Bloomberg BNA

Privacy and Security Law Report®



# Six Technology-Related Caveats in Government Investigations

BY JOHN REED STARK

## Introduction.

Much like the innovative and extraordinary scientific approach portrayed on the ''CSI'' television series, today's regulatory and law enforcement leaders are taking a similar leap, employing hi-tech tools and digital forensic methods to enhance their investigatory prowess. And much like it was for the fictional ''CSI'' Las Vegas crime lab pioneer Gil Grissom, this transformation is one of both ingenuity and necessity.

Consider the enforcement staff of the Securities and Exchange Commission (SEC). While the regulatory rulemaking and other statutory mandates called for by the Dodd-Frank Wall Street Reform and Consumer Protection Act have placed extraordinary constraints on an already over-extended SEC regulatory staff, budgetary woes and mounting political and public criticism have placed similar pressures on SEC enforcement staff. Consider also federal prosecutors at the Department of Justice (DOJ) who, similarly bleeding from their perceived spotty record against the perpetrators of the recent financial crisis,[1] face the same mounting strain and demands.

Now more than ever, government prosecutors and investigators, in particular those at the SEC and DOJ, must achieve quick results, must be innovative and creative, and most of all, must leverage technology to bolster efficiency and efficacy. In other words, all of law enforcement has to achieve more with less—and is taking advantage of technology to do so.

On the plus side, armed with a dedicated crop of digital forensic examiners together with state-of-the-art digital forensic laboratories, an eager SEC enforcement staff and DOJ prosecutorial workforce have technologically blossomed, pushing the envelope during the investigative process and taking advantage of the latest electronic tools, especially with respect to subpoenas and document requests. But on the minus side, SEC enforcement staff and DOJ prosecutors have also unfortunately and concomitantly entered into arguably uncharted legal territory, raising burgeoning and prickly investigatory issues that merit close scrutiny.

For instance, data-related challenges have always plagued defense counsel—especially when the terabytes of data of their corporate clients can reside in umpteen different domiciles including desktop and laptop computers, cellphones, tablets, internal and external networks and databases, intranets, SharePoint platforms, antiquated and legacy servers and systems, backup tapes, ''the cloud''[2] and the list goes on. For de-

*John Reed Stark is managing director in charge of the Washington office of Stroz Friedberg, a global digital risk management and investigations firm specializing in digital forensics, data breach and cybercrime response, data discovery, security risk science, and business intelligence and investigations. Formerly, Stark served for almost 20 years in the Enforcement Division of the U.S. Securities and Exchange Commission, the last 11 as chief of its Office of Internet Enforcement. He has served for 15 years as an Adjunct Professor of Law at the Georgetown University Law Center, where he taught a law course on Technology and the SEC.*

[1] *See e.g.*, Robin Sidel, *Jailed Banker is Rare Prize for U.S.*, Wall St. J., Nov. 12, 2012, at C1. *See also* James B. Stewart, *Another Fumble by the SEC on Fraud*, N.Y. Times, Nov. 17, 2012 (''With the commission already at two strikes in its most prominent mortgage fraud cases, 'it seems unable to either bring or prove a case,'' Professor Coffee said. 'The institutions can't be guilty without someone making a culpable decision, but the S.E.C. seems to be emulating Inspector Clouseau and is constantly losing the trail.' '')

[2] So-called ''cloud computing'' has many definitions, depending on whom you ask (and at what time of day). For certain, traditionally a company's or an individual's data have resided in a local, physical space: hard drive, CD, Zip disk, thumb drive, etc., but now data storage is migrating to storage facilities which have become casually referred to as ''the cloud.'' Of course, the data remain physically stored *somewhere* (probably on a server ''farm'' where space/rent is

fense counsel, knowing when to push back against the SEC staff or DOJ prosecutors (such as when to refuse to comply with an SEC subpoena or move to quash a grand jury subpoena because of failures relating to the relevance, scope, particularity and/or undue burden of a voluntary request or subpoena) has never been an easy decision.[3]

Indeed, in the context of an SEC investigation, taking the wrong turn when responding to an SEC subpoena or request (such as refusing to respond) can result in a costly and reputationally damaging SEC subpoena enforcement action, prompt the SEC enforcement staff to seek a broad and sweeping asset freeze, or even rile the staff inadvertently and escalate the staff's interest in a witness.[4]

Similarly, in the context of a DOJ investigation, contemplating whether to file a motion to quash a grand jury subpoena (for example, served on a target or subject) poses a similarly critical predicament given that the stakes are particularly high for a target or subject of an investigation (e.g., incarceration for a client or the employee of an enterprise). Moreover, most criminal defense counsel would probably prefer not to initiate a motion to quash, and would rather strike a more cooperative tone with a prosecution team. Finally, much like refusing to comply with an SEC subpoena, filing a motion to quash a grand jury subpoena can also have the unintended consequence of increasing unwanted and unnecessary (and costly) investigative scrutiny.

Along those same lines, any sort of data-related mishap during an SEC or DOJ production can trigger similarly dire consequences. For instance, when the production of data becomes a sideshow in an SEC or DOJ investigation, the government can suddenly increase its focus (in addition to concentrating upon the underlying misconduct) on whether the witnesses, targets, subjects *or counsel* have engaged in any shenanigans relating to the data (such as intentionally overlooking and therefore not producing a potentially inculpatory document).

Ultimately, by causing a data-related mishap, otherwise innocent witnesses can risk becoming defendants in a criminal action, perhaps charged with obstruction of justice in a parallel or independent proceeding (a typically much simpler charge to prove than the underlying white collar crime, such as insider trading, financial fraud, market manipulation, wire fraud, etc.) In addition, if the SEC enforcement or DOJ staff suspect a defense attorney of not being forthcoming with the responsive data of a witness, that defense attorney not only endangers his or her reputation but, given in particular the SEC's eagerness to refer matters to bar counsel, perhaps even imperils his or her license to practice law entirely.

## The Caveats.

To help calm and relax investigators and prosecutors and manage a law enforcement request or subpoena, consider the caveats below, first to help understand when to ''say when'' with respect to technologically innovative or overly aggressive SEC or DOJ subpoenas or voluntary requests, and second, to avoid any data related commotions altogether during the course of a regulatory or criminal investigation.

The caveats below: (1) highlight some of the government's latest forays into the outer limits of digital forensics; (2) advise on how to preempt SEC and DOJ digital forensic examiners from raising data-related questions or objections (such as challenging defense counsel with respect to the completeness or responsiveness of a complex data production or accusing a witness of intentionally failing to produce important responsive documents, emails, spreadsheets, PowerPoints and the like); and (3) provide some guidance as to when and how to step-up a digital defense to counter an unreasonable request or subpoena.

**1. Watch Out for Warrantless SEC Searches and Seizures and Overbroad Unspecified DOJ Requests.**

**SEC Investigations.** In addition to the standard broad definition of ''documents'' in an SEC subpoena, the SEC staff may add another equally exhaustive provision seeking so-called ''ESD,'' which stands for ''electronic storage devices.'' This provision, which the staff has begun employing recently, may go so far as to mandate the turning over of every conceivable piece of data-related equipment, appliance, gadget, etc. that can warehouse information (including laptops, desktops, network drives, thumb drives, printers, fax machines and the rest).

The implications of turning over an actual device to the SEC, DOJ or any other governmental entity is that a witness, target or subject is likely turning over a treasure trove of sensitive and private data, both known and unknown to the user. This data could include: (1) private and personal data of the user, as well as the user's friends, family, colleagues, clients, customers, etc.; (2) data protected by domestic or foreign statute or requiring notice of disclosure per contract; (3) relevant or non-relevant material loaded on to the machine by another user; (4) inculpatory information planted via a vi-

---

cheap), but from the user's perspective, the data is ''floating'' in an accessible place for all of his or her devices. Whatever its definition, this permanent trend of consolidation of potentially relevant data into massive digital floating third-party data warehouses: (1) has become a tremendous boon to federal and regulatory investigators; and (2) raises the danger, discussed throughout this article, that when the SEC staff, a grand jury or some other investigatory body subpoenas the contents of a cloud, they are engaging in an unlawful search and seizure lacking the requisite level of particularity, reasonableness, breadth and scope that courts require. *See e.g., United States v. R. Enters.*, 498 U.S. 292, 299 (1991) (stating that a grand jury may not ''engage in arbitrary fishing expeditions'' or base its investigation on ''malice or an intent to harass'').

[3] *See e.g., In re Two Admin. Subpoenas*, No. 05-MC-29-P-DMC (D. Me. Jan. 25, 2005) (''Pursuant to the Fourth Amendment, a subpoena duces tecum may be quashed or modified ''if compliance would be unreasonable or oppressive . . . a subpoena is not unreasonable or oppressive if the proponent establishes relevancy, admissibility, and specificity. . . . In the absence of privilege, courts normally will ask only whether the materials requested are relevant to the investigation, whether the subpoenas specify the materials to be produced with reasonable particularity, and whether the subpoena commands production of materials covering only a reasonable period of time.'') (citations omitted). *See also In re Grand Jury Matters*, 751 F.2d 13, 18 (1st Cir. 1984).

[4] SEC enforcement subpoenas are administrative subpoenas which are not self-enforcing—i.e., there is no formal avenue of objection other than to refuse to comply, which then leaves the decision up to the staff as to whether a subpoena enforcement action is warranted. N.B. Section 21(c) of the Exchange Act, 15 U.S.C § 78u(c), makes it a misdemeanor to ''willfully disobey a validly issued subpoena for testimony or documents without just cause, punishable . . . by a year in prison or a $1000 fine or both;'' however, recipients of subpoenas rarely if ever incur this statutory penalty.

  PVLR ISSN 1538-3423

rus or other form of malware; (5) privileged communications with counsel; or (6) a broad range of other types of information which would otherwise not be produced pursuant to an SEC or any other kind of governmental request or subpoena.

While certainly a clever and inventive attempt by the SEC enforcement staff to locate the proverbial smoking gun during an investigation, this troublesome provision of a subpoena seems more akin to a seizure than a document production. It is as if the SEC were requiring a witness to produce their filing cabinet to the staff complete with all of the files inside its drawers.

While their intentions are most certainly noble and their creativity worthy of praise, the SEC staff arguably lacks the authority for this sort of request. Should the staff pursue this new form of subpoena in federal court, the staff could lose. Specifically, Section 21 of the Securities and Exchange Act of 1934 sets forth the authority and the parameters of SEC staff subpoenas and states:

> For the purpose of any such investigation, or any other proceeding under this title, any member of the Commission or any officer designated by it is empowered to administer oaths and affirmations, subpoena witnesses, compel their attendance, take evidence, and require the production of any books, papers, correspondence, memoranda, or other ***records*** which the Commission deems relevant or material to the inquiry. Such attendance of witnesses and the production of any such records may be required from any place in the United States or any State at any designated place of hearing.[5]

The SEC staff's right to access ''records' arguably contemplates something akin to a document, and nowhere in the authoritative language of Section 21 is the staff granted license to access physical equipment such as a file cabinet (whether that file cabinet is made of metal, wood, circuitry or plasma).

Aside from potentially lacking the authority to seek ESD, the SEC staff subpoena for ESD is also troubling for another equally important reason. SEC (and DOJ, if referred to them by the SEC staff) forensic examiners will undoubtedly take advantage of the latest forensic tools and engage in a digital forensic deep dive into any piece of media, and what the examiners will discover is always difficult to predict.

For instance, the ESD will likely contain so-called ''non-active'' files, such as deleted recoverable files[6] or data located in the ''unallocated space''[7] of a hard drive. Thus, a witness producing ESD may be producing information, including whole bits of information as well as data remnants, fragments and artifacts, which he or she believed had already been deleted.

Thus, without the witness's knowledge, the ESD could contain the same litany of personal and private information described above as well as a broad range of other information, perhaps forgotten by the witness, hidden on the media or otherwise in ''not-so-plain'' view. Given the SEC's lengthy list of its ''Routine Uses of Information'' contained in its Forms 1662 and 1661,[8] the SEC staff could then refer that previously unknown information to any other investigative, prosecutorial or regulatory authority. Who knows? A teenage child, a friend of the family, or even a visiting contractor (!) could be using a homeowner's computer for unlawful purposes and left artifacts along those lines in unallocated space, and suddenly an otherwise innocent witness is arrested and carted off in handcuffs.

Unless absolutely certain of the active and deleted contents contained in the ESD, there exists tremendous risk for a witness who, in response to a subpoena or voluntary request, turns over that ESD to any branch of the government. If the SEC enforcement staff seeks ESD, consider escalating the issue up the chain of command and speaking with senior SEC officials about this disquieting and emerging practice. If the SEC staff refuse to relent, consider proposing an independent and reputable third-party digital forensics firm to conduct the review of the media, run key word searches, and even explore unallocated space—and then, after a privilege, relevancy or other review by counsel, produce the final, properly filtered results to the SEC staff.

**DOJ Criminal Investigations.** In the context of DOJ criminal (or other) government investigations, when handling a similar type of request to the SEC staff's ''ESD request,'' defense counsel should consider argu-

---

[5] 15 U.S.C. § 78u(b) (emphasis added).

[6] A ''deleted recoverable file'' is a file that is typically easily recovered with forensic software, such as a Microsoft Word document, PowerPoint presentation, PDF file, etc., where, perhaps unbeknownst to the user, a file record for that data still exists within the file system.

[7] The unallocated space and file slack of desktop or laptop personal computers typically provide important leads for digital forensic examiners. Here's why: Files saved to the hard drive of a computer are typically described as residing in ''allocated space,'' i.e., space on the hard drive allocated by the file system. When a user deletes these so-called ''active files,'' the files usually do not disappear from the hard drive. Rather, the operating system no longer allocates or saves that hard drive space for the file and simply designates that area of the hard drive as unallocated (i.e., unused) space. The data actually stay still—the file system just marks that portion of the drive as usable for other files. Within unallocated space, a digital forensic examiner can usually extract file artifacts, such as deleted files, temporary files (created when a user opens a file), file fragments, deleted internet history and other, albeit disorganized, but readable, bits of data. Indeed, evidence gleaned from unallocated space has become so important in the context of litigation that using a ''wiping program'' to render unrecoverable the artifacts from the unallocated space can even draw a discovery sanction from a judge. *See also TR Investors LLC v. Genger*, No. 3994-VCS (Del. Ch. Dec. 9, 2009) (finding defendant Arie Genger in contempt of court for ''wiping'' the ''unallocated space'' of the hard drive of his work computer and file server in the face of an order that prohibited him from ''tampering with, destroying or in any way disposing of any Company-related documents, books or records''). This approach similarly applies to so-called ''slack space'' (that portion of a cluster unused by an active file), which can also contain similar information.

[8] In its Form 1662 (and 1661 for regulated entities), the SEC lists what it considers to be the ''routine uses'' of information that staff may obtain during an investigation—broad and lengthy lists of possibilities. Those ''routine uses'' include disclosure to other law enforcement authorities, self-regulatory organizations, bar associations, state accountancy boards and other licensing organizations, trustees, receivers and court-appointed officers, and persons questioned during the course of an investigation. *See* U.S. Sec. and Exch. Comm'n, SEC 1662, *Supplemental Information for Persons Requested to Supply Information Voluntarily or Directed to Supply Information Pursuant to a Commission Subpoena*, *available at* http://www.sec.gov/about/forms/sec1662.pdf; U.S. Sec. and Exch. Comm'n, SEC 1661, *Supplemental Information for Entities Subject to Inspection by the Commission and Directed to Supply Information Other Than Pursuant to Commission Subpoena*, *available at* http://www.sec.gov/about/forms/sec1661.pdf.

ing that the government must limit its searches of hard drives, computers and other data storage devices with the same particularity required of any search, and that the government must: (1) explain how relevant data will be distinguished from irrelevant data; (2) note how the information will relate specifically to the underlying allegations; and (3) follow detailed protocols to avoid revealing nonresponsive information, privileged information and other protected or otherwise deemed private information.[9]

**2. Handle Data With Care.** After receiving an SEC, DOJ or other criminal or regulatory subpoena or request, once a witness locates all possible responsive information, as a matter of best practice, the next step is to begin collecting and preserving every byte possible of potentially responsive ''electronically stored information'' (ESI) in a forensically sound and evidentiary bulletproof manner. It is during this phase that the SEC and DOJ digital forensics lab personnel have begun recently to intervene by presenting a slew of questions pertaining to the data collections conducted by a witness. For instance, the SEC's forensics staff may ask to review the pre and post acquisition ''hash values''[10] of the data to verify proper imaging of the devices, or whether the forensic collection of the ESI was verified against an external time source (e.g., atomic clock) in order to determine the accuracy of the file system time stamps.

Given their typically vast scope and breadth and the likelihood of hypercritical digital oversight by SEC and DOJ forensics staff, defense counsel should strive for best practices, which can include ironclad ESI collecting methodologies, meticulous protocols and painstaking documentation of evidentiary transitions to ensure an easily defensible and rock-solid evidentiary authentication and chain of custody.

If possible, once ESI collection is completed, defense counsel should store the images in a forensic lab facility with state-of-the-art equipment and high-tech security including restricted access, video camera surveillance, evidence safes and other important security measures.

After the data are forensically collected and secured, counsel should consider warehousing the data in a data hosting facility with tools that allow for the smooth integration of the many different ESI types that can crop up, which vary especially during large corporate investigations. ESI relevant to an SEC or DOJ 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 such as SharePoint or more customized business collaboration platforms.

**3. Image Is Everything.** Just about every government production will involve the forensic imaging and reviewing of emails and other relevant data from laptop computers, desktop computers, network servers, backup tapes, mobile devices, iPads, etc. If possible, practicable, not too costly and otherwise reasonable, counsel should take the extra care to acquire ''forensic images'' of all devices. Acquiring a forensic image or the production of an exact sector-by-sector copy of any computer, storage device, etc. verifies the completeness and accuracy of recovery while not altering the original media, thus preserving the status quo. Imaging can preserve the ability to reconstruct deleted information, ascertain any evidence of wiping/defragmentation, answer new questions and evaluate the authenticity of data.

Concerned about spoliation or obstruction charges that could surface later on in the investigation and about the overall volatility and integrity of electronic evidence, government investigators will likely not only demand forensic preservation of all devices but might even become suspicious if the imaging seems at all subpar.

Also, defense counsel in particular in complex SEC or DOJ investigations, should remain mindful of the challenges created by the various iterations of business

[9] Although relatively few criminal federal cases have examined the reasonableness of subpoenas of digital data and a full presentation of the issue is beyond the scope of this article, there are a few cases that shed some light on the issue and are worthy of mention, the most notable of which being *In re Grand Jury Subpoena Duces Tecum*, 846 F. Supp. 11 (S.D.N.Y. 1994). In this case, the court held that a subpoena for a central processing unit, hard drive, and all computer-accessible data was unconstitutionally overbroad since the hardware contained documents having nothing to do with the grand jury investigation, reasoning that ''the expanded investigation does not justify a subpoena which encompasses documents completely irrelevant to its scope, particularly because the government has acknowledged that relevant documents can be isolated through key-word searching.'' The court stated that the correct way to balance relevance and particularity was to consider relevance at the level of categories of materials. In particular, it stated that documents, rather than storage media, were the appropriate category of materials to which to address a subpoena. Targeting hard drives, the court reasoned, would be like targeting file cabinets rather than files, and would necessarily produce irrelevant documents. Similarly, in *In re Amato*, No. 05-MC-29PDMC, 2005 WL 1429743 (D. Me. June 17, 2005), the District Court of Maine emphasized the importance of particularity. The subpoena at issue requested, among other things, ''[a]ny computer equipment and storage device capable of being used to commit, further, or store documents or data described [in the subpoena].'' The court found that requesting all devices ''capable of being used'' for data storage was, by definition, overbroad under the Fourth Amendment, citing to a number of search warrant cases and concluding that a subpoena that ''requests the turnover of all computers (and related objects) . . . with no express safeguard against a subsequent rummaging through, and seizure of, irrelevant as well as relevant data . . . cannot withstand Fourth Amendment reasonableness scrutiny.'' *See also People v. Carratu*, 755 N.Y.S.2d 800 (N.Y. Sup. Ct. 2003) (Defendant moved to suppress computer evidence seized from his home and was subsequently searched by the police department's computer forensic examiners claiming that the search warrants and supporting affidavits limited the search to documentary evidence relating to his illegal cable box operation, and thus the forensic examiner violated the Defendant's Fourth Amendment rights upon inspection of non-textual files with folder names clearly relating to other illegal activity. Granting the suppression motion, in part, the court stated, ''In view of the Fourth Amendment's 'particularity requirement,' a warrant authorizing a search of the text files of a computer for documentary evidence pertaining to a specific crime will not authorize a search of image files containing evidence of other criminal activity.'').

[10] A hash value is a result of a repeatable calculation (hash algorithm) that can be performed on a string of text, electronic file or entire hard drive's contents. Hash values are used to identify and filter duplicate files (i.e., email, attachments, and loose files) from an ESI collection or verify that a forensic image or clone was captured successfully.

  PVLR ISSN 1538-3423

collaboration platforms or 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, counsel should bear in mind that 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 a database schema, front-end reports, or workflows that are causing flawed database outputs.

**4. Sometimes—Look a Gift Horse in the Mouth.** After hearing defense counsel carp about the costs of a particular production, the SEC's forensics lab might tout their own solution, offering to conduct their own ''independent'' forensic analysis (free of charge) of any ESD (or image thereof) produced. Do not take the bait. The SEC staff might also represent that: (1) the lab's facility is hermetically sealed; and (2) the SEC forensic lab staff will only transmit to the SEC investigatory staff the ESI approved as responsive by the witness who produced the ESI.

While the intentions and goals of the SEC staff may indeed be pure, and may even be a sincere desire to help move the investigation along and save costs for a witness, the dangers of acquiescing far outweigh the benefits. Once turned over, any information contained on the ESD is subject to the SEC's ''Routine Uses of Information'' (see above at footnote 8), which the SEC staff does not have the authority to waive. Thus, should a witness opt to turn over ESD to the SEC enforcement forensic lab, no matter how ''independent'' the SEC lab purports to be and no matter how bona fide their objectives, there still exists significant risk that both witnesses and counsel will lose control of that ESD.

**5. If Possible, Watch Out for Native File Issues.** When the government subpoenas or requests documents, the safest manner to produce the documents is in ''Tagged Image File Format'' (TIFF), which strips out the text and the ''metadata''[11] from the original electronic file, and then provide in a separate load file the metadata associated with each TIFF file. Akin to providing a snapshot of the document as opposed to any sort of electronic version, producing TIFF files allows for easy Bates stamping,[12] easy redaction and, most of all, can provide a more evidentiary, concrete document version, which does not lend itself to easy alteration.

Of course, TIFF productions are an older form of file format, and if the SEC or DOJ staff scoffs at such a debatably ''antiquated'' approach, one alternative format is to convert electronic files to searchable PDF files. Indeed, Adobe created both the TIFF and PDF formats and designed PDF as a more functional replacement for the TIFF. PDF files are searchable, easily viewable, and also easily Bates stamped, redacted, etc. PDF files also retain some of their metadata (though not automatic, and dependent on the conversion software and settings used during the conversion process).

The government may also seek so-called ''native'' files, which are the actual electronic documents, presentations, spreadsheets, etc. in their original format.[13] However, the Bates stamping of native files by definition alters the file (including the metadata), and native files are trickier to redact, typically far more cumbersome to search, and, most of all, can be altered by the recipient.

Along those lines, should the government opt to use a native document as an exhibit for testimony or as the basis for a referral to a criminal authority, consider a polite objection, noting that the government would be using an exhibit that they could have altered and that could present unnecessary and unwelcome authentication challenges in the long run. Moreover, defense counsel may end up objecting to those exhibits not only during a subsequent court proceeding, but also during testimonial proceedings and depositions. These kinds of objections present thorny legal issues and inevitably disrupt the flow, tone and ease of testimony and depositions—a burden the government may not want to experience.

Perhaps the government official on the receiving end of these arguments will cave and withdraw the native file demand but others might be sticklers. They may have some specific reason for the request, want to be stubborn for tactical reasons or just not understand the complicated intricacies of 21st century data.

**6. Consider a Data-Handling Air-Drop.** Increasingly, especially in the context of SEC and DOJ investigations, foreign companies do not want (or are not permitted because of privacy restrictions) to transport their ESI outside of their home country's jurisdiction. Before responding to a government subpoena that goes beyond U.S. borders, defense counsel should consider using a

[11] Metadata is a term for descriptive information about a file which can be embedded inside an electronic file, and can include the name, type of file, creation date, last accessed date, last modified date, etc. Software may automatically create metadata or a user may create it.

[12] ''Bates stamping,'' (also known as Bates numbering, Bates branding, Bates coding or Bates labeling) is used to place identifying numbers and/or date/time-marks on images and documents as the documents are, for example scanned or digitally processed for production to the government providing identification, protection, and auto-increment numbering of the documents, images, etc.

[13] The Federal Rules are subject to debate on this point. Rule 34(b)(ii) of the Federal Rules of Civil Procedure (as amended Dec. 1, 2006) states that ''if a request does not specify the form or forms for producing electronically stored information, a responding party must produce the information in a form or forms in which it is ordinarily maintained or in a form or forms that are reasonably usable.'' *See* Committee on the Judiciary, 111th Cong., *Amendments to the Federal Rules of Civil Procedure* (2009), *available at* http://www.uscourts.gov/uscourts/RulesAndPolicies/rules/EDiscovery_w_Notes.pdf. The phrase ''in which it is ordinarily maintained'' has been construed as meaning in its native file format but is also the subject of frequent debate at e-discovery conferences, especially since that interpretation seems to have the reverse effect of rendering discovery more onerous and costly (e.g., the burden of having to buy (and learn) the software for the native files alone can increase costs and discovery complexities substantially). *See, e.g.*, *Armor Screen Corp. v. Storm Catcher, Inc.*, 2008 WL 5262707 (S.D. Fla. Dec. 17, 2008) (Defendants requested native file production, but were then unable to read files with a .SAV extension. Defendants then demanded the plaintiffs produce hard-copy printouts of the SAV files. Magistrate Judge Ann E. Vitunac refused to compel the plaintiff to grant the defendant's request because SAV files, openable by a number of ''statistical computer packages,'' would in fact qualify as a ''reasonably accessible format.'')

mobile data processing solution that can rapidly deploy data hosting and processing outside of the United States. A well-designed mobile data processing facility not only can provide a secure processing environment for resident reviewers, but it also can deliver assurances of compliance with country-specific ESI privacy regulations, which often arise in today's multinational business environment.

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 transborder 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 Privacy Framework or any other specific data protection rules promulgated by any particular country. Whenever data crosses any border (even borders between U.S. states), important privacy issues will always arise.

## Conclusion.

Back in the day, the last thing a government investigator wanted was for a witness, in response to a subpoena or request for documents, to ''back up the truck'' and deliver reams of documents in hundreds of boxes. But those days are long gone. Technology has clearly transformed the playing field for government investigations and prosecutions, empowering the government in ground-breaking and pioneering ways to examine, segregate and peruse data.

However, sometimes the government can become too resourceful for its own good. Merely because technology allows federal agents and SEC staff to conduct their own external audit of a document production or subpoena response or subpoena the universe in one fell swoop, that does not mean there exists authority or license to do so.

For example, requiring witnesses to produce their desktop computers or authorize a forensic deep dive into the unallocated space of a hard drive is like requiring a witness to consent to a polygraph test during his or her testimony or interview. It might just be going too far.

Unless any government agency has the authority to take advantage of all of its technological tools, it may make sense to push back on occasion, and risk the ramifications of prosecutorial retribution or subpoena enforcement. After all, the risks of pushing back, while significant, can pale in comparison to the risks of submitting an ESD, which could unknowingly contain falsely incriminating, inculpatory, misleading, fraudulent or otherwise private, irrelevant or privileged information.

Under any circumstance, the caveats in this article provide some guidance for handling data-related quandaries and some reminders concerning hidden but critical data-related issues—but above all, the old-adage of ''better safe than sorry'' should always remain paramount.

  PVLR ISSN 1538-3423