"E-Discovery" in the Criminal Context: Emerging Issues and Trends

Justin P. Murphy
Stephen M. Byers
Crowell & Moring LLP
Washington, D.C.

Janet I. Levine
Crowell & Moring LLP
Los Angeles, California

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. But what about e-discovery in criminal investigations and litigation? Criminal defense lawyers and prosecutors are generally 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. This article examines e-discovery issues in the context of subpoena compliance, search warrants and post-indictment discovery, including the extent to which the new civil rules and case law are influencing criminal practice.

I. Subpoena Compliance

A. The Duty to Preserve Electronically-Stored Information

In a typical white-collar criminal investigation, the first e-discovery issue confronted by defense counsel is usually the need to preserve relevant ESI. More often than not, this arises because the client has been served with a grand jury or other law enforcement subpoena for documents. 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, up to and including obstruction of justice charges where some degree of intent can be shown. Thus, the problems presented by voluminous, widely dispersed and constantly changing ESI can be particularly acute in the criminal context.

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 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 (in that case, from the SEC).[1] But when, exactly, does the duty arise?

In civil litigation, the basic rule is fairly well-developed: "[W]henever litigation is reasonably anticipated, threatened or pending against an organization, that organization has a duty to preserve relevant information."[2] 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 ("SOX"), 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: "Whoever knowingly alters, destroys . . . [or] falsifies . . . any . . . document . . . with the intent to impede, obstruct, or influence the investigation . . . of any matter within the jurisdiction of any department or agency of the United States . . . or in relation to or **contemplation** of any such matter or case, shall be fined . . . [or] imprisoned not more than 20 years, or both."[3]

Once the duty to preserve arises, the steps that must be taken do not vary significantly from civil litigation. Company counsel must move quickly to implement a "legal 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. [4] And the same common pitfalls must be avoided. For example, a system to ensure compliance with the hold order should be established, regular reminders should be issued, ESI system "auto-deletes" should be disabled, "self collection" of ESI by employees should ordinarily be avoided, ESI maintained by former and/or departing employees must be captured, and special ESI repositories such as dynamic or proprietary databases must be considered. Further, it is becoming standard in criminal practice to have forensic copies of computer hard drives imaged—especially hard drives of the "key" custodians relevant to the investigation. Finally, a forensic expert's involvement can be critical to the assessment and successful preservation of ESI in an enterprise environment, whether the company is large or relatively small.

Unlike civil litigation, special preservation challenges can arise in the criminal context when a matter must be kept confidential. In these circumstances, company counsel may be limited in the extent to which they can communicate with custodians of potentially relevant documents, such as through a broadly-distributed legal hold order or in the course of imaging computer hard drives. For example, the government subpoena could emphasize the need for strict confidentiality. In that situation, counsel will ordinarily want 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 company counsel is conducting an internal investigation and the government is not yet in the picture. For example, counsel may be investigating a whistleblower complaint and, like the government, must be careful not to tip off the potential targets of the investigation or expose the confidential informant. A possible approach in this circumstance 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. A solid record of preservation efforts and the basis for decision-making may be critical.

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. These views can affect judgments about culpability and cooperation, which can in turn influence charging decisions and plea negotiations. In addition, a failure to preserve potentially relevant information may adversely impact Sentencing Guidelines calculations by increasing the defendant's culpability score.[5] And it is not only the client who may be penalized: preservation failures can also have personal consequences for in-house and outside counsel as well.[6]

Apart from these collateral consequences, preservation failures can expose the client to an additional investigation for obstruction of justice.

Because many government investigators are skeptical by nature and may routinely encounter efforts to destroy evidence, they may assume bad intent unless good faith can be demonstrated. A similar reaction can be expected if the problem becomes public. Newspaper headlines tend to proclaim "Company Destroyed Evidence in Criminal Case" rather than "Company Inadvertently Deleted Potentially Relevant Documents."

In extreme cases where intent can be shown, any number of obstruction-of-justice statutes can be brought to bear. For example, in addition to § 1519, which is cited above, SOX contains another obstruction provision that is remarkably broad: "[w]hoever corruptly alters, destroys, mutilates, or conceals a record, document, or other object . . . with the intent to impair the object's integrity or availability for use in an official proceeding . . . shall be fined . . . or imprisoned not more than 20 years, or both."[7] Prosecutors are keenly aware of the potential ramifications of failures to preserve evidence, and the leverage that can result. A recent official DOJ publication observed: "it is crucial to understand that deliberately ignoring preservation requirements could result in prosecution for obstruction of justice."[8] Because obstruction is often easier to prove than the underlying crime, which may involve complicated issues ill-suited to a jury trial, prosecutors ordinarily will not pass up an opportunity to deploy their obstruction-of-justice arsenal.[9] And, even if a defendant is not prosecuted, evidence of intentional manipulation of ESI can hand the prosecutor powerful evidence of consciousness of guilt.

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 plaintiff's counsel during discovery in a civil discrimination lawsuit between private parties.[10] More recently, a judge in the Eastern District of New York referred a case to the U.S. Attorney for electronic discovery abuses. In *Gutman v. Klein*, the court entered a default judgment against the defendants for "the destruction of evidence . . . of the worst sort: intentional, thoroughgoing, and (unsuccessfully) concealed."[11] The court directed the Clerk of the Court "to send a copy of this Order, together with the Recommendation, to the United States Attorney for the Eastern District of New York for such action, if any, as he deems appropriate."[12]

B. International Data Protection Laws

Dealing with ESI overseas presents unique problems. Some elements 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 ("MLAT") 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 broadly to include any data that is identifiable to a person. Such laws, which place limitations on a company's right to "process" personal data, typically extend to emails created on a company's system, as those emails are identifiable to a person and, therefore, deemed "personal data." Thus, the data protection laws of European and other countries may impact a company's right to take steps to preserve, much less collect and produce, potentially relevant ESI from a foreign office or subsidiary. Further, these rules may apply to data that is "housed" on servers in the United States. Thus, counsel could quickly find themselves in a situation where they have violated the laws of a foreign country in order to comply with the U.S. government's demands. And violating the foreign country's data protection laws may subject a company to fines or criminal penalties. Accordingly, before "processing" ESI from a foreign office or subsidiary, it is advisable to consult with a privacy expert in the jurisdiction in question.

C. Conferring with the Government on ESI Issues

Federal Civil Rule of 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 potentially significant consequences that can result from spoliation. Coming to agreement in a criminal case can sometimes be more difficult because the symmetry of risks and interests between the two parties 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. It is nonetheless essential in most cases to sit down with government representatives to work through the problems presented by the collection and production of ESI.

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. This is essential if your client intends to make a burdensomeness argument to the government in an effort to gain concessions and reach compromises. It is often advantageous to have a third party forensic specialist assist with the preservation and collection of potentially relevant material so that the details of the problems you are encountering and proposed solutions can be substantiated and clearly communicated, including to the government's own IT experts. In many instances, third party experts can demonstrate for the government how the most pertinent ESI can be provided without subjecting a business to an overly broad and costly collection and production effort.

After having taken the necessary steps to ensure that ESI is being preserved, counsel should reach out to the government and consider the discussion similar to a Rule 26(f) conference. Such discussions can prevent problems down the road; both the company and 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. First, 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." Second, 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 invaluable insight into the government's case that the prosecutor would otherwise be hesitant to reveal.

An additional area of possible discussion with the government is the scope of preservation. Prosecutors are understandably much more hesitant to compromise on preservation than production issues, particularly if they have little experience dealing with ESI issues. However, where defense counsel can demonstrate a degree of burden that is obviously out of proportion with the benefit to be gained by preservation, a compromise can often be struck. For example, a prosecutor may agree that only the oldest and most recent set of backup tapes need to be preserved, rather than every single tape in the company's possession. Or there may be room for agreement on the extent of forensic imaging of computer hard drives, limiting that effort, for example, to key players. The risk is that you may get an answer you do not like and your ability to make reasonable judgment calls may be restricted.

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.

D. New Federal Rule of Evidence 502

Federal Rule of Evidence 502, which was enacted in September 2008, has the potential to significantly impact the parties' treatment of privileged materials in its compliance with a law enforcement subpoena.[13] 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 and waiver of the attorney-client privilege and work product protections. Three aspects of the rule have potential application in the context of subpoena compliance.

First, FRE 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, FRE 502(a) provides that subject-matter waiver will not apply to inadvertent disclosures of privileged material.

Second, FRE 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. FRE 502(e) gives those non-waiver agreements extra force.

Third, FRE 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 civil litigation. One would hope that the government would not typically take unfair advantage of inadvertent disclosures; but some plaintiffs lawyers are eager to exploit such slip-ups to gain a tactical advantage and squeeze out additional settlement dollars. In addition, it is not at all clear that such agreements would be binding on other elements of the government—such as regulatory enforcement agencies like the SEC—that may conduct subsequent or parallel investigations. FRE 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 FRE 502(d) in the criminal context, however, is uncertain. Approaching the court for an order memorializing an agreement on waiver is relatively straight-forward 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. In addition, FRE 502(d) contains a potential ambiguity as it speaks in terms of orders entered "in the litigation," rather than, for example, referring more broadly to a "proceeding." It would seem that an application to the supervising court by the defense or the government for a protective order or compulsion order—or some sort of joint approach by the parties—should qualify as "litigation" under the rule, but this conclusion is not crystal clear. 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.

II. 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 head-long 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 prohibition against "general" warrants and its 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.

The Fourth Amendment states that "no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."[14] If there is no probable cause for an item included in the search warrant, the warrant is overbroad.[15] By "limiting the authorization to search to the specific areas and things for which there is probable cause to search, the [particularity] requirement ensures that the search will be carefully tailored to its justifications, and will not take on the character of the wide-ranging exploratory searches the Framers intended to prohibit."[16]

Although a warrant must be sufficiently particular to withstand scrutiny, courts have been inconsistent in applying this "particularity" standard to warrants for ESI. For example, some courts have imposed tight *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 essentially in "plain view."[17]

A. *Ex Ante* Restrictions on ESI Searches

Some courts have given magistrate judges the authority to control how a search will be conducted, in advance of the search, to prevent the random or general examination of ESI unrelated to the investigation. In those instances, the government was required to submit a search protocol outlining the methods it intended to use to ensure the proposed search was reasonably tailored to find ESI related to alleged criminal activity. In other words, the government was required not only to identify **where** it would search and **what** it would seize, but **how** the search would be conducted.

In *In re Search of 3817 W. West End*, the government challenged whether a magistrate could "require the government to set forth a search protocol that attempts to ensure that the search will not exceed constitutional bounds."[18] The district court found that the magistrate possessed the authority to require a protocol to ensure that the search was "reasonably designed" to focus on the documents related to the alleged criminal activity.[19] The court explained the purpose of the protocol: "[T]o provide the Court with assurance that the search of the computer after its seizure would not consist merely of a random or general examination of other documents which, on a home computer, might contain sensitive information regarding health or other personal and private matters completely unrelated to the alleged criminal activity."[20] The court made it clear that the government's authority to seize the computers and search them was conditioned on the required search protocol being provided by the government.[21]

Other courts have criticized the approach endorsed in *3817 W. West End* but have nonetheless expressed skepticism in response to the government's claim that it must be allowed to rummage around at will.[22] For example, in *In the Matter of 1406 N. 2nd Avenue*, the court, although allowing the government to proceed without a search pro-

tocol, 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."[23]

Indeed, the DOJ Search and Seizure of Electronic Evidence guide cited in *1406 N. 2nd Avenue* does suggest that incorporation of search protocols in a warrant affidavit is appropriate without, of course, suggesting the 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."[24] Moreover, 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."[25] The guide explains that both the court and government agents can refer to the document as a guide when executing the search and that it helps "counter defense counsel motions to suppress based on the agents' alleged 'flagrant disregard' of the warrant during the execution of the search."[26] And, in certain circumstances, the guide suggests that computer forensic experts should be consulted to help devise a search to identify particular files that may be described in the warrant.[27]

B. The BALCO Two-Step Approach

The Ninth Circuit's decision in *United States v. Comprehensive Drug Testing, Inc.* ("BALCO decision") takes a different approach, and provides a useful frame of reference for these issues.[28] The BALCO decision stemmed from the highly publicized grand jury investigation of the Bay Area Lab Collective ("BALCO"), linked to Major League Baseball home run king Barry Bonds and the subject of a New York Times best selling book.[29] The BALCO decision is controversial because, in the view of some commentators and a dissenting judge, the majority's approach in that case went a long way towards gutting the principles of the Fourth Amendment when applied to the virtual world of ESI.

1. Facts

In connection with its ongoing investigation of BALCO, government agents developed probable cause to believe that at least ten Major League Baseball players had obtained steroids from BALCO.[30] The agents executed search warrants at an independent medical testing lab, seeking information about the ten named baseball players.[31] During the search, the government made duplicate copies of the lab's computer directories which included the intermingled data of more than 100 other baseball players' test results, as well as medical records for participants in thirteen other sports, businesses and sports competitions.[32] Based on the information in these directories, the government obtained additional search warrants relating to approximately 100 other baseball players who were listed in the database as having tested positive for steroids.[33] The Major League Baseball Players Association sought the return of the seized data relating all players other than the 10 named individuals in the initial search warrant, pursuant to Fed. R. Crim. P. 41(g).[34]

2. BALCO Majority Opinion

The majority opinion addressed two important issues: (1) did the government have the right to seize all of the information in the independent lab's test results directory, rather than segregating and seizing information within the scope of the warrant; and (2) once the information in the directory had been seized, did the government have the right to review all of it without any judicial supervision?

With regard to the seizure, the majority first rejected the notion that "government officials

should limit their computer searches to key words suggested by a searched party."[35] The court saw no duty for the government to rely on the independent medical testing lab's employees to highlight the particular files that would be "seizable" under the warrant because like most searched parties, they "had an incentive to avoid giving over documents the government might not know to miss."[36] The court also concluded that the government had "no reason to assume" that the relevant materials in the test results directory would be listed under the name of the specific baseball players listed in the warrant.[37] Based on these findings, the court concluded that the government "properly considered and respected the privacy interests, intrusiveness, and law enforcement needs posed by the searches in question" by removing only a copy of directory and taking only "limited" amounts of other relevant media.[38]

After finding that the government had properly seized the entire directory, the court ruled 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."[39] 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."[40] This "post-seizure motion" would, in the view of the majority, "afford[] the necessary protection[s] against unreasonable retention of property after a seizure of intermingled computer data."[41]

3. The Dissent

"What happened to the fourth amendment? Was it repealed somehow?"[42] This rhetorical question set the tone for Judge Sidney Thomas's strongly-worded dissent. Judge Thomas's "most profound disagreement" with the majority opinion was the conclusion that the government could legally seize all of the data simply because it was intermingled with data responsive to the warrant.[43] To Judge Thomas, 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'" and courts have "eschewed" the haphazard search and seizure of materials non-responsive to a valid search warrant for years.[44] Most importantly, Judge Thomas stressed that the government's entitlement to seize all records in the file because they were intermingled "puts Americans' most basic privacy interests in jeopardy."[45] He noted that the implications of "approving such behavior are staggering . . . . [u]nder the majority's holding, no laboratory or hospital or health care facility could guarantee the confidentiality of records."[46]

Moreover, the dissent suggested that the key advantages of electronic data storage—"the ease of searching and examining data"—were being ignored.[47] The agents could have utilized software programs to segregate non-relevant information from the database at issue; "for example, a simple search would have yielded the information responsive to the search warrant."[48] The dissent questioned why the majority would not use "the power of a relational database to protect legitimate privacy interests" rather than "discouraging—if not precluding—such a use." And, since intermingled data is an intrinsic part of "electronic databases, this restriction renders the Fourth Amendment a nullity in the electronic context."[49]

Judge Thomas also parted ways with the majority on the second key issue in the case: the extent to which the government was free to examine all the seized data. Judge Thomas

proposed that a neutral magistrate be required to examine the intermingled data, even if "proper" objections were not raised, to ensure that the private information the government is not entitled to seize remains private.[50] Under his proposal, Government agents who seize intermingled data would have to seek guidance from a magistrate on how to proceed. Judge Thomas was quick to add that his procedure would not impose impractical burdens on the government: the data is secure "and may be reviewed in an 'informed and deliberate' manner by a 'neutral and detached' magistrate, rather than being secreted for indiscriminate examination by government officials."[51]

4. The Upshot of BALCO

Computers have an extraordinary capacity to retain data and information that was simply not possible 20 years ago, and which will only expand exponentially in the future. Couple this storage capacity with the tendency of most individuals to maintain copies of personal and work related documents for lengthy periods of time—all "intermingled" on their computers or various systems—and the implications of the BALCO decision become clear: such personal data can be seized by the government not because there is any probable cause to believe it is related to a crime, but simply because the information happens to share space on a computer or system with other information that is specified on a valid warrant.

The BALCO decision is particularly alarming because of the implications for third parties. Any person's private information (such as the medical testing records at issue in BALCO), even if it is clearly outside the scope of the search warrant, can be seized by government agents without notice, either before or after the fact. And if that information is seized, a party would have to "object" to gain the intervention of a neutral magistrate. This would be a meaningless remedy in situations where a third party is unaware that his or her intermingled data had been seized. With government agents able to seize private ESI housed on databases or directories without a search warrant as along as there is other information on the 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 had in mind when enacting the Fourth Amendment.

C. Other Courts Applying the Two-Step Approach

Other courts have taken an approach similar to that advocated in the BALCO dissent. In *United States v. Carey*, the government seized two computers from the defendant while conducting a search for information related to drug distribution and possession.[52] The government obtained another warrant allowing it to search the computers and during that search, one of the agents opened a .jpeg file that contained what he believed was child pornography.[53] The agent downloaded 244 other image files and reviewed a sampling of them; when this was complete, "he returned to the computers to pursue his original task of looking for evidence of drug transactions."[54] The agent acknowledged that when he opened each of the subsequent .jpeg files, he was looking for evidence of child pornography, not for evidence of drug transactions.[55]

Rejecting the government's "plain view" argument, the Tenth Circuit determined that the agent's search for all but the first image file he opened had exceeded the scope of the search warrant and that the "unconstitutional general search" required suppression of the child pornography evidence.[56] The court rejected the government's argument that "this situation is similar to an officer having a warrant to search a file cabinet containing many drawers. Although each drawer is labeled, [the agent] had to open a drawer to find out whether the label was misleading and the drawer contained the objects of the search."[57] Instead, the court noted this

was not a case where files were ambiguously labeled or where each "drawer" had to be opened to determine its contents.[58] "Relying on analogies to closed containers or file cabinets may lead courts to "oversimplify a complex area of Fourth Amendment doctrines and ignore the realities of massive modern computer storage."[59]

Acknowledging that the "storage capacity of computers requires a special approach," the court concluded that a two-step process should be utilized.[60] "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."[61] The magistrate approval should also require the government to specify in the warrant the types of files that are being sought.[62]

Other courts have, like the BALCO dissent, been hesitant to accept generalized government assertions that wholesale seizer of ESI was necessary. In *United States v. Tamura*, the court noted that "large-scale removal of material" can be justified "where on-site sorting is infeasible and no other practical alternative exists," but that it was "highly doubtful whether the wholesale seizure by the Government of documents not mentioned in the warrant comported with the requirements of the fourth amendment."[63] Importantly, the Ninth Circuit concluded that the "essential safeguard required is that wholesale removal must be monitored by the judgment of a neutral, detached magistrate."[64]

D. Wide Latitude for the Government

However, most courts have been reluctant to endorse the *ex ante* or two-step special approaches. For example, in *United States v. Tylman*, the Central District of Illinois criticized the ruling in *3817 W. West End*, asserting: "that case is not binding on this Court, is without merit, and 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."[65]

Distancing themselves from the "special approach" discussed in *Carey*, other courts have invoked the "plain view" doctrine and focused on the "reasonableness" of the government's actions noted in *Tylman*. In *United States v. Gray*, the court upheld 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 or not they fell within the scope of the warrant.[66] In addition, despite testimony that search programs could have been used to determine the contents of a file without opening it, the court concluded that it was not reasonable to compel the government to always use the most sophisticated search methods. Courts also have argued that warrants failing to limit searches to specific emails 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.[67]

III. Post-Indictment Discovery

After indictment, the power imbalance between the government and the defendant in terms of demands for the production of evidence shifts back towards the defense. It is at this point that the government's duty to preserve and produce ESI comes into play.[68] 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. Reliance on civil procedure discovery rules in criminal cases represents new thinking about the duties of the government to make responsive and material information in its possession available to a criminal defendant.

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.[69] In *O'Keefe*, the defendants argued that the government had produced documents in a manner that made it impossible to identify the source or custodian of the document.[70] The court noted that there was no rule in criminal cases to guide judges in determining whether a production of materials by the government has been tendered in an appropriate form or format.[71] Recognizing that the "big paper case" would be the exception rather than the rule in criminal cases, the court stated that Rule 34 of the Federal Rules of Civil Procedure speaks directly to form of production.[72] 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."[73]

O'Keefe's importation of the civil rules into a criminal case has already been advanced by other criminal defendants. For example, in *United States v. Theodore Stevens*, the defense objected that the government had produced thousands of pages of documents in an unusable format that "appeared to be an undifferentiated mass, with no discernible beginning or end of any given document."[74] Citing *O'Keefe* and highlighting the unnecessary and increased burden to Senator Stevens, the defense argued that "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."[75] The defense also requested metadata and logs relevant to evaluating the validity of the government's forensic photography, arguing that the text of Fed. R. Crim. P. 16 expressly permits a defendant to inspect and to copy data, among other items and that "metadata is of course data."[76] The defense added "[t]here is nothing remarkable about asking the government to produce metadata. Courts routinely permit the discovery of metadata in the civil context . . . and there is no principled reason why it ought not be produced in a criminal case."[77]

The incorporation of the civil rules into a criminal case has also been acknowledged by the Department of Justice. A recent U.S. Attorney's Bulletin cited *O'Keefe* and cautioned that "[p]rosecutors should be aware that federal judges may hold them to certain standards common to civil litigation."[78]

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, addresses failures to preserve ESI. The rule provides that: "Absent exceptional circumstances, a court may not impose sanctions under these rules on a party for failing to provide electronically stored information lost as a result of the routine, good-faith operation of an electronic information system."[79] In addition, as the Commentary to Rule 37(f) indicates, the Rule only applies to information lost "due to the 'routine operation of an electronic information system—the ways in which such systems are generally designed, programmed, and implemented to meet the party's technical and business needs."[80]

Rule 37(e) 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 application in criminal cases.[81] In general, if the ESI deletion resulted from routine operation of the government's computer 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 ESI 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.[82]

However, some post-indictment discovery violations have resulted in significant sanctions for the government. In *United States v. Graham*, the government turned over vast amounts of discovery to defendants in a criminal tax case—approximately 1.5 million documents, numerous videotapes, recorded conversations and other media.[83] The government was slow to produce discovery and the defendants had great difficulty in coping with the large volume.[84] During this time, the court continued to schedule status hearings without setting a new trial date and without making findings that a continuance was in the interests of justice.[85]

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."[86] 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."[87]

IV. 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.

Endnotes

1. *See, e.g., Arthur Anderson v. United States*, 544 U.S. 696, 701, 707-08 (2005).

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

3. 18 U.S.C. § 1519 (emphasis added).

4. "The duty to preserve information includes an obligation to identify, locate, and maintain, information that is relevant to specific, predictable, and identifiable litigation. When preservation of ESI is required, the duty to preserve supersedes records management policies that would otherwise result in the destruction of ESI. A 'legal hold' program defines the processes by which information is identified, preserved, and maintained when it has been determined that a duty to preserve has arisen." *Sedona Conference Commentary on Legal Holds*, August 2007.

5. *See* U.S.S.G. § 8C2.5.

6. *See generally Qualcomm, Inc. v. Broadcom, Inc.*, No. 05-1958, 2008 WL 66932 at *20 (S.D. Cal. Jan. 7, 2008), *vacated*, 2008 WL 638108 (S.D. Cal. Mar. 5, 2008) (court relied on rules of professional conduct to impose sanctions on Qualcomm's counsel for failing to reasonably respond to requests for ESI production).

7. 18 U.S.C. § 1512(c).

8. *See* Andrew D. Goldsmith and Lori A. Hendrickson, *Investigations and Prosecutions In-*

volving Electronically Stored Information, United States Attorneys' Bulletin Vol. 56, No 3, May 2008. This bulletin also notes that preservation can be time intensive and that prosecutors should require documentation concerning methods used to preserve, collect, process and produce. *Id*. It is also worth noting that the newly published SEC "Enforcement Manual" specifically addresses E-discovery issues in § 3.2.6.2.3. The Manual "encourages" the Staff to request document productions in electronic format (on CD, DVD or hard drive media) and specifies that the Staff's requests should include the Division's technical data standards. The Manual notes that scanned collections, e-mail or native files produced by parties should be compatible with the software systems used by the Staff, Concordance and Opticon. The Manual adds that the Division has its own technology staff to respond to questions and to assist the Staff's review and management of electronic document productions. The Manual also provides guidance on bates stamping, privilege logs and business record certifications, including sample declarations for domestic and foreign records.

9. *See e.g., United States v. Stewart*, No. 03-00717 (S.D.N.Y. filed June 4. 2003); *United States v. Quattrone*, No. 03-00582 (S.D.N.Y. filed May 12, 2003).

10. *United States v. Lundwall*, 1 F. Supp. 2d 249, 254 (S.D.N.Y. 1998) (court found that the withholding and destruction of relevant documents in a lawsuit means that "the documents will never be considered by opposing litigants, their counsel or the Court. This conduct necessarily and fundamentally compromises federal court proceedings and . . . has the 'natural and probable effect' of interfering with the due administration of justice.").

11. *Gutman v. Klein*, No. 03-1570, 2008 WL 4682208, at *12 (E.D.N.Y. Oct. 15, 2008). In *Gutman*, the defendants had tampered with their computers, backdated files and used wiping programs after the litigation had commenced, among other actions. The court determined that defendants' bad faith "obliteration" of computer files "may well have deprived plaintiffs of crucial evidence." *Id*.

12. *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).

13. Federal Rule of Evidence 502 provides as follows:

The following provisions apply, in the circumstances set out, to disclosure of a communication or information covered by the attorney-client privilege or work-product protection.

a. Disclosure Made in a Federal Proceeding or to a Federal Office or Agency; Scope of a Waiver- When the disclosure is made in a Federal proceeding or to a Federal office or agency and waives the attorney-client privilege or work-product protection, the waiver extends to an undisclosed communication or information in a Federal or State proceeding only if:
   1. the waiver is intentional;
   2. the disclosed and undisclosed communications or information concern the same subject matter; and
   3. they ought in fairness to be considered together.

b. Inadvertent Disclosure- When made in a Federal proceeding or to a Federal office or agency, the disclosure does not operate as a waiver in a Federal or State proceeding if:
   1. the disclosure is inadvertent;
   2. the holder of the privilege or protection took reasonable steps to prevent disclosure; and

3. the holder promptly took reasonable steps to rectify the error, including (if applicable) following Federal Rule of Civil Procedure 26(b)(5)(B).

c. Disclosure Made in a State Proceeding- When the disclosure is made in a State proceeding and is not the subject of a State-court order concerning waiver, the disclosure does not operate as a waiver in a Federal proceeding if the disclosure:
   1. would not be a waiver under this rule if it had been made in a Federal proceeding; or
   2. is not a waiver under the law of the State where the disclosure occurred.

d. Controlling Effect of Court Order – A Federal court may order that the privilege or protection is not waived by disclosure connected with the litigation pending before the court--in which event the disclosure is also not a waiver in any other Federal or State proceeding.

e. Controlling Effect of a Party Agreement- An agreement on the effect of disclosure in a Federal proceeding is binding only on the parties to the agreement, unless it is incorporated into a court order.

f. Controlling Effect of This Rule- Notwithstanding Rules 101 and 1101, this rule applies to State proceedings and to Federal court-annexed and Federal court-mandated arbitration proceedings, in the circumstances set out in the rule. And notwithstanding Rule 501, this rule applies even if State law provides the rule of decision.

g. Definitions- In this rule:
   1. "attorney-client privilege" means the protection that applicable law provides for confidential attorney-client communications; and
   2. "work-product protection" means the protection that applicable law provides for tangible material (or its intangible equivalent) prepared in anticipation of litigation or for trial."

14. U.S. Const. amend. IV.

15. *Davis v. Gracey*, 111 F.3d 1472, 1478 (10th Cir. 1997).

16. *Maryland v. Garrison*, 480 U.S. 79, 84 (1987).

17. *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).

18. *In re Search of 3817 W. West End*, 321 F. Supp. 2d 953, 957 (N.D. Ill. 2004).

19. *Id.* at 955-56.

20. *Id. See also United States v. SDI Future Health, Inc.*, No. 05-0078, 2006 WL 4457335 (D. Nev. June 26, 2006) (Court found that categories of search warrant failed Fourth Amendment particularity requirement because warrant failed to limit general categories of business documents and financial records to the seizure of records relating to the criminal activity described in the affidavit. "It would not have been unreasonable or impossible for the Government to have included some date restrictions in the search warrant, such as restricting the search . . . to a time period corresponding to the period of the suspected tax evasion crimes." *Id.* at *27.

21. *In re Search of 3817 W. West End*, 321 F. Supp. 2d at 956.

22. *See In re Search of 3817 W. West End*, 321 F. Supp. 2d 953; *In re Search of the Premises Known as 1406 N. 2nd Avenue*, No. 05-28, 2006 WL 709036 (W.D. Mich. Mar. 17, 2006).

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

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

25. *Id.*

26. *Id.*

27. *Id.* Notably, a more recent Department of Justice "E-Discovery" bulletin does not address whether or not protocols should be utilized for search warrants. *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.

28. *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).

29. Mark Fairnaru-Wada & Lance Williams, *Game of Shadows: Barry Bonds, BALCO and the Steroids Scandal That Rocked Professional Sports* (2006).

30. *Comprehensive Drug Testing, Inc.*, 473 F.3d at 920.

31. *Id.* at 920-22.

32. *Id.* at 922-24.

33. *Id.* at 923-24

34. *Id.* at 923.

35. *Id. See also United States v. Fumo*, No. 06-319, 2007 WL 3232112 at *5, 7 (E.D. Pa. Oct. 30, 2007) (Defendants argued that they were entitled to search protocols and keywords used by government. The court found they were "irrelevant to the decision whether the warrants were overbroad or the seizures exceeded the scope of the warrants . . . . [T]here is no requirement that the government, in executing a warrant, limit itself to its search protocols or keywords, so long as the search and seizure actually conducted are supported by probable cause and within the scope of the particular descriptions recited in the warrants. Because deviations from search protocols and keywords are permissible, knowledge of those protocols and keywords will not allow [the defendant] or a court to draw conclusions about the reasonableness of the search actually conducted.").

36. *Comprehensive Drug Testing, Inc.*, 473 F.3d at 935.

37. *Id.*

38. *Id.* at 936.

39. *Id.* at 940.

40. *Id.* at 939.

41. *Id.*

42. *Id.* at 944

43. *Id.* at 962.

44. Id. at 962-63, *citing United States v. Tamura*, 694 F.2d 591, 595 (9th Cir. 1982).

45. *Id.* at 963.

46. *Id.* at 964.

47. *Id.* at 975.

48. *Id.*

49. *Id.* at 976.

50. *Id.* at 964-65.

51. *Id.* at 965.

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

53. *Id.*

54. *Id.*

55. *Id.*

56. *Id.* at 1276.

57. *Id.* at 1274.

58. *Id.* at 1275.

59. *Id.*

60. *Id.*

61. *Id.*

62. *Id.*

63. *Tamura*, 694 F.2d at 595-96. The *Carey* court noted that "although [*Tamura*] did not arise in the context of a computer search, we find the concept of "intermingled documents" helpful here." *Carey*, 172 F.3d at 1275 n.6.

64. *Tamura*, 694 F.2d at 596.

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

66. *United States v. Gray*, 78 F. Supp. 2d 524, 529 (E.D. Va. 1999).

67. *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: 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, 1165 (2007).

68. 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).

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

70. *Id.* at 18.

71. *Id.* at 18-19.

72. *Id.* at 19.

73. *Id.*

74. Defendant's Motion to Compel Discovery, *United States v. Stevens*, No. 08-231 (D.D.C. Sept. 2, 2008).

75. *Id.*

76. Defendant's Reply in Support of Motion to Compel Discovery, *United States v. Stevens*, No. 08-231 (D.D.C. Sept. 6, 2008).

77. *Id.* (citing *United States v. O'Keefe*, 537 F. Supp. 2d 14 (D.D.C. 2008)). Ultimately, the issues were resolved without a written opinion by the court.

78. *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.

79. Fed. R. Civ. P. 37(e).

80. *See* Fed. R. Civ. P. 37(f), Advisory Committee Notes to 2006 Amendment.

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

82. However, this is not unlike the rules that have long pertained to government destruction of physical evidence in the ordinary course. *See Arizona v. Youngblood*, 488 U.S. 51, 57 (1988); *In re: Sealed Case*, 99 F.3d 1175, 1178 (D.C. Cir. 1996).

83. *United States v. Graham*, No. 05-45, 2008 WL 2098044, at *1 (S.D. Ohio May 16, 2008).

84. *Id.* at *2-3.

85. *Id.* at *3.

86. *Id.* at *5.

87. *Id.* at *8. In an effort to provide a framework for more effective management of electronic evidence in criminal cases, The Director of the Administrative Office of the U.S. Courts ("AOUSC") and the Attorney General of the United States created the Administrative Office/Department of Justice Joint Working Group on Electronic Technology in the Criminal Justice System ("JET-WG"), which includes members of the criminal defense bar. 2003 Report and Recommendations available at: http://www.fjc.gov/public/pdf.nsf/lookup/CompInDr.pdf/$file/CompInDr.pdf