The HedgeFund LAW REPORT

Vol. 7, No. 20 May 23, 2014

ELECTRONIC COMMUNICATIONS

Six Privacy-Related Topics to Be Covered by a Hedge Fund Manager's Compliance Policies and Procedures (Part Three of Three)

By Lily Chang

This is the final article in our three-part series on employee privacy issues relevant to hedge fund managers. The first article in this series made the case, using examples, for why hedge fund managers should care about employee privacy. See "How Can Hedge Fund Managers Reconcile Effective Monitoring of Electronic Communications with Employees' Privacy Rights? (Part One of Three)," The Hedge Fund Law Report, Vol. 7, No. 13 (Apr. 4, 2014). The second article in this series identified the five primary sources of employee privacy rights. See "Three Best Practices for Reconciling the Often Conflicting Sources of Privacy Rights of Hedge Fund Manager Employees (Part Two of Three)," The Hedge Fund Law Report, Vol. 7, No. 14 (Apr. 11, 2014). This article discusses six topics that hedge fund managers should cover in their compliance policies and procedures under the general rubric of employee privacy. The overarching aim of this series is to assist managers in calibrating and communicating their employees' expectations of privacy – particularly in connection with electronic communications – in a manner consistent with best practices, relevant law and expectations of SEC examiners.

Privacy-Related Provisions in Compliance Policies and Procedures

No Reasonable Expectation of Privacy in Hardware, Software or Data

The second article in the series concluded with the idea that the reasonableness of expectations of privacy on the part of hedge fund manager employees is, in large measure, a function of how the manager sets and communicates expectations. In other words, privacy expectations in this context are not established in the abstract, but rather are crafted by specific acts and statements of the employer.

Consistent with this principle, the first and probably most important task to be accomplished by a hedge fund manager's policies and procedures (with respect to privacy) is to clarify that employees should not expect privacy in any of the manager's hardware, software or communication systems, or in any data entered into, legally extracted from or transmitted over such systems. (Data illegally extracted from a manager's systems raises trade secret and other intellectual property issues, in addition to securities law and privacy issues. See "Recent Developments Affecting the Protection of Trade Secrets by Hedge Fund Managers," The Hedge Fund Law Report, Vol. 6, No. 41 (Oct. 25, 2013).) The statement of this policy should be

forthright, unambiguous and easily accessible to employees. According to Michael McNamara, a partner at Seward & Kissel LLP, that policy should "clarify that the managers' computers, computer systems and any devices supplied by the company are company property. The policy should make it clear that all e-mail accounts, and all information and messages created, sent and received, are company property, and specifically state that employees have no expectation of privacy for any data stored or accessed on or through a company computer system."

Enunciating such a principle will accomplish at least five ends.

First, as indicated, it will undermine the reasonableness of any expectation of privacy – much like a "big boy letter" can, in theory, undermine the reasonableness of reliance on representations by a counterparty to a trade in illiquid assets. See "How Can Hedge Fund Managers Understand and Navigate the Perils of Insider Trading Regulation and Enforcement in Hong Kong and the People's Republic of China," The Hedge Fund Law Report, Vol. 6, No. 13 (Mar. 28, 2013) (discussion under the heading "Potential Availability of a 'Big Boy' Defense Under the Ordinance"). Sean O'Brien, managing partner of O'Brien LLP, observed on this point, "A firm's policies and procedures can go a long way toward destroying any claimed expectation of privacy. If your employer has told you it is going to review everything you do on your work computer, and that your computer is subject to review, it is incredibly difficult for you to come back later and say that you didn't know that. So setting forth these policies is something employers should do as a matter of fairness to their employees, and that also has a legal effect."

Second, an explicit statement of non-reliance helps align the expectations of the manager and its employees. As Holly Weiss, a partner at Schulte Roth & Zabel LLP, explained, "Most hedge fund managers as a matter of general practice tell their employees in their electronic communications policies that the employees have no expectation of privacy with respect to their communications on the firm's systems. They tell them that not because disclosure is required for access to the information, but because they want employees to know."

Third, such a statement facilitates monitoring of electronic communications for insider trading, other securities law or compliance violations and other issues. The first article in this series catalogued six reasons why hedge fund managers should monitor electronic communications of employees. See also "How Can Hedge Fund Managers Structure, Implement and Enforce Information Barriers to Mitigate Insider Trading Risk Without Impairing Securities Trading? (Part Four of Four)," The Hedge Fund Law Report, Vol. 7, No. 5 (Feb. 6, 2014).

Fourth, an explicit statement of principle on this point is an important adjunct to a manager's recordkeeping policies and procedures. Christopher Wells, a partner at Proskauer Rose LLP, described the interaction between employee privacy and manager recordkeeping, as follows: "Almost every hedge fund manager is going to say you must not do firm business on a personal computer or personal e-mail. That is because hedge funds are a regulated industry. The firm has an obligation to keep many communications by its employees – basically, anything relating to transactions for clients, marketing to clients or recommendations to clients regarding a purchase or sale of securities, including internal communications within the company with other company employees about whether or not to buy or sell securities. Since the company has to

keep those communications as a matter of law, it does not want employees to have those communications on a system that it does not have access to, which might prevent it from being able to keep that required record."

Fifth, clarity of communications with respect to expectations of privacy will facilitate access to information in connection with internal investigations, employee discipline or litigation. As Weiss noted, managers "do not want there to be any barriers to access if the need arises. For example, if the manager is investigating criminal behavior or other wrongdoing, the manager does not want to have somebody coming in and saying, 'I thought that information was private. You never told me it was not private.' Clearly communicating that the employee does not have a reasonable expectation of privacy takes care of that issue." For a discussion of internal investigations by hedge fund managers authored by Weiss' colleague Sung-Hee Suh, see "Ten Recommendations to Help Hedge Fund Managers Conduct Successful Internal Investigations," The Hedge Fund Law Report, Vol. 6, No. 9 (Feb. 28, 2013).

Regarding the mechanics of communicating expectations, sources identified two key points. First, notice is generally sufficient and consent, strictly speaking, is not required. Kenneth Laverriere, a partner at Shearman & Sterling, clarified that "Notice is, by and large, the game" with respect to communicating privacy expectations. "In many cases, consent is deemed to be given with notice. If you notify someone clearly and you remind them clearly of your policies, that is consent." That said – and second – McNamara, of Seward & Kissel, recommends obtaining an acknowledgment from each employee stating that the employee read and understood the manager's electronic communications and related policies and procedures.

Personal Computers Used for Business Purposes

Regarding use of personal computers for business purposes, the compliance tension is as follows: On the one hand, it is cleanest from a compliance perspective to prohibit the use of personal computers for business purposes outright – and some hedge fund managers are doing just that. As Wells observed, "You will find a lot of different policies out there, but an ever-increasing number of firms will say that you should not access personal e-mail from company computers, and you should not use any personal computers or personal cell phones for company business." O'Brien added that firms taking a stricter approach to compliance or relying more centrally on technology will often mandate use of company computers for manager business, or permit employees to connect personal computers to managers' systems only via specific connections (e.g., VPN or private cloud). See "Key Considerations for Hedge Fund Managers in Evaluating the Use of Cloud Computing Solutions (Part Two of Two)," The Hedge Fund Law Report, Vol. 5, No. 41 (Oct. 25, 2012).

On the other hand, given the proliferation of computing and communication channels, it is becoming increasingly difficult to effectively prohibit any use of personal computers for business purposes. In the view of Sam Whitaker, counsel at Shearman & Sterling LLP in London, it is preferable to recognize this reality in designing compliance policies and procedures than to knowingly draft a policy, the uniform enforcement of which is not practicable. As Whitaker told the HFLR, "you're in a much worse position if you have put in place a policy that forbids all

personal use, but in practice you just turn a blind eye to it because you can't prevent it." This is an instance of the broader proposition – frequently voiced in SEC speeches, at compliance seminars and in interviews – that one of the most common recurring examination deficiencies is a failure by a hedge fund manager to operate according to its own policies and procedures – that is, saying you'll do something then not doing it. Put another way, reality, resources and practicability should be considerations when hedge fund managers are drafting compliance policies and procedures relating to electronic communications, privacy or any other topic. This, among other things, is what the SEC staff means when it says that compliance policies and procedures should be tailored to a manager's business rather than "off the shelf."

Accordingly, Richard Rabin, a partner at Akin Gump Strauss Hauer & Feld LLP, identified a three-step middle ground between an outright prohibition on the use of personal computers for business purposes, and unlimited permission to do so. First, managers "should make clear that such devices are subject to inspection and monitoring." Second, managers "should clarify that employees have no expectation of privacy in personal devices to the extent they are used for business purposes." Third, managers "should consider having employees sign acknowledgments" of the foregoing two points.

Mobile Devices

As mobile devices (e.g., cell phones) and portable computers (e.g., laptops) converge in computing power, the volume of compliance challenges raised by the two categories of technologies increases and the differences in compliance challenges diminish. For the time being, however, mobile devices present at least two unique compliance issues. First, Kelli Moll, a partner at Akin Gump Strauss Hauer & Feld LLP, noted that recordkeeping on mobile devices generally remains more challenging than on desktops or even laptops. For this reason alone, many managers ban the use of mobile devices for conducting firm business. As Moll explained, "Many investment firms prohibit employees from using personal devices in conducting firm business because most firms are very concerned about recordkeeping, and typically there is no way to capture e-mail records or other documents generated on a personal device. So if any employee is using a cell phone and sends an e-mail pertaining to an investment recommendation, this is a record the investment firm is required to capture under the Advisers Act, but the use of such a personal device may circumvent the ability of the investment firm to maintain this record."

Second, Rabin (Moll's partner at Akin Gump) noted, "We are starting to see laws prohibiting employers from demanding to see employees' personal devices, such as iPhones and BlackBerrys. This is another reason why managers should consider requiring employees to use only firm-issued devices for work purposes. If these devices are the property of the firm, and employees are told they have no expectation of privacy in their use, firms can conduct inspections of those devices. If employees use their own iPhones to conduct firm business, firms' right to demand inspection can be less clear-cut." For a fuller discussion of the privacy and other issues raised by mobile devices, see "What Concerns Do Mobile Devices Present for Hedge Fund Managers, and How Should Those Concerns Be Addressed? (Part Three of Three)," The Hedge Fund Law Report, Vol. 5, No. 17 (Apr. 26, 2012).

Password Protection

Hedge fund managers should keep in mind – and should reflect in their policies and procedures – three principles applicable to password protection.

First, a manager's policies and procedures should clearly state that it has the right to access any work device or computer, even if the employee has protected the device or computer using a password of the employee's own creation. Blythe Lovinger, a partner at Kasowitz, Benson, Torres & Friedman, LLP, advised, "Employees should be clearly informed that password protecting does not give an employee a heightened sense of privacy. The purpose of passwords is to protect the firm's confidential and proprietary information, and its clients' confidential and proprietary information."

Second, if the manager's policies and procedures permit employees to use personal devices for work purposes, the policies and procedures should – as a counterweight – state that the employer can obtain the employee's password so that the employer can comply with its recordkeeping obligations under the Advisers Act. Rabin explained, "Regarding whether employees can put in passwords to prevent their employer from accessing their device, firms could not permit this, as they have an obligation to access and maintain business records and monitor employee communications. Firms should communicate with employees about the firms' compliance obligations, so that employees understand both the steps the firm is taking and the reason the firm is taking them."

Third, if the manager's policies and procedures do not permit employees to use personal devices for work purposes and the manager does not have grounds to suspect a compliance violation by the employee, password protection may be an effective way for the employee to maintain the privacy of a device and the information on it. As Weiss noted, "Password protecting your personal iPhone would, depending on how the situation arose, help you protect the information. If your personal computer is open but it cannot be accessed by the employer, that may help you protect what you are doing." Of course, as indicated above, a manager may not reasonably be able to expect total compliance with a total prohibition on business use of personal devices. Accordingly, an outright prohibition on business use of personal devices may work to contrary purposes because such a prohibition would undermine the manager's access to personal devices, which in turn would complicate its ability to comply (or confirm compliance) with the recordkeeping provisions of the Advisers Act.

The good news for hedge fund managers – at least in New York – is that in the unlikely event that a manager demands a password and the employee staunchly refuses, the manager may have the leverage of a termination to help persuade the employee to disclose the password. As Weiss explained, "If an employer needed to know what was on somebody's Facebook page for some reason, and went to the employee and said 'Give me your password," and the employee said 'No,' right now, an employee in New York (but maybe not in some other states) could be terminated for that. On top of that, if there was litigation, the courts could order the password to be disclosed."

Social Networks

Social networks raise at least two categories of concerns for hedge fund managers: access-related concerns and content-related concerns. With respect to access, a hedge fund manager employer's ability to access an employee's social media website will depend on what the manager's policies and procedures say, whether the site is being used for business purposes on business infrastructure and during business hours, and whether the site is password-protected. O'Brien summed up the interaction of these factors, as follows: "Employers can monitor social network postings if done from a work computer. If the social network is password-protected, that is going to increase the employee's ability to say that it's private, because many states have passed laws restricting employers' ability to obtain passwords. If the employee is accessing the social network on a work computer during work hours, and certainly if the access at all relates to work, the employee won't be successful in refusing to disclose the password, provided proper notice has been given."

With respect to content, social networks raise at least three categories of concerns. First is reputation, and according to Weiss, social media policies typically address this issue. "Many employers have social media policies that limit what employees can do on social media as it relates to the employer, and these dovetail with their electronic communications policies. They'll have limitations on an employee's ability to write about the firm, to express opinions about the firm or the business, to write about anything that affects the business, to defame people within the company or to say negative things about the company or its people." Second, despite those broad and typical prohibitions, Weiss noted that "employers have to be careful about impinging on their employees' rights under Section 7 of the National Labor Relations Act. An absolute restriction on mentioning the firm or the firm's name could be viewed as a violation of that act. Even saying negative things about a company or a supervisor has been found to be protected if in the context of concerted activity by employees." Third, social media raise securities law-related concerns such as insider trading, prohibited testimonials and general solicitation. See "SEC Issues Guidance for Investment Advisers on the Interplay of the Testimonial Rule and Social Media," The Hedge Fund Law Report, Vol. 7, No. 15 (Apr. 18, 2014).

Records of Instant Messages, Text and Deleted E-Mails

In the view of the SEC, instant messages, texts and deleted e-mails generally fall within the category of records required to be maintained for designated periods. On IMs, Wells observed, "Instant messaging is now treated very much the same as e-mail, and that has been a change over the last few years. The SEC now asks to see records of IM communications in the same way they ask to see e-mail communications, so companies have put in place systems to record IMs basically the same way they put in place systems a few years ago to record e-mails." On texting, Nathan Greene, a partner at Shearman & Sterling, noted, "Mobile devices are where a lot of the action is right now. So much of what people do today is on their phones, including texting. Depending on the size of the firm, you may have invested in technology that is in fact archiving texts, but you can only do that on your approved devices, so many firms have policies that tell employees what devices they're allowed to use." And on deleted e-mails, Lovinger

suggested, “Employees should be informed and understand that e-mail systems retain messages even after they’ve been deleted. So even though it appears messages have been erased, they are often backed up and can still be reviewed.”

These insights yield two general implications, one relating to practicability and the other relating to disclosure. The practicability point – which Greene highlighted – is that IMs, texts and deleted e-mails can only be maintained by a manager if conducted on devices or systems maintained by the manager. The disclosure point – which Lovinger adumbrated – is that employees and managers are both better off if employees are well aware that their IMs, texts and deleted e-mails will be archived for a period that is effectively indefinite. Reasoning backward, this disclosure should inject a note of caution into the thoughts and tidings that employees commit to IMs, texts and e-mails. Although the reality appears to be that despite years of incriminating and case-deciding e-mails, even smart people continue to commit dumb thoughts to electronic immortality.

Phone, Audio and Video

The foregoing discussion related to privacy in connection with electronic communications. But what about privacy in connection with physical activity – workspace privacy, audio and video recording, phone conversations and out-of-office conduct? As a general principle, hedge fund managers can monitor employees’ activities to the extent necessary to comply with applicable law. As Rabin said, “So long as a firm’s searches, reviews and inspections flow logically from its obligations under the Advisers Act or other applicable law, or otherwise have a reasonable basis, the firm’s position is defensible. Conversely, the more a firm’s monitoring activities look like voyeurism, having nothing to do with the legitimate needs of the firm or its investors, the more risk the firm takes on. The latter is not the type of activity we recommend and, frankly, not what we normally see.”

Workspace

While it would be counterintuitive to expect privacy in the open plan workspaces of most hedge fund managers, nonetheless, Weiss suggested that it is worth clarifying the absence of privacy in workspaces in a manager’s policies and procedures. “It is a good practice, within the employer’s policies, to make sure employees are on notice that there isn’t a right to privacy in their workspace, and that the employer has the right to access workspaces,” Weiss said.

Video Cameras

According to Lovinger, the chief legal considerations in videotaping employees are uniformity of treatment and avoiding physically invasive situations. “Employers may use cameras in the workplace for a number of reasons, including security reasons, to monitor employee productivity or prevent internal theft,” Lovinger said. “Some states have laws restricting how an employer can videotape its employees. Subject to state law requirements, the use of cameras should be permissible so long as such use does not target anyone in particular, and the cameras are not in an area that would be considered physically invasive, such as a restroom. There are instances

where an employer decides to videotape one or two people for a specific reason, and there is a risk that the employee may allege that he was videotaped because of his race or based on some other protected characteristic. If an employer is going to monitor employees through videotaping, it should be done across the board."

O'Brien added, however, that videotaping of employees remains rare in the hedge fund industry. "I'm not aware of many firms that on an ongoing basis film people and actually review the film, just to sort of see what people are doing. Nonetheless, employers that videotape should disclose that they are going to do it."

Audio Recording in Connection with Video

Lovinger noted, "There are some state laws regarding audio surveillance, so to the extent video cameras will also capture audio, there may be additional restrictions depending on the state where the firm's offices are located."

Monitoring Phone Communications

As for an employer's ability to monitor phone communications, Laverriere advised, "Under the federal wiretap laws, employers can monitor phone communications, but if it becomes evident that the employer may have captured or is monitoring a personal call, the general rule is that the employer must stop monitoring the call. The employer should utilize surveillance to the minimum extent necessary to achieve its purpose." On wiretapping law generally, see "Second Circuit Rules on Suppression of Wiretap Evidence and Application of the 'Knowing Possession' Element of Insider Trading in Upholding Raj Rajaratnam's Conviction for Insider Trading," The Hedge Fund Law Report, Vol. 6, No. 27 (Jul. 11, 2013).

Out-of-Office Conduct

Hedge fund manager employers may wish to monitor the out-of-office conduct of their employees to, for example, maintain compliance with the "bad actor" disclosure provisions of Rule 506, or with "pay to play" laws and rules. See "How Can Hedge Fund Managers Negotiate the Structuring, Operational and Due Diligence Challenges Posed by the Bad Actor Disqualification Provisions of Rule 506(d)?," The Hedge Fund Law Report, Vol. 6, No. 39 (Oct. 11, 2013); "Five Best Practices for Avoidance of Pay to Play Violations by Hedge Fund Managers or Their Covered Associates," The Hedge Fund Law Report, Vol. 4, No. 44 (Dec. 8, 2011). Weiss advised, "Disclosure in that instance would be a good practice. Also, hedge fund manager employers should consider New York's off-duty activities law, which generally protects from discrimination employees who perform certain lawful activities off-site and outside of work hours."