Bloomberg BNA

Securities Regulation & Law Report™

ENFORCEMENT

When to Say When: Handling Emerging Technology-Related SEC Enforcement Tactics

BY JOHN REED STARK

Armed with a dedicated squad of digital forensic examiners, together with a state-of-the-art digital forensic laboratory, an eager Securities and Exchange Commission Enforcement Division staff has technologically blossomed, pushing the envelope during the investigative process and taking advantage of the latest electronic tools, especially with respect to investigative subpoenas and voluntary requests.

Moreover, under an invigorated and freshly anointed SEC leadership team, SEC enforcement staff must achieve quick results, must be innovative and creative, and like any other modern enterprise, must leverage technology at every opportunity. However, employing embryonic technological prowess is not without costs and risks, and while bolstering effectiveness and swiftness, the staff can also venture into arguably uncharted territory, raising prickly legal issues that merit close scrutiny.

For defense counsel, knowing when to push back against the SEC staff has never been an easy decision.[1] Indeed, taking the wrong turn when responding to an SEC subpoena or request (such as refusing to respond[2])

John Reed Stark is Managing Director at the District of Columbia office of Stroz Friedberg, a global investigations, intelligence, and risk services company that provides expertise in digital forensics, cybercrime and incident response, security science, forensic accounting, compliance, due diligence, data discovery and analytics. Formerly, Mr. 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 also 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 and as an expert witness on behalf of the SEC.

[1] *See, e.g.*, *In re Two Admin. Subpoenas*, Docket No. 05-MC-29-P-DMC (Jan. 25, 2005 D. Me.)

("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).

[2] SEC enforcement subpoenas are administrative subpoenas that are not self-enforcing – i.e. there is no formal avenue of objection other than to refuse to comply, leaving the decision up to the staff as to whether a subpoena enforcement action is warranted. N.B. Section 21(c) of the 1934 Securities 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.

 ISSN 0037-0665

can strike a perceivably uncooperative tone,[3] and can result in a costly and injurious SEC subpoena enforcement action; can prompt the SEC enforcement staff to seek a broad and sweeping asset freeze; or can even rile the staff inadvertently and escalate the staff's interest in a witness or create other unintended consequences that increase unwanted, unnecessary and costly investigative scrutiny.

This article discusses some of the SEC enforcement staff's latest and most noteworthy technology-related investigatory practices together with some thoughts and suggestions for defense counsel on how to handle them. The sections below will not only help defense counsel decide when to ''say when'' to a technologically innovative but perhaps overly aggressive SEC enforcement staff, but will also provide guidance for how to fortify a digital defense to counter an unreasonable, unnecessary or arguably unlawful SEC investigatory assault.

'ESD' and Subpoenas Forthwith

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

Along the same lines, the SEC staff may, at the outset of a testimonial proceeding, serve a *forthwith* subpoena upon an individual demanding that individual turn his or her device over to the staff immediately, including a smartphone in a pocket or a laptop in a briefcase.

The process of issuing a *forthwith* subpoena, an investigative tool used ''sparingly'' by SEC enforcement staff, is described in detail in the SEC Enforcement Manual as follows (which even notes the delicate, and arguable lack of authority, for its use):

> 3.2.6.3 Forthwith Subpoenas in Investigations
>
> A forthwith subpoena may be issued where there is a reasonable good faith basis for believing that there is a risk of destruction or alteration of the documents. A forthwith subpoena demands production ''forthwith.'' For example, a forthwith subpoena may be issued if there is a danger that documents will be misplaced or destroyed unless produced immediately.
>
> Though a forthwith subpoena may be appropriate in certain circumstances, staff should be aware that courts have raised concerns regarding its use. For example, some courts have not condoned the use of forthwith subpoenas (*Consumer Credit Ins. Agency, Inc. v. United States*, 599 F.2d 770, 774 (6th Cir. 1979)), while other courts that have upheld forthwith subpoenas have cautioned against indiscriminate use (*Wong Sun v. United States*, 371 U.S. 471, 83 S. Ct. 407 (1963)).
>
> Staff should use forthwith subpoenas sparingly, when there is a reasonable good faith belief that a subpoena should require forthwith production. A reasonable good faith basis for issuing a forthwith subpoena may include seeking documents from an individual or custodian (1) that is uncooperative or obstructive, (2) that is a flight risk, and (3) who may destroy, alter or otherwise falsify records.
>
> Further Information:
>
> If the staff is concerned that there is a risk of the destruction or alteration of documents that the staff intends to subpoena, the staff should consult with the Trial Unit immediately to ascertain whether issuing a forthwith subpoena would be appropriate under the circumstances.[4]

Whether via subpoena *forthwith* or otherwise, seeking ESD is 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 enforcement staff arguably lacks the authority for this sort of request and should the staff pursue a subpoena enforcement action for a device in federal court, the staff will most likely lose. Section 21 of the Securities and Exchange Act of 1934 sets the authority and the parameters of SEC staff subpoenas, stating:

> 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. (Emphasis added)[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 or circuitry.

In addition to the questionable legality of the practice of seeking devices, the risks of turning over a device to the staff without the proper review of every byte of data residing on that device are considerable.

First, the active data on these devices could include:

1) irrelevant private and personal data of the user, as well as the user's friends, family, colleagues, clients, customers, etc.;

---

[3] On January 13, 2010, the SEC announced a series of initiatives designed to encourage individuals and entities to provide cooperation in enforcement investigations. Although the SEC has encouraged cooperation in the past, prior to this new initiative, it did not have formal mechanisms for ensuring that cooperation was recognized and for permitting individuals and entities to avoid enforcement actions or receive reduced sanctions if they provided cooperation of a significant nature. The initiative, which is documented in the SEC's revised Enforcement Manual, provides the SEC staff with new tools such as written cooperation agreements as well as deferred and non-prosecution agreements that have traditionally been used by the Department of Justice in criminal investigations. This policy, first formally articulated in the Commission's Seaboard Report in 2001, is always a lingering worry for SEC defense counsel when contemplating refusing an SEC voluntary request or subpoena. *See* Sec. & Exch. Comm'n, Release No. 2010-6, SEC Announces Initiative to Encourage Individuals and Companies to Cooperate and Assist in Investigations (Jan. 13, 2009), *available at* http://sec.gov/news/press/2010/2010-6.htm.

[4] Sec. & Exch. Comm'n Div. of Enforcement, Enforcement Manual 62 (2012), *available at* http://www.sec.gov/divisions/enforce/enforcementmanual.pdf.

[5] Section 21, Securities and Exchange Act of 1934.

  SRLR ISSN 0037-0665

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) privileged communications with counsel or attorney work product; or

5) a broad range of other types of information which would otherwise not be produced pursuant to an SEC voluntary request or subpoena.

Second, and more importantly, the unknown or inactive data on the devices could present even more serious dangers. This is because the SEC enforcement staff may undertake a digital forensic deep-dive into the devices' 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 a smartphone or any other 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 intentionally deleted (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, even a visiting contractor could be using a homeowner's computer for unlawful purposes and could have 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 turns over that ESD to the SEC staff. 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 budding practice.

If the SEC enforcement staff refuses to relent, consider proposing that an independent and reputable third party digital forensics firm conduct a review of the media vis-à-vis an appropriate methodology and protocol, run keyword searches, and even explore unallocated space – and then, after an appropriate privilege, relevancy or other review by defense counsel, produce the final, properly filtered, results to the SEC enforcement staff.

SEC Certification Requests

For many years, the SEC enforcement staff has at certain times requested from a witness a so-called ''certification'' relating to that witness's production of data. The certifications take on a range of shapes and sizes but typically require the witness or a high-ranking company official to attest to the overall completeness of a subpoena response.

For instance, the certification may require the signatory to attest that he or she: 1) is not aware of any specific document or information that is reasonably likely to be of material interest to the SEC staff but has not been produced; 2) has not requested any accommodation in order to prevent or delay the staff's receipt of any responsive document or information; and/or 3) will produce immediately to the staff any responsive document or other information that has not been previously produced but he or she discovers at some alternate point in time.

As to why this request occurs, the reasons will vary – sometimes because it is required for settlement; sometimes because of the circumstances of the investigation; sometimes seemingly at the whim of the SEC staff involved; sometimes perhaps even at the implicit request of the (known or unknown lingering in the background) assistant U.S. attorney running a parallel criminal investigation; or sometimes for reasons unknown to defense counsel or the witness (for example, because an SEC Commissioner mentioned the need for a certification on a similar matter in the past).

Under any circumstance, SEC enforcement staff certification requests (or demands) are occurring more and more these days, yet the terabytes of data belonging to today's corporations can reside in myriad different systems or assets including desktop and laptop computers, cell phones, tablets, internal and external

---

[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. Files saved to the hard drive of a computer are typically described as residing in ''allocated space,'' i.e., space on the hard drive in use 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 reserves 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. Note though that not every device has readable unallocated space – for instance, devices using Windows 7 with an SSD hard drive auto-wipe unused spaces to prepare them to receive more data (which contributes to their better performance) and can result in a lesser likelihood of finding anything probative or relevant in unallocated space under such conditions. However, having said that, 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*, Del. Ch., No. 3994-VCS, (Dec. 9, 2009), where the court found 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 Forms 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, SROs, 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* www.sec.gov/about/forms/sec1662.pdf and http://www.sec.gov/about/forms/sec1661.pdf.

networks and databases, intranets, Sharepoint platforms, antiquated and legacy servers and systems, back-up tapes, *the cloud*[9] and the list goes on. Thus, given that most witnesses ''don't know what they don't know'' about the location of all of their responsive data, being required to attest to the completeness of a data production can be unsettling to say the least.

Given the ease with which SEC staff can make a criminal referral for obstruction of justice, perjury, misleading statements, etc., no witness wants to find him or herself in the unfortunate position of having to explain to a skeptical SEC enforcement staff the circumstances of some sort of document mishap, such as when a responsive document is suddenly discovered weeks or even months after a production deadline. Even worse can be when another witness produces a document that was clearly also in a different witness's possession (such as an e-mail) but was somehow overlooked and not produced.[10] However, the reality is that such an unfortunate kind of data discovery happens all the time, and often creates a challenging, disruptive or even perilous situation, not only for the witness but also for his or her defense counsel.

Indeed, any sort of data-related predicament during an SEC production (such as not producing a potentially inculpatory document, even if done inadvertently) can lead to grim consequences for counsel. If the SEC enforcement staff suspects a defense attorney of hindering the production of responsive data from a witness, that defense attorney not only places his or her reputation at risk 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.

Persuading the SEC enforcement staff to retreat from a certification request or demand, as a condition for settlement or otherwise, can be a non-starter, especially if the Commission, the general counsel's office, or even enforcement's own chief counsel's office has required such a certification. Defense counsel may achieve some success by qualifying the language of the certification to a more scienter-based standard (i.e. requiring that the affiant have actual knowledge of data-related shenanigans concerning the discovered information) but that negotiation can be difficult if the SEC staff digs in its heels.

One solution some companies undertake is for the company or the witness to engage a third party neutral to draft an internal memorandum documenting the individual's or company's subpoena response methodology, protocols, etc. and opining as to its accuracy and efficacy. That way, should the SEC staff discover a document or other byte of information that an individual or company should have produced but was for some reason not produced, the individual or company will have a strong and solid good faith defense that the subpoena response process was taken seriously and handled carefully.

SEC Enforcement Preservation Ad Infinitum

The SEC enforcement staff has never been consistent with respect to making preservation requests accompanying its subpoenas, voluntary document requests and other investigatory inquiries. For instance, some SEC enforcement staff members:

—Never make any specific preservation requests and merely send a subpoena or voluntary document request on its own, leaving any preservation requirement implicit;

—Only mention preservation requirements during a testimonial proceeding and question the witness about preservation efforts;

—Only state (or sometimes merely reference) preservation obligations briefly in the introductory letter accompanying a voluntary request for documents or subpoena;

—Provide a massive, multi-page laundry list of preservation requirements, which includes preserving:

- All e-mail headers, footers and logs;
- All relevant databases;
- All relevant social media;
- All deleted files and file fragments;
- All data stored in online storage on mainframes, tablets, PCs, the cloud or smartphones;
- All offline storage, back-ups, archives, discontinued hard drives, tapes or thumbdrives;
- All programs and utilities;
- All failed storage devices or replaced storage devices;
- All personal devices of employees; and
- All hidden directories; or

—Provide an additional list of preservation tasks including requiring the witness or company to take affirmative steps to:

- Insure no compression, data defragmentation or other optimization tools are used on existing data;
- Insure no modifications are made to data processing without activity log; and

[9] ''Cloud computing'' has many definitions, depending on whom you ask (and at what time of day). For certain, traditionally a company or an individual's data has resided in a local, physical space such as a 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 remains physically stored somewhere (probably on a server ''farm'' where space/rent is 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 above, that when the SEC staff 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.'')

[10] Given that the SEC enforcement staff typically send the same subpoena to multiple employees, board members, and other witnesses, this is a particularly common and troublesome problem. That is why it is critical to engage an independent and meticulous methodology and protocol when collecting data for an SEC response. Thus, in the event that a responsive document is somehow overlooked, evidence can be presented to the SEC enforcement staff that the search for responsive documents was done responsibly, carefully and in good faith.

   ISSN 0037-0665

■ Record all decryption procedures.

Based on my experience, there is clearly a trend toward more cumbersome and technologically explicit SEC enforcement staff preservation requests, which will require meticulous attention by defense counsel at the outset and throughout the course of an SEC investigation.

The first step in handling a preservation request is to carefully review preservation requirements, not only with the relevant custodians of responsive data but also with the company's information technology (IT) group. If the preservation request is simply too costly and burdensome (and perhaps even too disruptive) for a company, then the next course of action is to confront the SEC staff and perhaps run your concerns up the chain to senior SEC officials – so long as you include a reasonable, technologically appropriate and well-documented alternative for preservation that achieves what the staff wants but does not bankrupt a client or cripple its operations.

The second step is for defense counsel to engage the SEC enforcement staff to confer and collaborate as to a solution that makes the most sense. Along those lines, having a proposed alternative is critical. The riskiest course of action with respect to preservation negotiations with SEC enforcement staff is for defense counsel to ''shoot from the hip,'' because the SEC enforcement staff will undoubtedly engage their own in-house experts to cross-examine defense counsel concerning the nature and details of any proposed preservation plan. Should defense counsel propose to the staff an unreasonable accommodation that does not pass technological muster, defense counsel will not only be putting their client's candor at risk but will also be risking damage to their own reputations.

Finally, given that the SEC enforcement staff will likely enlist their own cadre of digital forensic and technology experts (who probably drafted the preservation request in the first place), it may also make sense to engage an independent neutral technology firm to review preservation efforts, opine on their adequacy, participate in the preservation negotiations with the SEC enforcement staff and most importantly to handle the experts the SEC staff will have on their side.

The Data of the Board and Other BYOD Issues

Historically, the SEC enforcement staff has rarely pursued public company directors, typically only doing so when the directors have knowingly permitted or facilitated violations of the securities laws.[11] However, a heightened SEC focus on issues like SEC Rule 10b5-1 stock trading plans,[12] vigorous insider trading enforcement[13] and other political and media pressures have resulted in increasingly aggressive SEC enforcement investigations targeting members of the board of directors.[14]

Although typically insured to cover the costs of SEC investigations, and usually trained on how to conduct themselves when the SEC enforcement staff launches an investigation into their actions, corporate boardrooms are too often not adequately prepared for the technological intrusion that an SEC investigation can thrust upon them.

For instance, the SEC enforcement staff will consider within its investigatory purview any device or e-mail address used by a board member in conducting his or her board work. As a result, board members face very complex and challenging situations when responding to an SEC subpoena for all e-mails and documents relating to their board duties and responsibilities. For instance, some directors will use for their board work and or all of the following: 1) the director's e-mail address and devices (laptop computer, desktop computer, etc.) at his or her ''day job'' (i.e. his or her daily place of employment); 2) his or her personal e-mail address; or 3) his or her personal devices such as laptop computers, desktop computers, tablets, smartphones, etc.

Obviously, the board member who receives an SEC subpoena that covers the above devices and e-mail addresses will not only become immediately concerned about turning over personal e-mail addresses and de-

[11] *See, e.g., SEC v. Krantz*, filed Feb. 28, 2011 (www.sec.gov/litigation/complaints/2011/comp21867-directors.pdf) and SEC Administrative Proceeding File No. 3-14279, filed March 1, 2011 (www.sec.gov/litigation/admin/2011/33-9192.pdf). While these actions reflect the SEC's interest in bringing actions against these types of directors, they are consistent with the Commission's historical practice of pursuing cases against independent directors only when it believes that they personally have engaged in violative conduct or have repeatedly ignored significant red flags.

[12] In 2000, the SEC adopted Rule 10b5-1 to clarify ''what, if any, causal connection must be shown between the trader's possession of inside information and his or her trading.'' It provides that a trade is made ''on the basis of'' material nonpublic information ''if the person making the purchase or sale was aware of the material nonpublic information when the person made the purchase or sale.'' Rule 10b5-1 plans are especially useful for people presumed to have inside information, such as officers and directors. Specifically, a Rule 10b5-1 plan is a written plan for trading securities that is designed in accordance with Rule 10b5-1(c). Any person executing preplanned transactions pursuant to a Rule 10b5-1 plan that was established in good faith at a time when that person was unaware of material non-public information has an affirmative defense against accusations of insider trading, even if actual trades made pursuant to the plan are executed at a time when the individual may be aware of material, nonpublic information that would otherwise subject that person to liability under Section 10(b) of the Exchange Act or Rule 10b5-1. *See* SEC. & EXCH. COMM'N, RELEASE NOS. 33-7881; 34-43,154, SELECTIVE DISCLOSURE & INSIDER TRADING (Aug. 15, 2000), *available at* http://www.sec.gov/rules/final/33-7881.htm.

[13] SEC. & EXCH. COMM'N, SEC ENFORCEMENT ACTIONS: INSIDER TRADING CASES (2013), *available at* http://www.sec.gov/spotlight/insidertrading/cases.shtml (''Insider trading continues to be a high priority area for the SEC's enforcement program. The SEC brought 58 insider trading actions in FY 2012 against 131 individuals and entities. Over the last three years, the SEC has filed more insider trading actions (168 total) than in any three-year period in the agency's history. These insider trading actions were filed against nearly 400 individuals and entities with illicit profits or losses avoided totaling approximately $600 million. Many of these actions involved financial professionals, hedge fund managers, corporate insiders, and attorneys who unlawfully traded on material non-public information, undermining the level playing field that is fundamental to the integrity and fair functioning of the capital markets'').

[14] Susan Pulliam, Jean Eaglesham & Rob Barry, *Insider-Trading Probe Widens*, WALL ST. J., Dec. 11, 2012, at A1; Susan Pulliam & Rob Barry, *Insider Trades Eyed*, WALL ST. J., Nov. 28, 2012, at C1; Susan Pulliam & Rob Barry, *Executives' Good Luck in Trading Own Stock*, WALL ST. J., Nov. 28, 2012, at A1.

vices to defense counsel but may also, with respect to his or her ''day job'' e-mail addresses and devices, be explicitly prohibited from doing so without the express permission of his or her employer.

Of course, the board member could have pre-empted these issues had the company where he or she sits on the board provided the board member with, and restricted his or her use to, a board e-mail address and a board device (such as a laptop or tablet). However, in these days of instantaneous communication expectations, multiple devices and workstations and constant technological innovations enabling work from anywhere at any time, this is often unrealistic, onerous and tedious.

So what can the board member do? It is always worth discussing the situation with SEC enforcement staff and making an attempt to negotiate a narrowing of the scope of the staff's requests and subpoenas. However, if negotiation does not work, taking the issue further can cause worse problems. Indeed, the option of combating an aggressive SEC enforcement staff seeking information from a board member is particularly sensitive, and trying to reduce the scope of a broad SEC subpoena can easily backfire, raising the ire and suspicion of SEC staff members and prompting SEC enforcement staff to send an even broader subpoena targeting the board member personally.

The best option is to assign the board member's data collection responsibilities to a trusted third party who can gather the responsive information, carefully filter out data relating to the board member's other jobs as well as personal data and other non-responsive information, and, most importantly, can represent to the SEC enforcement staff and to the general counsel of the board member's day job that the data collection was carried out carefully, thoughtfully and independently.

N.B. that this problem can become particularly acute if the board member's day job is outside of the United States, where privacy protections can be far more cumbersome and mishandling can result in serious sanctions and border-crossing issues. In these situations, defense counsel should work with privacy experts and forensic teams that have extensive expertise preparing protocols consistent with the respective countries' electronically stored information privacy standards.

Given that privacy regulation is an extraordinarily fluid area, defense counsel and his or her forensics team must carefully monitor recent privacy developments, and stay current with the latest changes in international policies and requirements. For instance, the European Union data protection directive compels member nations to enact national data protection laws harmonized with the principles of the directive (or more stringent). The directive 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 Community (APEC) privacy framework or any other specific rules promulgated by any particular country. Whenever data crosses any border (even sometimes borders between U.S. states), important privacy issues will always arise.

BYOD. In light of the discussion above, it is worth noting that employees of today's corporations can face similarly complex, challenging and increasingly costly data collection situations because of the trend towards BYOD, or ''bring your own devices'' into the workplace.

For instance, even though an individual's work-related data may reside right alongside their private and personal information on his or her personal devices, the SEC enforcement staff will not necessarily draw any sort of distinction along those lines. Consider a company involved in an investigation and the SEC issues subpoenas for data possibly residing on the personal smartphone or laptop of a company employee; depending on the employee's use of his or her devices, or perhaps an agreement with the company (if any), the personal devices may be considered in the possession, custody or control of the company. Therefore, the company may end up reviewing all data on those devices, including personal and private information. Even worse, the company may discover incriminating evidence on the employee's device pertaining to a wholly unrelated situation and opt to turn that evidence over to the government.

While this problem is less of a concern outside of the United States because of stronger privacy protections (see discussion above concerning the EU ESI privacy standards), within the United States, when company employees co-mingle work and personal data on personal devices, they may have few options with respect to curtailing the SEC enforcement staff's efforts. Even if the employee quits and takes his personal device home, such an action may prompt the staff to serve a personal subpoena upon the now former employee, which can open up an entirely new and even more problematic (and costly) situation.

Conclusion.

Technology has clearly transformed the playing field for SEC enforcement staff, empowering the SEC enforcement division in groundbreaking and pioneering ways to identify, pinpoint, examine, segregate and peruse data. To their credit, when it comes to data and the ever elusive *smoking gun*, the SEC enforcement staff has become more creative, more resolved, more resourceful and more effective than ever.

Moreover, standing behind their administrative subpoenas and voluntary requests for data is not the SEC staff of yesteryear, but is rather a determined and scientifically astute corps of sophisticated adversaries, whose relent can be exasperating and whose hi-tech prowess should never be underestimated.

But, as legendary former SEC enforcement director and former federal Judge Stanley Sporkin told me and all of my rookie SEC enforcement colleagues almost 25 years ago during our orientation (and he has been quoted by so many), ''With great power comes great responsibility.''

So merely because technology facilitates the SEC enforcement staff's arguably warrantless searches and seizures; questionable costly and overly burdensome preservation requests; unqualified subpoena compliance certifications and attestations; and seemingly unrestrained forensic deep-dives into the personal lives of

   ISSN 0037-0665

U.S. citizenry — that does not mean there exists authority or even license to do so. However, knowing when to *push back* against SEC enforcement staff in the context of a subpoena response, certification request or other data related directive (and risk the consequences) is never easy for defense counsel, especially when at the same time, defense counsel is attempting to demonstrate a sincere and genuine intention of cooperation.

Clearly, to navigate the proper course, defense counsel must not only understand the ramifications and risks accompanying acquiescence to enforcement staff but must also have in hand some powerful ammunition to enable the launching of a subtle, quiet and respectful counter-offensive. It is indeed a whole new ballgame in the SEC enforcement division – where managing electronic data issues is paramount – and defense counsel must employ identical or superior technological weaponry, especially if he or she wants to avoid the ten-run rule.