BNA, INC.

WHITE COLLAR CRIME REPORT

BNA Employee-Owned Since 1947

VOL. 2, NO. 10 PAGES 293-324 JUNE 8, 2007

HIGHLIGHTS

Congressman Jefferson Indicted in Lengthy Probe of Alleged Corruption
Capping a long-running, highly publicized investigation, Rep. William Jefferson (D-La.) is indicted by a federal grand jury on 16 counts of alleged corruption, including bribery, conspiracy, racketeering, and violation of the Foreign Corrupt Practices Act. **Page 297**

Initiation of Ancillary Proceeding Wrong Remedy in KPMG Tax Fraud Case
A federal district judge who concluded that prosecutors violated the Fifth and Sixth Amendment rights of a group of KPMG employees accused of tax fraud by pressuring the firm not to pay their legal bills should not have invited the employees to litigate state law contract claims in an ancillary proceeding, the Second Circuit holds. **Page 308**

Fifth Circuit Blocks Fraud Prosecution for Violations of State Election Laws
A state elected official who allegedly violated state campaign finance laws cannot be prosecuted on federal mail fraud charges on a theory that he fraudulently received ''money or property'' in the form of salary and employment benefits as a result of his corruptly procured office, the Fifth Circuit decides. **Page 309**

Sidley Austin to Pay $39.4 Million Penalty for Abusive Tax Shelters
The law firm Sidley Austin LLP will pay a $39.4 million civil tax shelter promoter penalty to the Internal Revenue Service for promoting abusive tax shelters and failing to comply with tax shelter regulation requirements, but will not be facing criminal charges from the Justice Department. **Page 302**

CREA Head Faces Tax, Obstruction Charges Connected to Abramoff Probe
The Justice Department files charges of tax evasion and obstructing Senate proceedings against the head of the Council of Republicans for Environmental Advocacy, a nonprofit group linked to former Interior Secretary Gale Norton and an associate of jailed lobbyist Jack Abramoff. **Page 299**

Former Enron Broadband Exec Draws Two Years for Wire, Securities Fraud
A federal judge sentences former Enron Broadband Services executive Kevin Hannon to serve a two-year prison term and orders him to pay a $125,000 fine for conspiring to commit securities and wire fraud. **Page 307**

Analysis & Perspective

ELECTRONIC RECORDS : The government's aggressive use of the Sarbanes-Oxley Act's novel obstruction of justice provision may herald a new era in potential criminal liability for altering, destroying or disposing of records or other evidence well in advance of any actual federal proceeding or matter. **Page 318**

ALSO IN THE NEWS

HEALTH CARE FRAUD: The Department of Justice announces that Bristol-Myers Squibb Co. has agreed to plead guilty and pay a $1 million criminal fine for lying to the federal government about a patent deal involving the blood-thinning drug Plavix. **Page 302**

ACCOUNTING FRAUD: The Second Circuit, with one exception, upholds the fraud and conspiracy convictions of Adelphia Communications Corp. founder John Rigas and his son Timothy Rigas. **Page 310**

TAX FRAUD: Four current and former Ernst & Young tax partners plead not guilty to charges of tax fraud conspiracy and related crimes arising out of tax shelters promoted by the firm. **Page 299**

CYBERCRIME: A California appellate court upholds a Colorado physician's conviction for practicing medicine in California without a license even though the doctor neither was physically present in California during the commission of the offense nor acted through an agent located in the state. **Page 311**

SECURITIES FRAUD: A former hedge fund manager pleads guilty in federal court in New York to carrying out a securities fraud scheme that lost investors some $88 million. **Page 303**

 ISSN 1559-3185

Analysis&Perspective

ELECTRONIC RECORDS

The Other Shoe Drops: Using Sarbanes-Oxley Criminal Provision, DOJ Indicts Attorney for Destroying Evidence in Advance of a Proceeding

BY W. WARREN HAMEL & LOWELL M. ROTHSCHILD

In what appears to be the first use of a new Sarbanes-Oxley obstruction of justice provision, 18 U.S.C. § 1519, the U. S. Attorney for the District of Connecticut announced that an attorney has been indicted for destroying a computer that was alleged to have contained child pornography, prior to any knowledge of the initiation of a federal investigation. The aggressive use of this novel criminal statute heralds a new era in potential criminal liability for altering, destroying or disposing of records or other evidence well in advance of any actual federal proceeding or matter—and one in which individuals, organizations, and their attorneys will be forced to carefully analyze decisions about the disposition of records or other evidence that might relate to matters that, at some point in the future, are likely to become the subject of federal attention.

In 2002, Congress passed the Public Company Accounting Reform and Investor Protection Act, popularly known as the Sarbanes-Oxley Act, in response to the widespread financial and accounting scandals that had occurred in the period leading up to passage. One of the Sarbanes-Oxley Act's provisions amended the federal criminal obstruction of justice statutes to address gaps and inconsistencies between various obstruction provisions addressing the destruction of documents or other evidence relevant to a federal matter such as a criminal investigation or civil or administrative inquiry.

Mr. Hamel is a partner at the law firm Venable LLP and co-chairs the firm's SEC and White Collar Crime Group. Mr. Hamel specializes in defending individuals and entities being investigated for or charged with white collar crimes, conducting internal investigations, and advising clients on internal controls and preventive programs for corporate clients. Mr. Hamel was an Assistant U. S. Attorney in the U. S. Attorney's Office for the District of Maryland from 1990 to 2002, and was Chief of the office's Environmental Crimes and Enforcement Unit for the last five years of his service.

Mr. Rothschild is a partner in Venable's Environmental Practice Group. His practice includes civil compliance work and administrative, civil, and criminal litigation. While this work includes almost all environmental media, his focus is on large-scale development issues such as wetlands, water, NEPA, and endangered species.

Although relatively unnoticed at the time amidst the debate over the impact of more high-profile aspects of Sarbanes-Oxley on corporate and individual behavior,[1] the new provision, codified at 18 U.S.C. § 1519, considerably broadened the reach of potential criminal liability for destruction or alteration of records or other materials in advance of the initiation of a federal inquiry. Section 1519 essentially eliminated the requirement that a federal proceeding or investigation be under way at the time the records were altered or destroyed. The new provision substitutes a broader standard, i.e., that the records or materials destroyed must only be shown to be relevant to a matter within the jurisdiction of the federal government, where such matter is ''contemplated,'' and where the defendant's conduct was carried out with the intent to obstruct a federal inquiry that might, at some point, occur.

Fast forward to March 2007, when the U. S. Attorney for the District of Connecticut announced that an attorney, Philip Russell, had been indicted for destroying a computer that was alleged to have contained child pornography.[2] According to the allegations in the indictment[3] and the few public reports available,[4] Russell represented a church where the choirmaster and organist, John Tate, was alleged to have saved images of naked boys on a laptop computer. Russell was called in to investigate the circumstances and advise the church on an appropriate course of action. The indictment alleges that after arranging for Tate's resignation from church employment, and helping to make arrangements for Tate to travel to California, Russell took possession of the laptop computer. Russell then allegedly destroyed the computer containing the contraband images. Russell is charged with violations of 18 U.S.C. § 1512(c)(1) (obstruction of justice) and 18 U.S.C. § 1519.

[1] But see ''They Got Tougher,'' T. Kelly, W. Hamel, *Legal Times* (2003).

[2] *See* Press Release of U.S. Attorney's Office at http://www.usdoj.gov/usao/ct/Press2007/20070216.html

[3] *United States v. Russell*, Crim. No. 3:07CR-00031-AHN (D. Conn.)

[4] See, e.g., ''A Boundary Pushing Case,'' *The Baltimore Sun*, March 6, 2007 (from Associated Press wire story).

  WCR ISSN 1559-3185

What is unusual about the indictment is the absence of any allegation that Russell knew of a federal investigation or a federal inquiry directed at Tate or the contents of the laptop computer.[5] The indictment appears to charge that Russell destroyed evidence prior to his having any actual knowledge of the initiation of a federal investigation, on the basis that such an investigation might happen. In other words, the government's theory of the case assumes that he knew or should have known that the images on the computer would ultimately be relevant to a federal investigation. If the government's evidence indeed bears this out, and the case is proved and upheld on appeal, the government will have a more potent weapon for attacking obstruction of justice, one with very broad implications for individuals, organizations, and their counsel.[6]

I. Background to Adoption of Section 1519

Prior to the enactment of Sarbanes-Oxley, federal prosecutors relied on 18 U.S.C. § § 1503, 1505, and 1512 to prosecute cases involving destruction of evidence. Although these provisions provided some powerful tools, gaps in the statutory scheme required prosecutors to craft indictments with care. For instance, the government could prosecute a person directly engaged in the destruction of documents under Sections 1503 and 1505, but not under Section 1512. Defendants could be prosecuted under Section 1512 only if they ''corruptly persuade[d]'' another to destroy documents. A recent and notorious example of the use of Section 1512 is the government's prosecution of accounting firm Arthur Andersen, which involved allegations of destruction of documents after Andersen's client, Enron, had received an information request letter from the Securities and Exchange Commission.[7]

Prosecutions under Sections 1503 and 1505 were limited to circumstances in which a proceeding or investigation was actually under way at the time of the obstructive conduct. By comparison, Section 1512 allowed prosecution for document destruction in advance of an ''official proceeding,'' but the caselaw reflected considerable disagreement over how far in advance of a proceeding liability could extend. Decisions ranged from the narrow view that an official proceeding had to have commenced or been scheduled to commence,[8] to a very broad reading under which it would be enough for the defendant to have foreseen an official proceeding at some time in the future. [9] Other courts preferred to evaluate the reach of the statute on a case-by-case basis,[10] which gave little guidance to prosecutors and to the public.

Sarbanes-Oxley closed these loopholes and replaced uncertainty about the reach of the law with the broadest standard of liability for alteration or destruction of evidence. The Act added 18 U.S.C. § 1519 to the federal criminal code, broadening both the subject matter and the range of circumstances in which liability can attach for its destruction in advance of a federal proceeding.[11] Section 1519 provides:

> Whoever knowingly alters, destroys . . . or makes a false entry in any record, document or tangible object with the intent to impede, obstruct, or influence *the investigation or proper administration 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 . . . imprisoned not more than 20 years, or both.

(Emphasis added.)

The phrase ''any matter within the jurisdiction of any department or agency of the United States'' in part tracks the language of the federal false statement statute, 18 U.S.C. § 1001. The courts have consistently interpreted ''any matter'' under Section 1001 as including almost every conceivable area of interest on the part of a federal agency. Looking forward, the new Section 1519, read in pari materia with Section 1001, may also apply to matters that are only indirectly within the jurisdiction of the United States, such as where state and local governments, and even private contractors, receive substantial federal funding or exercise delegated federal authority.

Moreover, by explicitly making document destruction ''in relation to or contemplation of any such matter or case'' subject to criminal sanction, the Act substantially enlarges the scope of liability for evidence destruction in advance of the initiation of any federal action. The provision sweeps aside prior inconsistencies among the obstruction statutes as to the timing of evidence destruction in relation to a federal proceeding, and codifies the broadest standard for determining when criminal liability attaches. The Department of Justice took note of this new broad power in its Field Guidance on Sarbanes-Oxley, stating that Section 1519 ''explicitly reaches activities by an individual 'in relation to or contemplation of' any matters,'' and suggesting that the amended Section 1512 should be read in conjunction with the new Section 1519. Obviously, prosecutors were on alert for opportunities to test this new authority, and the Russell indictment offers one of the first instances in which it will be put to the test.

---

[5] The indictment does allege that a federal criminal inquiry was initiated three days prior to the destruction of the computer: ''On or about October 6, 2006, the [FBI] began a criminal investigation of Tate concerning his possession of child pornography and exploitation of children.'' Indictment ¶ 4. There is no allegation, however, that Russell or anyone else knew of the opening of that investigation.

[6] Motions to Dismiss the two Counts of the Indictment were filed on March 22, 2007, and April 19, 2007, respectively. The factual allegations and legal arguments in the Motions are based solely on the indictment and so provide no additional insight into either the facts or the government's theory of the case. Based on the two motions, Russell's counsel appears to read the indictment in a manner consistent with the analysis presented in this article.

[7] *See Arthur Andersen LLP v. United States*, 544 U.S. 696 (2005). Although the Supreme Court vacated the company's conviction on the basis of incorrect jury instructions at the trial, the company had by then been essentially destroyed by the prosecution and conviction.

[8] See, e.g., *United States v. Jackson*, 513 F.2d 456 (D.C. Cir. 1975).

[9] See, e.g., *United States v. Conneaut Industries, Inc.*, 852 F. Supp. 116 (D.R.I. 1994).

[10] See, e.g., *United States v. Frankhauser*, 80 F.3d 641 (1st Cir. 1996).

[11] The Act also amended Section 1512 by adding a new provision that allows prosecutors to charge the ''individual shredder'' as well as the ''corrupt persuader'' for obstruction by document destruction. 18 U.S.C. § 1512 (c).

II. Predicting the Future To Avoid Criminal Prosecution?

The government's aggressive use of Section 1519 against an attorney raises a number of serious questions for white collar practitioners. Although the government's evidence may show that the use of this new provision is unexceptional,[12] criminal defense practitioners nonetheless will want to reexamine the nature of the actions they take with respect to (1) advice to clients, (2) access to and use of client information, and (3) treatment of potential evidence, in light of the likelihood of more aggressive application of the statute. Indeed, this criminal provision of the Sarbanes-Oxley Act may well interact in quite unforeseen ways with the Rules of Professional Conduct and with recent advances in practices related to electronically stored information.

Several hypothetical examples highlight these issues. Suppose, for instance, that an attorney (''Attorney'') represents the individual who has possession of the laptop with child pornography on its hard drive (''Client''), rather than the organization employing the individual. While this is not the circumstance alleged in the Russell indictment, there is no reason to believe that the outcome would be any different from the government's perspective if it were. The client comes to Attorney and gives the attorney evidence on a laptop that could be used to prosecute the client.[13] Attorney does not specifically know of an investigation into Client's conduct and destroys the laptop. Under the view posited by the U. S. Attorney for the District of Connecticut, Attorney has violated Section 1519, presumably because Attorney should have assumed that an investigation into the client's conduct may eventually be forthcoming at some unspecified future time.

Certainly Section 1519 is not limited in a way that would exclude attorneys from its scope. Section 1519 criminalizes the acts of *anyone* who ''knowingly alters, destroys . . . or makes a false entry in any record, document or tangible object with the intent to impede, obstruct, or influence the investigation or proper administration 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. . . .''

The attorney may also have violated the Model Rules of Professional Conduct by destroying the laptop. Under the Model Rules, ''[i]t is professional misconduct for a lawyer to. . . commit a criminal act that reflects adversely on the lawyer's honesty, trustworthiness or fitness as a lawyer in other respects.'' Rule 8.4(b). Destruction of evidence is one such act.[14] On the other hand, what should Attorney do with the laptop? As discussed below, in most cases, the attorney would likely need to maintain custody of the laptop on behalf of the client (although in the case of child pornography, that would likely be, itself, a violation of the law).

Suppose, instead, that Attorney, after having advised the client that it is illegal to possess material such as that on the laptop, returns custody of the laptop to the client, and then Client destroys the laptop. Has Attorney aided and abetted the destruction of evidence?[15] Under the aiding and abetting statute, 18 U.S.C. § 2, Attorney could be liable as a principal for the client's obstructive conduct. See, e.g., *United States v. McKnight*, 799 F.2d 443 (8th Cir. 1986) (indictment for aiding and abetting obstruction of justice through destruction of bank records). Again, even if Attorney does not *know* that a federal inquiry has been initiated, such conduct appears to violate the Act, despite the more attenuated causation. The attorney's advice to the client that possession of the child pornography is a violation of federal law would support the allegation that the evidence destroyed related to an ''investigation or proper administration 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*.''

In addition to potential criminal liability as an aider and abettor, it also appears that, if the evidence is destroyed by the client, the attorney's action would also violate the Model Rules. Under Rule 1.2(d), ''[a] lawyer shall not . . . assist a client in conduct that the lawyer knows is criminal.'' If shredding the evidence is criminal under the Act, giving the evidence to the client knowing he will shred it is most likely ''assisting'' him in that illegal activity.

The combined effect of Section 1519 and the Model Rules leads to a simple question: How accurately can an attorney predict the future—both as to his client's actions and the likelihood of a federal investigation into the client's conduct? And if those predictions turn out to be wrong, will that result in criminal prosecution or discipline by the bar? Suppose, for instance, that the attorney advises the client not to destroy the evidence when he returns the evidence to the client, but the client destroys the evidence despite the advice. Or suppose that

[12] The government may, for instance, introduce evidence that Russell knew that an investigation by the federal government had been initiated by the time that he is alleged to have destroyed the laptop's hard drive.

[13] In the Russell case, that evidence was child pornography, the mere possession of which is illegal. 18 U.S.C. § 2252A(a)(5)(B). In a similar case, the attorney would have reason to believe that the client has broken the law. However, this fact is not dispositive in our hypothetical, since there are many other pieces of evidence a client could possess that would cause an attorney to have good reason to believe her client had broken the law—a murder weapon or a quantity of drugs, for example. There is no indication in the Russell indictment that the nature of the evidence provided to Mr. Russell was critical to his supposed knowledge of a potential investigation of a ''matter within the jurisdiction of any department or agency of the United States.''

[14] Note, though, that in some situations involving child pornography, destruction of the images on the laptop hard drive is not only not prohibited, it is statutorily mandated. There are only two statutory defenses to possession of child pornography, and one of them requires that the possessor ''promptly and in good faith, and without retaining or allowing any person, other than a law enforcement agency, to access any image or any copy thereof. . . took reasonable steps to destroy such image.'' 18 U.S.C. § 2252A(d)(2). This defense only applies to situations where an individual ''possessed less than three images of child pornography,'' id. at (d)(1), and thus may or may not be applicable in the Russell case.

[15] This is not such a hypothetical circumstance—the indictment in the Russell case alleges that Russell and church officials allowed Tate to return to his apartment on church property and remove various items, including ''child pornography.'' The indictment also alleges that Tate ultimately discarded these items, including ''most of his child pornography collection.'' *Id*. While this activity in itself is the basis for a Count in the indictment, it is one of the background facts upon which the indictment is based.

  WCR ISSN 1559-3185

the client offers Attorney the evidence, stating that if Attorney does not take possession of it, the client will destroy it. The attorney refuses, and the evidence is destroyed. Under the theory of the U.S. Attorney for the District of Connecticut, each of these might be a violation of the Act. If giving the client evidence presuming he will destroy it is ''knowing destruction'' under the Act, so is not taking evidence from Client when Attorney presumes that Client will destroy it if Attorney does not take possession. Once the ''knowing destruction'' occurs by another's hand, there is very little basis for distinguishing between a situation in which the attorney temporarily possesses the evidence and one in which the attorney could take possession but chooses not to. In either situation, the ''knowing destruction'' is the fact that Attorney knows that someone else plans to destroy the evidence, but does nothing to prevent it.

The failure to act, of course, is ordinarily not a basis for criminal liability, although there are some narrow exceptions.[16] If the foregoing analysis is correct, however, the enforcement of Section 1519 may in fact impose on Attorney a responsibility to obtain the evidence to prevent its destruction, and if Attorney does not do so, the Model Rules may require Attorney to disclose the client's intentions or actions to the government. While the Model Rules prohibit the disclosure of ''information relating to the representation of a client,'' Rule 1.6(a), creates an exception where the ''lawyer reasonably believes [it] necessary . . . to comply with other law.'' Rule 1.6(b)(6). If the Act would penalize Attorney for destruction by Client of evidence not in Attorney's possession, and the Model Rules prohibit the commission by Attorney of a criminal act that reflects adversely on his or her honesty, trustworthiness, or fitness, the only options for Attorney to avoid violating the Act and the Model Rules appear to be either to take possession of the evidence or to notify the government of her client's destruction (or intended destruction) of the evidence.

We do not believe that the drafters of Sarbanes Oxley intended such a result. Rather, this outcome appears to be the product of a statute that is too broadly drafted and an aggressive use of that provision that threatens to reach into the very heart of the attorney-client relationship.

III. Advising the Client: The Impact of Section 1519 On Client's Electronically Stored Information

The modern ubiquity of electronically stored information—in the form of documents, electronic records, or data—also raises a number of significant issues in relation to federal obstruction statutes. Recent changes in the Federal Rules of Civil Procedure[17] highlight the fact that civil practitioners have come to understand the enormous potential value of electronically stored information (ESI), such as metadata[18] and data that has been ''erased'' but not so effectively that it cannot be recovered by forensic information technology. Criminal investigators are just as focused on the value of ESI, and government demands for documents ranging from information request letters to grand jury subpoenas increasingly include detailed and comprehensive instructions for the production of ESI.

The aggressive application of Section 1519 presents a special peril for organizations with large quantities of ESI and information technology processes that automatically transfer, modify, or purge data or records. There are a number of circumstances under which a federal matter may arguably be ''contemplated'' under the statute. It is easy to envision circumstances in which evidence relevant to a matter within the jurisdiction of the federal government is destroyed without a single individual taking any affirmative action to order or cause such destruction. For instance, an employee might circulate an e-mail about a corporate matter and express concern that federal regulators may initiate an inquiry if they ever learn of it; or a whistleblower's complaint may prompt an internal investigation that in turn concludes that there is some evidence of a violation of a law or regulation—albeit perhaps not sufficient to prompt a disclosure to the authorities. In either case, if the company's document retention policy is not suspended as to documents and records relevant to the matter so identified, such an ''automatic'' destruction may occur. The same result would occur if the policy is suspended but the company employees fail to suspend IT systems or processes that transfer, modify or purge ESI relevant to the identified matter. In either case, a very aggressive use of Section 1519 could be the vehicle to pursue just such a case as a crime.[19]

---

[16] The exceptions include crimes such as misprision of a felony, 18 U.S.C. § 4, negligent violations of the Clean Water Act, and strict liability offenses under the Rivers and Harbors Act. In addition, the government could pursue certain responsible corporate officers under a theory of knowing failure to act to prevent a violation under certain environmental statutes.

[17] On December 1, 2006, new rules addressing electronically stored information (ESI) were adopted in FRCP 16, 26, 33, 34, and 37. New Rules 16 and 26(f) require a discussion of ESI at the beginning of litigation, including ''any issues regarding preservation of discoverable information.'' Also to be discussed are ''any issues relating to assertions of privilege or of protection as trial-preparation materials, including whether the parties can facilitate discovery by agreeing on procedures for asserting claims of privilege or protection after production and whether to ask the court to enter an order that includes any agreement the parties reach.'' Inadvertent production is also addressed in Rule 26(b)(5), which provides fallback procedures for post-production assertions of privilege. Rule 26(b)(2) places some limits on the production of ESI that is not ''reasonably accessible.'' The new portions of Rules 33 and 34 address the form in which ESI is to be produced. Rule 33 allows a party to object to an interrogatory on the ground that the answer is located in ESI that is just as easy for the requestor to obtain as the respondent. Similarly, Rule 34 allows a party to request that, and the respondent to object to, the ESI being produced in a particular fashion. Finally, new Rule 37 provides for protection if ESI is lost in circumstances resulting from the ''routine, good-faith operation of an electronic information system.''

[18] ''Metadata'' is information about a particular record or data set that describes how, when, and by whom it was collected, created, accessed, modified, and how it is formatted; it also includes other embedded data, such as spreadsheet formulas, comments, and edits. Metadata is typically not readily apparent to the user of the record or data set, although it can be retrieved, reviewed, altered, and stored along with the record or data set, and may be subject to production in discovery.

[19] Of course, the government would still be required to show that the failure to act in the face of the potential automatic destruction of evidence was inaction with the intent to ''impede, obstruct, or influence the investigation or proper ad-

Given the intense focus on ESI as a rich vein of evidence to be mined for possible proof of criminal violations, such issues are bound to arise, and the potential consequences for failure to effectively freeze records or ESI relevant to a criminal investigation are grave. This places a premium upon effective management of records and electronic data, including: (a) development of a comprehensive, enterprise-wide, and detailed understanding of what records and ESI are maintained by the organization and how the organization's IT systems maintain them and (b) adoption and implementation of a comprehensive records management policy that is tailored to the organization's business, records, and ESI. The policy and the records retention periods must be based on neutral and objective criteria and applied consistently throughout the organization. Such a policy, properly drafted and effectively implemented, and addressing all relevant records and ESI, will ensure both that documents that should be produced are available if required, and that those records that are not available due to the routine, consistent operation of the policy prior to any contemplation of a matter within the jurisdiction of a federal agency do not become the subject of a separate criminal inquiry.

The threat of Section 1519 and the challenge of managing ESI also creates a special need to implement robust litigation-hold procedures upon discovery of a matter that might trigger federal interest. Such procedures should include, among other things: (a) identification of all employees who may have discoverable records or ESI;[20] (b) distribution of the litigation-hold notice to all potential custodians; (c) involvement of IT staff in ESI preservation; (d) confirmation that all back-up tapes or other ESI stored on a computer network be preserved; and (e) temporary suspension of record destruction procedures, automatic deletion processes, computer and server recycling, system upgrades, and recycling of back-up tapes, pending the identification and sequestration of relevant records.

The foregoing is not a complete set of considerations by any means, and each organization will have specific issues applicable only to its business operations. The importance of creating an effective litigation-hold procedure, however, cannot be over-emphasized. The days of pleading ignorance of one's own systems, or inadvertent modification or destruction of electronic records due to a failure to understand an organization's business processes and IT systems, are fast coming to an end.

Clients need to understand the risk of criminal prosecution if they do not have control over their ESI. So do the attorneys who advise them. Much is at stake. An attorney's advice in carrying out an internal investigation may need to focus as much on preserving ESI throughout the organization as on the actual facts of the matter.

IV. Conclusion

The case of *United States v. Russell* may unfold in ways that show that the allegations amount to nothing more than traditional obstruction of justice—an individual, knowing that the FBI has initiated an investigation, destroys evidence to prevent it falling into the government's hands. If, however, the government's case fails to establish that Russell had actual knowledge of the investigation at the time that he is alleged to have destroyed the computer hard drive, or the government takes the legal position that it need show only that Russell contemplated the possibility of a federal inquiry, then indeed a new era of potential criminal liability, with all its attendant complications, has arrived. Attorneys and clients will need to carefully analyze their decisions about the disposition of records or other evidence that might relate to matters that, at some point in the future, are likely to become the subject of federal attention.

---

ministration of any matter within the jurisdiction of any department or agency of the United States . . . .''

[20] In some instances, a demand for records and ESI will be narrowly focused, and the group of employees likely to have custody of relevant materials will be readily identifiable. In other cases, the breadth of the demand may be such that the litigation hold must be applied to the entirety of the enterprise's records and ESI, pending either negotiations with the government to narrow the scope of the subpoena or further analysis of the records and ESI to cull the irrelevant from the relevant.

  WCR ISSN 1559-3185