



DIGITAL DISCOVERY & E-EVIDENCE



VOL. 9, NO. 10

REPORT

OCTOBER 1, 2009

CRIMINAL E-DISCOVERY

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.

Crowell & Moring’s Justin P. Murphy and Stephen M. Byers discuss how the world of criminal e-discovery is evolving, and how it impacts subpoena compliance, search warrants, and post-indictment discovery.

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

By JUSTIN P. MURPHY AND STEPHEN M. BYERS

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:

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.

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.

Subpoena Compliance

The Duty to Preserve ESI. 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 case law in the criminal arena on this point, but in general the same principle applies: the duty to preserve potentially relevant information 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.

Preservation Challenges. 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 might need to convince the authorities that the right balance was struck between preserving evidence and compromising the integrity of the internal investigation; a clear record of decision-making and steps taken can be critical in that effort.

Potential Obstruction Charges. 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

“It is crucial to understand that deliberately ignoring preservation requirements could result in prosecution for obstruction of justice.”

ANDREW D. GOLDSMITH AND LORI A. HENDRICKSON
UNITED STATES ATTORNEYS’ BULLETIN, MAY 2008

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

Civil Actions Leading to Criminal Charges. 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, courts have referred cases to U.S. Attorneys for criminal investigation of electronic discovery abuses, including by third parties.⁶

International Laws. Dealing with ESI overseas presents unique problems. Some arms of the DOJ, such as the Antitrust Division, generally forbear, as a matter of international comity, from exercising law enforcement authority overseas through a subpoena and therefore

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 See *Gutman v. Klein*, No. 03-1570, 2008 WL 5084182 at *2 (E.D.N.Y. Dec. 2, 2008); *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). See also *Sonomedica, Inc. v. Mohler*, 2009 WL 2371507 (E.D. Va. July 28, 2009) (finding third parties in contempt for violation of court’s orders, including spoliation of ESI, and referring case to U.S. Attorney’s office for criminal investigation).

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).

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 might 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 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.

Less Obvious Benefits. 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 impact significantly 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:

Codification of Common Law—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.

Clawbacks—Second, Rule 502(e) is designed to ensure that parties that enter into non-waiver 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 non-privileged 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 non-waiver agreements extra force.

Parallel Proceedings—Third, Rule 502(d) is intended to address a potential problem with the types of party agreements just described: those agreements might 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.

[T]he 21st century phenomenon of vast amounts of intermingled computer data has run headlong into the 18th century search and seizure strictures enshrined by the founders in the Fourth Amendment.

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 data has run headlong into the 18th century search and seizure strictures enshrined by the founders in 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.

Particularity and ESI. Courts have been inconsistent in applying the Fourth Amendment's "particularity" standard to ESI. For example, 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 and use data therein on the theory that all data in a computer is in "plain view."⁷

Most recently, in *United States v. Comprehensive Drug Testing, Inc.* ("CDT"), an *en banc* panel of the U. S. Court of Appeals for the Ninth Circuit essentially

rejected application of the plain view doctrine in this context and established stringent criteria for search warrants aimed at ESI.⁸ Because CDT is likely to be a touchstone for further jurisprudence in this area, it is worth close examination.

The Ninth Circuit's New Standards. *Comprehensive Drug Testing* was the result of efforts by government investigators in the BALCO steroid scandal to obtain drug testing records for 10 Major League Baseball players. The facts of the case are rather convoluted, involving a series of subpoenas and search warrants in three different judicial districts, but can be summarized as follows: in 2004, government agents executed search warrants at an independent medical testing laboratory, seeking information about the 10 baseball players, who had allegedly obtained steroids from BALCO.

During the search, the government made duplicate copies of the lab's computer directories, which included drug testing data for more than 100 other baseball players, as well 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.

Each of the district courts involved found a violation of the Fourth Amendment,⁹ but a panel of the Ninth Circuit disagreed, ruling in favor of the government.¹⁰

In August 2009, an *en banc* panel reversed the original panel ruling. The court confronted the ESI search conundrum head-on, stating in the opening paragraph of its opinion that the case was about "the procedures and safeguards that federal courts must observe in issuing and administering search warrants and subpoenas for electronically stored information."

The court rejected the government's argument that data beyond the 10 ballplayers was in "plain view." Such an approach, the court held, would "make a mockery" of procedures designed to "maintain the privacy of materials that are intermingled with seizable materials, and to avoid turning a limited search for particular information into a general search of office file systems and computer databases."

The court determined that "greater vigilance on the part of judicial officers" is required due to "the reality that . . . over-seizing is an inherent part of the electronic search process. . . ." In an attempt to ensure such vigilance, the court established the following explicit requirements:

- 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.

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 *United States v. Comprehensive Drug Testing, Inc.*, 2009 WL 2605378 (9th Cir. Aug. 26, 2009).

⁹ *United States v. Comprehensive Drug Testing, Inc.*, 473 F.3d 915, 944 (9th Cir. 2006) (quoting one of the district court opinions: "What happened to the Fourth Amendment? Was it repealed somehow?").

¹⁰ *Comprehensive Drug Testing, Inc.*, 473 F.3d 915.

■ 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.

Adoption of these rules represents the first serious attempt by a federal appellate court to fashion specific, comprehensive guidance for lower courts confronted with the inevitable clash between the Fourth Amendment and increasingly common broad seizures of intermingled ESI. As the court observed:

"[t]he pressing need of law enforcement for broad authorization to examine electronic records . . . creates a serious risk that every warrant for electronic information will become, in effect, a general warrant, rendering the Fourth Amendment irrelevant."

The Ninth Circuit is now leading the way in judicial efforts to avoid that result.

Increasing Judicial Skepticism. Applications for search warrants are, of course, *ex parte* proceedings and more often than not the government gets exactly what it wants. But judicial skepticism of the need for dragnet seizures of ESI seems to be increasing.

For example, a magistrate judge in the District of Columbia who is widely respected for his e-discovery expertise recently issued a written opinion rebuffing the government's request for authority to seize computer data because it had not made a sufficiently specific showing that the target's computer was related to the alleged crime.¹¹

The judge expressed his concern that under these circumstances a "forensic search of [the computer's] entire contents . . . appears to me to be the very general search that the 4th Amendment prohibits."¹²

There is no indication, however, that the judge considered the sort of two-step approach taken by the Ninth Circuit in *CDT*, in which a broad seizure is permitted, but subsequent review by the government is controlled to prevent an unbounded fishing expedition.

Other courts have employed a two-step approach similar to that required by the Ninth Circuit's ruling in *CDT*, although without dictating the manner in which the seized data must be handled.

For example, 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 the agent believed was child pornography.¹³ The agent downloaded 244 other image files, reviewed a sampling of them and then returned to looking for evidence of drug transactions.¹⁴

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.¹⁵ 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."¹⁶

Another approach taken by courts to mitigate the "general warrant" risk articulated by the Ninth Circuit in *CDT* is to give magistrate judges the authority to control how a search will be conducted. In those instances, the government has been required not only to identify *where* it would search and *what* it would seize, but *how* the search would be carried out.¹⁷

Judicial skepticism of the need for dragnet seizures of ESI seems to be increasing.

Even where such protocols were not imposed, some courts have defended their authority to impose them in other cases. 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."¹⁸

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."¹⁹

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."²⁰

¹⁵ *Id.* at 1276.

¹⁶ *Id.* at 1275. See also *Payton*, 573 F.3d at 864 (endorsing practice of seeking a second explicit warrant to search computer contents when agents "encounter a computer that they have reason to believe should be searched.").

¹⁷ *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).

¹⁸ *In re 1406 N. 2nd Avenue*, 2006 WL 709036, at *6 n.3.

¹⁹ Department of Justice, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*, July 2002.

²⁰ *Id.*

¹¹ *In re Application for Search Warrant*, Mag. No. 09-320 (D.D.C. June 3, 2009) (Facciola, M.J.).

¹² *Id.* See also *United States v. Payton*, 573 F.3d 859, 864 (9th Cir. 2009) (suppressing evidence resulting from search of computer where there was "no . . . evidence pointing to the computer as a repository for the evidence sought in the search.").

¹³ *United States v. Carey*, 172 F.3d 1268, 1271 (10th Cir. 1999).

¹⁴ *Id.*

Many courts, however, have been reluctant to impose restrictions on the government. 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.”²¹

Other courts have also focused on the “reasonableness” of the government’s actions.²² 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.²³

Post-Indictment Discovery

When the Shoe’s on the Other Foot. After indictment, the government’s duty to preserve and produce ESI usually comes into play.²⁴ The government’s failure to meet these duties often involves conduct that it would not tolerate from subjects and targets at the investigatory stage of the case, and courts are beginning to take the government to task for such failures.

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.²⁵ 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.²⁶

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.”²⁷

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.²⁸

Post-Indictment Safe Harbor? 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.²⁹

In general, if the ESI deletion resulted from routine operation of the government’s computer systems, it may be protected from sanctions. But this may constitute a double standard: as noted above, defendants can face severe sanctions—both explicit and subtle—for failure to preserve ESI during the investigatory phase of the case, even if that information was deleted in the ordinary course of business.

Conversely, the government in some instances may be protected for similar conduct if the principles of Rule 37(e) were applied in the context of post-indictment discovery.

Given the potential for grafting civil rules onto the criminal process, civil enforcement cases in which the government’s discovery failures have been the subject of judicial opinions may be particularly instructive.

For example, in *S.E.C. v. Collins & Aikman Corp.*,³⁰ the SEC produced 1.7 million documents, maintained in different databases and with different metadata protocols, to the defendant. In response to the defendant’s objection to this “data dump,” the SEC argued that although it had internally organized its documents in folders corresponding to the specific factual allegations, that compilation constituted attorney work product.

The court disagreed, stating “[i]t is patently inequitable to require a party to search ten million pages to

²¹ *United States v. Tylman*, No. 06-20023, 2007 WL 2669567, at *12-13 (C.D. Ill. Aug. 22, 2007).

²² *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 of a search of all the files on the computer was permissible to determine whether they fell within the scope of the warrant).

²³ *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.

²⁴ 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).

²⁵ *United States v. O’Keefe*, 537 F. Supp. 2d 14 (D.D.C. 2008).

²⁶ *Id.* at 18-19.

²⁷ *Id.*

²⁸ 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.”).

²⁹ *O’Keefe*, 537 F. Supp. 2d at 22 (D.D.C. 2008).

³⁰ *S.E.C. v. Collins & Aikman Corp.*, 256 F.R.D. 403 (S.D.N.Y. 2009).

find documents already identified by its adversary as supporting the allegations of a complaint.”³¹

The court also criticized the “SEC’s blanket refusal to negotiate a workable search protocol responsive to [the defendant’s] requests” as “patently unreasonable.”³² The court ordered the parties to meet and develop a search protocol that would reveal “at least some of the information defendant seeks.”³³

The court’s conclusion—that “[w]hen a government agency initiates litigation, it must be prepared to follow the same discovery rules that govern private parties”³⁴—may have application in the criminal context as well.

While the ruling in *Collins* may be encouraging to defense counsel confronting a massive ESI production from the government, the line between an impermissible “data dump” and permissible “open file” production remains unclear. In *United States v. Skilling*,³⁵ the defendant argued that the government’s production of hundreds of millions of pages violated the government’s *Brady* obligations as the “voluminous open file . . . suppressed exculpatory evidence.”³⁶

The Fifth Circuit disagreed, noting that the government did not simply dump several hundred million pages on the defendant’s doorstep. Instead, the government’s open file was electronic and searchable, the government produced a set of “hot documents” that it thought were important to its case or were potentially relevant to the defense, and the government created indices to these and other documents. The court added that “the government was in no better position to locate any potentially exculpatory evidence than was *Skilling*.”³⁷

³¹ *Id.* at 411.

³² *Id.* at 414.

³³ *Id.* at 415 (emphasis in original). The court also rejected the SEC’s blanket refusal to produce any incoming or outgoing e-mails and ordered the parties to develop a search protocol.

³⁴ *Id.* at 418.

³⁵ *United States v. Skilling*, 554 F.3d 529 (5th Cir. 2009).

³⁶ *Id.* at 576. The defendant added that “no amount of diligence, much less reasonable diligence” would have allowed him to effectively review the government’s disclosure. Defendant’s counsel estimated “it would have taken scores of attorneys, working *around-the-clock* for several years to complete the job.” *Id.*

³⁷ *Id.* at 577.

The *Skilling* decision, when taken with *Collins*, seems to indicate that the more voluminous the data dump, the more organization and indexing will be required from the government.

Potential for Dismissal. Failure by the government to properly plan and manage the production of ESI can result in dismissal of its case. 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.³⁸

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.”³⁹

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.”⁴⁰

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 or support staff can lead to critical mistakes affecting the outcome of your case.

³⁸ *United States v. Graham*, No. 05-45, 2008 WL 2098044, at *2-3 (S.D. Ohio May 16, 2008). See also *State v. Dingman*, 202 P.3d 388 (Wash App. 2009) (court reversed conviction and remanded for new trial after finding that trial court erred by denying defendant meaningful access to hard drives seized from his house).

³⁹ *Graham* at *5.

⁴⁰ *Id.* at *8.