Expecting the unexpected: how to prepare for, respond to, and survive a search warrant

USA | January 24 2015

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 to be seized. 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

Also available as part of the eCourse
2023 Corporate Counsel eConference

First appeared as part of the conference materials for the
45th Annual Corporate Counsel Institute session
"What to do When the Government Comes Calling"