What to Do When the FBI Knocks on Your Door

Employer and Employee Rights and Responsibilities

Federal Bar Association CLE
April 22, 2011

Introduction

- **Types of Information "Requests" from Government Authorities:**
  - Informal inquiries (consensual production of documents, computer files, employee interviews, etc.).
  - Administrative agency subpoenas.
  - Search warrants.
  - Grand jury subpoenas.
  - Formal requests/agreements for corporate "cooperation."

Today's Discussion

- Potential pitfalls for employers conducting/facilitating searches generally.
- What to do when the team of agents arrives with a search warrant.
- Maintaining, organizing, and producing information responsive to a subpoena.
- Corporate Cooperation: Constitutional, privilege and work product issues.

Potential Pitfalls for Employers

- **Criminal Obstruction of Justice:**
  - 18 U.S.C. §1503 (General Obstruction Statute)
  - 18 U.S.C. §1505 ("Obstruction of Proceedings Before Depts., Agencies, & Committees")
  - 18 U.S.C. §1512 ("Tampering With a Witness, Victim, or an Informant")
  - 18 U.S.C. §1519 (Part of Sarbanes-Oxley)

The Good News

- Everyone (including the government) knows that no process is perfect and that mistakes will be made.
- Obstruction charges/sanctions rare where company:
  - Responds properly to search warrants and subpoenas;
  - Properly warns/educates employees;
  - Honestly attempts to preserve responsive evidence; and
  - Undertakes a documented good-faith effort to collect all relevant documents.

Potential Pitfalls for Employers (*cont'd*)

- **Fourth Amendment/Article I, § 9.**
  - Applies only to *public* employers (unless private employer is acting at behest of government).
  - Prohibits "unreasonable" searches and seizures.
  - "[T]he government as employer indeed has far broader powers than does the government as sovereign." *Waters v. Churchill*, 511 U.S. 661, 671 (1994) (plurality opinion).
  - Employees can seek damages pursuant to 42 U.S.C. § 1983.

Potential Pitfalls for Employers (*cont'd*)

- **Fourth Amendment/Article I, § 9 (*cont'd*).**
- *O'Connor v. Ortega*, 480 U.S. 709 (1987):
  - 4th Amdt. implicated only if conduct infringed "an expectation of privacy that society is prepared to consider reasonable."
  - Case-by-case analysis.
  - Here, reasonable expectation of privacy:
    - Private office; didn't share desk or file cabinets with others.
    - No regulation or policy discouraging storing personal effects in offices.
  - "[P]ublic employer intrusions on the constitutionally protected privacy interests of government employees for noninvestigatory, work-related purposes, as well as for investigations of work-related misconduct, should be judged by the *standard of reasonableness* under all the circumstances. Under this reasonableness standard, *both the inception and the scope* of the intrusion must be reasonable." (Emphasis added.)

Potential Pitfalls for Employers (*cont'd*)

- **Fourth Amendment/Article I, § 9 (*cont'd*).**
- *Quon v. City of Ontario*, 130 S.Ct. 2619 (2010):
  - City provided pagers to certain members of law enforcement and audited some of the text messages.
  - Reversing 9th Circuit, Supreme Court held that search was reasonable:
    - Written policy notified employees of city's right to monitor e-mail and internet use. But Court didn't decide "expectation of privacy" issue—assumed *arguendo* that expectation existed.
    - "Inception" reasonable: employees had vastly exceeded allowable number of texts.
    - "Scope" reasonable: employer requested only two months of transcripts and redacted all messages sent while employee was off-duty.

Potential Pitfalls for Employers (*cont'd*)

- **Fourth Amendment/Article I, § 9 (*cont'd*).**
  - When purpose of search shifts from work-related misconduct to general criminal investigation, *O'Connor* "reasonableness" standard for work-related searches no longer applies (i.e., search is subject to probable cause/warrant requirements). *U.S. v. Taketa*, 923 F.2d 665 (1991).

Potential Pitfalls for Employers (*cont'd*)

- **Stored Communications Act (18 U.S.C. § 2701, *et seq.*):**
  - Generally prohibits "providers of electronic storage information" from releasing such information to third parties.
  - Provides cause of action against anyone who "intentionally accesses [such information] without authorization."
  - *Pietrylo v. Hillstone Restaurant Group*, Docket No. 2:06-cv-05754 (D.N.J. 2008)
    - Restaurant employees created MySpace group.
    - Password protected/labeled private ("EULA").
    - Owners got password, looked, fired employees.
    - Violation of SCA – even though employee consented, owners may have compelled password from employee.

Potential Pitfalls for Employers (*cont'd*)

- **Computer Fraud & Abuse Act (18 U.S.C. § 1030)**
  - Provides cause of action against one who "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer."

Potential Pitfalls for Employers (*cont'd*)

- **Surreptitious Recordings of Conversations:**
  - Unlawful for any person "to obtain or attempt to obtain the whole or any part of a conversation by means of any device . . . If all participants in the conversation are not specifically informed that the conversation is being obtained." ORS 165.540(1)(c).

Potential Pitfalls for Employers (*cont'd*)

- **Employee Polygraph Protection Act (29 U.S.C. § 2001, *et seq*.; *see also* ORS 659A.300):**
  - Employers *generally* prohibited from requiring or requesting employee or job applicant to take a lie detector test, or from taking adverse employment actions based on refusal to take such a test.

Today's Discussion

- Potential pitfalls for employers conducting/facilitating searches generally.
- What to do when the team of agents arrives with a search warrant.
- Maintaining, organizing, and producing information responsive to a subpoena.
- Corporate Cooperation: Constitutional, privilege and work product issues.

The Setting

- Large team of armed agents swarm the premises.
- Secure entrances and exits.
  - Nobody let in our out.
- Lead agent directs search.
  - Computers, trade secrets and privileged materials may be taken.
  - Employees will be interviewed.
- Process will take the entire day.

What to do?

- Felony to interfere with officers executing a search warrant.
- Felony to obstruct justice.
  - The FBI does not have a sense of humor.
- But the company and its employees have rights that must be protected.

Steps to Take

- Notify Outside Counsel.
  - Contacts agent in charge and/or prosecutor.
- Review the Warrant.
  - Check details on name and address.
  - Make sure search does not go beyond what's authorized.
  - Don't consent to additional searches.

Steps to take (*contd.*)

- Seek to avoid the seizure of privileged materials.
- Prepare an inventory of what's seized.
- Gather information on the government's investigation.

Steps to take (*contd.*)

- Limit/monitor government interviews of employees.
  - May send non-essential employees home.
  - Advise employees of their right not to talk and to be represented by counsel.
    - *Be careful not to go too far!*
  - Attempt to attend interviews as they happen.
  - Debrief employees interviewed outside of your presence.

Steps to take (*contd.*)

- After the Agents are Gone:
  - Contact the prosecutor.
  - Prevent document destruction.
  - Communicate with employees.
  - Commence an internal investigation.
  - Consider media strategy.
  - Consider motions for return of privileged and/or other documents that were seized.

Today's Discussion

- Potential pitfalls for employers conducting/facilitating searches generally.
- What to do when the team of agents arrives with a search warrant.
- Maintaining, organizing, and producing information responsive to a subpoena.
- Corporate Cooperation: Constitutional, privilege and work product issues.

Subpoenas vs. Search Warrants

- Might think that subpoenas are less disruptive than search warrants, but . . .
  - no "probable cause" required, so usually much broader in scope.
- Advantages to company of subpoenas:
  - opportunity to negotiate;
  - opportunity to protect privileged/confidential material; and
  - opportunity to consult with counsel.
- Note: No Fifth Amendment "Act of Production" protection for corporations (*Bellis v. U.S.*, 417 U.S. 85, 88 (1974)

Subpoena Compliance

- Rule # 1: Do ***not*** treat this like a routine civil discovery request.
  - Do ***not*** adopt the non-cooperative posture that companies sometimes adopt in civil litigation.
  - Risks associated with violating Rule # 1:
    - determination that company is not "cooperating";
    - search warrant;
    - obstruction charges.

Subpoena Compliance (*contd.*)

- **Step 1:** Litigation hold order to employees likely to have responsive information:
  - information (*including back-up tapes*) must be retained notwithstanding contrary provisions in retention policy;
  - no responsive information may be destroyed, etc. until counsel authorizes resumption of retention policy;
  - violation will result in disciplinary action, up to and including termination; and
  - written acknowledgement is required.
- Samples of notice & acknowledgement in materials.

Subpoena Compliance (*contd.*)

- **Step 2:** Advise employees of rights and obligations relating to the investigation:
  - Brief overview of investigation.
  - Procedures if contacted by government agents.
  - Offer of assistance in obtaining and (where appropriate) paying for individual counsel.
  - *Avoid any suggestion or implication of a direction not to cooperate.*
- Sample memo included in materials.

Subpoena Compliance (*contd.*)

- **Step 3:** Assign Roles
  - *Outside* counsel to coordinate process:
    - Objectivity.
    - Avoid risks of attack on privilege.
  - Custodian of records:
    - Involved in collection, review, and production.
    - May have to testify and/or sign affidavit of compliance.
    - Should be someone who is *not* a potential fact witness and *not* member of legal department.

Subpoena Compliance (*contd.*)

- **Step 4:** Negotiate Scope of the Subpoena
  - Speak with employees (IT personnel and relevant employees) to learn general volume, types of responsive info, and special issues (e.g., privileged materials, trade secrets).
  - Negotiate with government:
    - Narrow scope of overbroad requests.
    - "Rolling" production.
    - Protection for trade secrets/confidential information.
      - Sample protective order in materials.

Subpoena Compliance (*contd.*)

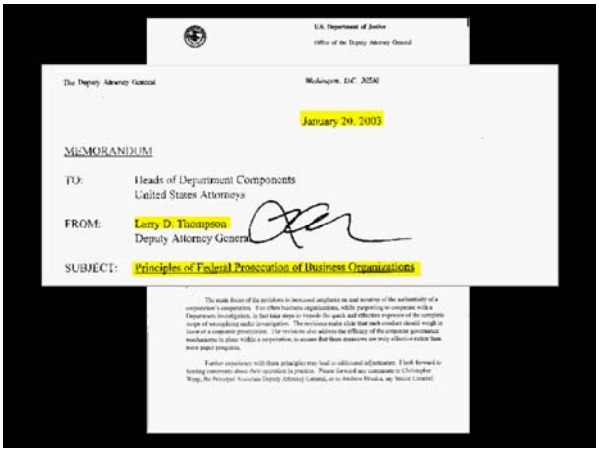
- **Step 5:** Collect and Review Responsive Materials:
  - Image and Bates number all documents (including electronic records).
  - Substantive review to assess areas for investigation and exposure.
  - Segregate privileged documents and create privilege log.
    - Inadvertent production can lead to disaster.
      - *But see* recently amended FRE 502(b).

Today's Discussion

- Potential pitfalls for employers conducting/facilitating searches generally.
- What to do when the team of agents arrives with a search warrant.
- Maintaining, organizing, and producing information responsive to a subpoena.
- Corporate Cooperation: Constitutional, privilege and work product issues.

Issues With Corporate Cooperation

- Background
  - 1999 "Holder Memo" and 2003 "Thompson Memo"



U.S. Department of Justice
Office of the Deputy Attorney General

The Deputy Attorney General
Washington, D.C. 20530

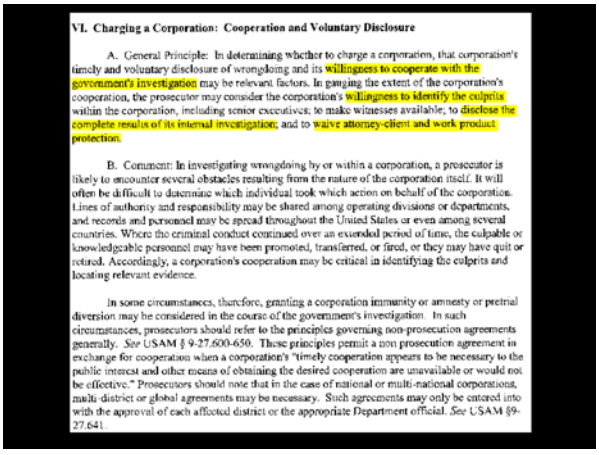
January 20, 2003

MEMORANDUM

TO: Heads of Department Components
United States Attorneys

FROM: Larry D. Thompson
Deputy Attorney General

SUBJECT: Principles of Federal Prosecution of Business Organizations



VI. Charging a Corporation: Cooperation and Voluntary Disclosure

A. General Principle: In determining whether to charge a corporation, that corporation's timely and voluntary disclosure of wrongdoing and its willingness to cooperate with the government's investigation may be relevant factors. In gauging the extent of the corporation's cooperation, the prosecutor may consider the corporation's willingness to identify the culprits within the corporation, including senior executives; to make witnesses available; to disclose the complete results of its internal investigation; and to waive attorney-client and work product protection.

B. Comment: In investigating wrongdoing by or within a corporation, a prosecutor is likely to encounter several obstacles resulting from the nature of the corporation itself. It will often be difficult to determine which individual took which action on behalf of the corporation. Lines of authority and responsibility may be shared among operating divisions or departments, and records and personnel may be spread throughout the United States or even among several countries. Where the criminal conduct continued over an extended period of time, the culpable or knowledgeable personnel may have been promoted, transferred, or fired, or they may have quit or retired. Accordingly, a corporation's cooperation may be critical in identifying the culprits and locating relevant evidence.

In some circumstances, therefore, granting a corporation immunity or amnesty or pretrial diversion may be considered in the course of the government's investigation. In such circumstances, prosecutors should refer to the principles governing non-prosecution agreements generally. *See* USAM § 9-27.600-650. These principles permit a non prosecution agreement in exchange for cooperation when a corporation's "timely cooperation appears to be necessary to the public interest and other means of obtaining the desired cooperation are unavailable or would not be effective." Prosecutors should note that in the case of national or multi-national corporations, multi-district or global agreements may be necessary. Such agreements may only be entered into with the approval of each affected district or the appropriate Department official. *See* USAM §9-27.641.

In addition, the Department, in conjunction with regulatory agencies and other executive branch departments, encourages corporations, as part of their compliance programs, to conduct internal investigations and to disclose their findings to the appropriate authorities. Some agencies, such as the SEC and the EPA, as well as the Department's Environmental and Natural Resources Division, have formal voluntary disclosure programs in which self-reporting, coupled with remediation and additional criteria, may qualify the corporation for amnesty or reduced sanctions.[4] Even in the absence of a formal program, prosecutors may consider a corporation's timely and voluntary disclosure in evaluating the adequacy of the corporation's compliance program and its management's commitment to the compliance program. However, prosecution and economic policies specific to the industry or statute may require prosecution notwithstanding a corporation's willingness to cooperate. For example, the Antitrust Division offers amnesty only to the first corporation to agree to cooperate. This creates a strong incentive for corporations participating in anti-competitive conduct to be the first to cooperate. In addition, amnesty, immunity, or reduced sanctions may not be appropriate where the corporation's business is permeated with fraud or other crimes.

One factor the prosecutor may weigh in assessing the adequacy of a corporation's cooperation is the completeness of its disclosure including, if necessary, a waiver of the attorney-client and work product protections, both with respect to its internal investigation and with respect to communications between specific officers, directors and employees and counsel. Such waivers permit the government to obtain statements of possible witnesses, subjects, and targets, without having to negotiate individual cooperation or immunity agreements. In addition, they are often critical in enabling the government to evaluate the completeness of a corporation's voluntary disclosure and cooperation. Prosecutors may, therefore, request a waiver in appropriate circumstances.[5] The Department does not, however, consider waiver of a corporation's attorney-client and work product protection an absolute requirement, and prosecutors should consider the willingness of a corporation to waive such protection when necessary to provide timely and complete information as one factor in evaluating the corporation's cooperation.

Issues With Corporate Cooperation

- Background
  - 1999 "Holder Memo" and 2003 "Thompson Memo."
  - NACDL Survey (March 2006): 75% of in-house and outside counsel agree that a "culture of waiver" existed.
  - *U.S. v. Computer Associates, Int'l, Inc.*
  - Coalition: ABA, U.S. Chamber of Commerce, Association of Corporate Counsel, NACDL, ACLU.
  - "McNulty Memo" (2006).
  - Current DOJ Policy (2009).

Current DOJ Policy (2009)

- **U.S. Attorney's Manual § 9-28.710:**
  - "What the government seeks and needs to advance its legitimate (indeed, essential) law enforcement mission is not waiver of [the privilege and work product protection], but rather the facts known to the corporation about the putative criminal misconduct under review. In addition, while a corporation remains free to convey non-factual or "core" attorney-client communications or work product—if and only if the corporation voluntarily chooses to do so—***prosecutors should not ask for such waivers and are directed not to do so***." (Emphasis added.)

Current DOJ Policy (2009)

- ***But see* U.S.A.M. § 9-28.720:**
  - "[T]he government's ***key measure of cooperation*** must remain the same as it does for an individual: has the party timely disclosed ***the relevant facts*** about the putative misconduct? That is the operative question in assigning cooperation credit for the disclosure of information—not whether the corporation discloses attorney-client or work product materials." (Emphasis added.)
  - **Query:** How do entities learn the key "relevant facts" *other than* through privileged interviews?

Issues With Corporate Cooperation

- Background
  - 1999 "Holder Memo" and 2003 "Thompson Memo."
  - NACDL Survey (March 2006): 75% of in-house and outside counsel agree that a "culture of waiver" existed.
  - *U.S. v. Computer Associates, Int'l, Inc.*
  - Coalition: ABA, U.S. Chamber of Commerce, Association of Corporate Counsel, NACDL, ACLU.
  - "McNulty Memo" (2006).
  - Current DOJ Policy (2009).
  - Consenting to government's request to search employee's computer, office, etc.

Who Has the Right to Consent?

- ***U.S. v. Ziegler*, 474 F.3d 1184 (9th Cir. 2007):**
  - Employee suspected of downloading child pornography.
  - IT administrator, working with FBI, monitored employee's internet use, copied hard drive, and turned over to FBI.
  - Employee had reasonable expectation of privacy:
    - Office was kept locked and not shared by others.
  - *But* exception to 4th Amdt. "where valid consent is obtained by the government."
    - including consent "from a third party who possessed common authority over or other sufficient relationship to the premises or effects sought to be inspected."
  - Employer's consent was valid:
    - "[T]he computer is the type of workplace property that remains within the control of the employer even if the employee has placed personal items in it."
    - "[E]mployees were apprised of the company's monitoring efforts through training and an employment manual, and they were told that the computers were company-owned and not to be used for activities of a personal nature."

Who Has the Right to Consent?

- **Similar analysis (and result) in *Thygeson v. U.S. Bancorp*, 2004 WL 2066746 (D. Or. 2004) (Magistrate Judge Stewart):**
  - But in that case, not even a reasonable expectation of privacy because:
    - Employee handbook made clear that computers were for company business only.
    - Company expressly reserved the right to monitor e-mails and computer files.
    - Company expressly reserved the right "to access and/or search workspace and equipment that has been assigned to you."
    - Employee had not password-protected his materials.

Who Has the Right to Consent?

- ***Compare Leventhal v. Knapek*, 266 F.3d 64 (2d Cir. 2001):**
  - Employee had reasonable expectation of privacy because:
    - Computer in a private office (not shared with anyone else).
    - Maintenance done only with advance notice.
    - No general practice of searching office computers.
    - No notice to employees that they should not have expectation of privacy in contents of office computers.
- ***U.S. v. Taketa*, 923 f.2d 665, 673 (9th Cir. 1991):**
  - Government employer cannot consent to search of employee's work space in which he has reasonable expectation of privacy (i.e., employer cannot consent to search that it could not conduct itself).

May *Employee* Consent to Search of *Employer's* Property?

- *Yes*, if employee has control as caretaker or has been entrusted with records. . . .
  - *U.S. v. Antonelli Fireworks Co.*, 155 F.2d 631, 636 (2d Cir. 1946)
- . . . or if the employee has been left in charge of the property, in which case he/she may have apparent authority to consent.
  - *U.S. v. Jenkins*, 46 F.3d 447, 456 (5th Cir. 1995).

QUESTIONS?