Hedge Funds Luncheon Series:

Ethics and “Bet-the-Company” Scenarios: When Conflicts and Misconduct Involve More than Just Legal Issues

Robert Leonard
Michael Mavrides
Christopher Wells
William Komaroff
Samuel Waldon
Hadassa Waxman

Proskauer

May 1, 2019

Scenario 1

Susan is GC/CCO of Big Asset Management LP. Friday afternoon at 4:00, John, who works in the Finance Department, walks into Susan's office and says "I need to talk to you. I have been looking at some of the indicative quotes that we receive back from brokers for certain non-traded or thinly traded securities, and I think that Trader Joe (one of the portfolio managers/traders) has been pre-populating indicative quotation forms with suggested valuations before sending them to the brokers, and that some of the valuations are very questionable."

Q: What should Susan think about (other than why this is happening on a Friday at 4:00) and what should she do first?

Scenario 2

Same facts, but John also says that he thinks that Mr. Big (the principal portfolio manager and principal owner of Big Asset Management LP) is aware of Trader Joe's activity, may have instructed Trader Joe what to do, and may have spoken to the brokers to arrange the misleading quotes.

Q: Does this change the analysis?

Scenario 3

Same as #2, but at the beginning of the conversation, John asks Susan to keep the information that he is about to provide confidential, and not to disclose to Mr. Big that John was the source of the information.

Q: Can/should Susan agree?

Scenario 4

Same as #1, but John says that Mr. Big told him that Mr. Big received non-public information about Company X at a cocktail party from a social acquaintance who is a senior executive of Company X, and who said something unintentional about next quarter's earnings after his fourth cocktail. John also knows that Trader Joe placed a large order to buy Company X stock at about the same time. But John does not know whether Mr. Big and Trader Joe spoke to each other, and Trader Joe has authority to trade stocks in his book independently of Mr. Big.

Q: How does this change the analysis? Does the nature of the possible violation (insider trading) (and possible defenses) change anything?

Scenario 5

Same as #4, but on Monday morning Susan receives a phone call from an attorney at the SEC and an attorney at the US Attorney's Office SDNY asking about the firm's trades….(?)

Q: What should Susan do?

Scenario 6

Same as #1, but after conducting an internal investigation (with the assistance of a supremely qualified law firm like Proskauer), Susan has now determined that Mr. Big did in fact conspire with brokers to produce false quotes for certain illiquid securities.

Q: What must Susan report and to whom?

Scenario 7

Same as #1, but John asserts that Mr. Big was using his company credit card to pay certain entertainment expenses unrelated to the business, and instructed John to charge the expenses to client accounts.

Q: Does that change the analysis?

What to do When the Government Shows Up at Your Door with a Search Warrant

Law enforcement continues to make use of search warrants in white collar cases. While we hope that you are never confronted with this situation, it is important to be prepared. The risks and anxiety associated with law enforcement searches can be minimized by taking certain steps – if and when you get that knock on the door.

First and foremost, deal with law enforcement in a professional and courteous manner. Do not obstruct the search or be confrontational in any way and make sure that employees do the same. Initiating the following steps as soon as law enforcement arrives at the door will minimize disruption to the company and help protect the company's rights.

On Arrival

- Designate a senior management employee as the initial point of contact with law enforcement and immediately contact the General Counsel and outside counsel, preferably criminal defense counsel. (Robert Leonard w: 212-969-3355, c: 914-419-9774 or rleonard@proskauer.com; Michael Mavrides w: 212-969-3670; c: 917-838-8026 or mmavrides@proskauer.com; Christopher M. Wells w: 212-969-3600; c: 917-374-5875 or cwells@proskauer.com; William Komaroff w: 212-969-3975, c: 917-721-8949 or wkomaroff@proskauer.com; Samuel Waldon w: 202-416-6858; c: 202-492-8118 or swaldon@proskauer.com; Hadassa Waxman w: 212-969-3040; c: 646-823-4016 or hwaxman@proskauer.com)
- Ask who the lead investigator is, request to see credentials of agents, keep a list of government officials participating in the search, and ask for the name of the prosecutor in charge of the investigation so that counsel can contact him/her.
- Request that law enforcement wait to begin the search until counsel arrives. Note, however, that law enforcement may decline this request.
- Accompany law enforcement to a conference room that will serve as a central location where counsel and/or the senior management person can talk to law enforcement away from other employees.
- Request and make a copy of the search warrant. Review it carefully so that you understand precisely what the government is looking for and where they are allowed to look for it. Remember that law enforcement can only search the areas authorized under the warrant and seize property identified in the warrant.
- The search is likely to disrupt the work day. A senior management employee may wish to instruct employees who are not essential to facilitating the search, customers, contractors and any other third parties to exit the premises before the search begins.

Understand Your Rights

- Ask the lead investigator to explain the purpose, scope and legal basis for the search, to identify the entities or employees who might be subject to search or interview, and to explain the anticipated search protocol. Note that law enforcement agents are not required and are unlikely to provide information not contained in the search warrant.

- Object to the seizure of any documents written to or by in-house or outside counsel. Those materials are most likely confidential and protected from disclosure by the attorney-client privilege. Law enforcement may search and seize property despite an objection to scope or assertion of the attorney-client privilege. If law enforcement seizes the items in question, contact counsel immediately and make a written note of the objection, law enforcement's response and the item(s) seized.
- If law enforcement does not have a copy of the search warrant or order or refuses to provide it, consult with counsel immediately. Do not orally consent to the search or sign any document consenting to a search without consulting with counsel. Likewise, you do not have to consent to expansion of the search beyond the warrant. If met with resistance, any such request should be immediately referred to the counsel before access is permitted (but understand they may not listen to you). Note that there are different rules in different jurisdictions regarding this issue.
- Law enforcement may request to interview employees. It is the employee's decision whether to respond to law enforcement questions. In making that personal decision, employees should be aware that they are not required to answer questions asked by law enforcement during the search. Employees who choose to answer law enforcement questions are not required to answer all questions; they have the right to end the interview at any time or to answer only some questions and not others.
  - If an employee is questioned by law enforcement during the search, the company may provide a lawyer to assist the employee in that interview. If questioned by law enforcement during the search and the employee would like representation by counsel, the employee should politely explain to law enforcement that he or she would like to consult with a lawyer. The employee may then contact his or her supervisor and the General Counsel.
- Do not obstruct the search or lie to agents – and advise employees of the same.

Documentation

- Counsel should immediately disseminate a written document preservation notice with detailed instructions that, among other things, employees should not destroy, remove, delete, tamper or alter any documents (including electronic files).
- If at all possible, documents and personnel subject to the search should be brought to law enforcement in the conference room. If law enforcement insists on leaving the conference room to search for documents or interview employees, a designated employee should accompany law enforcement, taking careful notes of places searched, items seized, documents requested, and people spoken to.
- Make copies of all seized records. If law enforcement seizes computers, hard drives, external disks or other electronic storage devices, the senior IT administrator should make a digital copy of each item before it is removed from the premises. Law enforcement should generally not be permitted to access the company's computer system. Rather, the accompanying response team member should offer to have digital copies of the information created and a senior IT administrator should be in charge of "imaging" or copying the information.
- As soon as the search is complete and law enforcement has left the company's premises, prepare a detailed report of what occurred.

Contact

Robert G. Leonard
New York
w: 212.969.3355
c: 914.419.9774
rleonard@proskauer.com

Michael F. Mavrides
New York
w: 212.969.3670
c: 917.838.8026
mmavrides@proskauer.com

Christopher M. Wells
New York
w: 212.969.3600
c: 917.374.5875
cwells@proskauer.com

William C. Komaroff
New York
w: 212.969.3975
c: 917.721.8949
wkomaroff@proskauer.com

Samuel J. Waldon
Washington, DC
w: 202.416.6858
c: 202.492.8118
swaldon@proskauer.com

Hadassa Waxman
New York
w: 212.969.3040
c: 917.838.8026
hwaxman@proskauer.com

13

Employee Rights: The US Perspective

Joshua Newville, Seth B Schafler, Harris M Mufson and Susan C McAleavey[1]

Introduction 13.1

Employees facing a corporate investigation have various rights that the corporation and the employees and their counsel should take into account from the moment they are made aware of the possibility of an investigation. This is the case regardless of whether a particular employee is a witness, subject or target. Employee rights also vary based on jurisdiction, the type of company (public or privately held), internal policies, the employee's seniority within the organisation and whether the government is or may be involved.

This chapter provides guidance regarding employee rights in the investigatory context. It highlights the issues and considerations that are unique to individual, rather than corporate, representation. In particular, this chapter addresses: (1) employee rights as provided by an employer and by federal and state law; (2) differences in employee rights in the context of an external (i.e., government-driven) investigation as compared with an internal investigation; (3) representation of individuals; (4) indemnification and insurance coverage for individuals; and (5) privilege issues particular to the representation of an individual.

Practitioners should be aware that this chapter is meant only to be an overview of United States law and that even within the United States, laws and court interpretation of those laws may vary by jurisdiction.

Rights afforded by company policy, manual, contracts, by-laws 13.2

Many companies have policies or guidelines relating to internal investigations, confidentiality, document collection, workplace searches, and/or indemnification,

1 Joshua Newville, and Seth B Schafler are partners, Harris M Mufson is senior counsel and Susan C McAleavey is an associate at Proskauer Rose LLP.

among other areas, in their by-laws, handbooks or other policy documents. Employee contracts or offer letters may likewise contain provisions that pertain to employee rights. These documents should be consulted to determine what rights employees have during an investigation. For example, a company's equal employment opportunity and whistleblower policies typically protect employees from retaliation for participating in an investigation. Other policies provide guidance regarding data collection processes, monitoring of electronic communications, and searches of an employee's property or company-provided devices. In many cases, companies have policies concerning electronic communications or property that permit searches of employee property and workspaces as appropriate. In the absence of written policies, companies may have established processes that, among other things, require an employee to receive notice and to authorise certain types of workplace searches.

Increasingly common sources of information – such as an employee's social media postings, emails, voicemails and internet use, video surveillance and searches of an employee's office, desk and locker – raise special issues regarding employee expectations of privacy. As privacy law continues to develop, counsel should check the status of applicable law.

13.3 Rights afforded by US law

Various federal, state and local laws contain employee protections that can affect the course of an internal investigation. Absent a contractual agreement with an employer, such as a severance agreement, former employees do not have any legal obligation to assist a former employer in an internal investigation. Of course, former employees may be compelled to provide documents or testimony through a subpoena.

13.3.1 The right to be free from retaliation

Certain federal, state and local laws protect employees from being retaliated against for testifying, assisting or participating in an investigation. For example, a number of federal employment laws prohibit retaliation, including, but not limited to, Title VII of the Civil Rights Act of 1964, the Americans with Disabilities Act, the Age Discrimination in Employment Act, the Fair Labor Standards Act, the Family and Medical Leave Act, the National Labor Relations Act, and the Occupational Safety and Health Act.

Several federal statutes have also codified whistleblower protections. The Sarbanes-Oxley Act of 2002 (SOX) prohibits retaliation against whistleblowers who (1) provide information to or otherwise assist in an investigation by a federal regulatory or law enforcement agency, any member of Congress, or any person with supervisory authority over the employee regarding any conduct that the whistleblower reasonably believes constitutes mail, wire, bank or securities fraud, a violation of any rule or regulation of the SEC or any federal law relating to fraud against shareholders, or (2) file, testify, participate in, or otherwise assist in a proceeding filed relating to alleged mail, wire, bank or securities fraud, violation of any rule or regulation of the SEC or any federal law relating to fraud against

shareholders.[2] The Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act)[3] created new anti-retaliation provisions for whistleblowers. Specifically, Section 922 of the Dodd-Frank Act provides anti-retaliation protections for whistleblowers who report possible securities law violations to the SEC.[4] Similarly, Section 748 of the Dodd-Frank Act,[5] amended the Commodity Exchange Act by establishing anti-retaliation protections for whistleblowers who report violations of the Commodity Exchange Act to the Commodities Futures Trading Commission (CFTC). In addition, the Consumer Financial Protection Act of 2010 (CFPA)[6] prohibits retaliation against employees for raising concerns about any violation of the CFPA that is subject to the jurisdiction of the Consumer Financial Protection Bureau.

The Dodd-Frank Act does not expressly authorise the SEC and CFTC to pursue anti-retaliation claims on behalf of whistleblowers. However, both agencies have adopted rules vesting themselves with authority to pursue enforcement actions.[7] In 2014, the SEC pursued an enforcement action against a registered investment adviser that allegedly removed a head trader from its trading desk and stripped him of his day-to-day trading and supervisory responsibilities after the company learned that the trader had made disclosures to the SEC.[8] The company settled the action only after agreeing to pay disgorgement of US$1.7 million, prejudgment interest of US$181,771 and a civil penalty of US$300,000.[9]

State and local fair employment practices laws may also contain anti-retaliation provisions.[10] These provisions sometimes can provide more robust employee protections. For example, following 2009 amendments, the Illinois Whistleblower Act now prohibits an employer from not only retaliating against an employee, but

---

2 18 U.S.C. Section 1514A.

3 12 U.S.C. Section 5301.

4 These provisions are codified in § 21F of the Securities Exchange Act of 1934, 15 U.S.C. § 77a (SEA). Courts are currently split about whether an individual must complain to the SEC to be covered by the anti-retaliation provision in the SEA. Whereas the Fifth Circuit has held that only individuals who provide information to the SEC are 'whistleblowers' the Second and Ninth Circuits have extended the anti-retaliation protection to individuals who have raised concerns about securities laws violations internally to their employers. Compare *Asadi v. G.E. Energy, LLC*, 720 F.3d 620 (5th Cir. 2013) with *Berman v. Neo@Ogilvy LLC*, 801 F.3d 145 (2d Cir. 2015); *Somers v. Digital Realty Trust*, 850 F.3d 1045 (9th Cir. 2017) (on appeal to the US Supreme Court, October term 2017, Dkt. No. 16-1276).

5 7 U.S.C. § 26.

6 Codified as § 1057 of the Dodd-Frank Act.

7 See 17 C.F.R. §240.21F; 17 C.F.R. § 165.20 and Appendix A.

8 See In re Paradigm Capital Mgmt., Inc., Exchange Act Release No. 72,393, Investment Advisers Act Release No. 3857 (16 June 2014).

9 Id.

10 See California Whistleblower Protection Act, Cal. Labor Code §§1102.5 to 1105; Florida Private Sector Whistleblower Act, Fla. Stat. Ann. § 448.102; Hawaii Whistleblowers Protection Act, Haw. Rev. Stat. § 378-62; Illinois Whistleblower Act, 740 ILCS 174/20.2; Maine Whistleblower's Protection Act, Maine Law Tit. 26 M.R.S.A. § 839; New Jersey Conscientious Employee Protection Act, N.J.S.A. §§ 34:19-1-34:19-8.

also threatening to retaliate against an employee if the act or omission threatened would constitute retaliation under the Act.[11]

13.3.2 The right to disclose – prohibiting blanket confidentiality restrictions during an investigation

13.3.2.1 A whistleblower's right to disclose violations of law

Following the passage of the Dodd-Frank Act, the SEC promulgated a series of rules intended to provide certain protections to whistleblowers. Included among these is SEC Rule 21F-17, which prohibits any person from taking "any action to impede an individual from communicating directly with the Commission staff about a possible securities law violation, including enforcing, or threatening to enforce, a confidentiality agreement . . . with respect to such communications."[12] In other words, companies subject to the SEC's jurisdiction may not take actions that prevent individuals, whether current or former employees, from reporting potential violations of securities laws to the SEC.

This rule has been broadly interpreted by the SEC and has resulted in several SEC enforcement actions. For example, in April 2015, the SEC settled an action against a company that had required employees to sign a confidentiality statement at the beginning of witness interviews conducted in the course of the company's internal investigations. The confidentiality statement 'prohibited [employees] from discussing any particulars regarding [the] interview and the subject matter discussed during the interview, without the prior authorization of the Law Department' and subjected employees to disciplinary action if they made unauthorised disclosures. Although the statement did not specifically reference reports to the government, the SEC concluded that the statement could have a chilling effect on employees considering making such reports.[13] The SEC has more recently penalised other employers who, in the SEC's view, adopted policies that could have a chilling effect on potential whistleblowers.[14]

The CFTC recently amended its whistleblower rules to conform with the SEC's rules. Specifically, the CFTC's rules now empower the agency to pursue anti-retaliation claims on behalf of whistleblowers and prohibit the use of

11 740 ILCS 174/20.2.

12 17 C.F.R. § 240.21F-17 (2011).

13 See *In re: KBR, Inc.,* Exchange Act Release No. 74619 (1 April 2015)

14 See *In re: BlueLinx Holdings Inc.,* Exchange Act Release No. 78528 (company assessed US$265,000 penalty based on restrictive severance agreements) (10 August 2016); *In re: Health Net, Inc.*, Exchange Act Release No. 78590 (company assessed US$340,000 penalty based on restrictive severance agreements) (16 August 2016); *In re: NeuStar, Inc.*, Exchange Act Release No. 79593 (company assessed US$180,000 penalty based on restrictive severance agreements) (19 December 2016); *In re: Sandridge Energy, Inc.*, Exchange Act Release No. 79607 (company assessed US$1.4 million penalty based on restrictive separation agreement) (20 December 2016); *In re: BlackRock, Inc.*, Exchange Act Release No. 79804 (company assessed US$340,000 penalty based on restrictive separation agreements) (17 January 2017) and *In re: HomeStreet Inc.*, Exchange Act Release No. 79844 (company assessed US$500,000 penalty based, in part, on a restrictive severance agreement) (19 January 2017).

confidentiality agreements and pre-dispute arbitration agreements that impede a whistleblower's communications with the CFTC.[15]

An employee's right to discuss the terms of employment 13.3.2.2

An employee's counsel should also be mindful of employee rights under the National Labor Relations Act, which protects the right of all non-supervisory employees (regardless of whether they are a member of a union) to discuss with co-workers discipline or ongoing disciplinary investigations involving themselves or fellow employees. The National Labor Relations Board (NLRB) has held that an employer may not give a generalised confidentiality instruction to witnesses in an investigation to protect the integrity of the investigation. Rather, an employer must first determine case by case whether in any given investigation, (1) witnesses need protection; (2) evidence is in danger of being destroyed; (3) testimony is in danger of being fabricated; or (4) there is a need to prevent a cover-up.[16] The DC Circuit Court of Appeals recently declined to address the NLRB's 'requirement of a case-by-case approach to justifying investigative confidentiality.'[17]

The right to representation 13.3.3

Legal representation 13.3.3.1

Generally, employees do not have a *per se* right to legal representation during an internal investigatory interview. However, employees may choose to obtain their own legal representation in an internal investigation. This is particularly the case when, among other things, employees have concerns that they may face personal legal risk (civil or criminal) as the result of an investigation, that their employment may be at risk, that the government may be involved or interested in the investigation, or where there may be a conflict between themselves and the company or their supervisors. As described in Section 13.4, the need for individual representation has become all the more acute given the United States Department of Justice's recent emphasis on prosecuting individuals in white-collar criminal cases.

Attorneys conducting the investigation generally may not speak to any witness represented by counsel in connection with the subject of the investigation without permission from the witness's counsel.[18]

15 17 C.F.R. § 165.20 and Appendix A.

16 See *Banner Health Sys.*, 362 N.L.R.B. No. 137, *3 (2015), aff'd in part 851 F.3d 35 (D.C. Cir. 2017).

17 *Banner Health Sys. v. N.L.R.B.*, 851 F.3d 35, 44 (D.C. Cir. 2017).

18 See Model Rules of Prof'l Conduct R. 4.2 ('In representing a client, a lawyer shall not communicate about the subject of the representation with a person the lawyer knows to be represented by another lawyer in the matter, unless the lawyer has the consent of the other lawyer or is authorised to do so by law or a court order.')

13.3.3.2 Separate representation and pool counsel

Whether the company will agree to arrange for separate representation involves analysis of contractual and other indemnification rights and potential conflicts of interest. For current or former senior officers and directors, advancement or indemnification of defence costs may be required by corporate by-laws or employment agreements (see Section 13.6). Costs may or may not be covered by insurers, depending on the terms of the relevant policies and the status of the investigation (see Section 13.6.1.2). Legal costs incurred in an internal investigation are often outside the scope of coverage.

Arranging for separate counsel for employees may benefit the entity in terms of co-operation credit with the government. The employees are protected by separate representation that is bound to act in their best interests. The entity may have greater credibility when reporting results of any inquiry if representation has been bifurcated.

In some circumstances, corporate entities arrange for 'pool counsel' to represent groups of current or former employees, to the extent they do not have conflicting interests. This arrangement can lead to reduced costs and greater efficiencies, and may facilitate information flow for the benefit of clients within the pool. However, if a conflict exists or arises between employees, the adverse client may have to be removed from the pool representation, or counsel may have to withdraw.[19]

13.3.3.3 Upjohn warnings

When investigatory interviews are conducted by company counsel (internal or external), *Upjohn* warnings, also known as corporate *Miranda* warnings, should be provided to employees by company counsel at the beginning of each interview. Derived from the United States Supreme Court case *Upjohn Co v. United States*,[20] an effective *Upjohn* warning puts the employee on notice, at a minimum, that: (1) the company's counsel (whether in-house or outside counsel) represents the company and not the employee being interviewed and, as such, an attorney–client relationship has not formed with the investigating attorney; (2) facts are being gathered to provide legal advice to the company; and (3) the investigation is confidential and covered by the attorney–client privilege but, critically, that the privilege belongs solely to the organisation and not to the employee, and the company may decide to waive the privilege and disclose the discussion to a third party, such as the government, without notifying the employee. Employees should also be given an opportunity to ask questions about the *Upjohn* warning and about the investigating attorney's role.

Upjohn warnings commonly include a request by company counsel to keep the discussion during the interview confidential. When giving *Upjohn* warnings, however, companies should *not* suggest that employees are prohibited from discussing

19 See ABA Model Rules, Rule 1.7, Comment 4.

20 *Upjohn Co. v. United States*, 449 U.S. 383 (1981).

the underlying facts with the government, as noted in the discussion above regarding SEC Rule 21F-17, or with the employee's own lawyer (see Section 13.3.2.1).

Similarly, employees and counsel representing employees should be aware of the NLRB's restriction on blanket confidentiality directives and its requirement that counsel be able to articulate how any of *Banner Health*'s four accepted bases for confidentiality apply to the particular investigation (see Section 13.3.2.2).

Counsel may consider providing *Zar* warnings to employees,[21] stating that information they provide may be turned over to the government, and that the employee could be prosecuted for possible obstruction charges if false information is provided. In a handful of cases, the government has successfully brought obstruction of justice charges based on misleading statements during the course of internal investigations, under the theory that the individual knew that the misleading information would be provided to the government. *Zar* warnings are not required by law. They are generally provided in the interest of fairness to the employee, taking into account the DOJ's focus on individuals. However, counsel must weigh the potential chilling effect on free flow of information as a result of the warning, as well as the risk that the government may later view the company as having 'overwarned' its employees.

Weingarten rights 13.3.3.4

Union-represented employees have a right to a union representative when questioned during an investigation if the investigation could lead to disciplinary action.[22] However, an employer is not obligated to inform an employee of his or her Weingarten rights or to ask whether an employee would like to have a union representative present at a meeting or interview. An employee who wishes to have union representation must affirmatively make such a request.[23]

The right to privacy 13.3.4

An employee's activities while using an employer's computer system are largely unprotected by personal privacy laws. Documents stored on an employee's work computer are generally considered to be company property, and many employers adopt written policies expressly stating that internet activity and emails sent or received on the employer's computer systems are not private and may be reviewed. Nevertheless, federal and state laws may be implicated in the collection of data and certain information that may be viewed as personal and private. For example, in *Stengart v. Loving Care Agency*,[24] the Supreme Court of New Jersey held that an employee could have reasonably expected that email communications with her lawyer through her personal, password-protected, web-based email account would remain private, and that sending and receiving them using a company laptop did not eliminate the attorney–client privilege.

---

21 *United States v. Zar*, No. 04-331 (ILG) (E.D.N.Y. 8 April 2004).

22 See, e.g., *NLRB v. J. Weingarten, Inc.*, 420 U.S. 251 (1975).

23 Id. at 257.

24 *Stengart v. Loving Care Agency, Inc.*, 990 A.2d 650 (N.J. 2010).

13.3.4.1 Recorded calls

States have enacted varying laws regarding listening to and recording phone calls. Forty-nine states have enacted legislation making certain kinds of electronic surveillance illegal. Ten states have laws that require the consent of all parties to a phone call or conversation in order for the conversation to be legally recorded. These are often referred to as 'two-party' consent states and include California, Connecticut, Florida, Illinois, Maryland, Massachusetts, Montana, New Hampshire, Pennsylvania and Washington.[25] The other states with surveillance laws generally require the consent of only one party for surveillance to be legal. In other words, in these states a person can lawfully record a conversation that they are a party to without informing the other party.[26]

Employers should also be mindful that the NLRB has held that a company policy prohibiting workplace recordings may unlawfully interfere with the rights of employees to engage in concerted activity regarding their terms of employment.[27]

13.3.4.2 Social media

With the advance of technology, many companies conduct searches of social media as part of an internal investigation. Similarly, certain social media activity of an employee may prompt a corporate investigation. The search and review of social media communications and postings can implicate various privacy laws. Numerous states have enacted laws restricting employers from requesting social media passwords, requiring employees to access social media in the employer's presence or requiring employees to divulge personal social media.[28] While some states have some exceptions for investigations of employee misconduct, requiring employees to provide their employers with the login information for their social media accounts is generally always prohibited.[29] There are also laws that restrict

---

25 Cal. Penal Code § 632 (a)-(d) ; Conn. Gen. Stat. Ann. § 52-570d Fla. Stat. Ann. §§ 934.01 to .03; 720 Ill. Comp. Stat. ANN. § 5/14-1, -2 ; Md. Code Ann. Cts. & Jud. Proc. § 10-402 ; Mass. Gen. Laws Ch. 272, § 99 ; Mont. Code Ann. § 45-8-213; N.H. Rev Stat. Ann. §§ 570-A:2 ; 18 Pa. Cons. Stat. §§ 5702, 5704; Wash. Rev. Code §§ 9.73.030 to 9.73.230.

26 See, e.g., Ariz. Rev. Stat. Ann. § 13-3005; D.C. Code Ann. § 23-542(b)(3); N.Y. Penal Law § 250.00(1); N.J. Rev. Stat. § 2A:156A-4(d); Ohio Rev. Code Ann. § 2933.52(B)(4); Tex. Penal Code Ann. § 16.D2(c)(4).

27 *Whole Foods Mkt., Inc. and United Food and Commercial Workers, L. 919 et al.*, 363 NLRB No. 87 (2015), aff'd *Whole Foods Mkt. Group, Inc., v. NLRB*, No. 16-0002-ag, 16-0346, 2017 WL 2374843 (2d Cir. 1 June 2017).

28 See, e.g., Cal. Lab. Code § 980; 19 Del. Code § 709A(b); Md. Code Lab. & Empl. § 3-712(b)(1); Nev. Rev. Stat. § 613.135; N.H. Rev. Stat. § 275:74; 820 Ill. Comp. Stat. § 55/10(b)(1).

29 See, e.g., Cal. Lab. Code § 980 (2012) (employer may require an employee to 'divulge personal social media reasonably believed to be relevant to an investigation of allegations of employee misconduct or employee violation of applicable laws and regulations,' but information must be used solely for the investigation); 820 Ill. Comp. Stat § 55/10 (2012) (employers may require employees to share specific content of personal online accounts (but not username and passwords) that has been reported to the employer for purposes of investigating employee misconduct); Wash. Rev. Code § 49.44.200 (2013) (employer may require an employee to share content (but not the

employers from encouraging an employee to add anyone to the list of contacts for his or her social media account.[30]

Employers who review information on social media sites can also implicate employee protections under the Stored Communications Act (SCA),[31] which prohibits unauthorised access to electronic communication services (ECS). At least one federal court has held that an employee's non-public Facebook posts are covered by the SCA.[32] Accordingly, employees who configure their Facebook and other social media privacy settings to restrict their posts from public access throughout the course of an investigation may benefit from the protections of the SCA. However, because only unauthorised access is prohibited under the statute, simply enhancing privacy settings may not be enough. An employer may be shielded from liability under the SCA if, for example, someone who is Facebook friends with an employee voluntarily provides the employer access to the employee's private posts.[33]

Of course, obtaining information that is available in the public sphere, such as through a Google search, would not typically implicate any laws or violate privacy rights of individuals.[34] Thus, concerns are raised only when an employer is seeking information that is outside of the public sphere or that can be learned only through 'friending' or obtaining access in contravention of privacy settings. Nevertheless, as these laws are evolving, it is critical for counsel to consider the state of local law.

Bring your own device (BYOD) 13.3.4.3

Some companies have BYOD policies to address employee-owned electronic devices that employees use on the job. BYOD policies can take many forms but commonly include an employer's right to access, monitor and delete information from employee-owned devices. These policies can raise employee privacy concerns because while the employee owns the device, the employer will want to maintain a certain degree of control over the use of the device to protect confidential information. When faced with an employer who requests to search an employee's mobile phone, tablet or other device, practitioners should always ensure that these searches conform with company policies and applicable law and are appropriately limited in scope. Consideration should be given to screening and search procedures to maximise location of relevant information and protection of non-relevant personal information.

---

login information) from his or her social media account as necessary to comply with applicable laws or investigate employee misconduct).

30 See, e.g., Col. Rev. Stat. § 8-2-127(2)(a). For example, under these rules, during an investigation, an employer cannot ask or require an employee to 'friend request' another employee on Facebook so that the employer can search through that employee's personal social media account.

31 18 U.S.C. § 2701 (2002), et seq., contained in Title II of the Electronic Communications Privacy Act of 1986, 18 U.S.C. § 2510 (2002), et seq.

32 *Ehling v. Monmouth-Ocean Hosp. Serv. Corp.*, 961 F. Supp. 2d 659, 669-71 (D.N.J. 2013).

33 Id.

34 See, e.g., *Doe v. City of N.Y.*, 15 F.3d 264, 268 (2d Cir. 1994).

13.4 Employee protection in internal versus external investigations

A number of different considerations come into play when an investigation involves – or has the potential to involve – external entities such as the government. In the United States, the Department of Justice (DOJ) has placed an emphasis on prosecuting individuals in white-collar cases. The DOJ has sent a strong message to companies that to obtain cooperation credit from the government in cases involving potential corporate culpability, companies should voluntarily disclose misconduct to the government and co-operate in the government's investigation. The government expects that companies will provide substantial facts regarding individuals potentially responsible for unlawful conduct.

13.4.1 Focus on individuals' conduct in investigations

The DOJ's renewed focus on individuals was recently set out in a memorandum by former Deputy Attorney General Sally Yates in September 2015, the 'Yates Memorandum'. At times, the DOJ may request that a company wait to individual employees until after the government interviews them (a 'de-confliction' request), further highlighting their focus on individual culpability. Counsel for individual employees, therefore, must keep this in mind as they consider the degree and nature of any co-operation with the company's investigation. (See Chapter 10 on co-operating with authorities.)

Employees and their counsel also should be mindful that while individuals have a right under the Fifth Amendment of the United States Constitution not to incriminate themselves, employers can require employees to co-operate fully during an investigation and can discipline or discharge them for failing to do so, even if the employee's basis for refusing to answer a question is self-incrimination.

Similarly employees and counsel should be aware that though company practices or policies may grant employees certain rights or protections in internal investigations, most policies contain a carve-out or other provision for requests from the government or for disclosures otherwise required by law (e.g., when the company is responding to a grand jury subpoena). For example, companies may be required by the government, via a subpoena, to produce personal employee information (e.g., emails, personnel files, telephone records).

13.4.2 The Fifth Amendment and compelled testimony

The Fifth Amendment provides that "[n]o person . . . shall be compelled in any criminal case to be a witness against himself." In *Kastigar v. United States*, the US Supreme Court held that the government can compel testimony from a witness over his or her assertion of the Fifth Amendment only if it grants that witness immunity against direct and derivative use of the compelled testimony.[35] Under *Kastigar*, if an individual's testimony is so compelled, and that individual is later prosecuted for an offence related to that testimony, the government has the 'heavy'

35 406 U.S. 441, 442 (1972).

burden of showing that it 'had an independent, legitimate source for the disputed evidence.'

The *Kastigar* principles also prohibit, in a US criminal prosecution, the direct or indirect use of a compelled statement made by a defendant to a foreign authority. Practitioners should keep in mind, however, that civil regulatory agencies are generally not prohibited from use of foreign compelled testimony. Certain non-US regulators, such as the UK's Financial Conduct Authority (FCA), do not generally allow a witness to assert the right against self-incrimination. Instead, failure to testify can potentially lead to imprisonment, while the compelled testimony is subject to 'direct use' – but not 'derivative use' – immunity.

Whether compelled non-US testimony can be used in a US criminal prosecution was recently addressed by the US Court of Appeals for the Second Circuit in *United States v. Allen*, a case brought in connection with the LIBOR scandal. In *Allen*, the defendants had previously been compelled to testify before the FCA before they were prosecuted in the US. The US Court of Appeals dismissed the defendants' indictment because prosecutors had relied on a witness who had been exposed to (and had read) the defendants' prior compelled statements. The Second Circuit held that the Fifth Amendment's prohibition on the use of compelled testimony applies even when a foreign sovereign has compelled the testimony. The court explained that, when the government makes use of a witness who has been exposed to a defendant's compelled testimony, *Kastigar* requires the government to prove 'that the witness's review of the compelled testimony did not shape, alter, or affect the evidence used by the government.' A generalised denial of taint did not satisfy the government's burden.

Representation 13.5

Need to collect information on behalf of client 13.5.1

Interviewing client 13.5.1.1

Prior to conducting an in-depth interview with an individual client, there are a number of steps counsel may want to undertake to ensure that the meeting is as efficient and effective as possible.

First, where appropriate, practitioners may request a briefing by company counsel about the subject matter, including not only a briefing about the individual client but also about the industry and relevant facts. This can be especially useful when the subject matter relates to a complicated industry or set of facts.

Second, practitioners should ask company counsel for all relevant documents, including documents on which their client appears, such as email correspondence and internal memoranda, as well as other background documents. Many companies will provide such documents.

Third, practitioners should ask the company if their individual client was previously interviewed by the company or any other parties and should request to be briefed on what their client said and to review memoranda drafted in connection with the interview.

Fourth, practitioners should ask their client about any relevant documents that he or she has access to and can provide.

Fifth, practitioners should familiarise themselves not only with documents provided by their individual client and by the company, but also with press reports, pleadings in civil and criminal actions related to the client, and any other relevant sources of information. These documents can be very useful in constructing an outline of topics to review with clients.

Sixth, prior to conducting the initial interview, counsel should construct an outline and, if possible, a chronology to ensure that all relevant topics are covered. This is especially crucial when clients are overseas and available time to conduct the interview is limited.

Finally, as noted in Section 13.5.1.2, if the government is already involved in the investigation and they are aware that counsel has been retained for the client, it may also be wise to speak with the government to understand the client's status as witness, subject or target and the basis for the government's interest. (See also Chapter 10 on co-operating with authorities.)

Interviews themselves should cover a wide array of topics, including the client's background, their knowledge of the matters under investigation, inculpatory and exculpatory information, relevant knowledge of other individuals and the company, among other topics. Clients can also serve as useful experts to help counsel understand the company, the industry, and other pieces of relevant information. The interviews should serve as an opportunity to carefully assess the client's status as a target, subject or witness of the investigation, so as to construct the best strategy for the representation.[36] Counsel should also ask questions that help assess the degree to which the client can provide useful information to the government as part of an overall approach. For example, if a client's conduct is under investigation, counsel should consider with the client whether an appropriate strategy is to position the client as a co-operator against others.

13.5.1.2 Requesting documents and information from:

Employer

As noted, counsel for individuals should ask the company for documents relevant to their client. Companies often amass a significant documentary record as part of their investigation. Counsel, for example, may request that the company provide access to all of the client's emails and any other relevant documents, regardless of whether the client is on the documents. In seeking to understand what that record says about an individual client, practitioners should consider how and whether they can leverage company work-product and thereby create efficiencies.

36 'A "target" is a person as to whom the prosecutor or the grand jury has substantial evidence linking him or her to the commission of a crime and who, in the judgment of the prosecutor, is a putative defendant.' U.S. Attorneys' Manual § 9-11.151. 'A "subject" of an investigation is a person whose conduct is within the scope of the grand jury's investigation.' Id. A 'witness' is someone that the government believes has relevant information but who is not considered to have any exposure in the investigation.

For example, if the company has conducted a comprehensive document review, company counsel can identify a more limited set of key documents, or it can provide all of the individual employee's documents along with coding to help guide individual counsel's review. The sharing of such work-product may warrant entering into a joint defence or common interest agreement with the company, which is discussed in Section 13.5.2.

Law enforcement

If counsel has been contacted by the government in connection with the client, counsel should use the first interaction with the government as an opportunity to ask a number of questions. Counsel, for example, should ask whether the government considers the client to be a witness, subject or target. The status provided by the government will govern the advice that counsel provides to the client going forward. Counsel can request that the government provide a preview of the government's interest in the client. Counsel can ask the government to describe the topics and questions the government would like to discuss with the client. Counsel can also ask the government to provide documents (or a list of documents) that the government would like to review with the client. Other interactions with the government are highly fact- and jurisdiction-dependent. The degree to which the government is willing to share information in advance of an interview often depends on the office investigating the matter and whether it is a domestic or global investigation, among other issues. There are a number of other factors that will go into decision-making regarding future interactions with the government, including whether to agree to an interview at all and how to respond to a grand jury subpoena, among many other things.

Other witnesses (and their counsel)

Other witnesses in the case can also be a useful source of information. If they are represented by their own counsel, the wisdom of entering into a common interest or joint defence agreement should be explored with the other witness's counsel (see Section 13.5.2), depending on the facts or circumstances. If they are not represented, then counsel can contact that witness to ask if they would be willing to meet and answer questions. It is almost always better for such contact to be through counsel and not through the client.

Joint defence agreements 13.5.2

The sharing with a third party of communications or other documents protected by the attorney–client or work-product privilege can, in some circumstances, result in the waiver of those protections. Joint defence agreements (JDAs), whereby parties who share a common legal interest agree to share such communications and documents, can preserve attorney–client privilege and work-product protections and can therefore facilitate the flow of information between parties, creating important efficiencies. For example, a company under investigation by a government agency and an executive of the company may share a common legal

interest. A JDA allows company counsel and counsel for the individual executive to share information with a lessened risk that such sharing would result in a waiver of the attorney–client and work-product protections. However, given the sensitive nature of the activities they govern, JDAs must be approached with care, as the company and executive would be precluded from sharing information that they learn from one another with the government without the consent of the other party.

Counsel should consider whether to enter into an oral or written JDA. There is no requirement that such agreements be in writing. However, written agreements enable all counsel to consider, at the outset, the scope of the agreement, the extent to which the parties truly share a common defence interest, and how shared information will be treated. In a dispute over the existence or scope of the agreement – for example, if a member of the joint defence group subsequently chooses to co-operate with the government – a written agreement can prove valuable. Some courts have expressed a preference for written JDAs if only to ensure that all clients fully understand the implications of the agreement.[37]

It is less common for counsel to enter into a written JDA during the early stages of an investigation, especially if the entity has not determined the scope of the issues and if or how it may seek cooperation credit. However, when the investigation reaches a more defensive posture with the government, written JDAs may be more common. Questions that can be addressed under the terms of a written JDA include the scope of the agreement and the information to be shared, how and whether information can be used between the parties to the agreement if they become adverse, approved uses of information if a party becomes a co-operating witness with the government, and any circumstances under which a party is required to leave the agreement. Often an entity will demand a provision in a JDA that allows it to disclose information to the government to further company interests or meet regulatory or legal obligations. Under those circumstances, a JDA may still be beneficial to an individual, as long as counsel is aware of the risks.

On the other hand, oral agreements have the benefits of convenience – less time negotiating the minutiae of a written agreement to cover scenarios that may never occur – and of not being capable of production in the event they become part of a discovery demand. It is not often that JDAs become the subject of a court challenge, and many practitioners do not utilise written agreements.

Whether a JDA is ultimately reduced to writing or not, practitioners should remember that JDAs only preserve privilege and work-product protections – they do not protect otherwise unprivileged materials. (See also Chapter 32 on privilege.)

37 See, e.g., *United States v. Almeida*, 341 F.3d 1318, 1327 n. 21 (11th Cir. 2003) ('In the future, defense lawyers should insist that their clients enter into written joint defense agreements that contain a clear statement of the waiver rule enunciated in this case, thereby allowing each defendant the opportunity to fully understand his rights prior to entering into the agreement.').

Indemnification and insurance coverage 13.6

Determining whether an individual is indemnified 13.6.1

Determining whether an employee has a right to be indemnified, both for legal fees and for a potential judgment or settlement, is critical and can involve a number of steps. These can include communications with company counsel as well as review of various sources of indemnification or advancement of fees.

Communications with employer/company counsel 13.6.1.1

Counsel for individuals should engage in a conversation with the employer or with company counsel to determine whether the company will agree to indemnify the individual and what the scope of the indemnification entails. If the company agrees to indemnify, counsel should seek written confirmation.

Potential sources of indemnification 13.6.1.2

By-laws

A company's obligation to indemnify or advance defence costs with respect to claims arising in the course of the individual's official duties is normally contained in the company's by-laws, which must be carefully scrutinised to identify any procedural or substantive limitations on corporate indemnification (such as entering into a written undertaking to repay all advanced costs if it is determined the costs are not indemnifiable) with particular focus on advancement of defence costs prior to a determination of the right to be indemnified. There may also be supplemental, specially negotiated indemnification agreements with particular individuals, and indemnification obligations may sometimes be contained in an employment agreement. All of these sources must be carefully reviewed.

Local law of the state of incorporation

The local law of the state of incorporation can have a significant impact on the scope of permissible indemnification. For example, for companies organised under Delaware law, indemnification is mandatory where the officer or director was 'successful on the merits or otherwise in the defense of any action, suit or proceeding.'[38] In a criminal proceeding, 'anything less than conviction constitutes "success" for purposes of DGCL §145(c).'[39] Significantly, Delaware does not require the officer or director to have been 'wholly' successful, but merely requires that indemnification be provided 'to the extent' of success.[40] With respect to derivative actions, indemnification is allowed solely for defence costs, not for judgments or settlements that may result.[41]

38 8 Del. C. § 145(c).

39 *Hermelin v. K-V Pharm. Co.*, 54 A.3d 1093, 1108 (Del. Ch. 2012).

40 13 William Meade Fletcher et al., *Fletcher Cyclopedia of the Law of Private Corporations* §3:17 (Perm ed. 1995).

41 8 Del. C. § 145(b). Such judgments or settlements, as well as defence costs, may be covered by insurance under Section 8 Del. C. § 145(g).

Between these two poles of mandatory and prohibited indemnification, there is a wide range of permissible indemnification that gives corporations the discretion to indemnify officers or directors for conduct taken in a corporate capacity.[42] Delaware law also permits, but does not require, a corporation to advance defence costs prior to a determination of eligibility for indemnification.[43] Consequently, corporations generally define their indemnification obligations by charter, by-law, or contract.

In addition to state law, federal law may sometimes place limits on the scope of corporate indemnification. For example, the Federal Deposit Insurance Corporation Rule on Golden Parachute and Indemnification Payments[44] may restrict the power of depository institutions to provide indemnification for claims of regulatory violations.

Company policies

In addition to provisions in corporate by-laws, indemnification provisions are sometimes contained in employment agreements and employee handbooks. These additional sources should also be checked.

Insurance policies of employer

D&O insurance

Most corporations will have purchased some form of directors and officers (D&O) insurance to cover their directors and officers from claims for wrongful acts in the course of their official duties. The coverage may also extend to employees. Such policies will normally cover the corporate organisation (usually in excess of a deductible or retained amount) for its loss, to the extent it is indemnifying the individual insureds, and provide coverage directly to the individual where the company is not providing indemnification. The first recourse of the individual should be to demand indemnification from the company pursuant to corporate by-laws or other agreements or provisions. It is imperative to ensure that a prompt notice of claim has been provided to the insurance company to ensure that coverage is available in the event the company fails to indemnify for any reason. The definition of 'claim' in the policy may include written demands for monetary or non-monetary relief, or formal or sometimes informal investigations. The definition of this term may determine the point from which defence costs may be covered under the policy.

In addition to traditional D&O insurance, many companies have 'Side A' coverage that provides additional protection solely for officers and directors (sometimes further limited to independent officers and directors). Inquiry should be made concerning the existence of such policies and prompt notice of claim must be given to the insurer.

---

42 8 Del. C. §145(a).

43 8. Del C. § 145(e).

44 12 C.F.R. § 359 (1996).

If there is any chance that an existing D&O policy will not be renewed, the existing policy will normally allow for notice of circumstances that may result in a future claim (as distinguished from notice of an existing claim). D&O policies that contain this option generally require that the notice identify specific circumstances that could give rise to a claim.

Other types of coverage

In addition to D&O policies, a company may have other types of policies that provide coverage for officers, directors and employees. These may include professional liability (errors and omissions, E&O) policies. All potential sources of coverage should be checked and notice given, if appropriate.

Advocating for indemnification when not otherwise clear 13.6.2

At times, the individual's right to indemnification may not be clear from corporate by-laws or other sources of indemnification rights. In these situations, counsel should be prepared to advocate for the benefits of indemnification. For example, for the result of an investigation to be considered credible, it may be necessary for the individual to receive independent advice and counsel without the potential for conflict with the corporation's interests. In appropriate circumstances, experienced counsel can engage in a degree of co-operation and share certain information with the company on a privileged basis that inures to the benefit of both parties. Practitioners should be aware that pressure from the government on companies not to indemnify employees, which may have marked government investigations in the past, has been held constitutionally improper and has been disavowed by the Department of Justice.[45]

Awareness of situations where indemnification may cease 13.6.3

Violation of company undertakings 13.6.3.1

As mentioned above, a company's obligation to advance defence costs prior to determination of entitlement to corporate indemnification may be conditional on a written undertaking to repay such costs in the event the costs are ultimately determined not to be indemnifiable. If the individual refuses to execute such an undertaking, the company may refuse to indemnify. Alternately, the company may be entitled to recoup its defence costs if the individual fails to abide by the

45 See *United States v. Stein*, 435 F. Supp. 2d 330, 363 (S.D.N.Y. 2006), aff'd, 541 F.3d 130 (2d Cir. 2008) (holding that government policy of treating the payment of legal fees as a factor in favour of indictment 'discourages and, as a practical matter, often prevents companies from providing employees and former employees with the financial means to exercise their constitutional rights to defend themselves. . . . It therefore burdens excessively the constitutional rights of the individuals whose ability to defend themselves it impairs and, accordingly, fails strict scrutiny.'); McNulty Memorandum, available at: https://www.justice.gov/sites/default/files/dag/legacy/2007/07/05/mcnulty_memo.pdf ('Prosecutors generally should not take into account whether a corporation is advancing attorneys' fees to employees or agents under investigation and indictment.').

terms of the undertaking (such as by failing to provide invoices on a timely basis) or if there is a determination of fraud or bad faith.

13.6.3.2 Assessing whether to co-operate with investigation

Counsel should consider various factors in determining the level of co-operation with the company under the circumstance of each case. These factors may include: (1) the willingness of the company to provide indemnification and other repercussions of a failure to co-operate; (2) the possibility that the client will have no counsel if the client cannot otherwise afford representation; (3) the sliding scale nature of co-operation, which can be negotiated with the company; and (4) employment considerations. Counsel should make clear to the client that no matter who pays the bills, the lawyer always owes a duty of loyalty to his or her individual client. (See also Chapter 10 on co-operating with authorities.)

13.6.4 Ensuring sufficient funds for protracted investigation

13.6.4.1 Understanding whether there is a limit to funds

Cap on insurance policy

To the extent the indemnification proceeds are coming from insurance, there may be a cap on the amount of such proceeds. Typically (although not always) defence costs in D&O policies are part of, and not in addition to, the limits of insurance. That means defence costs will erode the limits of the policy that may be available to pay for any judgment or settlement. In addition, costs of other individuals or the company (to the extent the company is also incurring covered costs) may contribute to exhaustion of the available limits of insurance.

Commitment of company to continued indemnification

In addition, the ability or willingness of the company to pay indemnification expenses may not be unlimited. To the extent the company is unable to pay for indemnification expenses due to financial impairment, this may allow the individual direct recourse to Side A insurance coverage under a D&O policy.

13.7 Privilege concerns for employees and individuals

13.7.1 In communications with other employees or company counsel

Employees do not enjoy protections over their communications with anyone other than their individual counsel. Practitioners may wish to advise their clients not to discuss the matters under investigation with colleagues, people involved in the underlying events, company counsel and others.

It is possible that company counsel will request an interview of the client with the client's individual counsel present. Before agreeing to such an interview, however, counsel should explain to his or her client that the privilege will not attach to such communications although it may be possible to conduct such interviews under a JDA.

If a client has already been interviewed by company counsel, individual counsel should seek to obtain the substance of that interview and investigate whether a

proper warning under *Upjohn* was given and whether the warning was adequately documented. An inadequate *Upjohn* warning or inadequate documentation of the warning may be a basis to limit the disclosure of statements made by the client in the interview. More specifically, if an individual was not provided a sufficient *Upjohn* warning, the individual can try to assert that it was his or her belief that an attorney–client relationship had developed and that, as a result, the company should be prevented from sharing the information or the government should be prevented from using the information, or both. Counsel should nonetheless understand that prevailing on such an argument can be difficult. Most of the federal appellate courts have adopted a version of the *Bevill* test, which provides that executives or employees seeking to assert a personal claim of attorney–client privilege over communications with corporate counsel must demonstrate five factors: (1) that they approached counsel for the purpose of seeking legal advice; (2) that when they approached counsel they made it clear that they were seeking legal advice in their individual rather than in their representative capacities; (3) that counsel saw fit to communicate with them in their individual capacities, knowing that a possible conflict could arise; (4) that their conversations with counsel were confidential; and (5) that the substance of their conversations with counsel did not concern matters within the company or the general affairs of the company.[46]

In communications with individual counsel paid for by employer 13.7.2

Employees' communications with their individual counsel are privileged regardless of whether counsel is paid for by the employer. Individual counsel owe a duty of loyalty to their individual clients, regardless of how counsel is being paid.

Use of employer email to conduct privileged conversations 13.7.3

With internal counsel 13.7.3.1

Communications with internal company counsel, if it falls within the parameters of the attorney–client privilege, will be the company's privilege and not the individual's privilege. However, as discussed in Section 13.7.1, in certain circumstances, the individual may seek to prevent the disclosure or use of the communication by asserting that it was his or her belief that the communication was privileged as to the employee.

With external counsel 13.7.3.2

Best practices include advising individual clients to communicate with their personal counsel using personal email, as opposed to workplace email, as there is at least the risk that the employer could review those emails or that someone may argue that the use of a workplace email account resulted in a waiver of any

46 See *United States v. Graf*, 610 F.3d 1148, 1159-1160 (9th Cir. 2010) (citing *In re Bevill, Bresler & Schulman Asset Mgmt. Corp.*, 805 F.2d 120, 123-125 (3d Cir. 1986)); see also *United States v. Int'l Brotherhood of Teamsters*, 119 F.3d 210, 215 (2d Cir. 1997) (personal privilege depended on whether employee made clear that he sought legal advice on personal matters).

applicable privilege. However, the law is mixed in this area, and the success of any such argument would be highly fact-specific.

Proskauer Rose LLP
11 Times Square
New York
NY 10036
United States
Tel: +1 212 969 3000
Fax: +1 212 969 2900
jnewville@proskauer.com
sschafler@proskauer.com
hmufson@proskauer.com
smcaleavey@proskauer.com

www.proskauer.com

Joshua Newville
Proskauer Rose LLP

Joshua Newville is a partner in the litigation department in the New York office of Proskauer Rose LLP. He is a member of Proskauer's white-collar defence and investigations and commercial litigation groups. Josh handles securities litigation, enforcement and regulatory matters, representing corporations and senior executives in civil and criminal investigations. In addition, Josh conducts internal investigations and advises registered investment advisers and other fund managers on regulatory compliance, SEC exams and related risks.

Prior to joining Proskauer, Josh was senior counsel in the US Securities and Exchange Commission's division of enforcement, where he investigated and prosecuted violations of the federal securities laws. Josh served in the enforcement division's asset management unit, a specialised unit focusing on investment advisers and the asset management industry. His prior experience with the SEC provides a unique perspective to help companies and individuals manage risk and handle regulatory issues.

Seth B Schafler
Proskauer Rose LLP

Seth B Schafler is a partner in the insurance recovery and counselling group. Seth has represented high-profile clients in precedent-setting cases spanning every type of insurance work for more than 25 years. He has extensive experience representing policyholders in coverage negotiations and disputes with their insurance companies, and litigating coverage issues in federal and state courts across the country.

Seth's experience covers a wide variety of insurance products including commercial general liability, directors and officers, professional liability, errors and omissions, fiduciary liability, property, business interruption, fidelity, marine and credit risk insurance, among others.

In addition to his litigation practice, Seth also advises his clients on any and all of their day-to-day insurance and coverage needs, including directors and officers liability insurance (D&O) and errors and omissions (E&O) matters.

Harris M Mufson
Proskauer Rose LLP

Harris Mufson is a senior counsel in the labour and employment law department in the New York office of Proskauer Rose LLP. He is a member of the employment litigation and arbitration, and whistleblowing and retaliation groups, and is a co-editor of Proskauer's 'Whistleblower Defense Blog'.

Adept at counselling clients at every turn of the litigation process, Harris represents employers in a variety of industries, including financial services, retail, health care, entertainment, sports and legal, with respect to a wide range of labour and employment law matters. These include compensation disputes, employment discrimination and retaliation, whistleblowing, sexual harassment, wrongful discharge, defamation, breach of contract, non-competition agreements and wage-and-hour issues. He regularly appears in state and federal courts, as well as in proceedings before the American Arbitration Association, the Financial Industry Regulatory Authority, JAMS, the Equal Employment Opportunity Commission, and other federal and state agencies.

Susan C McAleavey
Proskauer Rose LLP

Susan C McAleavey is an associate in the labour and employment law department in the New York office of Proskauer Rose LLP. She is a member of the firm's employment litigation and arbitration, and whistleblowing and retaliation groups. Susan represents employers in a variety of industries, including financial services, sports and entertainment, hospitality services, and healthcare, with respect to a wide range of labour and employment law matters, including compensation disputes, employment discrimination and retaliation, whistleblowing, sexual harassment, wrongful discharge, defamation, breach of contract and wage-and-hour issues. She handles federal and state litigations, arbitrations as well as administrative proceedings. In addition, Susan counsels clients on compliance with employment-related laws and on developing, implementing and enforcing personnel policies and procedures.