discussion

- Subpoenas
- Search Warrants
- Post-Indictment Discovery
- Use at Trial

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)
- The internal investigation conundrum
 - Preservation of data without tipping off subjects of investigation.

Preservation - Common ESI Pitfalls

- Backup tapes
- E-mail janitors/auto delete
- Hard drives and other local media
- Self-collection by employees
- Former and departing employees
- Dynamic and proprietary databases
- Third party repositories
- Lack of expert involvement

Potential Obstruction of Justice Crimes

- Spoliation may be potential crime in and of itself **and** be used to prove of 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 No. 06-1474*, 445 F.3d 266, 275-76 (3rd Cir. 2006) (target destroyed emails after receipt of GJ subpoena); *US 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: *US v. Lundwall*, 1 F Supp.2d 249 (SDNY 1998) (prosecution where defs allegedly withheld & destroyed docs sought during discovery in civil case)

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

Subpoenas - Discussions with Gov't (cont'd)

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

International Data Protection Laws

- Overseas ESI presents unique issues
- Gov't may defer production but will insist on preservation
- Foreign data protection laws impose specific requirements on entities holding “personal data”
- May violate laws of foreign country by complying with U.S. Gov't demands

Subpoenas – New FRE 502 and Privilege

- FRE 502(b): Inadvertent production does not trigger waiver if reasonable steps to prevent and prompt corrective action; no subject-matter waiver
- FRE 502(e): Agreements between the parties enforceable (e.g., clawback and quick peek)
- FRE 502(d): But only court orders enforceable in other proceedings (e.g., parallel civil litigation)
- Application of 502(d) in criminal proceedings uncertain

Search Warrants – The ESI Puzzle

- The 18th century vs. the 21st century: Reconciling the “particularity” requirement with the reality of “intermingled 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 Study

- *U.S. v. Comprehensive Drug Testing, Inc.*, 2009 WL 2605378 (9th Cir. Aug. 26, 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:
 - Magistrates 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 informed about when it has done so and what it has kept.

Search Warrants - Amendments to Rule 41

- Effective Dec. 1, 2009
- Rule 41(f)(1)(B): “[T]he inventory may be limited to describing the physical storage media that were seized or copied.”
 - Contrast *CDT*: Return should contain list of data obtained, returned.
- Rule 41(f)(1)(B): “The officer may retain a copy of the electronically stored information that was seized or copied.”
 - Contrast *CDT*: Copies should be returned or destroyed absent specific judicial authorization.

Search Warrants - Contrary Views to *CDT*

- No other circuit has imposed a filter-team procedure to searches of electronic media absent the presence of privileged information. Warrants permitting investigators to search through all contents of seized media have been approved.
 - See, e.g., *U.S. v. Khanani*, 502 F.3d 1281, 1290; *Brooks*, 427 F.3d at 1251-53 (approving warrant that permitted officers to look through computer for child pornography); *Guest v. Leis*, 255 F.3d 325, 335 (6th Cir. 2001) (law enforcement “may legitimately have checked” the contents of computer files to see whether they related to the warrant); see also *U.S. v. Gray*, 78 F. Supp. 2d 524 (E.D. Va. 1999) (search of all files on computer permissible to determine if any fall within scope of warrant).

Search Warrants – Judicial Supervision

- Judicial supervision of post-seizure search of data.
 - Similar to *CDT* but without specific rules re post-seizure handling of ESI, e.g., walling off case agents.
 - *U.S. v. Carey*, 172 F.3d 1268 (10th Cir. 1999)
 - Storage capacity of computers requires a special approach
 - Intermingled data may be seized if on-site sorting is not feasible
 - BUT documents must be sealed or held pending approval by magistrate of conditions for further search
 - *US v Burgess*, 2009 WL 2436674 (10th Cir. 2009), limits *Carey* to its facts; thus, may not be much left of *Carey*
 - *United States v. Tamura*, 694 F.2d 591, 595 (9th Cir. 1982)
 - Precursor to *Comprehensive Drug Testing*
 - “Essential safeguard required is that wholesale removal must be monitored by the judgment of a neutral, detached magistrate”

Search Warrants – Approval of Protocols

- Judicial pre-approval of search protocol in warrant
 - *CDT* ruling suggests this requirement.
 - Magistrate has the authority to require a protocol. *In re Search of 3817 W. West End*, 321 F. Supp. 2d 953 (N.D. Ill. 2004). Authority to seize the computers, and ultimately to search them, was conditioned on the government providing the required protocol. (In other words, not only where and what, but how.)
 - But the Supreme Court has stated that the Fourth Amendment does not require that warrants include a search protocol. See *U.S. v. Grubbs*, 547 U.S. 90, 98 (2006); *U.S. v. Dalia*, 441 U.S. 238, 255 (1979).
 - Other circuits have refused to require search protocols in warrants authorizing electronic searches. See, e.g., *U.S. v. Burgess*, 2009 WL 2436674, at *11 (10th Cir. 2009); *U.S. v. Cartier*, 543 F.3d 442, 447-48 (8th Cir. 2008); *U.S. v. Khanani*, 502 F.3d 1281, 1290-91 (11th Cir. 2007); *U.S. v. Brooks*, 427 F.3d 1246, 1251 (10th Cir. 2005); *U.S. v. Upham*, 168 F.3d 532, 537 (1st Cir. 1999).

Search Warrants – Plain View

- Inconsistent application of “plain view” doctrine.
 - *CDT* rejected application of plain view doctrine in ESI context
 - *U.S. v. Lemmons*, 282 F.3d 920 (7th Cir. 2002)
 - Computer file not in plain view when agent must enter commands into computer to access file
 - *U.S. v. Wong*, 334 F.3d 831 (9th Cir. 2003)
 - Computer file in plain view where incriminating images were “immediately apparent” to officers who opened files while conducting lawful computer searches
 - Called into doubt by *Comprehensive Drug Testing*

Search Warrants – Connection to Offense

- Gov't must show computer is related to the crime under investigation.
 - *In re Search Warrant*, Mag. No. 09-320 (D.D.C. June 3, 2009)
 - Without specific showing of this kind a search of the computer's entire contents is "the very general search the 4th Amendment prohibits."
 - *U.S. v. Payton*, 573 F.3d 859 (9th Cir. 2009)
 - Suppressing evidence where there was no indication that the computer was a repository for responsive material.

Post-Indictment Discovery

- 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)
 - Invoked by defense in *U.S. v. Stevens*:
 - production in “readily useable” format
 - production of metadata
 - Is *O’Keefe* the wave of the future?

Post-Indictment Discovery – Data Dumps

- No *Brady* violation for “open file” production of massive volume of ESI. *U.S. v. Skilling*, No. 06-20885, (5th Cir. Jan. 6, 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*, 2009 U.S. Dist. LEXIS 3367 (S.D.N.Y. Jan. 13, 2009).
 - Court found that SEC failed to follow common protocols for electronic document production, while in the agency's Enforcement Manual, the SEC imposes those common protocols on responding parties.
 - SEC’s claim of work product over its organized set of documents rejected.
 - SEC ordered to negotiate search protocol to identify and produce manageable volume of responsive material.

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”

Use at Trial – Getting ESI Into Evidence

- *Lorraine v. Markel American Ins. Co.*, 241 F.R.D. 534 (D. Md. 2007)
- Five hurdles
 - Whether the ESI is relevant;
 - Whether it can be shown to be authentic;
 - Whether it is hearsay;
 - Whether it is an original or a duplicate; and
 - Whether its probative value substantially outweighs the danger of the ESI's unfair prejudice against those it is used against

Use at Trial – Authentication

- Authentication of electronic computer records; party must show:
 - The business uses a computer;
 - The computer is reliable;
 - The business has developed a procedure for inserting data into a computer;
 - The procedure has built-in safeguards;
 - The business keeps the computer in a good state of repair;
 - The witness for the party seeking admission had the computer read out certain data;
 - The witness used proper procedures to obtain the readout;
 - The computer was in working order at the time the witness obtained the exhibit;
 - The witness recognizes the exhibit as the readout;
 - The witness can explain how he or she recognizes the readout; and
 - If the readout contains strange symbols or terms, the witness can explain the meaning of the symbols or terms for the trier of fact