JANUARY 2015

EXPECTING THE UNEXPECTED: HOW TO PREPARE FOR, RESPOND TO, AND SURVIVE A SEARCH WARRANT

It is a company's worst nightmare. Out of the blue, government agents appear at the reception desk armed with a search warrant, demanding access to company emails, files, and other proprietary data. Employees soon notice and become increasingly anxious and agitated as agents comb through their offices and begin to interview some of them. Neighboring establishments and the media then catch wind of what's happening. Camera crews arrive in time to capture grim-faced agents hauling box after box of corporate records out of the business and into awaiting evidence vans. The "raid" is the lead story on the evening news and featured on the front page of the next morning's paper.

For some companies, this nightmare scenario is an all-too-painful reality. Indeed, although search warrants are among the most extreme and intrusive government investigative tools, they are used with regularity to gather evidence from a wide variety of business organizations.[1]

A company's response in the minutes and hours after the government executes a search warrant can impact the outcome of the entire government investigation. A well-executed response can also help establish the foundation for an internal corporate investigation into the alleged conduct on which the search was predicated. Because the stakes are high when presented with a search warrant, every company should have a well-developed plan in place to react quickly in order to appropriately protect the company. Advance planning and employee training can greatly assist a company should it later become the target of a government inquiry and/or the subject of a government search warrant.

Such planning and training can likewise pay dividends for the internal investigation that will almost inevitably follow an unexpected government raid on a company. Robust corporate compliance programs often uncover suspicious conduct even in the absence of a government investigation. When an internal investigation is commenced apart from any government inquiry, the company typically can set the scope and pace of the investigation at its discretion. In contrast, where an internal investigation is triggered by a government search, it is important for the company itself to be able to gather information from the search for use in fashioning the ensuing internal investigation.

This White Paper provides a breakdown of what a company needs to know and do in the immediate wake of the execution of a search warrant, and the attached 10-step checklist offers a quick reference guide for in-house counsel when confronted with a search warrant.[2]

PREPARING FOR A SEARCH WARRANT

The in-house legal team at most companies will have no experience responding to the execution of a search warrant and, in all likelihood, will not know what the company ought to do when subjected to a government search. The fog of the moment while a search is proceeding is difficult enough for veterans of search warrants to deal with; it can be utterly paralyzing for first-timers.

To ensure that the best practices outlined in this publication are known to, and followed by, the right personnel in your company, appropriate effort should be expended in preparing for the possibility, however seemingly remote, that the company will be searched by the government at some point in the future. In particular, a written search warrant response protocol consistent with the guidance presented here would be advisable. Moreover, communication between relevant corporate personnel and outside counsel long before any government agents arrive with a search warrant can allow the company to prepare a response that is tailored to its particular needs.

RESPONDING TO A GOVERNMENT SEARCH WARRANT

Although the government may investigate a company for months or even years beforehand, a search warrant is often the company's first clue that it may be the target of an ongoing inquiry. The government is required to obtain the approval of a judicial officer (e.g., a magistrate judge) to conduct a warrant-based, nonconsensual search. In the search warrant affidavit, the government must explain its theory of criminal conduct, and then link that theory to the items sought in the search. The premises to be searched, the items to be seized, and the justification for the search must be set forth with reasonable particularity in the warrant and supporting materials. In other words, a search warrant should not be—and usually is not—a broad "fishing expedition" but instead an exercise targeted at specified places and things, and typically informed by substantial pre-warrant fact gathering.

Search warrants, then, are normally key events in government investigations, and companies need to prepare for, and respond to, the execution of warrants accordingly. In particular, it is critical for the company to manage the logistics of the search, and manage its employees.

MANAGING THE LOGISTICS OF THE SEARCH

Immediately Contact Counsel and Key Corporate Personnel. As indicated in the attached checklist, counsel (along with key corporate personnel) should be contacted immediately once it is determined that law enforcement officers intend to execute, or are in the process of executing, a search warrant on company property.

Control the Information Flow. The execution of a search warrant generally involves many agents, often from multiple agencies, descending upon the company in a manner that is unavoidably disruptive to business operations. Maintaining calm within the organization and effectively managing the flow of information to the agents should be two paramount goals. To avoid confusion, the company should designate one person to deal with the government agents and consider sending home all employees not essential to the search or ongoing business operations.[3]

Review the Warrant. Government agents executing a search warrant are generally required to leave a copy of the warrant at the premises searched. At the first opportunity, the corporate representative should request a copy of the warrant and supporting affidavit. The supporting affidavit, which sets forth the factual foundation for the warrant, will most likely be under seal at the time of the search and remain unavailable for some time. But the company can nevertheless learn important information from the warrant itself. For instance, the warrant is likely to contain information about the timeframe of the investigation, specify the types of data authorized to be seized, and detail any limitations on the scope of the search.

Monitor all Government Agents. It is important to identify and monitor all government agents participating in the search and to ensure that the agents limit their search to the information and scope set forth within the warrant. Broadening the search beyond the confines of the warrant is usually not permissible without getting additional authorization from a court. A company is not required to agree or consent to searches of areas beyond the scope of the warrant. Any request for such consent should only be considered by an authorized corporate representative and, ideally, with input from counsel. Although a company may ultimately decide to give consent to an expanded search, careful consideration of such a request will at least provide the company with an opportunity to weigh the pros and cons as apparent at the time, including the risk that additional searching may subject the company to further scrutiny on matters beyond those underlying the warrant and increase the burdens on its business operations.

Document Communications with Government Agents and Search Activities. As much as possible, memorialize the questions asked by agents to company employees or executives and the answers given. Also, keep track of and document other activities undertaken by agents during the search. Which rooms did they search and which rooms (if any) did they skip? Did they show particular interest in certain places or materials? Did they reference any particular employees or officers, or company customers or vendors? Such details may provide insight in assessing the exposure of the company and its personnel, and what the company itself ought to do to get to the bottom of the matter.

Protect Privileged Documents. During the search, agents may encounter items that are protected by the attorney-client privilege. For example, agents may attempt to search the offices of in-house legal counsel or offices of corporate executives who have regular communications with outside counsel for a variety of matters. Agents may also seek to seize company computers, hard drives and/or servers, all of which may contain information protected by the attorney-client privilege and work-product doctrine. It is critical for the company to advise agents of potentially privileged material. Department of Justice guidance instructs prosecutors to "ensure that privileged materials are not improperly viewed, seized or retained" during the course of a search warrant.[4] Thus, once the company alerts the government to the presence of potentially privileged materials, the prosecution should establish a "taint team," consisting of agents and lawyers not involved in the underlying investigation, to review the potentially privileged materials.[5] To adequately guard against the inadvertent seizure, review or disclosure of protected documents, the company should prepare a list of all in-house attorneys, as well as all outside counsel whose communications might fall under the protection of the attorney-client privilege.

Preserve and/or Obtain Copies of Materials Needed to Carry on Business Operations. In today's world, most corporate information is stored electronically on computers and servers rather than in hard copy. Justice Department guidance directs agents to be minimally intrusive and not overly broad in their search of electronic information at a business.[6] Whenever possible, ask the government's forensic team present during the execution of the search warrant to make copies of electronic materials rather than taking them offsite to be searched later. Further, before agents remove any electronic or hard copy materials gathered during the search, the company—through criminal counsel—should request copies of all materials necessary for ongoing business operations. If the agents insist on taking hard drives or computers with them, communicate with the lead prosecutor to have

the materials returned to the company as quickly as possible. Although unlikely, in cases where the prosecution team unduly delays in providing copies of seized materials needed to carry on with everyday business operations, the company may need to compel swift action through an application to the court.

Obtain an Inventory. Obtain a complete inventory of all company property seized before the agents leave the facility. The company has a right to this under Federal Rule of Criminal Procedure 41(f)(1).

MANAGING EMPLOYEES

The government's overall plan for executing a search warrant often includes a strategy for employee interviews. Department of Justice policy allows agents to interview a company's employees in certain circumstances, provided that the company is not represented by counsel on the particular matter about which the employees are being interviewed.[7] In the context of a covert investigation, the company rarely knows that it is being investigated at all, and so will likely not have engaged counsel on the subject matter of employee interviews. The timing of when to execute a search warrant (i.e., when to transform a covert investigation into an overt one), can be heavily influenced by whether the agents believe certain company employees will be available to be interviewed. In practice, this often means that investigators will plan the execution of a search warrant around potential "surprise" interviews of employees who are strategically important to the government's investigation. Such interviews may occur during the initial confusion caused by the search warrant itself, or even prior to the search while the employees are at home or on their way to work. The element of surprise is critical to government investigators, because once an organization is represented by counsel, an agent's ability to interview the company's employees outside the presence of corporate counsel can be much more limited.

Questioning by a government agent can be frightening and upsetting. Most employees do not know their rights or what the law allows and prohibits under these circumstances. Companies are well served by anticipating the possibility that their employees could be interviewed by government agents in the context of a search. Employees should be trained accordingly. More specifically, before agents ever appear at the company, employees should know that:

- Government investigations (and search warrants of businesses in particular) are not routine matters. They should be taken seriously. Even if an agent jokes or tries to develop a rapport with the witness, the employee should know that the agent could be recording every word, either overtly or covertly.
- An employee is not obligated to speak with any government agent and is generally well advised not to do so before consulting with counsel.[8] If the employee agrees to a government interview, he or she may terminate the interview at any time, may refuse to answer any question posed, and may also insist that an attorney be present during the interview.[9] Historically, the government has not been permitted to draw any negative inference from an employee's refusal to speak with government agents. Recent case law, however, suggests that employees who initially cooperate during a search may face additional scrutiny if they subsequently refuse to answer certain questions posed by government agents.[10] In light of the Supreme Court's comments in *Salinas v. Texas*, there is a heightened risk for both the company and the cooperating employee if the employee chooses only to answer certain questions or otherwise partially participate in a government-led interview.
- Given the perils associated with employee interviews, a company should strongly consider having counsel available for employees to consult with during the execution of a search warrant. Employees have the right to consult with an attorney before and during any interview with investigators, and it is generally prudent for employees to discuss with counsel their rights, obligations, and risks before talking with government investigators.
- If an employee agrees to an interview with a government agent, it is imperative that he or she only provide truthful, non-misleading answers. Intentionally providing false statements to a federal agent is a felony.[11] And even if inadvertent, the consequences of an inaccurate answer can be severe. For example, the government may believe the mistaken answers of an unprepared, frightened employee were, in fact, intentional. Moreover, whether intentional or inadvertent, everything that an employee says to the federal agent can be used against him or her, and often against the organization, in a future prosecution.

WHAT NOT TO DO

Being aware of the things a company should *not* do in response to a search warrant can be just as important as knowing the steps a company should take. In order to protect the company's best interests while responding to a search warrant, be sure to provide the information or access as required by law and do not take steps that would interfere with the government's investigation.

Specifically, the company and company personnel should *not*:

- Obstruct the execution of the warrant;
- Destroy, alter, remove, or hide records;
- Consent to a search or seizure beyond the area or

materials identified in a search warrant without appropriate, informed consideration of the potential benefits and disadvantages of such consent after consultation with counsel;
- Prohibit employees from speaking to government agents;
- Volunteer substantive details without appropriate authorization from designated corporate personnel after consultation with counsel; or
- Communicate about matters covered by the corporation's attorney-client privilege in such a way as to potentially waive the privilege.

If you have questions about how to manage your company's response or perceived "gray" areas in this what-not-to-do list, seek the advice of outside counsel.

FOLLOW-UP

Late-Discovered Materials. After the government has completed its search, it is not uncommon for a company to discover additional relevant materials that the government did not review or seize during its search. This could happen for any number of reasons, e.g., a single filing cabinet was inadvertently overlooked or a misfiled box of materials was only located after the government finished its search. Typically, there is no obligation to notify the government of late-discovered materials, but depending on the circumstance of the case, it may be prudent to do so. If such materials are discovered, the company should consider, with the advice of outside counsel, whether and how to alert the government to the existence of these materials.

"Clean-Up" Subpoena. In many instances, the government will anticipate the potential for late-discovered materials that were not seized during the search by issuing a "clean-up" subpoena. A clean-up subpoena either can be served at the time of the search, or in the days or weeks to follow. This subpoena will often request the production of a broad array of information, including many materials that may have already been seized during the search. The government's purpose in serving a clean-up subpoena is as the term implies—to clean up after the often-hurried search and collect relevant information the agents may have inadvertently left behind. A company's obligations with respect to a clean-up subpoena are the same as with a subpoena that did not follow a search, but a clean-up subpoena may afford a company with comparatively greater flexibility in negotiating aspects of the response, given that many of the requested items are likely to have already been obtained by the government through the original search.

Continued Dialogue. It is important to maintain an open line of communication with the government following a search and seizure. Often the government will "go silent" after it executes its search warrant as it reviews the seized materials and otherwise continues its investigation. By maintaining communications with the lead government agent through its outside counsel, the company can: (i) attempt to learn more about the government's investigation; (ii) better evaluate the company's status in the investigation (e.g., as a subject or target); (iii) establish a good rapport with the government for whatever might come next; and (iv) open discussions and negotiations about cooperation, information-gathering going forward, and the ultimate resolution of the matter.

APPLYING THE LEARNING FROM THE SEARCH TO AN INTERNAL INVESTIGATION

To be sure, a search warrant is about as invasive and threatening as a law enforcement activity can be. But it can also be regarded as an opportunity—an opportunity for the company to discover for itself whether corporate personnel or third parties connected to the company have engaged in misconduct that exposes the company to legal, financial, and/or reputational harm.

If the steps outlined in this publication are followed, the company subjected to a raid will have some understanding of the conduct at issue—if not the persons potentially involved—and can use that understanding to develop an internal investigation plan. Instead of merely awaiting instructions or requests from the government, and instead of being content to try to read the tea leaves that the government might offer to shed light on what is under investigation, a company should be determined to conduct its own investigation and quickly get ahead of the government in fact-gathering and analysis. A company that gets a handle on the facts is generally much better positioned to take remedial action (e.g., personnel changes, policy/process reform), mitigate the risk of ongoing violations, and negotiate an appropriate resolution to the matter.

CONCLUSION

Search warrants are a tool used increasingly often in the white collar context. Execution of a search warrant can have a profound effect on a company by disrupting operations, depleting employee morale, and, in some cases, tarnishing the public image of the company. Although it is impossible to prevent or completely eliminate the disruption associated with a search, preparation ahead of time can minimize the business disruption and place the company in the best possible legal position during and after the search.

10-STEP CHECKLIST FOR IN-HOUSE COUNSEL RESPONDING TO A SEARCH WARRANT

These steps provide guidance regarding how to respond when a company is presented with a government search warrant.

Step 1. Contact outside counsel. As soon as you learn that the government is executing a search warrant at your company, you should contact outside criminal counsel and request that the search be delayed until outside counsel arrives on site. Although the government is under no obligation to wait for counsel's arrival once the warrant has been approved by the court, having criminal counsel present to observe and monitor the search in real time can be helpful in protecting the company's interests, especially with regard to confidential trade secrets and privileged materials. All interactions with the government should proceed through, or with the advice of, outside counsel. Remember that any statements you make to the government may be attributed to the company.

Step 2. Gather basic information about the agents and purpose of the investigation. Collect basic preliminary information about: (i) the purpose behind the search, (ii) the identity of the lead government agent, (iii) the names of other agents, (iv) the agency leading the investigation, and (v) the lead prosecutor.

Step 3. Provide instructions to employees. Instruct all non-essential employees to leave the premises, but admonish departing employees not to take any materials out of the office or destroy or delete any paper or electronic files while the search is being executed. Instruct all employees regarding their rights in connection with the government's investigation, including the right not to speak with government agents and the right to consult with company counsel prior to or during any interview.

Step 4. Connect outside counsel with lead agent. Your outside criminal counsel should be conducting, or advising on, all communications with the government. Where possible, criminal counsel should negotiate reasonable procedures with the lead agent to ensure that the search will proceed smoothly and minimize any disruption to the business.

Step 5. Analyze the search warrant and any "clean-up" subpoena. Obtain a copy of the search warrant and any accompanying affidavits or "clean-up" subpoena. Request the search warrant affidavit but recognize that, for some period of time, the affidavit may be under seal and unavailable. Analyze any available materials to: (i) determine the terms and scope of the government's investigation, (ii) raise any defects in the warrant, and (iii) negotiate, if possible, an alternative method of production that will assure no evidence will be lost or destroyed.

Step 6. Communicate internally and prepare a public response. Communicate pertinent information about the government's investigation, requests, and deadlines to all relevant internal players. Then, organize a unified, company-wide effort to address the investigation and prepare a coordinated public response. Work with outside counsel and/or a public relations firm to formulate a crisis management plan, including a draft press release to respond to media inquiries.

Step 7. Protect privileged and/or confidential materials. Identify and protect any privileged, confidential, or trade secret materials that the agents have reviewed and seized. Inform agents of potentially privileged materials and request that such documents be segregated and kept under seal until privilege disputes are resolved. Quickly communicate with the lead prosecutor to ensure that a separate "taint team" is established to review the protected materials.

Step 8. Track and inventory all seized or produced records. To the extent possible, create a log to track all materials that end up in the government's possession, and make a copy of all records seized by or produced to the government. If possible, make copies of any materials that are necessary for ongoing business operations before the agents remove such documents from the premises. If agents insist on taking documents critical for business operations, use outside counsel to contact the lead prosecutor to negotiate a speedy return of such materials.

Step 9. Conduct debriefings with employees and memorialize the government's search activities. In the aftermath of a search warrant, the company is likely to initiate an internal investigation. Whether or not an internal investigation ensues, the company should conduct a privileged debrief with employees involved in the search warrant about their interactions with the government. Document these interactions (under the attorney-client privilege and work-product doctrine), as well as other actions or statements made by agents during the course of the search.

Step 10. Notify employees of document preservation obligations. Determine your company's status in the government's investigation. If your company appears to be the subject or target of the investigation, draft and distribute a document preservation notice internally.

ENDNOTES

1 Once probable cause has been established, the Department of Justice can execute a search warrant on all types of companies—from hospitals to hedge funds, from technology companies to manufacturers—to investigate any federal crime. *See* remarks by Assistant Attorney General for the Criminal Division Leslie R. Caldwell at Taxpayers Against Fraud Education Fund Conference (September 17, 2014), *available at* http://www.justice.gov/opa/speech/remarks-assistant-attorney-general-criminal-division-leslie-r-caldwell-taxpayers-against (describing new emphasis on search warrants, wiretaps, undercover operations and other criminal evidence-gathering tools in parallel proceedings initiated by qui tam cases); *see also* Remarks by Deputy Attorney General James M. Cole at the Foreign Corrupt Practices Act Conference (November 19, 2013), *available at* http://www.justice.gov/opa/speech/deputy-attorney-general-james-m-cole-speaks-foreign-corrupt-practices-act-conference ("Together, we are pursuing more cases than ever before, and we are using all of the investigative tools available to us from subpoenas to search warrants, from body wires to wiretaps.").

2 The analysis in this article pertains to federal search warrants executed on companies within the United States, as governed by Federal Rule of Criminal Procedure 41.

3 Departing employees should be instructed not to take any materials out of the office while a search warrant is being executed.

4 *See* U.S. Dep't of Justice, United States Attorneys' Manual § 9-13.420, available at http://www.justice.gov/usao/eousa/foia_reading_room/usam/title9/13mcrm.htm#9-13.420.

5 *Id*.

6 Office of Legal Education, Executive Office for United States Attorneys, Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations, Ch. II (C)(2)(d), *available at* http://www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf.

7 *See* U.S. Dep't of Justice, Criminal Resource Manual § 296, *available at* http://www.justice.gov/usao/eousa/foia_reading_room/usam/title9/crm00296.htm.

8 U.S. Const. amend. 5; *see, e.g., United States v. Kordel*, 397 U.S. 1 (1970). Importantly, this analysis is limited to private sector employees, rather than employees of a public entity. *See Garrity v. New Jersey*, 385 U.S. 493 (1967).

9 *See, e.g., United States v. Hampton*, 153 F. Supp. 2d 1262 (D. Kan. 2001) (finding government interview of company employee during execution of search warrant was not custodial—and thus not subject to *Miranda* rights—because agent informed employee she was free to leave and permitted her to consult with her attorney during the interview).

10 *Salinas v. Texas*, 570 U.S. _____, 133 S. Ct. 2174 (2013) (where cooperating individual does not expressly invoke his Fifth Amendment right, the government may draw an adverse inference from the individual's refusal to answer certain questions posed by investigator during a non-custodial interview).

11 *See*, *e.g.*, 18 U.S.C. § 1001.

LAWYER CONTACTS

For further information, please contact your principal Firm representative or one of the lawyers listed below. General email messages may be sent using our "Contact Us" form, which can be found at www.jonesday.com.

Charles M. Carberry
New York / Washington
+1.212.326.3920 / +1.202.879.5453
carberry@jonesday.com

Theodore T. Chung
Chicago
+1.312.269.4234
ttchung@jonesday.com

Richard H. Deane
Atlanta
+1.404.581.8502
rhdeane@jonesday.com

Samidh Guha
New York
+1.212.326.3721
sguha@jonesday.com

Karen P. Hewitt
San Diego
+1.858.314.1119
kphewitt@jonesday.com

Cheryl L. O'Connor
Irvine
+1.949.553.7505
coconnor@jonesday.com

Matthew D. Orwig
Dallas / Houston
+1.214.969.5267 / +1.832.239.3798
morwig@jonesday.com

Daniel E. Reidy
Chicago
+1.312.269.4140
dereidy@jonesday.com

Steve G. Sozio
Cleveland
+1.216.586.7201
sgsozio@jonesday.com

Neal J. Stephens
Silicon Valley
+1.650.687.4135
nstephens@jonesday.com

Brian A. Sun
Los Angeles
+1.213.243.2858
basun@jonesday.com

Hank Bond Walther
Washington
+1.202.879.3432
hwalther@jonesday.com

James R. Wooley
Cleveland
+1.216.586.7345
jrwooley@jonesday.com

Shireen M. Becker
San Diego
+1.858.314.1184
sbecker@jonesday.com

James C. Dunlop
Chicago
+1.312.269.4069
jcdunlop@jonesday.com

Caitlin A. Bell
Cleveland
+1.216.586.7584
cbell@jonesday.com