BNA

Privacy & Security Law Report®



# The 21st Century Genesis of the Bad Leaver

By John Reed Stark

*John Reed Stark is Managing Director and Deputy General Counsel 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. The author would like to thank Julia Cosans and Thomas Harris-Warrick for help with this article.*

## Introduction

Terry Childs, after having worked for the city of San Francisco as a network administrator for about five years, was growing restless. He had been disciplined for poor job performance, was upset with the way his department was being managed, and maybe $126,000 a year just didn't go as far as it used to.

So, he decided he was going to do something about it. According to an article in the *SFGate.com*, he ''engineered a tracing system to monitor what other administrators were saying and doing related to his personnel case''[1] and set Cisco network devices that could erase vital configuration data with a simple command. And when his supervisors decided it was time to let him go, he refused to relinquish his passwords for the Fiber-WAN that provided e-mail, internet and other services to the city's network.

Although the network was still operational, the city had no ability to change configurations, remove Terry's access to confidential information, or address problems as they arose. For almost two weeks, he held the network hostage until finally, after having been arrested, he turned the passwords over to Mayor Gavin Newsom. This case serves as the quintessential example of the ''bad leaver'' and illustrates the massive damage that one employee can cause.

Perhaps taking his cue from Childs, Jason Cornish, formerly an IT staffer at the U.S. subsidiary of Japanese drug-maker Shionogi, recently pled guilty to perpetrating a similar scheme.

[1] Jaxon Van Derbeken, *S.F. Officials Locked Out of Computer Network*, SFGate.com, July 15, 2008, http://articles.sfgate.com/2008-07-15/bay-area/17171009_1_computer-network-computer-system-access.

 ISSN 1538-3423

Logging in from a McDonald's restaurant (after resigning from Shiongi because of a dispute with management), Cornish remotely turned on a vSphere VMware management console, which he had secretly installed on the company's network. Once logged on, Cornish proceeded to delete 88 company servers from the VMware host systems, one by one. The attack effectively froze Shionogi's operations for a number of days, leaving company employees unable to ship product, to cut checks, or even to communicate via e-mail, the Department of Justice said in court filings.

Childs and Cornish, so-called ''bad leavers,'' or disgruntled former employees who *leave a company badly*, are examples of a 21st Century phenomenon and an evolving and dangerous threat to today's public and private corporations.[2]

Motivated by greed, bad leavers can harm the lifeblood of a company by stealing intellectual property like source code; by hijacking specialized collateral like marketing materials; by pilfering precious inventory like intellectual property, client lists or private data containing personally identifiable information (PII);[3] or even by accessing material, nonpublic information to perpetrate insider trading schemes.

Motivated by fear that misdeeds may be discovered, bad leavers can destroy or alter critical evidence or even plant on a company's servers forged documents such as a phony employment agreement or a fictitious whistleblower e-mail.

Even out of mere spite, bad leavers can cause irreparable damage to the internal workings of their former employers by sabotaging internal technology systems (from e-mail servers to video recorders), planting malicious viruses, or breaching firewalls and creating secret online backdoors to enable future sabotage. There is no limit to the kind of havoc a bad leaver can do.

Historically, employee terminations have caused companies relatively little concern. In the worst case scenarios, a bad leaver was escorted out with an armed guard who searched a few pockets and boxes for company property. Indeed, without access to the technical tools of the 21st century, employees traditionally possessed limited opportunity for theft or mischief.

Nowadays however, times have changed. Small external terabyte storage devices the size of a deck of playing cards, e-mail that can instantaneously traverse the globe, seemingly infinite storage space available 24-7 online, and even simple laser-printing capabilities have empowered bad leavers with extraordinarily effective weaponry and wherewithal.

Even when a bad leaver has signed an onerous (and legally enforceable) covenant not to compete, nonsolicit agreement or other post-employment related contract, bad leaver cases can still demand significant time, energy and resources and have become a drag on company management in today's world.

This article discusses: 1) how to identify potential bad leavers in advance; 2) what helpful steps to take after identifying a bad leaver, especially in the realm of digital forensics; and 3) privacy issues that often crop up during a company's investigation of a bad leaver.

## How to Recognize a Bad Leaver

Bad leaver cases fall under two main categories: prior and ongoing. Prior, or standard cases, describe situations in which the bad act has already taken place. These categories typically demand immediate attention concerning a bad leaver's actions and course of events.

Ongoing cases can involve situations in which the bad leaver has left, but continues to return virtually to his or her employer by breaching the firewall, or can involve a bad leaver's cohorts, or current employees who remain loyal to the bad leaver after his or her dismissal.

Given the scope and breadth of the potential damages associated with bad leavers, early recognition and detection can be vital. Sometimes the signs are obvious. For example, a disgruntled employee may be spotted sneaking around headquarters in the dead of night. Other cases, such as the quietly disgruntled employee, can be more challenging.

Some of the more obvious red flags signaling a bad leaver include changes in an employee's behavior or work schedule.

Sudden changes in the workplace (such as mergers or takeovers) can trigger the kind of discontent which can transform otherwise happy and productive employees into potential bad leavers. When employees feel devalued, left out of a financial windfall or otherwise disenfranchised, good workers can turn bad.

In addition to the more simplistic indicators discussed above, the right team of professionals can identify a far more comprehensive laundry list of risk indicators of bad leavers, even breaking them down by actual insider act. For example, a study has shown that three weeks prior to or after their resignations, intellectual property thieves (typically scientists, engineers or programmers) often start copying intellectual property in large volumes[4]—a strong risk indicator—leading some companies to routinely review copying and computer activity in this time frame after certain resignations. The risk indicators or warning signs differ for espionage, sabotage, fraud, etc. but can all prove useful for helping develop company protocols for addressing potential bad leavers.

Companies should consider training supervisors to spot these behavior changes as warning signs and heighten their awareness during times of corporate change or uncertainty.

However, training managers to become detectives of subjective deviations in behavior and monitoring for bad leaver warning signs is not often a practical or realistic option. Companies should therefore also consider implementing certain straightforward corporate-wide measures to help make identifying a potential bad leaver a less demanding job—such as conducting back-

[2] The term ''bad leaver'' likely comes from Great Britain, where my British colleagues have handled so many of these insider threat-related engagements, that they coined a term for them.

[3] The United States Department of Labor defines PII as any information that (i) directly identifies an individual (i.e., name, address, Social Security number, telephone number, e-mail address or any other identifying code or number) or (ii) combined data elements (i.e., gender, race, birth date, geographic indicator, etc.) intending to identify specific individuals indirectly. PII may also include information used for the physical or online contacting of a specific individual. This information may be stored on paper, electronically or in other media.

[4] Carnegie Mellon University Software Engineering Institute, *An Analysis of Technical Observations in Insider Theft of Intellectual Property Cases* (Feb. 2011), http://www.cert.org/archive/pdf/11tn006.pdf.

  PVLR ISSN 1538-3423

ground investigations, warehousing employee e-mail and implementing well-crafted exit procedures.

### *Background Checks, Employee E-mail Warehousing, Employee Exit Procedures and PII Procedures*

First and foremost, conducting a professional background investigation before hiring an employee can prevent a bad leaver from ever walking through the front door in the first place. Although background investigations may seem expensive at the forefront, they can save hundreds of thousands of dollars in weeding out potential threats and remediating bad leaver damage. Furthermore, a thoughtful and expansive module, or a set of questions directed at a potential employee's references, can not only complement a background check but can also fill in some of the blanks from an employment application.

Secondly, companies should consider storing their data, especially e-mail communications, in a manner that is easily accessible, reviewable and certifiable (as to authenticity, temporal proximity, etc.). Careful warehousing of electronic communications allows not only for fast and easy preservation of relevant data but can also prove useful for later tasks associated with forensic reconstruction.

Companies may also want to consider monitoring certain communications of employees, including e-mails, instant messages and perhaps even social networking sites. Companies typically store certain communications of employees such as e-mails and perhaps instant messages, some by choice (such as a sales company) and others by regulation (such as registered Securities and Exchange Commission entities like broker-dealers and investment advisers.)[5] Even social networking site interaction for certain SEC-regulated entities must be monitored and appropriately stored.[6]

However, before developing or modifying an electronic communications system to enable monitoring and/or storage, companies should consult with both legal and digital forensic experts. Legal experts should contribute because, even when statutorily mandatory, such monitoring and storing can raise important privacy and legal concerns. Digital forensics experts take part in the process because the resulting system should allow for the authentic, efficient, inexpensive and organized presentation of those communications.

Third, well-crafted exit procedures and protocols can mitigate any possible damage caused by a bad leaver. These steps can include terminating an employee's access to the premises, systems and processes; forensically identifying and preserving digital evidence relating to the employee (perhaps for all key, senior employees); safeguarding systems; securing and accounting for all company assets; and notifying the employee of the ramifications of any post-employment shenanigans.

Finally, given that data privacy protections vary by state, the cost and burden of addressing and remediating an unauthorized release of PII can be staggering. In order to avoid this kind of data privacy calamity, a company should maintain appropriate internal privacy safeguards and protocols to protect the PII of its clients, customers, employees, etc. By making it difficult for a bad leaver to make off with PII, a company can at least have some defense to the litigation, regulatory scrutiny or other disruption of operations resulting from the PII's unauthorized release.

### *Whistleblower Programs*

For better or worse, we all now work in the era of the whistleblower. Employee empowerment through whistleblowers has spread throughout all fields of endeavor. Not a day seems to pass without a headline about an angry employee portrayed as a modern day hero for uncovering some allegedly terrible practice committed by his or her employer.

Moreover, the reward for becoming a whistleblower now comprises far more than mere back-pay and reinstatement. Indeed, the term whistleblower has taken on an entirely new meaning as ''whistleblower status'' no longer just guarantees job protection; it can also result in rich financial reward.

Take for example, the recently enacted whistleblower provisions contained in the Dodd-Frank Wall Street Reform and Consumer Protection Act. These new provisions reward informants who provide certain types of information leading to successful securities actions, including SEC 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 violations, the new provisions will provide a particularly powerful incentive for whistleblowers with information on potential SEC violations, a category covering a diverse range of corporate actions.

Indeed, the 2008 Siemens joint SEC/DOJ Foreign Corrupt Practices Act (FCPA) prosecution alone, which resulted in a $1.6 billion dollar penalty against Siemens, would have yielded a whistleblower an astonishing award of as much as $496 million. No company is immune from a now legion of spectacularly incentivized

---

[5] SEC registered entities mandate such rules allowing the warehousing and archiving of all communications and subjecting them to review. For example, all records of a private fund maintained by an investment adviser are subject to periodic and special or so-called ''for cause'' examination by the SEC, including special examinations as the SEC may prescribe as necessary and appropriate in the public interest and for the protection of investors or for the assessment of systemic risk. Furthermore, the SEC is empowered to create broad record-keeping and reporting requirements for registered investment advisers to ''private funds.'' Advisors must make available to the SEC or its representatives any copies or extracts from such records as may be prepared without undo effort, expense or delay as the SEC or its representative may reasonably request. Additionally, SEC rules require each investment adviser to a private fund to file reports containing such information as the SEC deems necessary and appropriate in the public interest and for the protection of investors or for the assessment of systemic risk.

[6] *See, e.g.*, Financial Industry Regulatory Authority, Notice 10-06 , *Social Media Web Sites: Guidance on Blogs and Social Media Web Sites* (Jan. 2010), http://www.finra.org/web/groups/industry/@ip/@reg/@notice/documents/notices/p120779.pdf; Financial Industry Regulatory Authority, Notice 11-39, *Social Media Websites and the Use of Personal Devices for Business Communications: Guidance on Social Networking Websites and Business Communications* (Aug. 2011), http://www.finra.org/Industry/Regulation/Notices/2011/P124186 (responding to questions relating to Regulatory Notice 10-06 by providing further clarification concerning application of the rules to new technologies but not intended to alter the principles or the guidance provided in Regulatory Notice 10-06).

employees who may with the click of a mouse forward even the most baseless allegations to the SEC.[7]

How to counter or contain the ''whistleblower fever'' currently spreading across corporate America? One option is for corporations to assemble meaningful and effective whistleblower programs and policies, which can prevent a small inquiry from turning into an arguably retaliatory investigation.

Most importantly, companies should consider, when appropriate, investigating whistleblower complaints first by independently identifying, preserving and analyzing the data associated with the complaint. The key to the investigation will often reside within the data–which management can too often consider as an afterthought.

Some companies might find it worthwhile to implement an internal ombudsman program, handled by an independent investigative firm, to monitor, analyze and report employee complaints.[8] Such programs can provide employees, managers and shareholders alike with some degree of comfort that voices from the front lines are heard–and can slow or prevent the creation of a bad leaver.

Above all else, while it may make sense to characterize some whistleblower reports as heroic or even lifesaving, sometimes a whistleblower allegation is misguided or even false. Thus, the need for a company to initiate a careful and deliberate internal investigation, which capitalizes on any electronic evidence, is always paramount.

### *A Behavioral/Technological Approach*

Today, more sophisticated approaches to identifying bad leavers at earlier stages have gained considerable footing and popularity, as companies begin to understand their potentially devastating impact. One of these innovative new methodologies involves analyzing data from not only a technological, but also a behavioral, perspective.

Specifically, a behavioral sciences approach to internal investigations can prove valuable in detecting and tracing insider threats. The use of digital communications content, or behavioral recognition technology, provides a company with the ability to access a subject's emotional and psychological state. In turn, this aids in the identification of potential insider risk, which often involves bad leavers.

These programs provide a psycholinguistic analysis of a subject's emotional state, personality and risk, while tracking changes over time.[9] Behavioral recognition programs initially focused on locating and assessing employee disgruntlement that could manifest itself in espionage, sabotage, intellectual property theft, fraud and workplace violence. Now, programs can help determine intent, mental state and attitude in a litigation context.

The Robert Hanssen case demonstrates the effectiveness of behavioral recognition technology in identifying an insider threat. Warm Touch Software[10] tracked eight notes written by Hanssen, a former Federal Bureau of Investigation agent arrested in Feb. 2001 for spying for the Soviets. Warm Touch's analysis of these notes written by Hanssen while spying between Oct. 1, 1985 and Nov. 15, 2001 employed several indicators to mark and measure Hanssen's emotional state. These indicators, or retractors and qualifiers, measured anxiety and marked high measures of emotional stress over Hanssen's espionage time period when he was struggling with his relationship with his Soviet handlers.

As demonstrated in the Hanssen case, behavioral recognition technology holds tremendous potential in finding and assessing potential bad actors. Often the behavioral indicators found in data through psycholinguistic analysis strengthen expert technical forensic findings. Employing both behavioral and technological perspectives in analyzing data may aide in locating and assessing disgruntlement and insider risk. Even more importantly, this critical information might also provide an opportunity for an intervention, and a company can actually protect employees from themselves and from doing something that could haunt their careers forever.

## What Steps to Take After Identifying a Bad Leaver

After identifying a bad leaver, the most common difficulty lies in determining the damage a bad leaver has done or may do, especially if the damage relates to a data breach, source code theft, intellectual property robbery or other electronic data related crime. Critical elements to consider include: 1) the data preservation plan; 2) the composition of the ''strike team'' handling the situation; and 3) the digital forensics involved.

### *Preservation Plan*

Before assessing any damage inflicted by the bad leaver, the first steps should relate to evidentiary preservation efforts. Company executives should conduct preservation not haphazardly, sloppily or impetuously; but rather in a thoughtful, deliberate, fair and forensically sound manner.

In the proposed work plan for the preservation of evidence, at the outset, key categories of inquiry include:

---

[7] The Commission adopted final rules May 25 to implement the whistleblower program. The final rules will be effective Aug. 12. After Aug. 12, individuals wishing to be considered for an award under the Whistleblower Program will be required to submit the online ''Tips, Complaints and Referral'' ( TCR) questionnaire or the newly approved Form-TCR. The updated online questionnaire and Form-TCR will be accessible beginning Aug. 12 on the SEC website at http://www.sec.gov/complaint/info_whistleblowers.shtml.

[8] Such a program may not only provide an outlet for potential bad leavers, but may also demonstrate to regulators how seriously a company wishes to identify potentially unlawful or dangerous company practice. BP currently runs such a program (see, e.g., http://www.ombudsmanecp.com/).

[9] One such program, WarmTouch, generally applies algorithms to help analyze a subject from a behavioral perspective. For example, programs mark ''negative words'' (i.e., not, won't, can't, etc.) to equate anger; analyze the use of ''I vs. we'' to categorize an employee as a team player or an individual; and highlight a suspect's use of deemed psychological key words (i.e., zero, anything, quite, relieve, screws up, etc.) to associate a subject with a particular psychological state. These searches allow behavioral recognition technology to monitor an employee's communications and assess his or her psyche.

[10] WarmTouch Software is an example of one program that approaches cyber insider investigations from a behavioral sciences perspective. Warm Touch, derived from leadership profiling at Central Intelligence Agency (CIA) and forensic profiling work at the FBI Academy in Quantico, VA, helps reveal any behavioral problems that can serve as leading indicators of potentially bad employee behavior.

  PVLR ISSN 1538-3423

- **Communications:** *What communications need to be preserved? How did the bad leaver communicate? Did he or she use company e-mail, instant messaging or web e-mail to share files? Did the bad leaver use a mobile device such as a Blackberry, iPhone or iPad? Did the bad leaver work from a home computer and/or work computer?*
- **Access:** *What kind of access to specific trade secrets/shared drives/corporate network/ computers did the bad leaver enjoy? What is the job description pertaining to the bad leaver and what sort of access does that position allow?*
- **Co-conspirators:** *Whose communications need to be preserved? Are there possible co-conspirators and if so, are they still with the company? What sort of communications do the possible co-conspirators use?*
- **Back-up Systems:** *What back-up systems need preservation? What back-up systems does the company use generally? Does the back-up system operate continuously with an archive or does it ''tape over itself'' after a particular cycle, erasing prior back-ups after, for example, 30 days? What does the back-up restoration process entail and who should perform it?*
- **Temporal:** *What is the relevant time frame for preservation? When did the bad leaver depart and what projects/actions involved him or her before his departure? What were the last access/ modified/creation dates relative to his or her workplace? What temporal issues could be relevant to the functional analysis of the misconduct?*

### *Strike Team Formation*

Once a company has executed a preservation plan and protocol, if possible and appropriate, senior executives should consider an almost ''crime scene'' approach in handling the internal bad leaver investigation and select the proper ''strike team'' of professionals to handle the situation.

- **The Internal Investigation Team's Independence**: Instinctively, the bad leaver's supervisor(s) may feel inclined to lead the company's analysis of the bad leaver's desktop, laptop, cell phone, etc. However, given the dynamics of most bad leaver situations, the bad leaver's supervisors might lack the detachment and independence necessary to conduct a truly impartial analysis. If practicable, the team handling the bad leaver's aftermath should be as fair and neutral as possible–which can enhance credibility especially if the situation evolves into litigation or a referral to criminal, civil or regulatory authorities.
- **The Internal Investigation Team's Breadth:** Company executives should make sure the investigative team has the appropriate level of senior executive participation from relevant administrative departments. If possible, the team should at least initially consist of, or have input from senior ranking, ''C-level'' executives, including those from departments of information technology, human resources, legal counsel, public relations, and investor relations (if a public company). In certain situations, a company may even want to add someone with a behavioral background to assess the psychology of the bad leaver–most bad leavers do not end up in jail and could represent a continuing physical threat to the company or specific personnel.
- **The Internal Investigation Team's Digital Forensics Expertise:** Companies should also consider the value of an independent expert digital forensics team who can surround the scene with virtual ''yellow police tape.'' Leaving pristine in the short run any potential evidence left by a bad leaver until after the execution of a forensic identification, preservation and analysis plan can save time, money, and headaches in the long run. Bad leaver probes can be compromised, when, for instance critical logs, back-up tapes, hard drives or other data become corrupted or overwritten by non-expert investigators.

### *Digital Forensics Tasks*

Digital forensics, or the science of examining a digital device under forensically sound conditions and using forensically accepted methods to retrieve electronically stored evidence, has become an important scientific field, especially in the context of an investigation pertaining to a bad leaver.

Bad leaver matters can involve high volumes of information that can demonstrate timing, intent or bad faith, and which can hinge on document versions, data integrity and the uncovering of latent data. Just like on the hit TV series *CSI*, the proper collection of electronically stored information (or ESI) can be essential to ensuring the admissibility of evidence—one slip up and an entire case can fall apart.

Some digital forensics tasks that may prove useful in bad leaver situations include:

1. **Forensic imaging and reviewing of e-mails and other relevant data from laptop computers, desktop computers, relevant network servers, mobile devices, iPads, etc.** *Acquiring a forensic image, or the production of an exact sector-by-sector copy of any computer, storage device, network, 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, to ascertain any evidence of wiping/defragmentation, to answer new questions and to evaluate the authenticity of data. Given the volatility concerning internet evidence, forensic preservation of all devices allows for the searching of unallocated space and file slack*[11] *such as deleted files or web mail.*

[11] 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

2. **Forensic searching for any evidence of improper copying or taking of information.** *This part of the examination involves using forensic skills to determine what data storage devices, if any, were connected to the bad leaver's computer. This involves searching unallocated space for particular file names, looking for link files, and checking logs for the CD/DVD burning software, operating system and internet history—all in an effort to determine if the bad leaver potentially copied, deleted or transferred any information. For instance, when inserted into a Windows computer, removable media (such as thumb drives, external hard drives and other flash memory devices) can log an entry in the system. This captures the date and time of insertion and often times, the make and model of the device.*
3. **Searching for any useful evidence of other ''electronic footprints,'' such as wiping activity or internet surfing.** *The digital forensic examination of a desktop or laptop computer can provide examiners with the opportunity to analyze active files, shortcuts, application registry and archived e-mail—and begin to profile the bad leaver's computer-related activities. Additionally, examiners may obtain access to a bad leaver's deletion activity through deleted data recovery in order to understand a suspect's use of wipe, defrag or scrubbing utilities and mass deletions. Sometimes the more technologically sophisticated bad leavers employ wiping programs to attempt to hide their entire electronic trail (i.e., erase artifacts of activities) through the use of a wiping utility. While the use of some of these utilities may irretrievably delete data, their use and the timing of such use can prove inculpatory. Additionally, an examination of the internet and search history can uncover a history of web pages visited, downloads, searches and web-based mail and provide additional clues relating to the bad leaver's predeparture activities.*
4. **Reviewing of the ShellBag.** *Windows ShellBags can serve as another important tool for examiners to utilize in a digital forensic examination and provide another window into a bad leaver's electronic activities. The Windows registry keeps track of the display size of a folder window and stores the information in the registry. ShellBags, a part of the registry, tracks open windows as users click folders allowing examiners to see connections in different parts of networks. This information stays in the registry even after deleting a folder and can contain evidence regarding downloaded programs and desktop activity–more clues as to the actions and possibly the state-of-mind of the bad leaver.*
5. **Identifying and analyzing the bad leaver's use of confidential information after his or her departure and developing a confidentiality protocol.** *The development of appropriate reporting protocols should accompany a forensic investigation to protect against unauthorized disclosure of arguably confidential, private or otherwise privileged information discovered during an investigation (see* ***Privacy Rights*** *discussion infra). Identifying the types of documents and data that constitute confidential information, including reviewing file descriptions, will help examiners develop search terms (based on file types, words, codes, etc.) to identify confidential information without retrieving copious hits.*
6. **Imaging and reviewing other employees' data storage devices if evidence shows receipt of confidential information from the bad leaver (to help identify any co-conspirators).** *Bad leavers sometimes conspire with other employees, and companies should consider the potential relevance of all potentially relevant data and not overlook data relating to persons other than the bad leaver.*
7. **Searching for evidence of any communication with online repositories.** *Increasingly, companies also utilize any of the growing laundry list of online cloud repositories. Forensic examination of online storage (i.e., websites such as DropBox) not only provides an additional and perhaps even more pristine source of evidence, but can also lead to the discovery of leaked confidential information.*
8. **Tracing the bad leaver's printing trail.** *Analyze documents a user accessed recently and review metadata in Word documents, PDFs, etc. for the ''last print'' date. Examiners should also review computer spool files (created when a user sends out a print job), as well as print server logs.*

The above tasks illustrate how digital forensics can help preserve information relating to claims or defenses, take advantage of all available digital evidence and prepare for possible litigation and e-discovery. Recovering data from a digital device under forensically sound conditions can prove essential in bad leaver investigations, and if carried out correctly, can expose critical evidence, even the proverbial ''smoking gun.''

## *A Note on Cell Phones, Text Messages and Unallocated Space*

The ESI within mobile telephone devices has evolved to become a potential treasure trove of evidence and discovery in investigations and litigation, including SEC insider trading cases, anti-trust matters, investigations

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), 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.

  PVLR ISSN 1538-3423

pertaining to FCPA prosecutions[12] and a broad range of others action types.[13]

Today, in addition to personal notes, calendar events, photos, music, video and other sources of information, mobile devices can operate an enormous assortment of other programs (commonly referred to as ''apps''), which can warehouse a broad range of ESI potentially relevant to a civil or criminal proceeding or investigation. For these reasons, the use of a mobile device by a bad leaver provides an increasingly sizeable, and potentially very relevant, amount of data.

For instance, if a bad leaver used an iPhone, there exist certain forensic possibilities unique to that device, such as the fact that when an iPhone snaps a photo, it may also record the location of the iPhone when the photo was taken. This geolocation function could prove very useful in a range of scenarios. Additionally, when iPhone users ''sync'' their iPhones with iTunes, the device can create an encrypted or unencrypted back up which contains certain contents of the phone including: contacts, calendar, events, photos, bookmarks, voice memos, etc. in an organized and unobfuscated manner. Successfully harvesting these features can not only provide key information but can also present that key information in an organized manner, with a proven methodology.

Mobile devices can also require special forensic navigation techniques. For instance, with some mobile devices, failing to disable its transmitter could actually allow the owner of the device to remotely clear its memory and destroy permanently relevant ESI.

Companies should also watch out for problems caused by powering down a mobile device the wrong way. Volatile memory (such as ''random access memory,'' or RAM, used for instance in mobile devices) can be lost when a device loses power while nonvolatile memory (such as ROM, or ''read only memory,'' also used in mobile devices) is not.

Similarly, accessing or powering up the ''subscriber identity module'' or ''SIM'' card typically found in mobile devices at the wrong point in the forensic process might not only unintentionally wipe data from its memory or trigger a ''password-protect'' lock, it might even reset dates and time stamps of messages—which can seriously muck up authentication of that evidence later on at trial.

The bottom line: Unless bad leavers physically demolish their devices, there is always the possibility of a successful forensic extraction of potentially relevant information. Although a bad leaver might believe that he or she has removed evidence from the device's memory, key artifacts and remnants of the data may occasionally linger in unallocated space and a good forensic methodology could potentially piece some activity back together.

## Privacy Rights

In most bad leaver situations, e-mails will likely have the most evidentiary value, so the focus of the work will be to review relevant network and local e-mails (derived from active and deleted files) to search for any inculpatory behavior.

But whether or not a company or its attorney can examine all e-mails and other potentially personal information residing on company servers, desktops, laptops, mobile devices, etc. can present thorny legal issues and can require consultation with inside and/or outside counsel. Some companies even go so far as to hire immediately a third party investigative firm to warehouse and safeguard the potentially relevant data and wait for a legal or even judicial determination concerning analysis of, for example, the possibly private e-mails of a bad leaver.

Accordingly, before reviewing a bad leaver's company e-mails, private e-mails (i.e., Yahoo, Hotmail, etc.), looking in unallocated space and other hidden areas of desktops and laptops or perusing a bad leaver's text messages, companies should remain mindful of any privacy-related red flags.

For instance, the ''cache'' or ''cookies'' of a bad leaver's hard drive might allow another user to log on to the bad leaver's computer, take advantage of pre-populated user name and password fields and read the bad leaver's potentially private e-mails. While tempting and simple to execute, this kind of review can raise privacy issues later on down the road.

Even in the instance of company e-mail or text messages, where a company maintains a strict policy that all company e-mails belong to the company (and even if employees consent to the policy every time they log on to the company's network), the information may still

---

[12] 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 Securities and Exchange Commission to keep books and records that accurately reflect business transactions and to maintain effective internal controls. Given the SEC's new specialized FCPA unit; the whistleblower provisions contained in the Dodd-Frank Wall Street Reform and Consumer Protection Act (which reward informants who provide certain types of information leading to successful securities actions, including FCPA actions); a hefty SEC budget increase; and increased SEC-Department of Justice Collaboration, 2011 and beyond will undoubtedly result in an onslaught of FCPA enforcement actions and prosecutions.

[13] A few examples:

- Because of 300 unearthed and thought-to-be-deleted iPhone text messages and phone logs, constables in Sydney, Australia reportedly dropped five criminal charges, including rape, against a defendant accused of raping the 18 year-old daughter of a neighbor (and were also even ordered to pay the defendant's legal costs);
- Police in Cambridge, Massachusetts arrested a man for running an automobile ''chop shop,'' who insisted he was innocent. However, the police were apparently able to boost their case considerably when forensic examiners discovered that the wallpaper background on his cell phone was a photo of the defendant in the driver's seat of a stolen Ferrari;
- In Bloomington, Ill., a man was suspected of taking photos of a neighbor's son while fondling himself. Although upon checking the suspect's mobile phone, the police found no specific photos of the neighbor in question, examiners reportedly did discover more disturbing and arguably incriminating photos on the suspect's phone, which assisted the officers in obtaining a confession from the suspect; and
- By working with service providers, Idaho law enforcement officials tracked a specific user's cell phone to within a few feet, bringing to justice a man who had allegedly shot a woman at a Twin Falls Comfort Inn Hotel.

carry with it certain legal and constitutional protections.[14]

Another issue that can arise in these situations is when a company discovers a bad leaver's e-mail correspondence with his or her attorney (either on a private or a company e-mail account). Whether a company should review this information; image the information, but not review it; seek a third party to warehouse this information; or simply return the e-mails to the bad leaver all present embryonic legal issues that can warrant thorough consideration.[15]

Additionally, with the right professional care and a protocol that carefully tracks not only what data were found, but where data were found, sometimes restricted data can lose the protections provided by law. For example, information protected by the attorney-client privilege can lose its status and protections based on where or to whom the information was sent.

Privacy concerns can also span international borders. For example, FCPA violations often involve rogue employees and bad leavers, and also often 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 raise an array of cross-border issues. FCPA investigators and lawyers should work with privacy lawyers and forensic teams that have extensive expertise preparing protocols consistent with European Union (EU) and/or relevant ESI privacy standards.

As one of its basic principles, the EU data protection directive, which compels member nations to enact national data protection laws, prohibits the processing of personal information without, among other things, the notice to and consent of, the data subject. This could arguably include the data on a bad leaver's cell phone even if that cell phone is owned by the bad leaver's former employer.

The EU data protection directive also 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. There may also be considerations relevant to the Asia-Pacific Economic Community privacy framework or any other specific rules promulgated by any particular country. Overall, whenever data crosses any border, privacy concerns will undoubtedly surface.

### *Bad Stayer and Black Bag Operations*

Internal threats to a company can also stem from so-called ''bad stayers,'' or rogue employees still employed but posing a threat. For instance, bad stayers include employees who supervisors suspect may be leaking confidential or proprietary information to competitors; may be contemplating a theft of intellectual property; or may be trading securities based on material, nonpublic information gleaned from company files.

In bad stayer situations, companies should consider the same preservation notions involved in bad leaver situations, identify all relevant data and devices and begin preservation efforts.

Companies should also consider limiting the bad stayer's access to technology especially if he or she enjoys a high level of access and especially in sensitive situations such as suspected corporate espionage or unlawful insider trading. In the most serious situations, companies may want to consider the so-called ''black bag operation.'' Black bag operations entail implementing a significant monitoring protocol concerning the bad stayer and can involve clandestine efforts by company management.

Companies should bear in mind, however, that black bag operations can raise legal questions for company counsel and can even present physical dangers to per-

---

[14] In the recently decided *City of Ontario vs. Quon*, No. 08-1332, 560 U.S. ___ (June 17, 2010) , the Supreme Court weighed in on employee privacy expectations, holding unanimously that employers can read text messages—including personal ones—sent by workers on their company cell phones if they have reason to believe that workplace rules are being broken. However, the Court seemed especially mindful to neither reject nor accept a broad right of privacy for employees, noting that it would tread carefully in deciding how far an employer can go in the future: ''Prudence counsels caution before the facts in this case are used to establish far-reaching premises that define the existence and extent, of privacy expectations enjoyed by employees when using employer-provided communication devices . . . At present, it is uncertain how workplace norms, and the law's treatment of them, will evolve . . . A broad holding concerning employees' privacy expectations vis-a-vis employer-provided technological equipment might have implications for future cases that cannot be predicted.'' Although the *Quon* decision involves a governmental employer, the decision has ramifications for private employers as well, and as technology continues to evolve and workplaces continue to change, privacy issues in this context clearly remain ripe for further adjudication in the future.

[15] For instance, in these kinds of situations, when courts examine whether the bad leaver has waived attorney-client privilege because he or she used a corporate server for those communications, they might employ the four factors test first particularized in a New York federal bankruptcy case, *In re Asia Global Crossing Ltd*, 322 B.R. 247 (S.D.N.Y. 2005). In *Asia Global Crossing*, executives used corporate e-mail to communicate with their attorneys about actual or potential litigation involving their employer. The judge concluded that the attorney-client privilege would be inapplicable if: 1) the company or organization had a policy that prohibited personal use; 2) the company regularly monitored the use of computers and e-mail; 3) third parties had a right to access computers and e-mails; and 4) the company notified the employee that monitoring was taking place, or the employee was otherwise aware of the use and monitoring policies. Additionally, the New Jersey Supreme Court ruled March 30, 2010 that attorneys for an employer violated the privacy rights of a former employee and the rules of professional conduct by reading e-mails the employee sent to her counsel on a company laptop through her personal password-protected Yahoo e-mail account. *Stengart v. Loving-Care Agency, Inc.*, 2010 WL 1189458 (N.J. March 30, 2010) (ruling for the plaintiff even though the employer had a general policy stating that the employee should have no reasonable expectation of privacy in communication sent over company equipment). In *Holmes v. Petrovich Dev. Co., LLC*, 2011 Cal. App. LEXIS 33 (Cal. App. 3d Dist. Jan. 13, 2011), a California court ruled that e-mails sent by an employee to her attorney from a computer in her workplace were not protected by attorney-client privilege. However, unlike the *Stengart* case, this employee used a company e-mail account (rather than a personal web mail account) to send the e-mails. The court noted that the employee had been (1) told of the company's policy that its computers were to be used only for company business; (2) warned that the company would monitor its computers for compliance with this policy; and (3) advised that employees using company computers have no right of privacy.

  PVLR ISSN 1538-3423

sonnel involved. Thus companies should consult with counsel and skilled investigators (and perhaps even with law enforcement) before proceeding with a black bag operation.

## Conclusion

The so-called bad leaver is a 21st century phenomenon. Until relatively recently, what existed for the most part were merely ex-employees who tried to make off with a few of the company's pads and pencils and perhaps set off a false fire alarm during their last day on the job. Nowadays, however, bad leavers have become a far greater threat to modern corporate enterprise, using technology not only to orchestrate their sabotage but also to hide their activities.

Indeed, yesterday's disgruntled employees have evolved into today's bad leavers, whose digital mayhem can cause an immeasurable amount of expense, aggravation and drag.

To combat this growing epidemic requires a thoughtful and deliberate game plan, designed to preempt, counteract and remediate bad leaver situations.

In crime scene investigations, whether involving homicides or financial transgressions, specially trained law enforcement experts have always investigated physical evidence employing techniques such as fingerprinting and DNA testing. Today, law enforcement experts have supplemented those now traditional scientific investigative techniques and have begun employing digital forensics with the same precision and rigor.

In the aftermath of a bad leaver, companies should take a similar technological leap and make the most of the evidentiary value of information properly preserved, extracted, discovered or gleaned through the digital forensic scrutiny of the data, media and systems touched by a bad leaver.

Yes, bad leavers can still probably slash the tire of their bosses without detection. However, bad leavers will have a far tougher time destroying e-mails or texts, wiping out the artifacts of their attempted deletions, tampering with any logs of their network activities or obfuscating any other electronic evidence of their malfeasance. Because while technology has certainly empowered bad leavers, technology can also contribute exponentially to their downfall.