The HedgeFund LAW REPORT
The definitive source of actionable intelligence on hedge fund law and regulation

www.hflawreport.com Volume 7, Number 14 April 11, 2014

Electronic Communications

Three Best Practices for Reconciling the Often Conflicting Sources of Privacy Rights of Hedge Fund Manager Employees

By Lily Chang

This is the second article in our three-part series guiding hedge fund managers through the motley patchwork of authority governing employee privacy rights and employer privacy obligations. The crux of the challenge is as follows: securities regulation and best practices require hedge fund managers to exercise considerable vigilance over employee communications. To cite one headline example, a hedge fund management company can be held criminally liable for failing to adequately supervise employees that engaged in insider trading, and the DOJ and SEC understand adequate supervision to include continuous and vigorous monitoring of e-mails, chats and other electronic communications. On the other hand, non-securities regulation and other authority grant employees certain privacy rights in their electronic and other communications. How can hedge fund managers comply with applicable securities regulation while also complying with applicable privacy regulation – especially where the two regimes conflict? Outlining an answer to that question is the goal of this series.

This article discusses the five primary sources of employee privacy rights, then offers three best practices for reconciling these often conflicting sources. The first article in this series detailed six reasons why hedge fund managers need to monitor electronic communications of employees and highlighted two settings in which procedures other than electronic communication monitoring are most effective. 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 third article will describe factors bearing on the reasonableness of an employee's expectation of privacy, the benefits and limits of specific policies regarding electronic communication monitoring and best practices in this area.

State Common Law

Just as all politics is local, so is much of the most relevant common law. In keeping with this adage, state tort law plays a significant role in defining the privacy rights of employees. While the specific elements of state common law privacy rights of action vary by state, Kenneth Laverriere, a partner at Shearman & Sterling, explained that those elements typically include "a reasonable expectation of privacy, a breach of that expectation and injury as a result of the breach. Laverriere noted that "in grappling with that expectation, courts tend to come down more on the side of the employer than the employee." But the specific outcome in any scenario depends on the facts, relevant state law, the leanings and jurisprudential worldview of the court hearing the dispute and – importantly for hedge fund managers – the actions of the employer bearing on the reasonableness of employees' privacy expectations.

New York, for example, is known to have an employer-friendly privacy jurisprudence. As Sean O'Brien, managing partner of O'Brien LLP, explained, "Courts in New York

The HedgeFund LAW REPORT
The definitive source of actionable intelligence on hedge fund law and regulation
www.hflawreport.com Volume 7, Number 14 April 11, 2014

have held that when an employee is communicating in any way, on any subject, using the company's computers, the information communicated by the employee is subject to review by the employer, provided that the employer has given clear notice to employees that such communications will be monitored. One case involved an employee communicating with his personal lawyer through company e-mail and in plainly privileged communications, and it was held that even those communications could be reviewed by the employer because they ran through the employer's computers." O'Brien's advice to employees in New York, accordingly, "would be to do nothing that you want the least bit private through the company e-mail system, or even in your private e-mail system, particularly if you are talking about company-related business."

New Jersey, on the other hand, is known as generally protective of employee privacy rights, noted Lloyd Chinn, a partner at Proskauer Rose LLP. Chinn provided the following example: "There was a case in New Jersey, *Stengart v. Loving Care Agency*, that found that an employer had in a sense exceeded its rights in reviewing its employees' e-mail. There, the employee used a company-issued laptop, but accessed the employee's own personal Yahoo e-mail account, and sent her lawyer information about claims that she was bringing against her employer. Unbeknownst to the employee, the laptop was saving copies of those e-mails. The court held that the company's policy was unclear as to whether it covered the use of personal password protected web-based e-mail accounts on company equipment, and the court found that the plaintiff took steps to protect her privacy by using a personal password protected e-mail account instead of a company e-mail address. Accordingly, the court found that there was a breach of the privacy interest of the employee. In New York, on the other hand, there are cases like *Scott v. Beth Israel Medical Center*, where the court held that the employee had waived the attorney-client privilege by using the employer's computer system to communicate with his attorney."

Regardless of the state in which a hedge fund manager is organized or in which it conducts business, the actions of the manager can impact the reasonableness of an employee's expectation of privacy, thus affecting the first prong of the typical common law privacy action identified above by Laverriere. In other words, the first thing an employee plaintiff must prove when bringing a common law action for breach of privacy is a reasonable expectation of privacy. A hedge fund manager can take certain actions to buttress the argument that any expectation of privacy on the part of an employee in relevant communications was not reasonable. Christopher Wells, a partner at Proskauer Rose LLP, noted that regardless of the state common law default rules, one effective way to undermine the reasonableness of an employee's expectation of privacy – or, phrased more positively, to align employer and employee expectations with respect to privacy – is to explicitly "contract out" of privacy rights via relevant disclosure in the compliance manual. As Wells said, "The compliance manual should make clear that there is no applicable common law right of privacy. In a sense, the compliance manual is a contract with the employee because the employee has to acknowledge and agree to comply with it. Effectively, the employee has contractually waived any privacy right as to any communications on company computers or facilities." Although this point is phrased in terms of litigation strategy, the same ideas would influence the negotiating leverage of hedge fund manager employers in settlement discussions regarding breach of privacy claims by employees because parties bargain (and settle or fail to settle)

The HedgeFund LAW REPORT
The definitive source of actionable intelligence on hedge fund law and regulation
www.hflawreport.com Volume 7, Number 14 April 11, 2014

"in the shadow of" their understandings of relevant law. See, e.g., "How Hedge Fund Managers Can Use Arbitration Provisions to Prevent Investor Class Action Lawsuits," The Hedge Fund Law Report, Vol. 5, No. 26 (Jun. 28, 2012).

State Statutory Law

State statutes can also intersect with the privacy rights and expectations of employees of hedge fund managers. Two examples include wiretapping statutes and actual or potential state laws on employer access to employee social media websites.

Holly Weiss, a partner at Schulte Roth & Zabel LLP, explained New York's wiretapping law and its relevance to hedge fund manager employers, emphasizing New York's one-party consent regime and the permissibility of reviewing recorded calls. "The New York wiretapping statute has not been applied to prevent employers from reviewing stored communications, as opposed to monitoring them as they are being transmitted," Weiss explained. "There is a difference between taping then listening, and tapping into a call while someone is talking. Tapping into a call would be covered by the ECPA [discussed below] and other wiretapping statutes. Although employers are permitted to record employee phone calls, most employers usually do not record every call. Rather, employers usually record only calls needed for business purposes. In New York, only one party on a phone call needs to consent to the recording of the call. If employers record calls, they need to make sure their employees are informed. These New York state laws are criminal laws that do not provide for a private cause of action by employees."

Weiss also addressed employer access to employee social media websites, noting that various states have either adopted or considered statutes prohibiting employers from requiring employees to turn over usernames and passwords to social media websites. Weiss noted that New York has considered but not yet adopted such a law. Michael McNamara, a partner at Seward & Kissel LLP, indicated that New Jersey has adopted such a law. Richard Rabin, a partner at Akin Gump Strauss Hauer & Feld LLP, addressed California's efforts in this area, and highlighted the ability of state privacy statutes to conflict with federal mandates. "When California took up legislation on a password protection law," Rabin related, "FINRA wrote a letter to the California state legislature urging it to include an exemption for FINRA-regulated entities that have an obligation to monitor, supervise and maintain business-related records. California refused this request, and instead enacted the law as written, without any such exemption. So you get into these conflicts where a federal law will say one thing and the state law will say another. FINRA-regulated entities can argue that the federal law pre-empts the state one, but who wants to be in litigation arguing such issues?" See "Understanding the Regulatory Regime Governing the Use of Social Media by Hedge Fund Managers and Broker-Dealers," The Hedge Fund Law Report, Vol. 5, No. 47 (Dec. 13, 2012).

Kelli Moll, a partner at Akin Gump Strauss Hauer & Feld LLP, particularized the challenge of reconciling conflicting state and federal law in this area, explaining, "it is hard to monitor something that you have no access to. Often in the securities business, you have a personal trading policy prohibiting employees from trading in names in which funds are invested. The SEC expects you to be able to monitor and test whether you have actual compliance with such a policy, which typically involves getting brokerage statements and having somebody (often the CCO) review them for

The HedgeFund LAW REPORT
The definitive source of actionable intelligence on hedge fund law and regulation
www.hflawreport.com Volume 7, Number 14 April 11, 2014

any trading in fund positions that are in violation of the policy. It's a real tension if you have a policy prohibiting use of personal devices to conduct firm business and a related obligation to monitor compliance with the policy, but at the same time a law prohibiting access to personal devices. With a law like California's, this tension is especially pronounced." See "Key Legal and Operational Considerations for Hedge Fund Managers in Establishing, Maintaining and Enforcing Effective Personal Trading Policies and Procedures (Part Three of Three)," The Hedge Fund Law Report, Vol. 5, No. 6 (Feb. 9, 2012).

Federal Law

As employers, hedge fund managers should be cognizant of at least three federal statutes bearing on employee privacy rights.

First, as indicated in the first article in this series, managers should be aware of the Computer Fraud and Abuse Act (CFAA). In particular, managers should conduct their electronic communications monitoring activities in a manner consistent with the CFAA, and should consider the CFAA among other claims or recommendations to prosecutors in the event of theft of trade secrets. 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).

Second, managers should understand the Electronic Communications Privacy Act of 1986 (ECPA) and – more importantly – the broad exceptions to the ECPA. The ECPA generally makes it a crime to intercept e-mail, phone communications and other electronic communications without appropriate authorization. However, Chinn identified two broad exceptions to the ECPA of particular relevance to hedge fund managers. "The first is business use, or business extension, as it is called under the statute. The business extension exception basically means that an employer can monitor communications if it does so in the ordinary course of business using a qualified device, as defined in the statute and the cases. There is also an exception called the service provider exception, which basically permits an employer that is providing wired or electronic communications to retrieve information maintained on that entity's system to protect that entity's own property rights. For the most part, when an employer is monitoring communications of employees made on the employer's systems, the ECPA is not going to prohibit that monitoring largely because of these two broad exceptions." Laverriere added that hedge fund managers can mitigate the likelihood of violating the ECPA by clarifying in policies, procedures, training and other communications with employees that the manager monitors employee communications in the ordinary course of business.

Third – and outside the historical ambit of relevant considerations – hedge fund managers should be cognizant, qua employers, of the National Labor Relations Act (NLRA). Rabin, of Akin Gump, explained, "About five years ago, I don't think anyone thought of the NLRA as a law that had particular relevance to the hedge fund community. People thought about it as applying to union organizing efforts at retail, manufacturing and other industrial establishments. But in its decisions, the National Labor Relations Board (NLRB) has suggested that non-supervisory employees have the right to use social media for concerted protected activities, and the NLRB has been extremely broad in what it views as protected." Rabin continued by identifying two specific concerns for hedge fund managers. "One is the whole issue of

The HedgeFund LAW REPORT
The definitive source of actionable intelligence on hedge fund law and regulation
www.hflawreport.com Volume 7, Number 14 April 11, 2014

surveillance. The NLRB has stated that social media policies should not suggest to employees that their employer is peering over their shoulders. In the NLRB's view, this would have the effect of 'chilling' union organizing efforts or other protected activity. So while monitoring and recordkeeping efforts likely are required under the Advisers Act, these activities pose a potential risk for hedge fund managers under the NLRA. Second, there's the separate issue of the content of employer social media policies, and what policies may violate the NLRA. For example, many managers have policies stating that if employees use social media for recreational purposes, they can't mention their affiliation with the firm, comment on the firm or comment on the employees' activities for the firm. Managers have these policies to ensure that employees don't make misleading or otherwise improper statements online, breach confidentiality or otherwise put the firm at risk. But the NLRB would probably find such a policy unlawful because it may 'chill' the right of non-supervisory employees to engage in concerted protected activities. The NLRB would liken such a policy to banning employees from using picket signs to protest over a particular issue." See "How Can Fund Managers Address the Regulatory, Compliance, Privacy and Ethics Issues Raised by Social Media?," The Hedge Fund Law Report, Vol. 5, No. 44 (Nov. 21, 2012).

Proskauer's Chinn offered thoughts to hedge fund managers on how to anticipate and address the NLRB's concerns. "From the NLRB's perspective, there are some emerging thoughts around what employers can do to avoid running afoul of the NLRB's concerns about social media policies. If you had to boil it down to just a couple of statements, what the NLRB is looking for is that the employer be as specific as possible as to the kind of conduct or statements it is prohibiting on social media, and to give examples of that conduct. For example, the NLRB views mere prohibition of discussing anything that is 'confidential' as being potentially overbroad. The NLRB will say the mere restriction on discussing confidential or nonpublic information on social media is overbroad. However, the NLRB has also said that a specific restriction on revealing things like trade secrets or private and confidential information, or a restriction that uses descriptive language around the particular kinds of information that you are specifically prohibited from discussing in social media, would be acceptable. Those are some broad guidelines for having a social media policy that doesn't run afoul of the NLRB's concerns."

The methods of addressing the NLRB's concerns identified in the preceding paragraph appear to be consistent with existing SEC guidance on social media use by hedge fund managers. See "SEC Risk Alert Discusses When Social Media Interactions May Constitute Prohibited Hedge Fund Client Testimonials," The Hedge Fund Law Report, Vol. 5, No. 14 (Apr. 5, 2012). However, in the event that the concerns or compliance expectations of those authorities diverge, sources agree that hedge fund managers would be better served by complying in the first instance with SEC guidance. As Chinn explained, "This is a place where there are some conflicting values at stake. If you have a situation where you have an obligation imposed by the SEC, and that obligation clashes with a common law privacy interest or the NLRB's viewpoint, most regulated employers are going to take the view, 'Look, if I'm required to do this by the SEC, I'm going to in the first instance adhere to that obligation and worry secondly about whether there is a privacy concern at stake.' The argument would be that any privacy or NLRB-related rights would be overshadowed by the compelling interest in complying with applicable securities regulations."

The HedgeFund LAW REPORT
The definitive source of actionable intelligence on hedge fund law and regulation
www.hflawreport.com Volume 7, Number 14 April 11, 2014

Fourth Amendment

The Fourth Amendment is not directly applicable to hedge fund managers because they are private employers rather than government employers. Nonetheless, McNamara, of Seward & Kissel, noted that hedge fund managers have been looking to Fourth Amendment jurisprudence in ascertaining what constitutes a reasonable expectation of privacy, and how to balance an employer's need for information with an employee's right to privacy. The thrust of the case law in this area is that hedge fund manager employers play a fundamental role in defining the reasonableness of privacy expectations. In other words, reasonableness here is not solely a function of observing the behavior of a large group, as it is in other tort contexts, but rather of how a hedge fund manager describes its policies and procedures to its employees. By analogy, you cannot move the bar of reasonableness by describing your driving habits to the local Department of Motor Vehicles or to passengers in your car. But you as a hedge fund manager employer can raise the bar of reasonableness by clearly communicating to employees that you continuously monitor all e-mails, chats and other communications, and that employees should not expect any privacy in electronic communications over desktop or 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).

McNamara elaborated: "The Supreme Court had the opportunity a few years ago in *Ontario v. Quon*, 130 S. Ct. 2619 (2010), to deal with this issue. It was a Fourth Amendment case and it involved a dispute over the review of alphanumeric texts that had been created by an employee on an employer-owned device. After an investigation in which the transcripts of the device were reviewed as part of a routine audit, the employer discovered that a lot of the employee's texts were sexual in nature, and he was disciplined for it. The employee alleged a violation of the Fourth Amendment, and the case ultimately worked its way up to the Supreme Court. Employment lawyers were expecting some guidance on the issue of an employee's reasonable expectation of privacy. Ultimately, the Supreme Court made it clear that it was reluctant to delve into the issue; that things were changing very quickly, technology was changing, society's expectations were changing and that what is a reasonable expectation of privacy was something that they didn't want to define at that point because they were concerned that it would have far-reaching implications."

However, McNamara added, "in *Quon*, Justice Kennedy specifically discussed cell phones and text message communications. There is an interesting sentence in the opinion about how some people may consider them essential means or necessary instruments for self-expression or self-identification. Then he talks about employer policies shaping the reasonable expectations of employees, especially to the extent that such policies are clearly communicated. It's likely that those kinds of factors and considerations will play out in litigation involving the reasonable expectation of privacy – the type of device, the nature of the communication and the clarity of the employer's policies – and certainly it is important for employers to consider all of that as they're thinking about these issues and the right balance between the employer's need to monitor, on the one hand, and the employee's reasonable expectation of privacy, on the other hand."

The HedgeFund LAW REPORT
The definitive source of actionable intelligence on hedge fund law and regulation
www.hflawreport.com Volume 7, Number 14 April 11, 2014

European Law

Hedge fund managers – especially those with offices, employees, affiliates, investments or investors in the E.U. – should be conversant with at least two categories of European authority bearing on employee privacy: the Data Protection Directive and the E.U. Convention on Human Rights. "Both impact the ability to monitor and record employee activities," noted Sam Whitaker, counsel at Shearman & Sterling LLP in London. "Above and beyond that, each individual European member state often has its own additional legislation about potential criminal sanctions for unlawfully intercepting communications. In the U.K., we have additional legislation that makes it unlawful in certain circumstances and indeed a criminal offense to unlawfully intercept or monitor certain communications. Again, there is a fairly wide carve out where you get consent from the individual and you have notified the individual previously in writing that monitoring and interception may be carried out. This underlines the importance of having proper policies and procedures in place."

With respect to the Convention on Human Rights, Whitaker elaborated, "The basic principle is that the individual has a right to privacy and a private life. Although it doesn't go all the way, the way to counter that in the workplace in the context of employee monitoring would be to put in place proper policies and consents so that you effectively make clear to employees that there is no expectation of privacy within the use of e-mail and telephones. It's not an absolute answer in terms of European legislation because the courts and regulators would still expect the employer to carry out monitoring in a proportional way, so that you're not doing it randomly but only to the extent necessary, and for specific purposes. But a basic starting point is to make sure you've got the policies and the consent in place so there is no expectation of privacy."

And with respect to the Data Protection Directive, Whitaker cautioned, "One of the most difficult issues from the European Data Protection Directive relates to the transfer of personal data outside of the European Economic Area, because the Directive includes very tight restrictions on the extent to which such personal data can be transferred. In practice, people breach it all the time because they're not particularly aware of it, but the restrictions are nonetheless in place and may at some point be more vigorously enforced. It is standard practice in policies and contracts to try and deal with that issue by getting upfront consent from employees to transfer personal data outside of Europe." See "Four Imminent Changes to E.U. Data Protection Laws of which Private Fund Managers Should Be Aware," The Hedge Fund Law Report, Vol. 7, No. 12 (Mar. 28, 2014).

Reconciling Conflicting Laws and Practices

Three broad themes emerge from the foregoing discussion. First, there is no single source of authority governing employee privacy and employer obligations. Rather, authority in this area derives from a patchwork of sources. Second, those sources are often conflicting. Third, employers have some influence over the reasonableness of employee expectations.

Three suggested best practices emerge from the foregoing three themes. First – paraphrasing a suggestion made above in the discussion of the NLRA – in the event of a direct

The HedgeFund LAW REPORT
The definitive source of actionable intelligence on hedge fund law and regulation
www.hflawreport.com Volume 7, Number 14 April 11, 2014

conflict between securities and non-securities regulation, hedge fund managers would typically be better served by complying with securities regulation. As Rabin advised, "Managers should ensure their compliance with the Advisers Act first, and then turn to other state and federal statutes, including the NLRA and state laws, and determine how they can best comply. The legal landscape will depend on such issues as where a firm is located, its size, its employees' usage of social media and its lines of business. There will not be a cookie-cutter approach, and at the end of the day, managers whose employees use social media will take some degree of risk, because it will be impossible to simultaneously comply with the letter of all these conflicting laws." As a practical matter, however, best compliance practices for relevant securities and non-securities (e.g., labor) regulation appear at present to be consistent with one another.

Second, for hedge fund managers, state privacy law is the general principle and federal law is the specific exception. In other words, employee privacy rights and employer obligations with respect to privacy are primarily governed by state law. As O'Brien explained, "Fundamentally, managers should look to the state law of the state in which they are doing business. A lot of hedge fund managers are Delaware LLCs or Delaware LPs, but they're doing business in the state of New York or in the state of Connecticut. So they are going to look fundamentally to New York or Connecticut state law for privacy, but then federal law for specific applications, such as review of the ECPA or the CFAA. So there is an interrelationship there, but fundamentally privacy law is going to be state-law driven in the first instance and secondarily driven by federal statutes."

Third, managers should communicate clearly and unambiguously with employees regarding their monitoring of electronic communications. Doing so will appropriately set expectations, and adjust the contours of reasonableness in a manner that redounds to the employer's benefit. Rabin advised, "Particularly given the conflicts between existing laws, and the impossibility of complying with all such laws, managers should cut square corners in this area. They should have clear written policies regarding their compliance obligations, their recordkeeping practices and their monitoring of employees' use of company devices and systems, and they should alert employees that they should have no expectation of privacy in engaging in these activities. Firms should strongly consider getting employees to sign these policies, indicating their understanding and consent. That way, employees are duly informed of the rules ahead of time, and the manager best positions itself for any future dispute." McNamara agreed, and emphasized the importance of going beyond the default rules: "In advising an employer, we would never assume, just because it's a workplace computer, that therefore all the information on it belongs to the employer and there is no reasonable expectation of privacy. We recommend that employers make it clear to their employees that these computers are company property, that any e-mail used on the computer is company property, that there is no expectation of privacy and that the company reserves the right to monitor that information with or without notice – in part because the state of the law is uncertain and we want to minimize potential issues. It's not so obvious that if you provide an employee with a BlackBerry or an iPhone that the employee then uses at least in part for personal use, that it is completely the company's property. So making that clear and giving people notice is important."