AN A.S. PRATT PUBLICATION
SEPTEMBER 2017
VOL. 3 • NO. 7

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

Pratt's Privacy & Cybersecurity Law Report

VOLUME 3 NUMBER 7 SEPTEMBER 2017

LexisNexis®

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the **Editorial Content** appearing in these volumes or reprint permission, please contact:
Deneil C. Targowski at 908-673-3380
Email: ..... Deneil.C.Targowski@lexisnexis.com
For assistance with replacement pages, shipments, billing or other customer service matters, please call:

Customer Services Department at ..... (800) 833-9844
Outside the United States and Canada, please call ..... (518) 487-3385
Fax Number .... (800) 828-8341
Customer Service Web site ..... http://www.lexisnexis.com/custserv/
For information on other Matthew Bender publications, please call

Your account manager or ..... (800) 223-1940
Outside the United States and Canada, please call ..... (937) 247-0293

ISBN: 978-1-6328-3362-4 (print)
ISBN: 978-1-6328-3363-1 (eBook)

ISSN: 2380-4785 (Print)
ISSN: 2380-4823 (Online)

Cite this publication as:
[author name], [*article title*], [vol. no.] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [page number] (LexisNexis A.S. Pratt);
Laura Clark Fey and Jeff Johnson, *Shielding Personal Information in eDiscovery*, [1] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [233] (LexisNexis A.S. Pratt)

An A.S. Pratt™ Publication
Editorial

Editorial Offices
630 Central Ave., New Providence, NJ 07974 (908) 464-6800
201 Mission St., San Francisco, CA 94105-1831 (415) 908-3200
www.lexisnexis.com

MATTHEW BENDER

(2017–Pub. 4939)

Editor-in-Chief, Editor & Board of Editors

Pratt's Privacy & Cybersecurity Law Report is published nine times a year by Matthew Bender & Company, Inc. Periodicals Postage Paid at Washington, D.C., and at additional mailing offices. For customer support, please contact LexisNexis Matthew Bender, 1275 Broadway, Albany, NY 12204 or e-mail Customer.Support@lexisnexis.com. Direct any editorial inquires and send any material for publication to Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc., 26910 Grand Central Parkway Suite 18R, Floral Park, New York 11005, smeyerowitz@meyerowitzcommunications.com, 718.224.2258. Material for publication is welcomed—articles, decisions, or other items of interest to lawyers and law firms, in-house counsel, government lawyers, senior business executives, and anyone interested in privacy and cybersecurity related issues and legal developments. This publication is designed to be accurate and authoritative, but neither the publisher nor the authors are rendering legal, accounting, or other professional services in this publication. If legal or other expert advice is desired, retain the services of an appropriate professional. The articles and columns reflect only the present considerations and views of the authors and do not necessarily reflect those of the firms or organizations with which they are affiliated, any of the former or present clients of the authors or their firms or organizations, or the editors or publisher.

POSTMASTER: Send address changes to *Pratt's Privacy & Cybersecurity Law Report,* LexisNexis Matthew Bender, 630 Central Ave., New Providence, NJ 07974.

A Guide to Corporate Internal Investigations – Part II

By Jennifer L. Chunias and Jennifer B. Luz*

In this two-part article the authors set forth a framework of best practices and considerations for conducting effective internal investigations, as well as the most common pitfalls to avoid. This second part of the article focuses on witness interviews, a public relations strategy, and concluding the investigation. The first part of the article, which appeared in the July/August 2017 issue of Pratt's Privacy & Cybersecurity Law Report, *discussed the threshold issue to consider when deciding whether to investigate, staffing the investigation, goals and parameters of the investigation, and document review.*

This second part of a two-part article discusses corporate internal investigation witness interviews, a public relations strategy, and concluding an investigation.

WITNESS INTERVIEWS

Witness interviews are a key part of the investigative process and, along with documents, are generally the primary source of information that will be gathered during the investigation. While interviews have great potential to provide useful information, they come with significant challenges. Thoughtful planning and execution are critical to maximize the former and minimize the latter. Careful consideration should be given to who should conduct the interviews and whether anyone from the company should be present.

It generally is best if attorneys conduct the interviews. For one thing, having an attorney conduct the interview strengthens the argument that what is said during the interview is covered by the attorney-client privilege and that notes or memoranda documenting the interview are similarly privileged.[1] Further, counsel generally have more training and experience in synthesizing relevant facts and questioning witnesses.

Other logistical factors also play a significant role in conducting effective interviews. The timing and location of the interviews should be convenient for the employee. The

* Jennifer L. Chunias, a partner in Goodwin Procter LLP's Litigation Department, specializes in white collar criminal defense and government and internal investigations, as well as post-closing disputes and litigation. Jennifer B. Luz, a counsel in the firm's Litigation Department, focuses her practice on securities litigation, SEC enforcement, government investigations, internal corporate investigations and complex litigation. The authors may be reached at jchunias@goodwinlaw.com and jluz@goodwinlaw.com, respectively. Ms. Chunias and Ms. Luz would like to thank Matthew Harrington, an associate at Goodwin Procter LLP, for his assistance preparing this article.

[1] *Upjohn Co. v. United States*, 449 U.S. 383, 394-399 (1981) (attorney-client privilege protects attorney notes taken during interviews with employees during internal investigation).

interviewer should make the employee feel comfortable. If the employee is "on guard," it is less likely that he or she will be candid during the interview.

Interviews should be conducted of all company personnel likely to have knowledge regarding the relevant transaction or the alleged violation. Before interviewing personnel, counsel should review the relevant documents and interviews, prepare an outline of topics to be covered with the witness, and select the documents that should be shown to the witness during the interview. The interviews should be prioritized, as the order in which they are conducted makes a difference. The investigative team also should be alert to sensitivities in interviewing directors and senior management, and consider whether senior management really needs to be interviewed. On the other hand, it is important to ensure that all necessary interviews are conducted and that there is no perception of favoritism shown to senior management.

When considering whom to interview, the investigative team should also look beyond current employees. Former employees may have knowledge of the alleged wrongdoing. If that is the case, assess whether they are willing to cooperate. An employee's willingness may be influenced by the circumstances under which she or he left the company. If the employee left on unfavorable terms, she or he may be less likely to assist the company. And if particularly disgruntled, the employee may pose a risk of disclosing unfavorable information to the government or the media. By diligently researching these matters, investigators increase the likelihood of gaining useful information and simultaneously reinforce another benefit of internal investigations: reducing surprises.

Conducting the Interview

Suffice to say, it is critical to preserve the attorney-client privilege and the work product doctrine at each stage of an internal investigation. Employee interviews are subject to the attorney-client privilege. Recordings of interviews, however, may be considered purely factual communications that, as verbatim transcriptions, are not subject to the attorney work product doctrine.[2] Accordingly, it is best not to record interviews and instead have the interviewer (or, more likely, another attorney in the room) take written notes which include his or her thoughts and mental impressions. Because opinion work product receives greater protection than fact work product, it is more likely that written notes including an attorney's thoughts and impressions will be protected.[3]

Counsel also should give the employee an *Upjohn* warning. In *Upjohn v. United States*, the U.S. Supreme Court held that communications between company counsel

[2] The Federal Rules of Criminal Procedure also require production of contemporaneously recorded statements after the witness has testified on direct examination at trial. Fed. R. Crim. P. 26.2.

[3] However, counsel should be aware that the fact that interview memoranda contain mental impressions can result in complexities later if the memoranda are disclosed to the government as part of a company's cooperation efforts.

and company employees are privileged, but the privilege belongs to the company, not to the employee. Providing the warning makes clear that counsel represents only the company. Anything the employee states in the interview is privileged only between counsel and the company. The company may choose to waive the privilege in the future, and in that event, the employee's statements may be disclosed to the government. If clearly given, an *Upjohn* warning sets the boundaries of the interview and removes any doubt about whether counsel represents the employee. This is also particularly important in light of the Yates Memo, which also highlights the potential tension between the interests of the company and the interests of employees.[4]

Of course, if employees know that they will not control the fate of their own statements, they may be less likely to speak candidly with the interviewer. But given the ethical consequences posed by an ambiguous or altogether omitted *Upjohn* warning, some loss of candor is a necessary risk.

After giving the *Upjohn* warning, counsel should clarify his or her role. Inform the employee about the scope of counsel's representation and the general purpose of the investigation. But stick to generalities. It is best not to discuss strategies and theories of the case with people who do not need to know them. In the same vein, consider whether anyone from the company should be present during the interviews. Sometimes this may be preferable, but usually it is best to minimize the presence of observers in the room. Think twice about addressing sensitive topics with employees. The employee may repeat the information the interviewer discloses to the government or become otherwise unfavorable to the company's case. These tips are small parts of a bigger objective: carefully controlling what information is disclosed, and to whom.

Separate Counsel, Joint Defense Agreements, and Indemnification[5]

In some circumstances, it may be appropriate to recommend that a current or former employee hire separate counsel. This may be advisable if, for example, the employee's interests may become adverse to the company's interests at some time in the future. In

[4] The position of the Yates Memo on cooperation credit creates a tension for companies. On the one hand, it incentivizes the company to investigate immediately and disclose information relating to individual wrongdoers as soon as it becomes aware in order to qualify for cooperation credit and receive more favorable settlement terms. On the other hand, employees' knowledge that information shared during the investigation may be promptly shared with the government may discourage honesty and forthrightness for fear that the employee will be implicated. The policy also increases the tension between a Board, who must keep the best interests of the corporation first, and management, who may themselves be implicated of wrongdoing in information provided to the government. Executives may hire their own counsel more quickly, which may complicate the timing and logistics of the investigation and increase the need for complicated joint defense agreements.

[5] This section is intended to provide general information regarding the use of JDAs, with a focus on federal law. Courts' recognition of the existence and scope of the joint defense privilege varies across federal and state jurisdictions, and practitioners should research local law to confirm applicability to their particular circumstances.

today's climate, this has the potential to happen sooner rather than later, given the company's incentive to provide information to the government that may be detrimental to the interest of a particular employee. The same holds true if the government may interview the employee down the road. So, too, if counsel representing the company faces a conflict of interest. Even if there is no current conflict, counsel may potentially be forced to withdraw if a conflict becomes evident at a later date.

If an employee does obtain separate counsel, company counsel should explore the possibility of a joint defense agreement ("JDA") between the company and the employee. The joint defense privilege, sometimes a "common interest privilege," was recognized by courts as early as 1964 as an exception to the normal rule that attorney-client privilege and attorney work product protections are waived whether otherwise privileged communications or materials are disclosed to a third party.[6] Pursuant to this exception, privileged communications between a client and his attorney, and that attorney's work product, remained protected even if disclosed to certain third parties. In essence, pursuant to the joint defense privilege, information is permitted to be shared among defendants as if they were represented by joint counsel, but with each defendant having the benefit of individual counsel to fully protect and advocate for its own separate interests.

The privilege can be asserted defensively, to avoid having to disclose information to the government, and also offensively, to prevent another party to the joint defense group from disclosing joint defense information. The party seeking to establish the existence of a joint defense privilege and assert its protections must demonstrate that

(1) the communications were made in the course of a joint defense effort;
(2) the communications were designed to further the joint defense effort;
(3) the communications were intended to be kept confidential; and
(4) the privilege has not otherwise been waived.[7]

JDAs need not be written and can be formed by anything from simple oral undertakings to detailed written agreements.[8] Some attorneys choose not to reduce agreements to writing so that the agreements are not subject to production.[9] Others wish to avoid lengthy negotiations regarding nuanced waiver and limitations concerning issues that may or may not ever come into play.

At the same time, there are risks to JDAs. It is important for counsel to remember that, even though they are preparing a joint defense, they still owe an independent professional duty to their individual clients. Company counsel must do what is best for the company; the employee's counsel must do what is best for the employee. If counsel

[6] *See Continental Oil Co. v. United States*, 330 F.2d 347, 350 (9th Cir. 1964).
[7] *See, e.g., Continental Oil Co.*, 330 F.2d at 350.
[8] *Id.*
[9] Some courts have held that JDAs are not privileged and are subject to production for at least *in camera* review. S*ee, e.g., United States v. Stepney*, 246 F. Supp.2d 1069, 1074-75 (N.D. Cal. 2003).

anticipates that their clients' interests may diverge in the future, they should structure the JDA accordingly. One solution is to restrict the JDA to a limited issue on which the parties have common interests. Furthermore, the common interest privilege only protects the confidentiality of information exchanged to further the joint defense.

Companies may also want to consider indemnifying their current and former employees and advancing their legal fees, if they have separate counsel. In some cases, company executives may be entitled to such indemnification by agreement with the corporation, while other employees may need to negotiate a form of undertaking. From the company's perspective, providing such indemnification may improve employee cooperation, save time, and improve the company's control over the litigation. The government, however, may view indemnification as inconsistent with cooperation or as an endorsement of misconduct. Companies should compare the perceived benefit from indemnification with the risk that the government will adopt this view, and the consequences if it does so.

Preemptive Disciplinary Action

Not surprisingly, investigations often identify misconduct. In these instances, the company may consider taking preemptive disciplinary action against the responsible individuals. Whether or not this is advisable will depend on a variety of factors, including the seriousness of the employee's conduct and strength of evidence against him or her, the need to stop further misconduct, and the company's obligations under federal and state employment laws. For instance, while discipline may be helpful in that it stops or limits the actions of people who are damaging the company's interests, it may also be harmful by creating discontented, disloyal employees who become more willing to cooperate with the government *against* the company. However, sometimes the wrongdoers' actions are so egregious that there is no question discipline will be administered; it is just a matter of timing. If discipline is inevitable, the company may wish to put the matter behind it by addressing it early. The company also should consider what will happen if the company *does not* discipline the wrongdoers. If the company must discipline someone to prevent future harm from occurring, the case for preemptive action becomes stronger.

The company needs to consider how the government will interpret discipline. Depending on the circumstances, the government could plausibly interpret it as a good faith effort to remedy the problem, or as an admission of wrongdoing. Finally, depending on the seniority of the personnel and the nature of the conduct warranting discipline, such employment actions could trigger some reporting requirement, which could cause the subject of the investigation to become known outside the company earlier than anticipated.

ESTABLISH A PUBLIC RELATIONS STRATEGY

Corporate misconduct can damage a company's reputation. Controlling the timing and content of the information disseminated to the public is important. Companies, in conjunction with counsel, should designate a spokesperson to whom all outside inquiries should be directed. In-house or outside counsel may be adept at handling these inquiries. Another option is hiring a public relations firm. Companies should be aware that disclosure of investigation reports to the public may waive attorney-client privilege merely by referencing protected information. Mandatory disclosures made in the normal course of business—including, for example, quarterly reports—should conform to the public relations strategy. The goal is to control the message to the greatest extent possible. But at no point should the public relations message trump the litigation strategy. And, indeed, public relations mistakes can adversely impact the investigation itself. Early public denials, pronouncements of innocence, or, worse yet, statements of questionable veracity may provoke the government into a more vigorous investigation than it would otherwise undertake. Above all, the goal of an investigation is to resolve the alleged misconduct in the way that best suits the company's interests. Public relations should not be ignored, but it also should not distract from that goal.

CONCLUDING THE INVESTIGATION

The final considerations after the investigative team's work plan is complete are (1) how to report out the investigative team's findings, and (2) how to proceed with the information that has been ascertained. While the company's next steps and decisions about possible disclosures will ultimately be dictated by the investigative team's substantive findings, decisions regarding the form of the investigative report to senior management and the company's boards should be considered at the outset of the investigation.

Reports

At the conclusion of the investigation, counsel may wish to prepare a written report which summarizes the investigation, predicts risk of liability, presents arguments against prosecution, and recommends corrective action the company can take. There are many reasons why counsel may do this. A written report can be a useful tool to present the investigative team's findings to management or the company board. This is particularly the case if the factual evidence is voluminous or the issues are particularly complex. A report may be necessary to justify and document employee disciplinary actions that arise out of the investigation. It may also be used as the basis for an eventual oral or written submission to the government, if the company chooses to do so. The report can highlight the remedial measures the company takes to prevent similar misconduct in the future, and the report may be necessary proof of the

thoroughness of the investigation. Whatever the reason, counsel should consider the benefits and risks of drafting a written report before beginning the task.

A report can demonstrate the thoroughness of the investigation, setting forth the company's goals in opening the investigation, as well as the steps it has taken to achieve those goals. Indeed, if a report is not prepared, the government may suspect the investigation was cursory. The company should understand, however, that a report, if prepared, may have to be disclosed. If a written report is prepared, it may be inevitable that the government will request a copy once the investigation becomes known to them. And once privilege has been waived, the report can be obtained for use by private litigants. Thus, counsel and consultants should anticipate the risk of having to produce the report when they draft it.

As counsel consider the question whether to prepare a report at the end of an investigation, it is worthwhile to return to the beginning: the goals of the investigation. Will an oral report, rather than a written one, accomplish the goals and objectives of the investigation? If a written report will not further the goals, it may be better to avoid it. But if a report will meaningfully address the investigation's goals, it may be worth producing one.

Whether the report of the investigative findings is delivered orally or in written form, it usually includes:

(1) identification of the evidence or allegations that prompted the investigation and a statement that the investigation was conducted in anticipation of litigation and for the purpose of providing legal advice;
(2) a description of the work plan that was implemented;
(3) a summary of the relevant background facts;
(4) analysis of the key evidence;
(5) an outline of the pertinent law;
(6) an application of the law to the evidence;
(7) a description of the remedial measures that should be considered (or have been taken) as a result of any issues identified during the investigation; and
(8) a recommendation as to whether there should be a self-report or disclosure to the government.

Disclosure to the Government

Depending on the circumstances, at the end of an investigation the company may be forced to decide whether to voluntarily disclose the contents of the investigation to the government. As with producing a report, voluntary disclosure may persuade the government that the company has greater transparency and integrity. In other words, the company is not hiding anything from the government; it is simply investigating an alleged problem and reporting what it found. This, in turn, may lead to a more favorable resolution of the issue. Of course, self-reporting will not necessarily

prevent prosecution, but it may lead to better settlement terms by demonstrating cooperation and good faith. And, at a minimum, voluntary disclosure provides the government with the company's version of the facts. The government may use these facts to structure its own investigation, allowing the company to shape the matter as it moves forward.

Disclosure also has significant risks that the company should consider before it proceeds. First, disclosure to the government may waive the attorney-client privilege and work product protection in all other contexts. And by waiving privilege, the company may provide a roadmap for liability to civil litigants, including class action litigants. Although the case law is not uniform, courts typically do not uphold non-waiver or selective waiver agreements.[10] To reduce the possibility of waiver, the company should frame disclosures in terms of possible settlement negotiations with the government. Settlement discussions generally receive greater protection, but even these ultimately may not remain privileged. The company also should consider entering into a confidentiality agreement with the government, in which the government agrees not to disclose company information to third parties.

Second, disclosure can chill future discussions between company employees and attorneys and may thereby impair the corporation's ability to detect and prevent future wrongdoing. If employees believe that the company will report misconduct to the authorities, they are less likely to cooperate with the company's investigation. The company does not want to develop an "us vs. them" relationship with its own employees.

Third, the company should be careful about preemptively disclosing materials. It should time the disclosures so as not to interfere with the ongoing investigation (if indeed it is ongoing) and to ensure that unnecessary materials are not disclosed. To do so, it may seek to limit the disclosure to a limited issue or subject matter.

Sometimes, an internal investigation uncovers misconduct that is not yet on the government's radar screen. Should the company disclose this misconduct? Here again, the government may view voluntary disclosure as forthcoming, but disclosure may not prevent prosecution. At the same time, if the government is already conducting its own investigation, and if it is likely to discover the misconduct anyway, self-reporting may be the preferred course.

Following the Yates Memo, and consistent with its goal of incentivizing companies to provide the government with information concerning culpable individuals, the

[10] *Compare Diversified Industries, Inc. v. Meredith*, 572 F.2d 596, 611 (8th Cir. 1978) (holding that a company's disclosure of witness interview memoranda to SEC constituted limited waiver and allowing company to withhold memoranda in subsequent third party lawsuit) *with In re Pacific Pictures Corporation*, 679 F.3d 1121, 1127 (9th Cir. 2012) (rejecting limited waiver doctrine); *In re Qwest Communications International Inc.*, 450 F.3d 1179, 1192 (10th Cir. 2006) (same); *In re Columbia/HCA Healthcare Corp. Billing Practices Litigation*, 293 F.3d 289, 297 (6th Cir. 2002) (same).

Department of Justice has recently issued more concrete guidance to companies regarding self-disclosure and its effect on cooperation credit. In April 2016, for example, the Department of Justice issued an "FCPA Enforcement Pilot Program" with the goal of motivating companies to self-disclose FCPA related misconduct. The credit awarded to a company under the pilot program depends on how closely it follows the issued guidance. As stated by the Department of Justice:

> [I]f a company chooses not to voluntarily disclose its FCPA misconduct, it may receive limited credit if it later fully cooperates and timely and appropriately remediates – but any such credit will be markedly less than that afforded to companies that do self-disclose wrongdoing. By contrast, when a company not only cooperates and remediates, but also voluntarily selfdiscloses misconduct, it is eligible for the full range of potential mitigation credit.

Similarly, the Department of Justice released additional guidance in November 2016 encouraging companies to self-disclose criminal export control and sanctions violations before the company perceives an imminent threat of disclosure or a government investigation has been initiated. The Guidance also confirmed that full cooperation and/or self-disclosure can earn the company a more lenient penalty or the possibility of entering into a non-prosecution agreement with the government regarding such export violations. As in all areas, a company must balance any benefit of potential government leniency following self-disclosure against the costs associated with any government investigation.

Remedial Measures

Based on the information gathered during the investigation, the investigative team should recommend and the company should decide what remedial measures, if any, should be undertaken. Disciplining employees tends to demonstrate that the company takes wrongdoing seriously. Some discipline may be necessary from a business standpoint to ensure that employees do not continue to cause trouble. There is a risk that employee discipline could be viewed as an admission of wrongdoing. And, if disciplined, employees could refuse to cooperate with the company and instead cooperate with the government. Unwarranted or overly severe discipline may also damage morale. Employees who feel a connection to their colleagues may take the discipline personally. If the company does decide to discipline an employee, it may have to create a memorandum or report to justify its action. That record, though, may be deemed part of the employee's personnel file and may need to be disclosed.

If the investigation revealed evidence of potential ongoing or recurring violations, the company also should consider taking procedures necessary to prevent any further

violations. This might include instituting new procedures, instituting new training sessions, revising compliance materials or developing new internal audits or oversight committees to review compliance on a periodic basis. Policing internal misconduct through an investigation is, in many ways, no different than other business matters. It is best to be thorough in preparation and action, learn from mistakes, and make improvements when necessary.

CONCLUSION

An internal investigation can be a critical tool when allegations or evidence of misconduct within a company, or within a company's industry, arise. Internal investigations of every size require balancing efficiency with quality, thoroughness, and completeness. And above all else, an effective internal review requires careful planning at the outset. While the best compliance program and training regime cannot completely prevent some types of misconduct—or, at the very least, allegations of misconduct—from occurring, practical preparedness and a carefully scoped internal review of the situation is the best defense.