SETON HALL | LAW

Internal Investigations in the Workplace: Hot Topics, Pitfalls, and Ethical Implications

Timothy P. Glynn
Associate Dean and Professor of Law
Seton Hall University School of Law

Mike Martinez
Partner
Mayer Brown LLP

Overview

- Who Should Conduct the Investigation?
  - Focus on Attorney Investigators
    - Potential Pitfalls
    - Attorney-Client Privilege Issues
- How Should the Investigation Be Conducted?
  - Investigatory Interviews
    - Dual Representation Issues
    - Techniques
  - Fact Gathering (Documents and Files)
    - Covert or Secret Monitoring
    - Other Privacy Concerns

WHO? ATTORNEYS AS INVESTIGATORS

POTENTIAL PITFALLS

- Costs
- Dual representation issues/conflicts of interest
- Lawyer as witness issues
- Privilege waiver and related complications
- *Assuring adequate independence*
  - Particularly for in-house counsel

ASSURE ADEQUATE INDEPENDENCE

- One should not lead an internal investigation if he or she:
  - Is potentially implicated
  - Is in the same department or unit as one potentially implicated
  - Reports to someone potentially implicated
  - Cannot be impartial or appear impartial for some other reason, including prior knowledge of or dealings with a complaining or implicated party
  - May be constrained in withdrawing or otherwise fulfilling ethical obligations
- Investigations of suspected wrongdoing by senior management always should be conducted by someone outside of the company.
  - *See* AMERICAN COLLEGE OF TRIAL LAWYERS, RECOMMENDED PRACTICES FOR COMPANIES AND THEIR COUNSEL IN CONDUCTING INTERNAL INVESTIGATIONS 9-10 (2008)

ATTORNEYS AS INVESTIGATORS

BENEFITS

- Expertise and experience in the particular area
- Knowledge of potentially relevant law
- *Attorney-client privilege (and work product) protection*
  - There is no "self-critical analysis privilege"

    See, e.g., Slaughter v. Nat'l R.R. Passenger Corp., No. Civ. A. 10-4203, 2011 WL 780754 (E.D. Pa. Mar. 4, 2011) (refusing to recognize the self-critical analysis privilege and discussing its rejection in most other courts as well as its uneven treatment elsewhere)

A/C Privilege and Work Product Doctrines

Attorney-Client Privilege:

Protects confidential communications between an *attorney* and his or her *client* for the purpose of rendering or receiving legal advice; thus the privilege can only attach if the communications are with an attorney who is acting as such (or one acting as an attorney's agent)

- Protects only communications, not facts
- Subject to waiver (and likely to be waived in some investigations)

Work Product Doctrine:

Protects documents and tangible things prepared in anticipation of litigation by or for a party or its representative unless other side can show substantial need and undue hardship

- Also subject to waiver

EMERGENT PRIVILEGE ISSUES

U.S. *ex rel.* Barko v. Halliburton, 2014 WL 1016784 (D.D.C. Mar. 6, 2014)

- FCA qui tam plaintiff-relator sought documents relating to defendant's Code of Business Conduct investigations.
- The court held that the attorney-client privilege and work product doctrines do *not* protect the documents because the investigations were undertaken pursuant to regulatory law and corporate policy rather than for the primary purpose of obtaining legal advice or in preparation for litigation.
- The court suggested that the primary purpose test only can be satisfied if the investigations would not have occurred "but for" the purpose of obtaining legal advice or preparing for trial.

In *In re Kellogg Brown & Root, Inc.*, 756 F.3d 754 (D.C. Cir. 2014), the court granted defendant's petition for writ of mandamus, in effect, *REVERSING Barko*.

- The court adhered to the "primary purpose" test but rejected the district court's "but for" approach, stating the test does not "draw a rigid distinction between a legal purpose on the one hand and a business purpose on the other." *In re Kellogg Brown & Root, Inc.*, 756 F.3d at 759.
- Communications can have more than one primary purpose.
- New formulation: "In the context of an organization's internal investigation, if one of the significant purposes of the internal investigation was to obtain or provide legal advice, the privilege will apply. . . ." *Id.* at 761.

EMERGENT PRIVILEGE ISSUES

OTHER CLARIFICATIONS IN *KELLOGG BROWN & ROOT*:

1) Investigations conducted or overseen by in-house counsel can receive privilege protection.

2) Communications by those serving as agents of attorneys, such as those individuals conducting interviews during an attorney-led internal investigation, can be protected by the attorney-client privilege.

3) There are no "magic words" in employee interviews needed to trigger protection.

This broad privilege protection was recently upheld a second time via writ of mandamus after remand:

In re Kellogg Brown & Root, Inc., 796 F.3d 137 (D.C. Cir. 2015)

EMERGENT PRIVILEGE ISSUES

STILL, BE CAREFUL:

- *Kellogg*'s permissive "significant purpose" approach has not been widely adopted elsewhere.
- *Kellogg* has been distinguished where non-attorney investigators were not clearly acting as agents for or assisting attorneys.
  - Wultz v. Bank of China Ltd., 304 F.R.D. 384 (S.D.N.Y. 2015); Szulik v. State Street Bank & Trust Co., 2014 WL 3942934 (D. Mass. Aug. 11, 2014).

Emergent Privilege Issues

Suggestions

- Do not be over inclusive – simply housing investigations in or under the legal department is not enough.
- Consider building into compliance systems some kind of early detection mechanism to identify matters likely to raise significant legal concerns or produce litigation, and then remove them to the legal department or outside legal counsel to conduct the investigation.
- Document attorney supervision and direction.
- Give and document *Upjohn* warnings.
- Clearly mark documents and communications that are privileged or work product.

EMERGENT PRIVILEGE ISSUES

In re Information Management Services, Inc., Derivative Litigation, 81 A.3d 278 (Del. Ch. 2013)

- A corporation's right of access to work e-mails from its executives to their personal attorneys meant officers did not have reasonable expectation of privacy in those e-mails (and, hence, the communications were not privileged).
- The officers should have taken more significant and meaningful steps to defeat access, such as shifting to a webmail account or encrypting their communications.

<u>Lessons</u>

- As soon as officers, directors, and employees retain separate counsel, in-house counsel should advise them not to use the corporation’s email system to communicate with their counsel.
- Failure to do this raises some risks for the corporation and corporate attorneys as well.

Other Privilege Limitations

- The selective waiver doctrine continues to be widely rejected.
  - *See, e.g., In re* Pacific Pictures Corp., 679 F.3d 1121 (9th Cir. 2012) (rejecting the doctrine and discussing how all but one other federal circuit court has refused to adopt it).
- In a shareholder suit arising from the Wal-Mart Mexico scandal, Delaware reaffirmed the so-called *Garner* doctrine, which allows shareholder access to privileged attorney-corporate client communications under certain circumstances (in derivative suits and suits demanding corporate information).
  - *See* Wal-Mart Stores, Inc. v. Indiana Electrical Workers Pension Trust Fund IBEW, 95 A.3d 1264 (Del. 2014).

How: Investigatory Interviews

- *Upjohn* warnings (a.k.a. "corporate *Miranda* warnings")
  - Hot topic since *U.S. v. Nicholas*, 606 F. Supp. 2d 1109 (C.D. Cal. 2009), *rev'd in part*, U.S. v. Ruehle, 583 F.3d 600 (9th Cir. 2009); *see also* MRPC 1.13(f)
- Essential elements of the warning
  - The attorney represents the corporation, *not* the employee.
  - The interview's purpose is to provide legal advice to the corporation.
  - Employee statements will be shared with corporate decision makers.
  - Interview communications are covered by the attorney-client privilege, but the privilege is owned by the corporation.
  - The corporation can waive the privilege without the employee's consent.

Emergent Issues in Investigatory Interviews

- The safest course for in-house or existing corporate counsel conducting interviews may be to get written waivers of potential conflicts.

  Cf. Nicholas, 606 F. Supp. 2d at 1116-17; MRPC 1.9(a)

- Representation/conflict of interest and related ethical concerns might extend to counsel's interactions with employees and non-employees.

  See Speeney v. Rutgers, 369 F. App'x 357 (3d Cir. 2010) (vacating summary judgment against victims of sexual harassment by former university professor in their action against the university's attorneys, in which they claimed malpractice and breach of fiduciary duty arising from alleged prior interactions with the attorneys suggesting they represented the victims).

Emergent Issues in Investigatory Interviews

- Limits on confidentiality mandates

1) NLRB: Blanket confidentiality mandates likely violate employees' right to engage in "concerted activity for mutual aid and protection" under Section 7 of the NRLA.

Banner Health Sys., 358 NLRB No. 93 (2012); *In re* Verso Paper, Case 30-CA-089350, 2013 WL 1702453 (N.L.R.B.G.C. Jan. 29, 2013)

- Employers cannot order employees not to talk about work-related matters.
- More limited directives to keep interview communications confidential may be justified by privilege and other interests, *but* employees may need to be informed that they can otherwise discuss workplace matters with co-employees.

2) SEC: It is a violation of Rule 21F-17 (under Dodd-Frank) to require witnesses in internal investigations interviews to sign confidentiality statements with language warning that they could face discipline if they discuss matters with outside parties without prior approval.

In re KBR, Inc., File No. 3-16466, SEC Release No. 74619 (Apr. 1, 2015)

- Companies cannot take any action that impedes whistleblowers from reporting possible securities violations to the SEC.

Heavy-Handed Interview/Interrogation Tactics

- **"False Confession" litigation on the rise**
  - *See* Saul Elbein, *When Employees Confess, Sometimes Falsely*, N.Y. Times, Mar. 8, 2014, at BU1 (discussing the rise of "false confession" litigation)
  - *See, e.g.*, Robles v. Autozone, Inc., 2008 WL 2811762 (Cal. Ct. App. July 22, 2008)
- **False Imprisonment**
  - *See, e.g.*, MacKenzie v. Linehan, 969 A.2d 385 (N.H. 2009) (recognizing false imprisonment claim arising from employee's supervisor blocking the exit door for thirty seconds)
- **Other potential claims include fraud, intentional infliction of emotional distress, and defamation**
- **Ethical concerns for attorney investigators include:**
  - MRPC 4.1 (prohibiting false statements of material fact or law to a third person and omissions that assist in fraud)
  - MRPC 4.4(a) (prohibiting means that have no substantial purpose other than to embarrass, delay, or burden a third person, or methods of obtaining evidence that violate the legal rights of such a person)
  - Attorneys may be accountable for investigators they supervise. *E.g.*, MRPC 5.3

How: Fact Gathering and Privacy Protections

- An issue of growing concern is the extent to which document, electronic file, and communications searches breach privacy protections or other laws.

- Covert, secretive, or deceptive surveillance or interception create risks:

  - ✓ Recall "pretexting" scandal at Hewlett-Packard. *See Hewlett-Packard Settles 'Pretexting' Suit*, N.Y. Times, Feb. 14, 2008.
  - ✓ *See* Ehling v. Monmouth-Ocean Hosp. Serv. Corp., 872 F. Supp. 2d 369 (D.N.J. 2012) (finding an employee's allegations that her postings to a Facebook page accessible only by those invited by the employee sufficient to plead a reasonable expectation of privacy in her page, when supervisor compelled another employee with access to the page to view it in front of the supervisor).
  - ✓ *See* Burrow v. Sybaris Clubs Int'l, Inc., 2013 WL 5967333 (N.D. Ill. Nov. 8, 2013) (refusing to find secret monitoring of employees' personal and business telephone conversations protected by the ordinary course of business or other exceptions to the federal wiretapping statute).

- ❖ Instead, expedite legitimate fact-gathering methods (just before litigation hold)

Fact Gathering and Privacy Protections

- A particularly hot issue is the scope of privacy protections for employee emails, password-protected social media accounts, and other electronic communications.
- Historically, employee privacy claims involving employee electronic or stored communications on employer-provided equipment almost never succeeded.
- Today, successful claims remain rare, but we are beginning to see them with more frequency, as well as important statutory developments.
- Traditional theories:
  - Electronic Communications Privacy Act and Stored Communications Act
  - Tort law: Intrusion upon seclusion and the public policy doctrine
  - Occasional contract, tort, and other theories in some states

Fact Gathering and Privacy Protections

- Privacy claims involving *employer-provided* email, social media accounts, or other electronic communications almost never succeed, because employees rarely can establish a reasonable expectation of privacy in such communications.
  - Recall *In re* Information Management Services (officer emails to counsel)
  - Only a serious failure on the part of the employer to maintain and enforce an electronic communications policy will result in liability.
- Privacy claims involving *personal*, *password protected* employee email communications are more likely to succeed.
  - Key issues in the investigations context are the reach and clarity of the employer's electronic communications and computer use policy and the justification and scope of the search.

Fact Gathering and Privacy Protections

- Such privacy breaches also raise ethics concerns.

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

Stengart used her company-issued laptop to exchange e-mails with her lawyer through her personal, password-protected, e-mail account. She later filed an employment discrimination lawsuit against Loving Care Agency, Inc. In anticipation of discovery, Loving Care hired a computer forensic expert to recover all files stored on the laptop including the e-mails, which had been automatically saved on the hard drive. Loving Care's attorneys reviewed the e-mails and used information culled from them in the course of discovery.

Fact Gathering and Privacy Protections

- The court held that the employer's computer use policy did not defeat Stengart's reasonable expectation of privacy because it did not address personal email or warn that the company might retrieve such emails.
- But the court went further, holding that, given the important public policy concerns underlying the privilege, *even a more clearly written policy giving unambiguous notice* that such emails might be retrieved would not defeat Stengart's expectations or justify review of the emails:

  "We find that the Firm's review of privileged e-mails between Stengart and her lawyer, and use of the contents of at least one e-mail in responding to interrogatories, fell within the ambit of RPC 4.4(b) and violated that rule." *Id.* at 666.

Fact Gathering and Privacy Protections

- *Stengart's* finding of a violation is interesting, because, on its face, New Jersey's version of Rule 4.4(b) appears not to apply to searches of stored communications or reviewing communications retrieved:

  > A lawyer who receives a document and has reasonable cause to believe that the document was inadvertently sent shall not read the document or, if he or she has begun to do so, shall stop reading the document, promptly notify the sender, and return the document to the sender.

- But the *Stengart* court interpreted the rule broadly . . .

Fact Gathering and Privacy Protections

- *Stengart*'s future application is unclear.
  - Its interpretation of 4.4(b) has been rejected by ABA. *See* ABA Formal Opinion 11-460 (Aug. 4, 2011) (interpreting Model Rule 4.4(b)).
  - The more controversial aspects of its reasoning have yet to be adopted in any other jurisdiction.

- But, even if *Stengart* is widely rejected, attorney investigators need to be concerned with MRPC 4.4(a):

  > In representing a client, a lawyer shall not use means that have no substantial purpose other than to embarrass, delay, or burden a third person, *or use methods of obtaining evidence that violate the legal rights of such a person*.

Fact Gathering and Privacy Protections

- Thus, when conducting an internal investigation, be conscious of whether your searches of computer files or monitoring of communications run afoul of privacy protections.
- Given concerns about cybersecurity and information privacy, protections may expand.

  There is growth in statutory protections in particular:
  - For example, since 2012, there has been a wave of legislation prohibiting or restricting employer demands for access to job applicants' and employees' social media accounts.
  - New Jersey's new law is highly restrictive, even in the investigations context. *See* N.J. STAT. ANN. § 34:6B-6 (West 2014).
  - New York and Pennsylvania have proposed legislation pending.
  - The National Conference of State Legislatures tracks developments:

    http://www.ncsl.org/research/telecommunications-and-information-technology/employer-access-to-social-media-passwords-2013.aspx

Fact Gathering and Privacy Protections

- These statutory protections often are more restrictive in the investigations context than standard privacy doctrines, which tend to allow access for any legitimate business reason.
- For example, look at the investigations exception in the New Jersey social media law:

> Nothing in this act shall prevent an employer from conducting an investigation:
>
> (1) for the purpose of ensuring compliance with applicable laws, regulatory requirements or prohibitions against work-related employee misconduct *based on the receipt of specific information about activity on a personal account by an employee*; or
>
> (2) of an employee's actions *based on the receipt of specific information* about the unauthorized transfer of an employer's proprietary information, confidential information or financial data to a personal account by an employee.

N.J. Stat. Ann. § 34:6B-6 (West 2014).

Steps to Reduce Risks of Privacy Breaches During Investigations

- Computer use and electronic communications policies should be reviewed for clarity and thoroughness *before* any investigation.
- HR or compliance should ensure adherence to these policies in practice.
- Investigators should not review the content of communications in employee's personal email accounts unless the employer's policies expressly address review of such communications.
- Even then, the safe course is to avoid reading what appears to be attorney-client communications (and perhaps other highly sensitive communications) in personal email stored on employer equipment.
- Investigators should understand and adhere to the limits on reviewing social media content.
- Attorneys and clients should keep current on privacy law developments, and train employees and non-attorney investigators accordingly.

The End