



# PRIVACY & SECURITY LAW



## REPORT

Reproduced with permission from Privacy & Security Law Report, 9PVL1517, 11/01/2010. Copyright © 2010 by The Bureau of National Affairs, Inc. (800-372-1033) <http://www.bna.com>

### Preparing for the Perfect Storm: What Every Foreign Corrupt Practices Act Lawyer Should Know About E-Discovery



By JOHN REED STARK

*John Reed Stark is Managing Director in charge of the Washington office of Stroz Friedberg, a digital forensics and e-discovery consulting firm. Formerly, Stark served for almost 20 years in the Enforcement Division of the Securities and Exchange Commission, the last 11 of which as Chief of its Office of Internet Enforcement. He also has served for the past 15 years as an adjunct professor of law at the Georgetown University Law Center, where he teaches a course on Technology and the SEC and Advanced Securities Regulation.*

#### Introduction

Whether a company is conducting an internal Foreign Corrupt Practices Act (FCPA)<sup>1</sup> investigation or handling contentious FCPA litigation against the U.S. Securities and Exchange Commission (SEC) and/or the U.S. Department of Justice (DOJ), FCPA matters are inherently complex, high stakes, and international in scope, and present a broad range of challenging e-discovery issues, especially relating to privacy.

2011 and beyond will represent “the perfect storm” for any entity or individual suspected of violating the FCPA, as SEC and DOJ, the two federal agencies that share jurisdiction over FCPA violations, are now poised to initiate an unprecedented campaign of FCPA-related enforcement investigations, actions and criminal prosecutions. Here is why:

- **A Specialized SEC FCPA Unit.** For the first time in its history, the U.S. Securities and Exchange Com-

<sup>1</sup> The U.S. Foreign Corrupt Practices Act of 1977 (FCPA) generally prohibits U.S. companies and citizens, foreign companies listed on a U.S. stock exchange, or any person acting while in the United States, from corruptly paying or offering to pay, directly or indirectly, money or anything of value to a foreign official to obtain or retain business (the “Antibribery Provisions”). The FCPA also requires “issuers” (any company including foreign companies) with securities traded on a U.S. exchange or otherwise required to file periodic reports with the SEC to keep books and records that accurately reflect business transactions and to maintain effective internal controls (the “Books and Records and Internal Control Provisions”).

mission on January 13, 2010 created a specialized enforcement unit solely dedicated to FCPA investigations and enforcement actions (*see* <http://www.sec.gov/news/press/2010/2010-5.htm>);

- **New Whistleblower Provisions.** The new whistleblower provisions contained in the Dodd–Frank Wall Street Reform and Consumer Protection Act reward informants who provide certain types of information leading to successful securities actions, including FCPA actions, with between 10 percent and 30 percent of any recovery over \$1 million. The provision may also apply to “related actions” initiated by the DOJ or other federal, state, and foreign law enforcement agencies. Given the large penalties frequently collected for FCPA violations, the new provisions will provide a particularly powerful incentive for whistleblowers with information on potential FCPA violations. Consider the 2008 Siemens joint SEC/DOJ FCPA prosecution, which resulted in a \$1.6 billion dollar penalty against Siemens and would have yielded a whistleblower an astonishing award of as much as \$496 million. No company is immune from the disgruntled employees, unhappy investors or portfolio companies, peeved competitors and the like who are now spectacularly incentivized to forward even the most baseless allegations to the SEC;
- **A Hefty SEC Budget Increase.** The Dodd-Frank Act also provides the largest budget increase in the SEC’s history, preliminarily authorizing a steady series of increased appropriations that will virtually double the SEC’s budget over the next four fiscal years. In addition, the Act gives the SEC the discretion to tap into a new \$100 million reserve fund—which will be replenished in \$50 million annual increments—to supplement its budget. The new funding will undoubtedly be used to bolster enforcement efforts, especially FCPA enforcement, which the SEC staff has designated as a top priority. Specifically, the SEC has announced its plans to hire 800 additional staff members to help with its investigations into securities fraud and boost its surveillance capabilities, including 374 employees in 2011, increasing its staff levels to some 4,200 employees; and
- **Increased SEC/DOJ Collaboration.** Kicking off its new FCPA initiative, the SEC recently hosted its own “FCPA Boot Camp” for SEC and DOJ staff, a training exercise designed to improve an already close relationship between these two agencies.

## The FCPA and E-Discovery

What often happens during FCPA investigations is that lawyers can neglect the importance of data management and tend to view the management of electronically stored information (ESI) as a secondary and purely technical process. Yet, what is required for FCPA matters, many of which are high stakes “bet the company” matters, is a unique combination of digital forensics expertise, specialized litigation prowess, significant investigatory experience and quality assurance management. More than just ensuring complete, accurate and user-friendly results, handling ESI in the context of an FCPA investigation can be almost akin to handling DNA in a murder investigation.

Indeed, the handling of ESI during an internal FCPA investigation is especially critical. ESI productions that

are found incomplete, inaccurate or sloppily-handled not only create significant liability and drive up costs, but most importantly, generate distrust from authorities, especially the SEC. Failures pertaining to the identification, collection and analysis of ESI especially in an FCPA matter, can tarnish the reputations of the attorneys representing witnesses and defendants, significantly increase the costs of the investigation, enhance the amount of penalties involved, and increase the likelihood of personal liability or even jail time for the involved individuals (especially when a prosecutor, investigator or judge believes an ESI mishap was an intentional attempt to obstruct justice).<sup>2</sup>

To help FCPA practitioners keep their data handling from turning into a sideshow, this article presents a top ten list of e-discovery directives and ideas to bear in mind. Given that every FCPA matter presents a slew of privacy-related issues, the notions set forth in this article should also prove equally valuable for privacy practitioners who often serve as an important part of an FCPA legal team.

### 1. Location, Location, Location.

The typical definition of “documents” in a government subpoena is incredibly broad and essentially seeks any ESI of any possible type. Moreover, many subpoena “document definitions” nowadays often go so far to demand identification of the search methodology (including search terms, protocols, syntax use, etc.) used to locate responsive ESI. Many government demands now also even request inventory lists of the type of media searched, including “local” media (i.e. media not residing on a network) such as hard drives, thumb drives, cellular phones, etc.), back-up media, off-site media and any other traditional and nontraditional places which might warehouse ESI.

Accordingly, the first step in handling an FCPA-related subpoena or document request is to locate all potentially responsive ESI. Failing to produce even one responsive document can have disastrous consequences for both the company and its attorneys, and can transform a minor FCPA inquiry into a full-scale international investigation. Yet, as with many such FCPA-related requests, the typical definition of “documents” is extraordinarily broad, complicated and confusing—and with respect to responsive data, the reality for most companies is that their officers and employees *simply don’t know what they don’t have*.

ESI resides everywhere for most companies—from file cabinets, closets and document warehouses to desktop computers, laptop computers, thumb drives, cell phones, SharePoint, databases and myriad other locations. Whether a complex extraction from a global multi-terabyte database or a cloud-based extraction

<sup>2</sup> For example, in one of the more comprehensive recent opinions discussing eDiscovery issues of preservation and spoliation, a federal magistrate judge not only sanctioned the president of the defendant company in a copyright infringement matter, but even went so far as to mention possible prison time unless he paid the plaintiff’s legal fees. *See Victor Stanley Inc. v. Creative Pipe Inc.*, 2010 WL 3703696 (D. Md. Sept. 9, 2010) (“[F]inding . . . that Pappa’s pervasive and willful violation of serial court orders to preserve and produce ESI evidence be treated as contempt of court, and that he be imprisoned for a period not to exceed two years, unless and until he pays to Plaintiff attorney’s fees and costs that will be awarded to the Plaintiff . . .”).

from an East Asian server farm, the first step is to design a methodology and approach to identify the location of all relevant data.

## **2. Handle with Care.**

Once located, the next step is to begin collecting and preserving every byte of potentially responsive ESI in a forensically sound and evidentiary bulletproof manner. Given their typically vast scope and breadth, FCPA collections in particular require ironclad ESI-collecting methodologies, meticulous protocols and painstaking documentation of evidentiary transitions, insuring an easily defensible and rock-solid evidentiary authentication and chain of custody.

Insuring hard drives used during collections are pristine; employing secured methods of transferring data (such as use of encryption) when transporting those hard drives; and performing thorough background checks on all collections personnel to insure their reliability as custodians or expert witnesses are all typical indicia of conscientious data collection. During FCPA investigations in particular, nothing can be left to chance and an FCPA digital forensics team must maintain constant vigilance for potential evidentiary vulnerabilities or other challenges to the authenticity or integrity of ESI-handling procedures.

Once ESI collection is completed, FCPA related ESI should be stored in a forensic lab facility with state-of-the-art equipment, high-tech security, including restricted access, video camera surveillance, evidence safes, etc.

## **3. Be Gil Grissom Not Gil-igan.**

Handling the identification, preservation and analysis of ESI can be every bit as important as when scientist Gil Grissom of the hit television series *CSI* handles DNA evidence. Well-heeled digital forensic experts in an FCPA matter can add value on numerous fronts to an FCPA related engagement. First, forensic know-how allows a company and its attorneys to sharpen their focus precisely on the most probative data, critical during any FCPA internal investigation. Second, effective forensics teams or strong processing utilities can de-duplicate and filter most ESI types saving unnecessary data hosting fees later on, speeding up ESI processing, and reducing expenses overall. Finally, given the intricacies of the databases and ESI storage facilities typically involved in FCPA matters, having a strong digital forensic team on call will allow for rapid deployment to address corruption, spoliation and other issues that crop up at the last minute, e.g. the night before an FCPA's presentation of their investigative report to the SEC.

## **4. Find the Right Host.**

After FCPA related data is forensically collected and secured, it should be warehoused in a data hosting facility with tools that allow for the smooth integration of the many different ESI types that will crop up. ESI relevant to an FCPA matter will undoubtedly come in many types, from Word documents, Excel spreadsheets, PowerPoint presentations, PDFs and other common formats, to the more complex data formats residing within immense enterprise databases.

With respect to data gleaned from multiple applications, employ a data tool with capabilities that enable culling and production of a broad range of ESI types into their native as well as searchable formats as well as

easy-to-use advanced query tools for many different kinds of logic searches—both Boolean and natural language. Given the extraordinary amount of ESI involved in a typical FCPA investigation, a good FCPA tool should also have numerous options for setting search parameters and a broad array of redaction tools for user-tailored flexible editing.

Also, remain mindful of the challenges created by databases. First, preserving, authenticating, analyzing, and accurately producing data from enterprise databases requires special skills and methodologies, and can depend on the industry of the company involved (e.g. insurance, financial, design, telemarketing, consumer electronics—each business may utilize an entirely different enterprise architecture which can present different ESI-related challenges.) Second, during an FCPA investigation, a digital forensics team may ultimately have to authenticate database output for use in a trial, or may be called upon to identify problems with database schema, front-end reports, or workflows that are causing flawed database outputs.

E-mail threading is also an important need during, in particular, FCPA investigations. In recent speeches, SEC and DOJ officials have indicated their desire to charge more individuals with FCPA violations (as opposed to entities), and promise to vigorously analyze all employee communications to achieve this goal. Hence, email has evolved into the primary government focus during an FCPA investigation. As a result, handling email, particularly complex threads, during an internal investigation can be tricky. Be sure to obtain a visual depiction of email threads, allowing reviewers to see, analyze and bulk code entire email conversations and also identify any emails missing from the review population.

Finally, plan for the large, segmented, multi-party situations typical in an FCPA investigation. FCPA lawyers typically require subschema of ESI that permits restricted access by various parties, with each warranting varying levels of access and security rights, not only providing a unique database for each part of the matter, but also controlling costs and providing economies of scale for all parties.

## **5. Get the Paper, Get the Paper.**

FCPA matters will always involve a lot of paper, and FCPA lawyers should be prepared to deal with a large volume of scanned hardcopy documents and employ a forensics team that can make equal sense of a room full of boxes or a room full of servers. FCPA matters will typically involve various types of paper (e.g., forms, reports, etc.), which require a review tool with artificial intelligence capabilities to identify document types and extract key data fields from the face of documents. By “normalizing and standardizing” all information in one centralized repository, an FCPA review team can seamlessly search paper and electronic ESI within the same platform, which translates into better organization, increased convenience—and hefty cost savings in the long run.

## **6. Consider Privacy in a Global Context.**

FCPA matters involve travel to, and handling of ESI in, the far reaches of the world, where the violation of a privacy law can result in serious sanctions and border-crossing issues. FCPA lawyers should work with privacy lawyers and forensic teams that have extensive expertise preparing protocols consistent with European

Union (EU) ESI privacy standards. Given that privacy regulation is an extraordinarily fluid area, an FCPA lawyer and his or her forensics team must monitor carefully recent privacy developments, and stay current with the latest changes in international policies and requirements. For instance, the EU Data Protection Directive (95/46/EC) compels member nations to enact national data protection laws harmonized with the principles of the directive (or more stringent) and has basic principles pertaining to, among other things, the processing of personal information, the security of data, notification to supervisory authorities, transfer restrictions and a slew of other complex and varied trans-border data flow rules and restrictions. The laws promulgated pursuant to the directive vary by nation, as does the degree of enforcement and consultation with data privacy experts is critical. There may also be considerations relevant to the Asia-Pacific Economic Cooperation (APEC) Privacy Framework or any other specific rules promulgated by any particular country. Whenever data crosses any border (even borders between U.S. states), important privacy issues will always arise.

### **7. Gumshoe Work.**

Reliably ascertaining the facts is always pivotal in FCPA inquiries and will always entail a certain modicum of pure gumshoe work. FCPA lawyers should employ a private investigations firm as part of their ESI collection teams to assist with locating witnesses, developing information regarding witness credibility, assessing the strength of financial and electronic evidence, performing background checks, and generally remaining on hand for ESI related crisis. Today's private investigators are more Mickey Mouse than Mickey Spillane—often more comfortable at a desk armed with a wireless mouse rather than on the streets in a trench coat armed with a Colt 45. Indeed, a broad range of publicly available databases can sometimes yield the pertinent evidence and useful information upon which successful FCPA investigations often hinge so an FCPA team should always have a seasoned team of private investigators at their disposal throughout an investigation.

### **8. Linguistic Challenges.**

By definition, FCPA matters involve foreign persons and/or entities, and companies and lawyers handling FCPA matters need the capability to process documents in non-romance languages. Be sure to employ an ESI hosting tool that has integrated Unicode processing and hosting into the investigative process and can perform search and retrieval of hieroglyphic languages such as Chinese, Japanese, Korean, Hebrew and Russian. It also goes without saying that every FCPA team should employ software that has some translation capabilities for French, German, Spanish, Russian, Italian, Japanese, Chinese, Korean and other non-English ESI.

### **9. Going Mobile.**

More and more, especially in the context of an FCPA investigation, foreign companies will not want (or not be permitted because of privacy restrictions) to trans-

port their ESI outside of their home country's jurisdiction. An FCPA forensics team should have at its disposal some sort of mobile processing *Safe Harbor* certified capability that can rapidly deploy data hosting and processing beyond U.S. borders, not only to provide a secure processing environment for resident reviewers, but also to deliver ironclad assurance of compliance with country-specific ESI privacy regulations, which often arise in today's multinational business environment.

### **10. Review Reviewers.**

Because of the size and scope of a typical FCPA investigation, many law firms will employ large document review teams to handle the initial review of relevant documents. While this strategy has many advantages, managing these review teams is always a tremendous concern. Choose a hosting tool that offers a custom-tailored reporting interface so senior attorneys can monitor carefully the quality, speed and efficacy of work performed by reviewers. This crucial oversight functionality provides valuable intelligence, allowing an FCPA lawyer to track the time reviewers spend viewing a document, as well as the quality of their analysis and decisions.

### **Conclusion**

Neither DOJ nor the SEC have the resources to conduct the large scale international investigations almost always required when a potential FCPA violation arises. So what has evolved instead is a cottage industry of FCPA lawyers who traverse the globe performing FCPA investigations on behalf of their clients and then "self-reporting" their results to both DOJ and the SEC. Sometimes an FCPA lawyer might even self-report to DOJ or the SEC the general nature of a potential violation, and then, with the acquiescence of SEC and/or DOJ officials, initiate their own internal investigation of a company.

This lack of judicial oversight of an FCPA lawyer's handling of ESI during an internal investigation (as there would be, for example, during the discovery phase of a civil or criminal proceeding where a judge can issue sanctions for ESI handling failures) is not an excuse for lax attention to ESI management. Indeed, many FCPA investigations culminate with a written report and presentation to SEC and/or DOJ officials where the FCPA attorney recommends remediation. Given the obvious gravity of this report and presentation, its veracity and reliability, especially its handling of ESI, must be beyond reproach.

Whether conducted at the behest of the government or at the behest of a corporate client (and perhaps even unknown to the government), FCPA investigations in particular will always present a unique bevy of ESI-related challenges. By following the range of simple notions set forth above, FCPA lawyers can tackle these challenges head-on—and can avoid creating data-related mishaps, which can not only jeopardize the credibility and integrity of a client's defense, but can also impugn the reputations of the team of FCPA lawyers handling the matter.