When Responding to a Criminal Subpoena Turns Electronic

This article first appeared in *The New York Law Journal*, March 22, 2010.

by Mark R. Hellerer and Wayne C. Matus

Mark R. Hellerer
Litigation
+1.212.858.1787
mark.hellerer@pillsburylaw.com

Wayne C. Matus
Litigation
+1.212.858.1774
wayne.matus@pillsburylaw.com

Mark R. Hellerer is a partner in Pillsbury's corporate investigations and white-collar defense practices.He was a former assistant U.S. attorney in the Southern District of New York, where he was chief of the major crimes unit. Pillsbury partner Wayne C. Matus serves as heads of Pillsbury's national e-discovery team. Sandra Barragan, as associate at the firm, assisted in the preparation of this article. All reside in the firm's New York office.

Companies served with a criminal subpoena often face a challenging dilemma. With hundreds of gigabytes, or even a few terabytes, of electronically stored information (ESI) on their servers and employees' hard drives, how do they ensure an adequate response to the subpoena without their electronic discovery costs spiraling out of control?

In the civil context, parties are encouraged to meet, confer and cooperate in the selection of key words or other search methodologies. In a criminal investigation, however, no parallel system exists.

Strict compliance with a subpoena seeking ESI may be extraordinarily burdensome and unreasonable both in time and expense. While a subpoenaed company may correctly believe that conducting highly targeted searches would result in its producing documents directly relevant to the government's investigation, the company is often at risk as to whether the protocols it employs may later be deemed by a prosecutor or regulator to be insufficient. The consequences could range from a motion to compel compliance with the subpoena to actual charges of obstruction of justice.

Unfortunately, these issues are rarely presented to courts for resolution, because companies do not wish their first significant interaction with the criminal prosecutor to be a motion to quash the subpoena. Initial dialogue with the government about ESI in a criminal investigation raises a unique set of issues. The government will likely argue that any discussion over narrowing the scope of the subpoena, through use of specific search terms or otherwise, might reveal information about its investigation that it does not wish to show at that stage. On the other side, a company may not wish to reveal its methods for responding to the subpoena, which it may regard as attorney work product.

These are important issues that are not readily resolved. Moreover, because currently no Department of Justice guidelines exist addressing ESI issues, there is a tremendous disparity in how these questions are resolved from district to district around the country.

Through broader application of Federal Criminal Rule 17(c) and more widespread use of practices currently available in the civil context, however, the government and the subpoenaed corporation can

address their concerns in a more productive and efficient manner.

Applying Rule 17(c) in the ESI Context

The power to subpoena is not unlimited. While a subpoena does not have to specify the search terms or methodology to be implemented, it must be reasonable under Federal Criminal Rule 17(c).[1] Reasonableness, of course, depends on many factors, including the scope of the requests and the burden on the party responding to the subpoena.

The unique challenges presented by government requests for ESI in the criminal context were recently addressed by the Ninth Circuit in *United States v. Comprehensive Drug Testing Inc. (CDT)*.[2] The CDT court imposed drastic limitations on the manner in which the government can search electronic evidence. It noted that the potential for producing massive amounts of electronic data, most of it irrelevant to the case, "calls for greater vigilance on the part of judicial officers in striking the right balance between the government's interest in law enforcement and the right of individuals to be free from unreasonable searches and seizures."[3]

Though the *CDT* decision involved allegations of the government's misuse of electronic evidence obtained by search warrant, the court specifically stated the intent was "to guide our district and magistrates judges in the proper administration of search warrants and grand jury subpoenas for electronically stored information."[4]

As the *CDT* court clearly understood, the potential for the government to demand too much electronic data by subpoena is just as prevalent, and problematic, as its potential to seize too much data by search warrant. Most often, the criminal prosecutor issuing a subpoena does not include with it a list of search terms the company can use to search for responsive ESI, thus leaving to defense counsel the obligation of determining how to search ESI for responsive documents.

The government usually argues that the company, rather than the government, is in the best position to know what terms would most likely yield documents responsive to the subpoena. The prosecutor, therefore, will often refuse to "sign off" on a list of search terms suggested by the target's counsel, for fear that key terms were omitted from the list. This forces the subpoenaed company to "live or die" by its list, if it turns out later that a responsive document was not produced.

Where the prosecutor suggests his own list of search terms, the list may include several "flood" terms, generating thousands of false hits. In still other cases, the prosecutor may assert that any use of search terms is inappropriate and every electronic document from relevant custodians must be reviewed manually to ensure that every responsive document is produced.

Yet, the inability to respond to a subpoena by using targeted searches may render the subpoena unreasonably broad, similar to a subpoena that explicitly seeks an unreasonably broad category of documents.

Over 100 years ago, in *Hale v. Henkel,* the U.S. Supreme Court held that subpoena requests must be particularized.[5] Since then, many courts have found subpoena requests to fail this test where they seek production of entire storage devices or overly broad categories of documents.[6]

Given how much data can be contained in ESI, a subpoena that is not sufficiently particularized to allow the recipient to identify responsive documents through targeted search terms or other electronic searching methodologies may well run afoul of these same principles. In fact, the burdens, as measured in time and cost, of running broad searches in e-mail and loose files can be much greater than searching entire file cabinets for responsive documents.

The Benefits of Negotiation

Although no criminal rule requires parties in a criminal investigation to negotiate over the scope and methods of ESI production, some courts may soon impose such a requirement.

In *United States v. O'Keefe*, 537 F.Supp.2d 14, 24 (D.D.C. 2008), a criminal matter, the court applied the Federal Rules of Civil Procedure to resolve an e-discovery dispute over the manner of ESI production.[7] The court noted that, "It is foolish to disregard the [Civil Rules] merely because this is a criminal case, particularly where, as is the case here, it is far better to use these rules than to reinvent the wheel when the production of documents in criminal and civil cases raises the same

problems."[8] Courts in criminal matters have previously referred to the civil rules where they deemed them helpful,[9] but *O'Keefe* appears to be the first time a court has done so with respect to ESI.

Several working groups have recognized for some time the need for increased discussion on ESI issues.

In 2003, a Joint Working Group on Electronic Technology in the Criminal Justice System, sponsored by the Judicial Conference of the United States, including both federal prosecutors and defense attorneys, published a report recommending ways for the two groups to work jointly on effective and efficient handling of ESI.[10] In 2008, the Sedona Conference published its Cooperation Proclamation, which encourages parties to collaborate by jointly developing searches and document retrieval methodologies, and identifying the form of production during discovery so that minimal effort and money is spent on non-substantive issues.[11]

In our view, the recommendations of these groups need to be applied more broadly in the criminal context. It should not be unreasonable for prosecutors and defense counsel to engage in a voluntary meet and confer session with respect to ESI similar to that required under FRCP 26(f).[12] Such a conference would provide the practitioner with the opportunity to avoid making unilateral decisions that may have dire consequences. Indeed, in *United States v. Graham*[13] the court faulted both the government and the defense for not addressing issues relating to the production of ESI earlier in the case, which might have avoided the court's need to dismiss the indictment under the Speedy Trial Act.

Should an informal meet and confer session fail to resolve the parties' differences, company counsel could consider suggesting to the government ways to address their concerns so that they need not file a motion to quash the subpoena. One such method could be a more formalized meet and confer process overseen by a magistrate judge or a special master approved by the government, similar to the civil litigation context. One benefit of such an approach is that the government could share information about its investigation in camera with the magistrate judge or special master, who could then oversee the negotiation process while keeping the goals and the scope of the government's investigation in mind.

In a promising development, the Department of Justice recently appointed a national coordinator for all criminal discovery initiatives. His role is to develop guidelines to assist federal prosecutors in meeting their obligations in criminal discovery, including in the area of retrieval and production of ESI. Although establishing guidelines for prosecutors in negotiating production of ESI from subpoenaed companies is not yet part of his directive, adding such responsibility could prove beneficial to both the government and the defense bar.

Search Methodologies: Pros and Cons

Most would agree that in reviewing ESI to locate documents responsive to a subpoena, use of electronic searching methodologies is a reasonable alternative to manual review of every single e-mail and electronic file.

While a responding party cannot guarantee that every responsive document will be located using a searching methodology, neither can such a guarantee be made when conducting manual review. As one court noted, "the mere suspicion that a document containing relevant evidence might be located in defendant's computer files does not justify the production of all email communications or computer records."[14]

The literature on use of searching methodology in responding to subpoenas presumes that searching methodologies may not necessarily be the better method, but it is a necessary method due to the massive amounts of data that are now stored electronically. According to the Sedona Conference's Best Practices, given the "exponential increase in the volume of information existing in the digital realm, the venerated process of 'eyes only' review has become neither workable nor economically feasible," and may, in fact, be "indefensible."[15]

Just as the *CDT* court required the government to devise search protocols "designed to uncover only the information for which it had probable cause..."[16] the government should also draft its subpoenas and

work together with defense counsel to devise a search protocol designed to collect only the information relevant to its investigation. The Department of Justice Antitrust Division Grand Jury Manual explicitly contemplates such negotiations over broadly-worded requests. It states that:

it is usually advisable to request more documents than fewer with the idea of modifying the particular paragraph when opposing counsel substantiates the difficulty.[17]

DOJ's new national coordinator for criminal discovery initiatives should consider incorporating new guidelines into the U.S. Attorney's Manual to address situations in which strict compliance with the subpoena would require review of massive amounts of data that is likely not relevant to the investigation.

To be sure, not all searching methodologies are created equal. Especially at the early stages of an investigation, thegovernment may not fully trust defense counsel independently to devise a list of search terms reasonably calculated to yield the documents most relevant to its investigation. Indeed, several courts that have reviewed the adequacy of parties' searching methodologies developed solely by attorneys have stated that the parties were required to consult an expert.[18]

The subpoenaed company and the government can avoid unnecessary and costly searches by working together to focus the terms and method used.[19]Another method of reducing costs and ensuring that the government is reasonably likely to receive responsive documents is to agree with the government to search documents iteratively.[20] After the search terms and method have been agreed upon, the company can select a sample of a few hundred documents and then produce the results after processing to assure the government that responsive documents are being located and provided to it. If the sample fails, an iterative process could follow to allow for the revision and refinement of the search terms and methodology.

Conclusion

The need to control ESI review production costs, while still retrieving relevant documents, is as significant on the criminal side as it is on the civil. However, the issue has escaped substantial attention because of the reluctance of defense lawyers to challenge the government and risk alienating the prosecutor.

In our view, the discussion over reasonable responses to ESI requests in criminal investigations needs to take more cues from the area of civil litigation, where attorneys, statisticians and ESI vendors have already been working together to devise more efficient ways to retrieve relevant data while minimizing costs.

While the government and subpoenaed companies regularly resolve ESI production issues through good faith negotiations, that is too often not the case. A more formalized meet and confer process guided by the directives of Rule 17(c), along with potential judicial oversight, could prove useful in addressing this growing problem.

Endnotes

1 See Fed. R. Crim. P. 17(c)(a court may quash or modify a subpoena "if compliance would be unreasonable or oppressive.")

2 579 F.3d 989 (9th Cir. Aug. 26, 2009).

3 Id. at 1006.

4 Id. at 994 (emphasis added).

5 See *Hale v. Henkel*, 201 U.S. 43, 77 (1906) (government's request for all contracts and correspondence between the subpoena target and six different companies violated the "general principle of law with regard to the particularity required in the description of documents.")

6 See, e.g., *In re Grand Jury Subpoena Duces Tecum Dated Nov. 15, 1993,* 846 F.Supp. 11, 12-13 (S.D.N.Y. 1994) (Mukasey, J.) (holding that subpoenas must seek categories of documents, not categories of filing cabinets or electronic storage devices); *Thompson v. Jiffy Lube Int'l Inc.,* No. 05-1203, 2006 WL 1174040, at *3 (D. Kan. May 1, 2006) ("On its face, a request for the production of all corporate and employee email…is overly broad."); *In re Grand Jury Proceedings Witnesses Bardier and Wheeler,* 486 F.Supp. 1203, 1207 (D. Nev. 1980) (government's subpoena seeking "all other records not specifically enumerated above which reflect or are related to the financial activities of those (fourteen) individuals or entities listed" was overbroad).

7 *United States v. O'Keefe,* 537 F.Supp.2d 14, 24 (D.D.C. 2008).

8 Id. at 18.

9 See, e.g., *United States v. Morrison,* 521 F.Supp.2d 246 (E.D.N.Y. 2007); *United States v. Gigante,* 971 F.Supp. 755 (E.D.N.Y. 1997).

10 See "Report and Recommendations, Joint Administrative Office/Department of Justice Working Group on Electronic Technology in the Criminal Justice System Draft Report and Recommendations" (2003), available at http://www.fjc.gov/public/pdf.nsf/lookup/CompInDr.pdf/$file/CompInDr.pdf (last visited on March 3, 2010).

11 The Sedona Conference Cooperation Proclamation, The Sedona Conference® Working Group Series (2008), available at http://www.thesedonaconference.org (last visited on March 3, 2010).

12 See Fed. R. Civ. P. 26(f).

13 *United States v. Graham,* No. 1:05 Cr. 45, 2008 WL 2098044 (S.D. Ohio May 16, 2008).

14 *Thompson,* 2006 WL 1174040, at *3.

15 "The Sedona Conference Best Practices Commentary on the Use of Search and Information Retrieval Methods in E-Discovery," 8 The Sedona Conference Journal 189, 198-99 (2007).

16 *Comprehensive Drug Testing Inc.*, 579 F.3d at 1006.

17 DOJ Antitrust Grand Jury Manual III.D.1.b.2, available at http://www.usdoj.gov/atr/public/guidelines/206782.htm#IIID1.

18 See, e.g., *United States v. O'Keefe,* 537 F.Supp.2d at 24; *Equity Analytics LLC v. Lundin,* 248 F.R.D. 331, 333 (D.D.C. 2008); *Victor Stanley Inc.,* 250 F.R.D. 251, 260 n. 10 (D. Md. 2008).

19 19. See "The Sedona Principles, Second Edition: Best Practices Recommendations & Principles for Addressing Electronic Document Production" ("The Sedona Principles"), Principle 11 at 57, The Sedona Conference® Working Group Series (2007), available at http://www.thesedonaconference.org; The Sedona Conference Cooperation Proclamation, at 4.

20 20. See The Sedona Principles, Principle 11 at 57.

Pillsbury Winthrop Shaw Pittman LLP | 1540 Broadway | New York, NY 10036 | 1.877.323.4171

Pillsbury Winthrop Shaw Pittman LLP