BNA, INC.

WHITE COLLAR CRIME REPORT

BNA Employee-Owned Since 1947

VOL. 4, NO. 4 116-120 FEBRUARY 13, 2009

E-DISCOVERY

'E-Discovery' in the Criminal Context: Considerations for Company Counsel

BY JUSTIN P. MURPHY & STEPHEN M. BYERS

The rules governing the preservation, collection, production, and use of electronically stored information (ESI) are developing rapidly in the context of civil litigation, spurred in part by amendment of the Federal Rules of Civil Procedure in 2006 to deal with some of the complications presented by voluminous electronic evidence. Criminal defense lawyers and prosecutors, on the other hand, generally are far behind their civil counterparts in grappling with these issues and have no formal procedural rules to guide the way. But the world of criminal e-discovery is evolving every day, particularly in the contexts of subpoena compliance, search warrants, and post-indictment discovery.

Mr. Byers is a partner in Crowell & Moring LLP's Washington, D.C., office and a member of the firm's White Collar & Securities Litigation and E-Discovery and Information Management groups. He can be contacted at sbyers@crowell.com and (202) 624-2878. Mr. Murphy is a counsel in the firm's Washington, D.C., office and a member of the White Collar & Securities Litigation and E-Discovery and Information Management groups. He can be contacted at justin.murphy@crowell.com and (202) 624-2536.

Subpoena Compliance

The Duty to Preserve ESI. In a typical white collar criminal investigation, the first e-discovery issue confronted by defense counsel is usually the need to preserve relevant ESI. Civil litigators also must deal with this issue at the outset of a case, but there is an important distinction: The consequences—both direct and collateral—of failing to preserve relevant evidence can be far more severe in criminal cases. Thus, the problems presented by voluminous, widely dispersed, and constantly changing ESI can be particularly acute.

The first step is determining when a duty to preserve ESI has been triggered. Service of a subpoena is one obvious trigger, but the duty can arise prior to that point. A classic example is the prosecution of Arthur Andersen LLP in the Enron case for destruction of documents at a time when the firm could reasonably expect a government investigation but had not yet received a subpoena. But when, exactly, does the duty arise?

In civil litigation, the basic rule is fairly well-developed: ''Whenever litigation is reasonably anticipated, threatened or pending against an organization, that organization has a duty to preserve relevant information.''[1] There is scant caselaw in the criminal arena on this point, but in general the same principle applies: The duty to preserve potentially relevant information

 ISSN 1559-3185

arises when a government investigation is threatened or pending or can be reasonably anticipated. The obstruction-of-justice provisions in the Sarbanes-Oxley Act of 2002, which were enacted in reaction to the conduct at Arthur Andersen described above, echo this standard, making it clear that a government investigation need not have commenced and a subpoena need not have been issued for the duty to preserve to arise.[2]

Once the duty to preserve arises, one must move quickly to implement a hold order that tracks the government's information request (if available) to ensure that employees are on notice of the types of ESI that must be maintained. It is also becoming a standard in criminal practice to have forensically imaged hard drives—especially for ''key'' players. Further, the involvement of a forensic expert can be critical to the assessment and successful preservation of ESI in an enterprise environment, whether the company is large or relatively small.

Unlike in civil litigation, special preservation challenges can arise in the criminal context when a matter must be kept confidential. In these circumstances, counsel may be limited in the extent to which they can communicate with custodians of potentially relevant documents, such as through a broadly distributed hold order or in the course of imaging computer hard drives. In some situations, counsel may wish to confer with the government to reach an agreement on how to balance the need for secrecy against the need to preserve relevant information. A more difficult situation arises when counsel is conducting an internal investigation and the government is not yet in the picture. Here a possible approach is to take only surreptitious steps to preserve ESI, such as capturing ''snapshots'' of e-mail accounts from servers. This approach risks the loss of other data, such as ESI stored on hard drives that is deleted either nefariously or in the ordinary course of business. Should a government investigation ensue, counsel may need to convince the authorities that the right balance was struck between preserving evidence and compromising the integrity of the internal investigation, and a clear record of decision-making and steps taken can be critical in that effort.

As noted above, the consequences of failing to preserve potentially relevant ESI can be broader and more severe in criminal cases. For starters, failing to maintain relevant ESI, or at least build a record of thorough, good-faith efforts to do so, can color the views of prosecutors and agents at the outset of a case. This can affect judgments about culpability and cooperation, which can ultimately influence charging decisions and plea negotiations. In addition, a failure to preserve potentially relevant information may adversely impact calculations under the U.S. Sentencing Guidelines by increasing the defendant's culpability score.[3] Apart from these collateral consequences, preservation failures can expose the client to an additional investigation for obstruction of justice. Because most government investigators are skeptical by nature and often encounter efforts to destroy evidence, they may assume bad intent unless good faith can be demonstrated.

In extreme cases where intent can be shown, any number of obstruction-of-justice statutes can be brought to bear. Because obstruction is often easier to prove than the underlying crime, which may involve complicated issues ill-suited to a jury trial, some prosecutors may favor the use of these statutes. Most prosecutors are keenly aware of the potential ramifications of failures to preserve evidence and the leverage that can result. An official Justice Department publication observed: ''It is crucial to understand that deliberately ignoring preservation requirements could result in prosecution for obstruction of justice.''[4]

Finally, it is notable that the mishandling of ESI by private litigants in civil actions can also lead to criminal penalties. In *United States v. Lundwall*, the district court determined that the defendants could be prosecuted under 18 U.S.C. § 1503 for allegedly withholding and then destroying documents sought by plaintiffs' counsel during discovery in a civil discrimination lawsuit between private parties.[5] More recently, a judge in the Eastern District of New York referred a case to the U.S. attorney for electronic discovery abuses.[6]

International Laws. Dealing with ESI overseas presents unique problems. Some arms of the DOJ, such as the Antitrust Division, take the view that they have no authority, as a matter of international comity, to exercise law enforcement authority overseas through a subpoena and therefore will not require production of foreign documents. However, they will certainly require that relevant ESI (which may ultimately be obtained via a Mutual Legal Assistance Treaty or produced voluntarily) be preserved. But counsel must tread carefully in preserving and producing such material.

Foreign data protection laws, particularly in Europe, impose specific requirements on entities holding ''personal data,'' which is defined very broadly. Such laws, which place limitations on ''processing'' personal data, typically extend, for example, to virtually all company e-mails. Thus, the data protection laws of European and other countries may impact a company's right to even preserve, much less collect and produce, potentially relevant ESI from a foreign office or subsidiary, including in some cases data ''housed'' in the United States. Accordingly, before ''processing'' ESI from a foreign office or subsidiary, it is advisable to consult with a privacy expert in the jurisdiction in question.

Conferring With the Government on ESI Issues. Federal Rule of Civil Procedure 26(f), as amended in 2006, requires that parties meet and confer to address and avoid problems with ESI early in the litigation process. There is no criminal rule analog to Fed. R. Civ. P. 26(f), but the

[1] *Sedona Conference Commentary on Legal Holds*, August 2007; *Zubulake v. UBS Warburg*, 229 F.R.D. 422 (S.D.N.Y. 2004).

[2] *See* 18 U.S.C. § 1519 (punishing document destruction in ''contemplation'' of a federal investigation).

[3] *See* U.S.S.G. § 8C2.5.

[4] *See* Andrew D. Goldsmith and Lori A. Hendrickson, *Investigations and Prosecutions Involving Electronically Stored Information*, United States Attorneys' Bulletin Vol. 56, No. 3, May 2008.

[5] *United States v. Lundwall*, 1 F. Supp. 2d 249 (S.D.N.Y. 1998).

[6] *Gutman v. Klein*, No. 03-1570, 2008 WL 5084182 at *2 (E.D.N.Y. Dec. 2, 2008). *See also Bryant v. Gardner*, No. 07-5909, 2008 WL 4966589 (N.D. Ill. Nov. 21, 2008) (court ordering defendant to show cause why issue of false declaration should not be referred to U.S. attorney's office, rather than a direct referral).

  WCR ISSN 1559-3185

need to identify and address ESI issues early on is just as (and perhaps more) important in a criminal matter given the significant consequences that can result from spoliation. However, reaching agreement in a criminal case can be more difficult because the symmetry of risks and interests between the two parties that is common in civil litigation generally does not exist; the government will be far less worried about the ''boomerang'' effect of imposing unfair burdens on defense counsel.

Before engaging the government in such a discussion, it is critical to understand your client's electronic systems, where materials are located, and how they can be harvested in a cost-effective manner. It is often advantageous to have a forensic specialist assist with the mapping, preservation, and collection of potentially relevant material not only to be sure the job is done right, but to aid in communicating clearly and effectively with the government. Such experts may be able to convince the government that the most pertinent ESI can be produced without incurring undue expense.

After having taken the necessary steps to ensure that ESI is being preserved, counsel should reach out to the government and consider a discussion similar to a Rule 26(f) conference. Such discussions can prevent problems down the road; both the company and the government should reach a common understanding on the scope of the production. This can include, for example, the date ranges of materials to be reviewed and produced, the specific custodians whose ESI should be examined, the use of search-term filters to cull the data prior to review and production, and the form of production to the government.

There are more subtle benefits to this dialogue as well. Such discussions may provide defense counsel with their first opportunity to influence and affect how the government will view the client, particularly a corporate client potentially on the hook for the aberrational conduct of one or more ''rogue employees.'' In addition, discussion of issues such as which custodians should be considered ''key'' and which aspects of the subpoena are most important to the government may provide valuable insight into the government's case that the prosecutor would otherwise be hesitant to reveal.

Finally, if company counsel uncovers intentional efforts by employees to delete or otherwise manipulate relevant ESI in response to an investigation, such incidents must be addressed immediately. By getting to the bottom of such matters, taking all reasonable steps to rectify the situation (such as by restoring deleted documents from backup tapes or through forensic examination of hard drives), and, in certain circumstances, reporting promptly to the government, a company might very well earn a complete free pass on obstruction issues while the government pursues the employees involved.

New Federal Rule of Evidence 502. Federal Rule of Evidence 502, which was enacted in September 2008, has the potential to significantly impact the treatment of privileged materials in the context of a law enforcement subpoena. The new rule was driven primarily by concern with the immense costs associated with thoroughly reviewing huge amounts of ESI in an effort to avoid production of privileged material. Three aspects of the rule have potential application in the context of subpoena compliance.

First, Rule 502(b) essentially codifies the majority common law rule on inadvertent production. Specifically, inadvertent production of privileged documents will not constitute a waiver as long as reasonable steps were taken to prevent disclosure and the party holding the privilege took prompt and reasonable steps to rectify the error. In addition, Rule 502(a) provides that subject-matter waiver will not apply to inadvertent disclosures of privileged material.

Second, Rule 502(e) is designed to ensure that parties that enter into nonwaiver agreements receive the full protection of those agreements. This would apply, for example, to ''clawback'' agreements—under which the government agrees to promptly return any inadvertently produced privileged material—and ''quick peek'' arrangements—under which documents are produced wholesale prior to privilege review and the party receiving the documents selects which nonprivileged materials it wants to retain. Clawback agreements in particular are becoming more common in the context of law enforcement subpoenas in an effort to speed up and reduce the costs of review and production. Rule 502(e) gives those nonwaiver agreements extra force.

Third, Rule 502(d) is intended to address a potential problem with the types of party agreements just described: Those agreements may be binding in the proceeding at hand, but not necessarily in other proceedings. This dynamic is especially important in the criminal context because of the implications for parallel proceedings such as civil litigation and investigations by regulatory agencies. Rule 502(d) provides that a federal court order limiting waiver, such as a clawback arrangement in the form of an order, applies with full force in any other federal or state proceeding, even as to third parties.

The application of Rule 502(d) in the criminal context, however, is uncertain. Approaching the court for an order memorializing an agreement on waiver is relatively straightforward in civil litigation. In the typical criminal case, however, one or both parties would have to approach the court responsible for supervision of the grand jury proceedings out of the blue. One can also imagine why a prosecutor amenable to a clawback agreement would be hesitant to approach the court for an order, unless there was a very clear benefit, such as receiving a document production in a matter of weeks rather than months.

Search Warrants

The unique challenges presented by the very nature of ESI create problems in the context of search warrants as well. In particular, the 21st century phenomenon of vast amounts of intermingled computer documents has run headlong into the 18th century search and seizure strictures of the Fourth Amendment. On the one hand, computers can store millions of pages of documents, some of which can be hidden or disguised to undermine the government's search. Therefore, searches pursuant to lawful warrants need to be somewhat invasive. On the other hand, this inevitable invasiveness must be reconciled with the Fourth Amendment's requirement for particularity in identifying ''the place to be searched and the . . . things to be seized.'' A vast landscape of contradictory case law is developing as courts grapple with this conundrum.

Courts have been inconsistent in applying the Fourth Amendment's ''particularity'' standard to ESI. For ex-

ample, some courts have imposed *ex ante* restrictions on the government, requiring that warrants for ESI searches focus specifically on particular files or types of electronic evidence. Conversely, other courts have permitted generalized descriptions of computer equipment to be searched and more or less given the government free rein to examine data therein on the theory that all data in a computer is in ''plain view.''[7]

***Ex Ante* Restrictions on ESI Searches.** Some courts have given magistrate judges the authority to control how a search will be conducted. In those instances, the government was required not only to identify *where* it would search and *what* it would seize, but *how* the search would be carried out.[8] Where the government has claimed that protocols should not be required, some courts have criticized this assertion.[9] For example, in *In the Matter of 1406 N. 2nd Avenue*, the court, although allowing the government to proceed without a search protocol, noted that ''[t]he Government's argument that a search protocol should never be required appears disingenuous, particularly since the Department of Justice manual, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations,* July 2002, encourages that search warrant requests include an explanation of the search methodology.''[10]

The DOJ Search and Seizure of Electronic Evidence guide cited in *1406 N. 2nd Avenue* does, in fact, suggest that incorporation of search protocols in a warrant affidavit is appropriate without, of course, suggesting that such an approach should be mandatory. The guide notes that a ''successful computer search warrant'' should explain ''both the search strategy and the practical considerations underlying the strategy in the affidavit.''[11] Importantly, it addresses intermingled ESI, remarking that the ''affidavit should also explain what techniques the agents expect to use to search the computer for the specific files that represent evidence of crime and may be intermingled with entirely innocuous documents.''[12]

The BALCO Case. The Ninth Circuit's decision in *United States v. Comprehensive Drug Testing Inc.* takes a different approach and provides a useful frame of reference for these issues.[13] In 2004, government agents executed search warrants at an independent medical testing laboratory, seeking information about 10 baseball players who had obtained steroids from BALCO. During the search, the government made duplicate copies of the lab's computer directories, which included the intermingled data concerning more than 100 other baseball players' test results as well as those of athletes in other sports. On the basis of the information in these directories, the government obtained additional search warrants relating to the approximately 100 other baseball players who were listed in the database as having tested positive for steroids.[14]

The court upheld the search, finding that the government could seize all the information in the directory, rather than segregating and seizing information within the scope of the warrant. The court found that the government had no duty to rely on company employees to highlight the particular files that would be ''seizable'' under the warrant and that there was ''no reason to assume'' that relevant materials would be listed under the name of the specific baseball players listed in the warrant. In upholding the seizure of the directory, the court added that ''while the government may seize intermingled data for off-site review to minimize intrusiveness of a computer search, it may not retain or use the evidence after proper objections are raised, unless a magistrate subsequently reviews and filters the evidence off-site.'' Notably, under this approach the discovery of intermingled documents in a database would not automatically prompt a neutral magistrate's review; instead, such a review would occur only upon a ''proper post-seizure motion by the aggrieved parties.''

A strongly worded dissent, quoting the district court judge, began: ''What happened to the Fourth Amendment? Was it repealed somehow?'' The dissent's ''most profound disagreement'' with the majority opinion was the conclusion that the government could legally seize all the data simply because it was intermingled with data responsive to the warrant. The ''wholesale seizure for later detailed examination of records not described in a warrant . . . has been characterized as 'the kind of investigatory dragnet that the fourth amendment was designed to prevent.' '' The dissent agreed with the lower court judge who said the ''implications of approving such behavior are staggering,'' and added, ''Under the majority's holding, no laboratory or hospital or health care facility could guarantee the confidentiality of records.'' This dissent also proposed that a neutral magistrate be required to examine the intermingled data, even if objections were not raised, to ensure that the private information the government is not entitled to seize remains private.[15]

The BALCO decision has been subject to much debate because of its apparent blessing of the wholesale seizure of highly personal information well outside the scope of a search warrant and the arguably limited mechanism for judicial supervision of review of such data by the government. This is particularly troubling where, as in the BALCO case, the seized data is relevant to third parties who are unaware of the seizure and who previously were outside the scope of the investigation. With government agents able to seize private ESI housed on databases or directories without a search warrant as long as there is other information on the

[7] *Compare United States v. Riccardi,* 405 F.3d 852 (10th Cir. 2005), *with United States v. Lacy*, 119 F.3d 742 (9th Cir. 1997). *See also Bytes, Balco, and Barry Bonds: An Exploration of the Law Concerning the Search and Seizure of Computer Files and an Analysis of the Ninth Circuit's Decision in United States v. Comprehensive Drug Testing Inc.,* 97 J. Crim. L. & Criminology 1151, 1156 (2007).

[8] *In re Search of 3817 W. West End*, 321 F. Supp. 2d 953, 955-56 (N.D. Ill. 2004) (district court holding that magistrate possessed authority to require protocol to ensure that the search was ''reasonably designed'' to focus on the documents related to criminal activity).

[9] *See id.*; *In re Search of the Premises Known as 1406 N. 2nd Avenue*, No. 05-28, 2006 WL 709036 (W.D. Mich. Mar. 17, 2006).

[10] *In re 1406 N. 2nd Avenue,* 2006 WL 709036, at *6 n.3.

[11] Department of Justice, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations,* July 2002.

[12] *Id.*

[13] *United States v. Comprehensive Drug Testing Inc.,* 473 F.3d 915 (9th Cir. 2006), *reh'g granted*, 545 F.3d 1106 (9th Cir. Sept. 30, 2008).

[14] *Id.* at 920-24.

[15] *Id.* at 965.

  WCR ISSN 1559-3185

same database or directory that is responsive to the search warrant, it would seem we are coming perilously close to exactly the kind of ''general warrant'' the founders sought to prohibit in enacting the Fourth Amendment.

Other Cases Applying the Two-Step Approach. Other courts have taken an approach similar to that advocated in the BALCO dissent. In *United States v. Carey*, a government agent executing a search warrant for information (including computers) related to drug distribution and possession opened a .jpeg file that contained what he believed was child pornography.[16] The agent downloaded 244 other image files, reviewed a sampling of them and then returned to looking for evidence of drug transactions.[17] Rejecting the government's ''plain view'' argument, the Tenth Circuit determined that the agent's search for all but the first image file exceeded the scope of the search warrant.[18] Acknowledging that the ''storage capacity of computers requires a special approach,'' the court concluded that ''where officers come across relevant documents so intermingled with irrelevant documents that they cannot feasibly be sorted at the site, the officers may seal or hold the documents pending approval by a magistrate of the conditions and limitations on a further search through the documents.''[19]

Wide Latitude for the Government. Most courts have been reluctant to endorse the *ex ante* or two-step special approach. For example, in *United States v. Tylman*, the court criticized the ruling in *3817 W. West End*, asserting: ''That case . . . has been ignored by other courts addressing the same issue. . . . How a search warrant is to be executed is normally left to the discretion of the agents, and the exercise of that discretion remains subject to a subsequent review for reasonableness.''[20] Other courts have also focused on the ''reasonableness'' of the government's actions.[21] Some courts also have argued that warrants failing to limit searches to specific e-mails or ESI files are reasonable because file names can be modified, disguised, or changed and that the government should not be bound by the ''self-labeling'' selected by the targets of a search when executing a warrant.[22]

[16] *United States v. Carey*, 172 F.3d 1268, 1271 (10th Cir. 1999).

[17] *Id.*

[18] *Id.* at 1276.

[19] *Id.* at 1275.

[20] *United States v. Tylman*, No. 06-20023, 2007 WL 2669567, at *12-13 (C.D. Ill. Aug. 22, 2007).

[21] *United States v. Gray*, 78 F. Supp. 2d 524, 529 (E.D. Va. 1999) (upholding a seizure of child pornographic images under a warrant permitting the examination and seizure of materials relating to the unauthorized access of a government computer because a search of all the files on the computer was permissible to determine whether they fell within the scope of the warrant).

[22] *United States v. Adjani*, 452 F.3d 1140, 1150 (9th Cir. 2006); *United States v. Hill*, 459 F.3d 966, 978 & n.14 (9th Cir. 2006) (files may be disguised, relevant documents may be intermingled with irrelevant ones, and ''there is no way to know what is in a file without examining its contents''). *See also Bytes, Balco, and Barry Bonds*, *supra* note 7, at 1165.

Post-Indictment Discovery

After indictment, the *government's* duty to preserve and produce ESI comes into play.[23] Although the Federal Rules of Criminal Procedure do not specifically address e-discovery, the influence of the Federal Rules of Civil Procedure on criminal practice in this area is already apparent.

In *United States v. O'Keefe*, the court held that a document production by the government must adhere to standards similar to those set forth in Rule 34 of the Federal Rules of Civil Procedure.[24] In *O'Keefe*, the court noted that there was no rule in criminal cases to guide courts in determining whether a production of materials by the government has been in an appropriate form or format.[25] Recognizing that the ''big paper case'' would be the exception rather than the rule in criminal cases, the court observed: ''The Federal Rules of Civil Procedure in their present form are the product of nearly 70 years of use and have been consistently amended by advisory committees consisting of judges, practitioners, and distinguished academics to meet perceived deficiencies. It is foolish to disregard them merely because this is a criminal case, particularly where . . . 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.''[26] *O'Keefe's* importation of the civil rules into a criminal case has already been advanced by other criminal defendants and has been acknowledged by a recent U.S. Attorney's Bulletin.[27]

While Rule 34 of the Federal Rules of Civil Procedure offers a logical application to criminal proceedings, there are other civil e-discovery rules that may have future applications in criminal law as well. For example, Rule 37(e) of the Federal Rules of Civil Procedure, the so-called ''safe harbor'' provision that addresses failures to preserve ESI, could potentially provide a ''safe harbor'' for the government in its post-indictment discovery obligations, an aspect of the new civil rules also noted by the *O'Keefe* court as having possible relevance in criminal cases.[28] In general, if the ESI deletion resulted from routine operation of the government's com-

[23] Fed. R. Crim. P. 16. The government has a duty to preserve all material exculpatory evidence. A failure to preserve, whether or not government acted in bad faith, is a breach of defendant's due process rights. *See United States v. Branch*, 537 F.3d 582 (6th Cir. 2008).

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

[25] *Id.* at 18-19.

[26] *Id.*

[27] *See United States v. Stevens*, No. 08-231 (D.D.C. Sept. 2, 2008), Defendant's Motion to Compel Discovery (''even civil litigants must either produce documents as they are kept in the course of business or label the documents in response to requested subject areas. Where the government produces documents in 'an undifferentiated mass in a large box without file folders or labels, then these documents have not been produced in the manner in which they were ordinarily maintained as [Fed. R. Civ. P. 34] requires' and thus the government has equally failed to meet its obligations under Fed. R. Crim. P. 16.''); Goldsmith and Hendrickson, *Investigations and Prosecutions Involving Electronically Stored Information*, *supra* note 4 (in citing *O'Keefe*, noting that ''[p]rosecutors should be aware that federal judges may hold them to certain standards common to civil litigation.'').

[28] *O'Keefe*, 537 F. Supp. 2d at 22 (D.D.C. 2008).

puter systems, it may be protected from sanctions. This ''pass'' received by the government may constitute a double standard: Defendants face severe sanctions (including potential criminal prosecution) for failure to preserve ESI, especially if that information was deleted in the ordinary course of business after a defendant's duty to preserve had arisen. Conversely, the government in some instances may be protected for similar conduct if the principles of Rule 37(e) were applied in the criminal context.

However, some post-indictment discovery violations have resulted in significant sanctions for the government. In *United States v. Graham*, the government was slow to produce millions of documents and other media, and the defendants had great difficulty in coping with the large volume.[29] The court dismissed the indictment for Speedy Trial Act violations but acknowledged that discovery was at the heart of the matter: ''In this case, the problem . . . is and has been discovery . . . . One, the volume of discovery in this case quite simply has been unmanageable for defense counsel. Two, like a restless volcano, the government periodically spews forth new discovery, which adds to defense counsels' already monumental due diligence responsibilities. Three, the discovery itself has often been tainted or incomplete.''[30] In dismissing the case, the court noted that although the government did not act in bad faith, ''discovery could have and should have been handled differently.''[31]

Conclusion

E-discovery issues cut across various phases of white collar criminal cases, and the law in this area is evolving rapidly as ESI becomes the dominant form of evidence. Defense counsel and prosecutors would be wise to keep up with these developments lest they learn the hard way what most sophisticated civil litigators have already come to appreciate: Ignoring ESI issues because they are ''too technical'' or seem the province of junior attorneys can lead to critical mistakes affecting the outcome of your case.

[29] *United States v. Graham*, No. 05-45, 2008 WL 2098044, at *2-3 (S.D. Ohio May 16, 2008).

[30] *Id.* at *5.

[31] *Id.* at *8.

  WCR ISSN 1559-3185