AMERICAN BAR ASSOCIATION SECTION OF ANTITRUST LAW
AND
THE INTERNATIONAL BAR ASSOCIATION

2014 INTERNATIONAL CARTEL WORKSHOP

FROM LENIENCY TO SEARCH WARRANTS: THE HOLY GRAIL OF COMPLIANCE AND WHAT TO DO WHEN THE FBI IS IN THE LOBBY

Robert Bloch, Kelly Kramer, and Stephen Medlock
Mayer Brown LLP
1999 K Street, N.W.
Washington, D.C. 20006
rbloch@mayerbrown.com
202-263-3203

Cavalieri Waldorf Astoria
Rome, Italy
February 19-21, 2014

TABLE OF CONTENTS

Page

FROM LENIENCY TO SEARCH WARRANTS: THE HOLY GRAIL OF COMPLIANCE AND WHAT TO DO WHEN THE FBI IS IN THE LOBBY

Robert Bloch, Kelly Kramer, and Stephen Medlock[1]

I. Introduction

Few things are more traumatic for a company than the execution of a search warrant by U.S. law enforcement agents. Employees panic, the media picks up the story, customers wonder if they should do business with the company, banks consider calling lines of credit, and civil plaintiffs almost invariably file class actions. A search warrant always comes as a surprise, but the fact is that companies do have opportunities to head off the execution of a search warrant before it ever happens as well as prepare for the unexpected.

This paper discusses some of the key opportunities companies have to head off, prepare for, and respond to a search warrant. After a brief analysis of the law and Department of Justice policies relevant to antitrust compliance and search warrant execution, this paper addresses three topics: (1) how a company can design an effective antitrust compliance program, (2) what policies a company can adopt to minimize the business disruption associated with a search warrant, and (3) how a company should react initially to an antitrust investigation after the search is over. This paper offers practical advice and checklists for in-house and outside counsel for each of these topics.

II. Heading off an Investigation and a Search Warrant: The Critical Importance of Compliance Programs

Three weeks ago you were named the Senior Vice President and General Counsel for a multinational manufacturing company. To help you get oriented, you convene a series of meetings with members of the Legal Department to understand the company's risks and exposures. During one of these meetings, a junior attorney mentions that the company has not updated its antitrust compliance program in years. You think that you probably should update the company's procedures, but the company is not involved in any antitrust litigation now and

[1] Mr. Bloch is a partner and the Global Practice Leader of Mayer Brown LLP's Antitrust Practice Group. He specializes in antitrust law, complex civil litigation and white collar criminal defense. Mr. Kramer is a partner and co-chairman of the Mayer Brown LLP's white collar defense and compliance practice. Mr. Medlock is an associate in Mayer Brown LLP's Litigation & Dispute Resolution practice where he focuses on all aspects of antitrust law and litigation

the Legal Department's budget is tight. "Let's put this off until next year," you say.

* * *

On the day that a search warrant is being executed, you might not remember this conversation. You will be too busy dealing with the search itself, but you may have missed the best opportunity to avoid a search entirely. A robust and ongoing antitrust compliance program is essential to identifying and minimizing antitrust risk. Indeed, detecting potential criminal antitrust violations early has important consequences for criminal and civil liability. The Antitrust Division's corporate leniency program, the Division's amnesty plus/penalty plus policy, and the substantial cooperation discount all incentivize early detection of illegal activity and cooperation with a subsequent government investigation.[2] This section will discuss each of these policies before suggesting particular antitrust compliance measures.

A. The Holy Grail of Antitrust Compliance is Prevention, but When that Does Not Work, It is Corporate Leniency

1. Corporate Leniency

Being the first company to inform the Antitrust Division of the U.S. Department of Justice about a price-fixing conspiracy has significant advantages. Through the Antitrust Division's leniency program, a company "can avoid criminal conviction and fines . . . by being the first to confess participation in a criminal antitrust violation, fully cooperating with the [Antitrust] Division, and meeting other specified requirements."[3] A company seeking leniency must meet six requirements:

1) it must provide the Antitrust Division with information that the Division has not received from any other source;[4]

2) once the company discovers the illegal activity, it must take prompt and effective action to terminate it;[5]

---

[2] *See, e.g.*, Constance K. Robinson, *Get-Out-of-Jail-Free Cards: Amnesty Developments in the United States and Current Issues*, 8 SEDONA CONF. J. 29, 31-32 (Fall 2007) (examining each program).

[3] Antitrust Div., U.S. Dep't of Justice, *Corporate Leniency Policy* 1 (Aug. 10, 1993) [hereinafter "Corporate Leniency Policy"].

[4] *Id.*

[5] *Id.* As used in the Corporate Leniency Policy, "discovery of illegal activity" means "the earliest date on which either the board of directors or counsel for the corporation (either inside or outside) was first informed of the

3) the company must report its illegal activity "with candor and completeness and provide[] full, continuing and complete cooperation;"[6]

4) the confession must be a "corporate act;"[7]

5) if possible, the reporting corporation should make restitution to injured parties;[8] and

6) the reporting corporation must not have coerced another part to participate in the illegal activity or been the leader or originator of the activity.[9]

Time is of the essence when seeking leniency.[10] By design, the corporate leniency program creates "a true 'prisoner's dilemma' and a race to the courthouse among cartelists."[11] The Antitrust Division "grants only one corporate leniency per conspiracy, and in applying for leniency, the company is in a race with its co-conspirators."[12] Therefore, once a company learns about its participation in criminal antitrust conduct, it is advisable to contact the Antitrust Division as soon as possible.[13]

After a company communicates its intent to seek corporate leniency, the Antitrust

---

conduct at issue." SCOTT D. HAMMOND & BELINDA A. BARNETT, ANTITRUST DIVISION LENIENCY PROGRAM – FREQUENTLY ASKED QUESTIONS, CCH Trade & Reg. Rep. ¶ 50,235, at 12 (Nov. 19, 2008), http://www.justice.gov/atr/public/criminal/239583.pdf. A company terminates participation in the conspiracy "promptly" when it effectively terminates its anticompetitive conduct at about the same time it seeks a marker from the Antitrust Division. *Id.* at 14. A company terminates its part in anticompetitive activities by stopping any further participation in those activities. *Id.*

[6] Corporate Leniency Policy, *supra* note 3, at 2. If a company receives conditional corporate leniency, it must (1) provide "a full exposition of all facts known to [it] relating to the anticompetitive activity being reported;" (2) provide, without a subpoena, "all documents, information, or other materials in its possession, custody, on control, wherever located, not privileged under the attorney-client privilege or work-product privilege, requested by the Antitrust Division;" (3) use its best efforts to secure the cooperation of its current and former directors, officers, and employees—including facilitating interviews with the Antitrust Division, grand jury testimony, and testimony at trial; and (4) paying restitution to any person or entity injured as a result of the anticompetitive activity. Antitrust Div., U.S. Dep't of Justice, Model Conditional Corporate Leniency Letter 2-3 (Nov. 19, 2008), http://www.justice.gov/atr/public/criminal/239524.pdf [hereinafter, "Corporate Leniency Letter"].

[7] Corporate Leniency Policy, *supra* note 3, at 2.

[8] *Id.*

[9] *Id.* A company will be denied leniency only if it was "clearly the single organizer or single ringleader of a conspiracy." HAMMOND & BARNETT, *supra* note 5, at 16. The conspirator with the largest market share is not necessarily disqualified from receiving leniency. *Id*. If more than one company played a "decisive role" in the conspiracy, all of the conspirators are potentially eligible for leniency. *Id*.

[10] *Id.* at 12.

[11] John M. Taladay, *Time for a Global "One-Stop Shop" for Leniency Markers*, 27 ANTITRUST 43, 43 (Fall 2012); *see also* Donald C. Klawiter, *Corporate Leniency in the Age of International Cartels: The American Experience*, 14 ANTITRUST 13, 13 (Summer 2000) ("the Antitrust Division's Leniency Policy has made corporate decision making in criminal antitrust investigations move light years faster than it did before") (internal footnote omitted).

[12] HAMMOND & BARNETT, *supra* note 5, at 2.

[13] *Id.* at 2 & n.4 (listing contact information for Deputy Assistant Attorney General for Criminal Enforcement and Antitrust Division field offices).

Division will often grant a "marker" to it. Markers "hold an applicant's place in the line for leniency while the applicant gathers more information to support its leniency application."[14] The Antitrust Division grants two types of markers: (1) those that name the leniency applicant and (2) those where the applicant wishes to remain anonymous.[15] In either case, a company that wishes to obtain a marker must:

1) report that it has some information regarding a possible antitrust offense,
2) disclose the general nature of the conduct involved, and
3) identify the industry, product, or service involved in specific terms.[16]

A company does not need to admit to an antitrust violation in order to receive a marker;[17] it must state that there is evidence of a possible violation.[18]

The evidentiary standard for receiving a marker depends on whether the Antitrust Division already has information regarding the potential antitrust violation.[19] If the Antitrust Division is not investigating the industry, the standard can be quite low—simply recounting rumors heard by an internal whistle-blower may be enough.[20] On the other hand, if a company has already received a grand jury subpoena or has been searched by the FBI, the evidentiary bar is much higher.[21]

The duration of a marker depends on whether the company remains anonymous. Typically, an anonymous marker is only given for "two or three days" while company counsel gathers additional information regarding the possible antitrust violation.[22] In contrast, a named applicant is likely to receive a 30-day period to perfect its marker.[23]

The benefits of corporate leniency are substantial. First, if a company complies with the

[14] *Id.* at 2.
[15] *Id.* at 3 & n.6.
[16] *Id.* a 3.
[17] *Id.*
[18] *Id.*
[19] *Id.*
[20] *Id.*
[21] *Id.*
[22] *Id.* at 3 n.6.
[23] *Id.* at 4.

program's requirements, it will not be charged criminally for the antitrust offenses reported.[24] Second, in some cases, a company may be able to receive leniency for additional offenses that are "usually integral" to the antitrust offense.[25] For example, if a company's employees communicated with other cartel members via mail, telephone, fax, or email, the company may also receive corporate leniency for charges of mail fraud, wire fraud, or conspiracy to defraud.[26] Third, the scope of corporate leniency granted to a company can expand to include related, subsequently discovered anticompetitive activity—provided that the company has not tried to conceal the subsequently discovered conduct, continues to cooperate with the investigation, and the company meets the same six criteria for leniency with respect to the newly discovered conduct.[27] Fourth, in some cases, former officers, directors, and employees may be covered by the Antitrust Division's grant of corporate leniency.[28]

Corporate leniency has its limits, however.[29] The Antitrust Division's corporate leniency program only binds the Antitrust Division.[30] Corporate leniency does not protect a company from prosecution for other, unrelated offenses that may be uncovered during the company's internal investigation.[31] In addition, employees covered by the corporate leniency letter that are called to testify at trial or before a grand jury are still subject to criminal penalties for perjury, making false statements or declarations in grand jury or court proceedings, contempt, and obstruction of justice.[32] Finally, although rare, one court has held that a conditional corporate leniency agreement may not be enforceable if the company or an executive fails to comply with the terms of the agreement.[33]

---

[24] Corporate Leniency Policy, *supra* note 3, at 1.
[25] HAMMOND & BARNETT, *supra* note 5, at 7.
[26] *Id.*
[27] *Id.* at 8.
[28] Corporate Leniency Letter, *supra* note 6, at 2 n.3.
[29] *See* HAMMOND & BARNETT, *supra* note 5, at 7.
[30] *Id.*
[31] The U.S. Department of Justice's Principles of Federal Prosecution of Business Organizations provide guidance for companies that wish to self-report these crimes in exchange for a non-prosecution agreement. *See* U.S. Attorneys' Manual 9-28.000, http://www.justice.gov/usao/eousa/foia_reading_room/usam/title9/28mcrm.htm.
[32] Corporate Leniency Letter, *supra* note 6, at 5.
[33] *See* Stolt-Nielsen, S.A. v. United States, 442 F.3d 177, 184-87 (3d Cir. 2006).

2. Amnesty Plus

Beyond the well-known rewards under the Corporate Leniency Program,[34] a company that is "second in the door" can also recognize significant benefits.[35] For example, under the Antitrust Division's amnesty plus program, a company that is under investigation for one conspiracy may still be able to receive corporate leniency for a separate, unreported conspiracy.[36] In addition to corporate leniency for this second conspiracy, the Antitrust Division will recommend that the company be fined significantly less than it otherwise would have for participating in the first conspiracy.[37] The "discount" that a company will receive for the first conspiracy depends on several factors, including: (1) the strength of the evidence presented by the company regarding the leniency product, (2) the significance of the violation reported in the leniency application, and (3) the likelihood that the Antitrust Division would have discovered the second conspiracy without the assistance of the company.[38] As antitrust practitioners have recognized, the amnesty plus program "provides a powerful incentive for a corporation to expand its internal investigation and come clean as to all potential antitrust violations."[39]

3. Downward Departures

Even if amnesty plus is not possible and another company has secured corporate leniency, a "second-in" company can still obtain some benefits from early and significant cooperation with an Antitrust Division investigation.[40]

- If a company's cooperation reveals that the conspiracy was broader than previously identified, the Antitrust Division will not use this self-incriminating information when

---

[34] *See, e.g.*, Scott D. Hammond, Deputy Assistant Attorney Gen. for Criminal Enforcement, Antitrust Div., U.S. Dep't of Justice, Speech to the 24th Annual National Institute on White Collar Crime: The Evolution of Criminal Antitrust Enforcement Over the Last Two Decades (Feb. 25, 2010), http://www.justice.gov/atr/public/speeches/255515.pdf.

[35] Scott D. Hammond, Deputy Assistant Attorney Gen. for Criminal Enforcement, Antitrust Div., U.S. Dep't of Justice, Address to the 54th Annual Am. Bar Ass'n Sec. of Antitrust Law: Measuring the Value of Second-In Cooperation in Corporate Plea Negotiations 1 (Mar. 29, 2006), http://www.justice.gov/atr/public/speeches/215514.pdf [hereinafter "Second-In Cooperation"].

[36] HAMMOND & BARNETT, *supra* note 5, at 8.

[37] *Id.* at 9.

[38] *Id.*

[39] Klawiter, *supra* note 11, at 14-15.

[40] *See* Second-In Cooperation, *supra* note 35, at 2.

determining the applicable fine under the U.S. Sentencing Guidelines.[41] This can result in a substantial reduction of the second-in company's fine.[42]

- A second-in company can receive a downward departure under the U.S. Sentencing Guidelines if it provides substantial cooperation to the Antitrust Division.[43] The typical cooperation discount for a second-in company is between 30% and 35% off of the minimum of the Guidelines fine range.[44] For example, Odfjell Seachem A.S., a parcel tanker company, agreed to cooperate with an Antitrust Division investigation on the day that it was searched; it made its key personnel available to the Antitrust Division for interviews; and two of its foreign executives agreed to travel to the United States, plead guilty, and serve jail time.[45] As a result, Odfjell received a 30% cooperation discount.[46] Even if a company does not have "second-in" status, a lesser cooperation discount may be available under the Guidelines.[47]

- A second-in company may also receive additional protection for its employees.[48] Typically, a handful of employees are "carved out" of a corporate plea agreement with the Antitrust Division, and must negotiate their own plea agreements.[49] When a second-in company provides significant cooperation to the Antitrust Division, "the Division will typically carve out only the highest-level culpable individuals . . . mid-to-lower-level employees who provide significant evidence furthering the investigation will be offered non-prosecution protection under the corporate plea agreement."[50] A second-in company can maximize the number of employees "carved in" to the plea agreement through early and significant cooperation.[51] For instance, in *United States v. Crompton Corporation*, Crompton was a "second-in" company.[52] Through its cooperation, only three high level executives were carved out of the corporate plea agreement.[53] In contrast, the third-in company, Bayer A.G., had five high-and-mid-level employees carved out of its plea

[41] *See* U.S.S.G. § 1B1.8(a)-(b).
[42] Second-In Cooperation, *supra* note 35, at 4.
[43] *See* U.S.S.G. § 8C4.1.
[44] Second-In Cooperation, *supra* note 35, at 5.
[45] *Id.* at 5 n.8.
[46] *Id.* However, the substantial cooperation discount will not be applied to the minimum range of the fine Guidelines if the company had a significant leadership role in the conspiracy. *See* U.S.S.G. § 8C2.8(a)(2) (enhancing criminal fine based on "the organization's role in the offense"). In addition, a company may be subject to the Antitrust Division's Penalty Plus program if it discovers conduct that would qualify for the Amnesty Plus program and fails to report it. *See, e.g.*, Robert E. Bloch, et al., *Leniency and Plea Bargaining in Cartel Investigations in the United States and Europe* 11 (2008), http://www.mayerbrown.com/public_docs/Leniency_PleaBargaining_Cartel Investigations.pdf.
[47] Second-In Cooperation, *supra* note 35, at 5.
[48] *Id.* at 8.
[49] *Id.*
[50] *Id.*
[51] *Id.*
[52] *Id.* at 2; *see also* Plea Agreement, United States v. Compton Corp., No. CR 04-0079 MJJ (N.D. Cal. Mar. 28, 2004) (ECF No. 40).
[53] Second-In Cooperation, *supra* note 35, at 8; *see also* Plea Agreement, United States v. Conway, CR 04-0302 MJJ (N.D. Cal. Nov. 4, 2004) (ECF No. 11) (carved out of Crompton plea agreement); Plea Agreement, United States v. Eisenberg, CR 04-0296 MJJ (N.D. Cal. Nov. 18, 2004) (ECF No. 11) (same).

agreement.[54]

While these benefits are not uniform,[55] they, nonetheless, reward companies that detect and report anticompetitive activity early in a criminal investigation.[56]

4. Practical Benefits

Promptly detecting and reporting illegal activity has benefits beyond corporate leniency and downward departures. A company can avoid the trauma and negative impact on employee morale that inevitably follow the execution of a search warrant. A company may also be able to avoid negative press accounts that harm corporate reputation and goodwill with customers. While these reputational damages can be hard to quantify, they may last longer than many of the other effects of a criminal investigation.

Receiving corporate leniency also has substantial benefits in follow-on civil litigation.[57] Section 213 of the Antitrust Criminal Penalty Enhancement Reform Act ("ACPERA")[58] limits exposure to civil damages for a conspirator who has a "currently effective" leniency agreement with the Antitrust Division and who cooperates satisfactorily with the Antitrust Division and with private litigants in related civil actions.[59]

B. Corporate Compliance Procedures

In light of the significant incentives for early detection and reporting, companies should institute a robust antitrust compliance program.[60] Companies in industries that are currently subject to antitrust investigations in the United States or other jurisdictions should pay particular

---

[54] Second-In Cooperation, *supra* note 35, at 8.
[55] *Id.* at 2.
[56] *Id.*
[57] Such follow-on cases are exceedingly common after a grand jury returns an indictment or a guilty plea is entered. *See, e.g.*, Compl., Nespole v. Micron Tech., Inc., 228 F. Supp. 2d 1379 (S.D.N.Y. June 21, 2002) (No. 02 CV 4798) (ECF No. 1) (class action complaint); In re Micron Techs., Inc. Sec. Litig., 247 F.R.D. 627, 631 (D. Idaho 2007) ("On June 17, 2002, the U.S. Department of Justice (DOJ) issued a federal grand jury subpoena to Micron, seeking documents relating to communications between DRAM manufacturers regarding the pricing and sales of DRAM chips. DOJ also issued subpoenas to the other two largest global manufacturers of DRAM, Samsung and Infineon Technologies.").
[58] Antitrust Criminal Penalty Enhancement and Reform Act of 2004, Pub. L. No. 108-237, 118 Stat. 665 (2004).
[59] *Id.* at §213(a)-(b); *see also id.* at § 213(a), 118 Stat. at 666 ("the amount of damages recovered by or on behalf of a claimant from an antitrust leniency applicant . . . shall not exceed that portion of the actual damages sustained . . . which is attributable to the commerce done by the applicant in the goods or services affected by the violation.").
[60] Suggested corporate compliance procedures are summarized in the checklist at Appendix A of this paper.

attention to antitrust compliance, and should also consider hiring outside counsel to perform an antitrust audit to determine if there is any anticompetitive conduct occurring that could put the company in jeopardy.

Two considerations are critical to the success of an antitrust compliance program: (1) the support of senior executives and (2) a corporate culture that promotes respect for law and ethics.[61] Without these prerequisites, an antitrust compliance policy may not be worth the paper on which it is written.[62] For an antitrust compliance policy to be truly effective, senior management (outside of the law department) should communicate their support for the policy in ways that are clear and visible, such as discussing the policy with direct reports, endorsing the policy in training materials, and calling attention to the policy in internal publications.[63]

While antitrust compliance programs are not identical and a one-size-fits-all approach rarely works, companies should consider taking the following steps to minimize antitrust risk:

- Update Antitrust Compliance Policies. Review and update corporate antitrust compliance statements, codes of ethics, and codes of conduct to reflect the company's policy of following all relevant antitrust laws, and include company-specific compliance procedures. At a minimum, this written policy should emphasize (a) management's adherence to all applicable antitrust laws, (b) employee responsibility and accountability for antitrust compliance, and (c) the harsh sanctions for non-compliance.[64]

- Antitrust Compliance Handbook. Publish and distribute an antitrust compliance handbook to all employees (and, perhaps, to competitors).[65] The handbook should provide employees with information regarding U.S. antitrust law (and the laws of other applicable competition regimes), potential criminal penalties, the company's general antitrust compliance policy, and specific examples of how employees should comply with the policy. For example, a company might require outside or in-house counsel to monitor

[61] William B. Lawrence, *Protecting Against Problems—Corporate Compliance Programs*, 57 Antitrust L. J. 601, 602 (1988).
[62] *Id.* at 602-03.
[63] *Id.* at 603.
[64] *See, e.g.*, 1 Materials on Antitrust Compliance § 1:11 (West Feb. 2013) (suggesting elements of corporate antitrust compliance policy).
[65] In *United States v. Stolt-Nielsen S.A.* (*Stolt-Nielsen III)*, for example, Stolt-Nielsen followed a number of these procedures to comply with the Antitrust Division's corporate leniency program. 524 F. Supp. 2d 609, 611-12 (E.D. Pa. 2007). These included instituting a new antitrust policy, publishing an antitrust handbook that was distributed to all employees and competitors, holding mandatory antitrust training sessions, requiring all employees to sign certifications that they will comply strictly with the new antitrust policy, and informing competitors of Stolt-Nielsen's intent to comply with the policy. *Id*.

the proceedings of certain trade associations.[66]

- Employee Certifications. Require employees to certify in writing that they will comply with the company's antitrust policy.[67]

- Mandatory Training Programs. Require all or some of its employees (e.g., all employees in sales) to attend training courses regarding the company's antitrust policy and antitrust best practices in high-risk situations, such as interactions with competitors at trade shows or social events. The best training programs promote an open dialogue so employees can feel that they have a handle on antitrust concepts, which can be complex for the uninitiated.[68] While "canned" presentations have some value, most employees will learn more during interactive presentations that allow sufficient time for questions and answers.[69]

- Pricing Decisions and Competitive Intelligence. Employees should understand the antitrust implications of pricing decisions and competitive intelligence. Companies should consider implementing procedures that call for employees to carefully document the reasons why the company is raising its price, especially if a company is determining whether to follow a price increase announced by a competitor. Likewise, documenting the source of competitive intelligence in writing can avoid later uncertainty regarding whether the competitive intelligence was obtained through illegal means.[70]

- Segregation of Pricing Authority. Companies should consider separating the employees with pricing authority from those that participate in trade associations and joint ventures with competitors. Setting up "walls" between these employees can provide a defense to claims that a trade association or joint venture facilitated anticompetitive activity.

- Internal Reporting Structure. Companies should consider setting up a means for employees to quickly report suspected anticompetitive activity to the legal or compliance department. This reporting structure can take on several forms, such as anonymous "hotlines"[71] or internal leniency programs that allow employees to come forward without fear of termination.[72]

---

[66] *See, e.g.*, William M. Hannay, Corporate Compliance Series: Designing an Effective Antitrust Compliance Program § 3:3 (2013) (most companies also prepare and distribute explanatory materials relating to antitrust law in pamphlet form and online over the Internet.").
[67] *See, e.g., id.* at § 3:55.
[68] *See* Lawrence, *supra* note 61, at 605-06.
[69] *Id.*
[70] Murray S. Monroe, *Trade and Professional Associations: An Overview of Horizontal Restraints*, 9 U. DAYTON L. REV. 479, 500 (1984) ("Since price-fixing is anathema, document any pricing decisions").
[71] *See, e.g.*, Harvey L. Pitt & Karl A. Groskaufmanis, *Minimizing Corporate Civil and Criminal Liability: A Second Look at Corporate Codes of Conduct*, 78 GEO. L. J. 1559, 1636 n.448 (June 1990) (suggesting that a company could install an employee hotline or create an ombudsman position); Alan J. Statman, *Antitrust Compliance Program for Energy Companies*, 8 Nat. Resources & Env't 28, 64 (Spring 2008) (proposing that employees report potential antitrust violations to a compliance officer through a hotline).
[72] *See, e.g.*, Donald C. Klawiter & Jennifer M. Driscoll, *A New Approach to Compliance: True Corporate Leniency for Executive*, 22 Antitrust 77, 78 (Summer 2008) (suggesting design for internal leniency program).

- Audits and Spot Checks. Training, updated policies, and structural changes are much more effective if they are backed up by continued monitoring by experienced antitrust counsel. Some companies will undertake a full-scale audit to detect any antitrust risk. Others will have counsel perform spot checks of areas of potential antitrust risk—such as joint ventures, trade association representatives, or pricing strategy teams.[73]

The exact compliance procedures used will depend, to some extent, on the company. Considerations such as recent industry history, competitor's antitrust vulnerabilities, how the company perceives antitrust risk, and the available resources will drive the compliance program. There are significant advantages to implementing these procedures. The Antitrust Division rewards a company that reports anticompetitive conduct early with corporate leniency or, at the very least, a substantial cooperation discount.

III. The FBI is in the Lobby: Responding to a Search Warrant

Your phone rings on your drive into the office. The general manager of one of the company's sales divisions tells you that FBI agents are at the office with a warrant. He tells you that the FBI has begun collecting documents, calendars, expense reports, and other hard copy files. They have seized some employees' smart phones. One FBI agent is talking to the office IT manager about imaging hard drives. The general manager thinks that some of these hard drives may contain emails from the company's legal department.

The FBI asked all of the staff to sit in a conference room. They are calling them out one by one to speak with two agents in another room.

It gets worse. The general manager tells you that he has talked with other members of the sales leadership team. The FBI visited the homes of two sales executives after dinner last night. One of them told the FBI that he was "happy to work with them," and allowed the FBI agents to copy files from his laptop. The sales executive remembers being asked some questions about communications with competitors, but says that he did not tell the FBI anything useful.

"What should I do," the general manager asks?

* * *

Management-level employees should not be left to ask what they should be doing when the FBI executes a search warrant. In an ideal world, the FBI's arrival would trigger the company's search warrant response policy. For companies that have not adopted such policies, a

[73] *See, e.g.*, Joseph Murphy & William Kolasky, *The Role of Anti-Cartel Compliance Programs in Preventing Cartel Behavior*, 26 Antitrust 61, 62 (Spring 2012) ("Institute auditing and monitoring processes that detect cartels and violations of the company's compliance program.").

call like this signals the start of a stressful, confusing, and dangerous day. This section discusses the law and procedural rules relevant to the execution of a search warrant, and suggests critical elements of a corporate search warrant response policy.

A. The Legal Basis for a Search Warrant

1. Probable Cause

Under Rule 41 of the Federal Rules of Criminal Procedure, a U.S. Magistrate Judge may issue a warrant for "(1) evidence of a crime; (2) contraband, fruits of crime, or other items illegally possessed; (3) property designated for use, intended for use, or used in committing a crime; or (4) a person to be arrested or a person who is unlawfully restrained."[74] The magistrate judge may only issue a search warrant on the request of a federal law enforcement officer or government attorney,[75] and may only do so upon a showing of probable cause.[76]

The Fourth Amendment protects "[t]he right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures,"[77] and forbids the issuance of a warrant absent "probable cause."[78] The probable cause requirement is not a particularly high bar—the government does not need to establish its allegations against the target of the search with certainty.[79] "In making a determination of probable cause the relevant inquiry is not whether particular conduct is 'innocent' or 'guilty,' but the degree of suspicion that attaches to particular types of non-criminal acts."[80] Thus, when the "totality-of-the-circumstances" show "a fair probability that contraband or evidence of a crime will be found in a particular place" specified in the search warrant, a warrant will issue.[81]

Probable cause is a "flexible, common sense standard."[82] When determining whether probable cause exists, "magistrate judges are vested with substantial discretion to draw all

[74] FED. R. CRIM. P. 41(c).
[75] FED. R. CRIM P. 41(a)(2)(C); FED. R. CRIM P. 41(b).
[76] U.S. CONST. AMEND. IV.
[77] *Id.*
[78] *Id.*
[79] Illinois v. Gates, 462 U.S. 213, 283 (1983).
[80] *Id.* at 243-44 & n.13.
[81] *Id.* at 238.
[82] Florida v. Harris, 133 S. Ct. 1050, 1053 (2013) (quoting Gates, 462 U.S. at 239).

'reasonable inferences' from the Government's evidence."[83] The Supreme Court has also cautioned that courts should not adopt a "grudging or negative" attitude towards warrants.[84] In addition, courts should not resort to a "hypertechnical" reading to invalidate a warrant.[85] Therefore, "the probable cause requirement should not require agents to be clairvoyant in their knowledge of the precise forms of evidence or contraband that will exist in the location to be searched."[86]

Moreover, the same evidentiary constraints that bind the government at trial are not applicable to a search warrant. For example, a court may find that probable cause exists even when a warrant application is based on hearsay, so long as there is a substantial basis for crediting the hearsay.[87]

Despite the flexibility and deference accorded to a magistrate judge, probable cause has limits. A federal law enforcement officer making the search warrant application must have more than a "bare suspicion" that a crime has been committed.[88] Law enforcement agents are forbidden from obtaining "general warrants;" they must conduct tailored searches and seizures to "minimize[] unwarranted intrusions upon privacy."[89]

In addition, the information in the warrant application must be current and support the conclusion that probable cause exists at the time the warrant is executed.[90] The Supreme Court

---

[83] United States v. Biglow, 562 F.3d 1272, 1281 (10th Cir. 2009) (quoting Gates, 462 U.S. at 240); *see also*

[84] Massachusetts v. Upton, 466 U.S. 727, 733 (1984) (quoting United States v. Ventresca, 380 U.S. 102, 108 (1965)).

[85] Gates, 462 U.S. at 236 (quoting Ventresca, 380 U.S. at 109); *see also* Biglow, 562 F.3d at 1282 ("The Fourth Amendment's strong preference for warrants compels us to resolve 'doubtful or marginal cases' by deferring to a magistrate judge's determination of probable cause.") (internal quotation marks omitted).

[86] H. MARSHALL JARRETT, ET AL., OFFICE OF LEGAL EDUCATION, EXECUTIVE OFFICE FOR U.S. ATTORNEYS, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS 64 (3d ed. 2009), http://www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf.

[87] Sgro v. United States, 287 U.S. 206, 210 (1932).

[88] *See* Brinegar v. United States, 338 U.S. 160, 175 (1949).

[89] Andresen v. Maryland, 427 U.S. 463, 482 n.11 (1976).

[90] *See, e.g.*, United States v. Wagner, 989 F.2d 69, 75 (2d Cir. 1993) ("[T]he facts in an affidavit supporting a search warrant must be sufficiently close in time to the issuance of the warrant and the subsequent search conducted so that probable cause can be said to exist as of the time of the search and not simply as of some time in the past."). When determining whether a probable cause finding is stale, a reviewing court considers "the defendant's course of conduct; the nature and duration of the crime; the nature of the relevant evidence; and any corroboration of the older and more recent information." United States v. Czuprynski, 46 F.3d 560, 567 (6th Cir.) (en banc).

recognizes that evidence of a crime can be kept in business files for months and still not be stale.[91] "Courts have also noted that advances in computer forensic analysis allow investigators to recover files even after they are deleted, casting greater doubt on the validity of 'staleness' arguments."[92]

2. Particularity

The Fourth Amendment also requires that every warrant "particularly describ[e] the place to be searched, and the persons or things to be seized."[93] The particularity clause requires that "[a]s to what is to be taken, nothing is left to the discretion of the officer executing the warrant."[94]

In a white collar investigation, it can be difficult to draft a specific description of the records to be seized. As a result, courts have upheld warrants seeking broad categories of information in some investigations.[95] As the Eleventh Circuit reasoned: in "cases . . . involving complex financial transactions and widespread allegations of various types of fraud, reading the warrant with flexibility entails an awareness of the difficulty of piecing together the 'paper puzzle.'"[96] Therefore, in these cases, courts have approved of "warrant[s] [that] . . . set[] forth generic classifications of the items to be seized together with an illustrative listing which enables the executing officer to ascertain and identify with reasonable certainty the items that the magistrate has authorized him to seize."[97]

While some flexibility is granted to law enforcement officers in this circumstance, "[a]gents cannot simply request permission to seize 'all records' from an operating business unless agents have probable cause to believe that the criminal activity under investigation pervades the entire business."[98] Likewise, warrants seeking "any and all data" regarding a broad

---

[91] Andresen, 427 U.S. at 478 n.9 ("It is eminently reasonable to expect that such records would be maintained in those offices for a period of time.").
[92] H. MARSHALL JARRETT, *supra* note 86, at 69 (collecting cases).
[93] U.S. CONST. AMEND. IV.
[94] Marron v. United States, 275 U.S. 192, 196 (1927).
[95] *See, e.g.*, United States v. Davis, 226 F.3d 346, 352 (5th Cir. 2000).
[96] United States v. Wuagneux, 683 F.2d 1343, 1348-49 (11th Cir. 1982).
[97] United States v. Triumph Capital Grp., Inc., 211 F.R.D. 31, 57 (D. Conn. 2002).
[98] H. MARSHALL JARRETT, *supra* note 86, at 73.

list of items may violate the particularity clause.[99] As a result, search warrants often "identify records that relate to a particular crime . . . to include specific categories of . . . records likely to be found."[100]

In antitrust investigations, magistrate judges typically approve searches where the warrant describes the things to be seized with broad language, provided the language provides some guidance for distinguishing irrelevant materials.[101] For example, in *In re Vinton Construction Co.*,[102] the Antitrust Division obtained a warrant to investigate whether Vinton Construction Company conspired with Streu Construction Company to fix bids for highway construction work between January 1, 2000 and January 12, 2004.[103] The warrant described categories of documents and electronic media that were likely to contain evidence of this crime, including:

> Notes, memoranda, correspondence, electronic mail messages (e-mails), reports, and other records and documentation relating to any agreements, meetings, conversations, or other communications or contacts between or among Vinton Construction Company or any of its officers or employees and any officer or employee of Streu Construction Company or any other company that performs highway construction work on projects within the State of Wisconsin for the period January 1, 2000 up to and include [January 12, 2004].[104]

The warrant gave the officers performing the search specific guidance on how to separate items that were responsive and non-responsive to the warrant—it described the information sought with reasonable particularity, offered an illustrative list of types of media where the information might be found, and provided a limited, relevant time period.[105]

Where the government has been able to develop more detailed information about anticompetitive conduct, the warrant will often specify the names of employees whose records

---

[99] United States v. Fleet Mgmt. Ltd., 521 F. Supp. 2d 436, 443-44 (E.D. Pa. 2007) (emphasis and internal quotation marks omitted); *see also* United States v. Otero, 563 F.3d 1127, 1132 (10th Cir. 2009) (warrant authorizing seizure of "any and all information and/or data" was unconstitutionally unparticular) (internal quotation marks omitted).
[100] H. Marshall Jarrett, *supra* note 86, at 73.
[101] *Id.* at 70.
[102] Case No. 04-m-712 (E.D. Wisc. 2004).
[103] *See* Search Warrant, *In re* Premises Located at Vinton Constr. Co., located 2705 N. Rapids Rd., Manitowoc, Wisc. 54220-1110, Case No. 04-m-712 (E.D. Wisc. Jan. 12, 2004).
[104] *Id.* at Ex. B.
[105] *Id.*

should be seized.[106] For instance, in *In re Vinton Construction Co.*, the search warrant called for the seizure of "[a]ll travel vouchers . . . and any other documents that record or reflect transportation, hotel, entertainment, meals or other expenses or details of the travel of [two employees] from January 1, 2000 up to [January 12, 2004]."[107]

3. Antitrust Division Procedures

a. The Warrant

According to the Antitrust Division Manual, the Antitrust Division views "warrants . . . as an extraordinary method of criminal discovery . . . [that] should be sought only when an attorney has a substantial basis for doing so."[108] Under this policy, Antitrust Division attorneys may seek a search warrant only where under the circumstances, "[it] may be essential to prevent the further concealment or the possible destruction of . . . evidence."[109]

A warrant application in an antitrust investigation is usually supported by an affidavit signed by an FBI agent.[110] "The affidavit must include sufficient facts to establish probable cause both that the crime was committed and that evidence of the crime is at the search location."[111] When the Antitrust Division applies for the warrant, the affidavit will be filed under seal.[112]

b. Preparation for the Search

Once the magistrate judge issues the search warrant, it must be executed within 14 days.[113] Prior to the search, staff attorneys from the Antitrust Division will meet with the FBI agents who are conducting the search to discuss the facts of the case and review the types of items that are to be seized,[114] and prepare the FBI agents to conduct interviews with select

---

[106] *Id.*
[107] *Id.*
[108] U.S. Dep't of Justice, Grand Jury Manual III-175 (1st ed. Nov. 1991).
[109] *Id.* at III-176.
[110] *See, e.g.*, James M. Griffin & Brian R. Meiners, *Preparing For and Responding to a Federal Bureau of Investigation Search of Corporate Premises in the United States* 5 (Feb. 2010); FED. R. CRIM. P. 41(d)(2)(B).
[111] U.S. Dep't of Justice, Antitrust Div., Antitrust Division Manual III-91 (5th ed. July 2013) [hereinafter, "Antitrust Division Manual"].
[112] *Id.*
[113] FED. R. CRIM. P. 41(e)(2)(A).
[114] James M. Griffin & Brian R. Meiners, *supra* note 110, at 8.

employees of the target company.[115] The Antitrust Division will also coordinate with other competition enforcement agencies to coordinate the timing of searches, service of subpoenas, and interviews around the globe.[116]

c. Drop-in Interviews

Although a search warrant does not compel company personnel to submit to interviews, FBI agents will attempt to interview employees while executing the search warrant on a voluntary basis.[117] In addition, on the evening before the search warrant is executed, or the morning of the search, Antitrust Division attorneys and FBI agents may attempt "drop-in" interviews with select employees.[118] These interviews are extremely dangerous for employees and the company.[119] Typically, neither the company nor the employees will be aware of the antitrust investigation, and will not have retained outside counsel.[120] Employees who have not been trained to handle a drop-in interview may also make incriminating statements or fail to answer incriminating questions without first invoking their Fifth Amendment rights.[121]

One recent Supreme Court case, *Salinas v. Texas*,[122] exacerbates these dangers. In *Salinas*, Genoveno Salinas voluntarily answered a police officer's questions about a suspected murder without being placed in custody or being read his *Miranda* rights.[123] Eventually, the officer asked Mr. Salinas whether a ballistic test would show that shell casings found at the scene of the crime were fired from Mr. Salinas' shotgun.[124] In response, Mr. Salinas did not invoke his

---

[115] *Id.*; *see also* Antitrust Division Manual, *supra* note 111, at III-91 ("the search is conducted by a team of agents, who may also seek to interview individuals on site").
[116] R. Hewitt Pate, Acting Assistant Attorney Gen., Antitrust Div., U.S. Dep't of Justice, Address before the British Institute of International and Comparative Law: Anti-Cartel Enforcement: The Core Antitrust Mission 9-10 (May 16, 2003) ("It is no longer uncommon for international antitrust authorities to discuss investigative strategies and to coordinate searches, services of subpoenas, drop-in interviews, and the timing of filing of charges in order to avoid the premature disclosure of an investigation and the possible destruction of evidence.").
[117] *See* Ray V. Hartwell, III, *Advising the "Also Ran:" "Drop Ins," Search Warrants, and Defense Strategy When the Race for Leniency is Lost* 5 (Feb. 10, 2010).
[118] *See id.*
[119] *Id.*
[120] *Id.*
[121] *Id.*
[122] 133 S. Ct. 2174 (2013).
[123] *Id.* at 2177.
[124] *Id.* at 2177.

Fifth Amendment rights.[125] Instead, he declined to answer, "[l]ooked down at the floor, shuffled his feet, bit his bottom lip, cl[e]nched his hands in his lap, [and] began to tighten up."[126] The Court held that Mr. Salinas could not challenge the admission of his silence and refusal to answer the question at trial because "he did not expressly invoke the privilege against self-incrimination in response to the officer's question."[127] As a result, employees that do not expressly invoke their right against self-incrimination may find their silence or refusal to answer questions used against them in criminal prosecutions.[128]

In some cases, such as the marine hose investigation, the Antitrust Division may choose to arrest executives on the day of the search or detain them as material witnesses instead of meeting with them for drop-in interviews.[129] This may occur when the Antitrust Division believes that an individual will leave the United States and be outside the reach of a grand jury subpoena or search warrant.[130]

d. Execution of the Warrant

The warrant must be executed between 6:00 a.m. and 10:00 p.m. local time (which is defined as "daytime" in Rule 41), unless the magistrate judge expressly authorizes execution at another time.[131] The search will be conducted by a team of federal agents.[132] The agents may use force, if necessary, during the course of their search. It is a crime to attempt to prevent or obstruct the search.[133] While no staff attorney from the Antitrust Division will be on-site during the search,[134] they will likely be in constant telephone communication with the agents as the agents execute the search.[135] When executing the warrant, the agents must give a copy of the

[125] *Id.* at 2178.
[126] *Id.* at 2178.
[127] *Id.* at 2178.
[128] *See id.* at 2178.
[129] *See* Press Release, U.S. Dep't of Justice, Eight Executives Arrested on Charges of Conspiring to Rig Bids, Fix Prices, and Allocate Markets for Sales of Marine Hose (May 2, 2007), http://www.justice.gov/atr/public/press_ releases/2007/223037.pdf.
[130] *Id.* at 1 (noting that executives from the United Kingdom, France, Italy, and Japan were arrested).
[131] FED. R. CRIM. P. 41(a)(2)(B), 41(e)(2)(A)(ii).
[132] Antitrust Division Manual, *supra* note 111, at III-91.
[133] 18 U.S.C. §§ 1501, 1509, 1512, 2231.
[134] *Id.*
[135] *See id.* ("No staff attorney should be present during the search, but an attorney should be available by telephone

warrant to a representative of the target company.[136]

Once the search begins, agents may complete the search in any manner, so long as it is reasonable.[137] As a general rule, "[a] container that may conceal the object of a search authorized by a warrant may be opened immediately; the individual's interest in privacy must give way to the magistrate's official determination of probable cause."[138] This may include the seizure of computers, tablets, and smart phones for off-site analysis.[139] In many cases, rather than seizing this hardware, FBI agents will make an "image copy"[140] of the hard drive or other storage media, which can be analyzed later off-site.[141] During this off-site analysis, FBI agents are allowed briefly to peruse each file until "the point [where] . . . the warrant's inapplicability to [the file] is clear."[142]

Because agents will be searching and seizing documents and electronic information without any prior review by the owners or custodians of those documents, there is a possibility that the agents may seize privileged information.[143] The Department of Justice views the

---

for consultation with the agents.").

[136] FED. R. CRIM. P. 41(f)(1)(C).

[137] Dalia v. United States, 441 U.S. 238, 258 (1979) ("the manner in which a warrant is executed is subject to later judicial review as to its reasonableness."); United States v. Ramirez, 523 U.S. 65, 71 (1998) ("The general touchstone of reasonableness which governs Fourth Amendment analysis . . . governs the method of execution of the warrant.").

[138] United States v. Ross, 456 U.S. 798, 823 (1982).

[139] H. MARSHALL JARRETT, *supra* note 86, at77 ("Because examining a computer for evidence of [a] crime is so time consuming, it will be infeasible in almost every case to do an on-site search of a computer or other storage media for evidence of [a] crime.").

[140] An image copy "duplicates every bit and byte on the target drive including all files, the slack space, Master File Table, and metadata in exactly the order they appear on the original." United States v. Vilar, No. S305CR621KMK, 2007 WL 1075041, at *35 n.22 (S.D.N.Y. Apr. 4, 2007) (quoting Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 541 (2005)).

[141] *See* United States v. Turner, 28 F.3d 981, 983 (9th Cir. 1994) ("once an item in an individual's possession has been lawfully seized and searched, subsequent searches of that item, so long as it remains in the legitimate uninterrupted possession of the police, may be conducted without a warrant.") (quoting United States v. Burnette, 698 F.2d 1038, 1049 (9th Cir. 1983)).

[142] *See* United States v. Heldt, 668 F.2d 1238, 1267 (D.C. Cir. 1981); United States v. Giannetta, 909 F.2d 571, 577 (1st Cir. 1990) ("the police may look through . . . file cabinets, files and similar items and briefly peruse their contents to determine whether they are among the documentary items to be seized.").

[143] Barry M. Sabin & Matthew R. Lewis, *Protection of the Attorney-Client Privilege in Criminal Investigations*, 8 SEDONA CONF. J. 105, 108 (Fall 2007) ("When a search warrant is used in a criminal case, there is arguably potential for agents to seize and review materials that may contain attorney-client privileged information.").

attorney-client privilege as "one of the oldest and most sacrosanct privileges under the law."[144] It recognizes "[t]he value of promoting a corporation's ability to seek frank and comprehensive legal advice," which "is particularly important in the contemporary global business environment."[145] In addition, trampling on a company's privilege could lead to a "lengthy pretrial process" that "focus[es] upon the actions of government actors rather than the indicted defendants."[146] Therefore, the Department of Justice forbids FBI agents from searching and seizing privileged information.[147]

Department of Justice guidelines regarding searching electronic information state that "[w]hen agents seize a computer that contains legally privileged files, a trustworthy third party must examine the computer to determine which files contain privileged material."[148] Courts have different views on who this trusted third party should be.[149] In a few cases, courts have approved the use of a government "taint team," a set of government attorneys that are not involved in the investigation and are separated from the investigation by an ethical wall.[150] These attorneys review the seized information for privilege and then hand over unprivileged materials to the attorneys responsible for the investigation. More recently, courts have criticized

[144] Memorandum from Paul J. McNulty, Deputy Attorney. Gen., U.S. Dep't of Justice, on Principles of Federal Prosecution of Business Organizations 8 (2006), http://www.justice.gov/dag/speeches/2006/mcnulty_memo.pdf; *see also* Memorandum from Mark R. Filip, Deputy Attorney Gen., U.S. Dep't of Justice, on Principles of Federal Prosecution of Business Organizations 8 (Aug. 28, 2008) (same), http://www.justice.gov/opa/documents/corp-charging-guidelines.pdf.

[145] Mark R. Filip, *supra* note 144, at 8.

[146] Barry M. Sabin & Matthew R. Lewis, *supra* note 145, at 106; *see also In re* Grand Jury Subpoenas, 454 F.3d 511, 517 (6th Cir. 2006) ("Indeed, the government concedes that the leaking of privileged materials to investigators would raise the specter of *Kastigar*-like evidentiary hearings, and argues that it would therefore act conservatively, and err on the side of caution, in assessing the existence of privilege and in screening privileged documents from investigators.").

[147] H. MARSHALL JARRETT, *supra* note 86, at110.

[148] *Id*.

[149] *Id.*

[150] *Id.*; *see also* Black v. United States, 172 F.R.D. 511, 516 (S.D. Fla. 1997) ("The Plaintiffs have a serious concern that disclosure to taint team prosecutors would not protect the confidentiality and privacy rights they here assert. Recognizing that this approach has been utilized by several courts in the past the Court nevertheless concludes that [these] procedures . . . will assure a fair and proper balance between protection of Constitutional rights and proper disclosure.").

our rejected this approach.[151] In *United States v. SDI Future Health, Inc.*,[152] for example, the court observed "[f]ederal courts have taken a skeptical view of the Government's use of 'taint teams' as an appropriate method for determining whether seized or subpoenaed records are protected by the attorney-client privileged."[153] In *In re Grand Jury Subpoenas*,[154] the Sixth Circuit cautioned that when using a taint team "the government's fox is left in charge of the [suspect's] henhouse, and may err by neglect or malice, as well as by honest differences of opinion."[155] It is increasingly the case that the government will allow a company to conduct its own review of seized materials within a short period of time after the seizure for privilege before "producing" those documents and a privilege log to the attorneys leading the investigation.

The application of the plain view doctrine to an electronic search also poses many issues for the company and law enforcement.[156] The Ninth Circuit discussed these issues at length in *United States v. Comprehensive Drug Testing, Inc.*[157] In *CDT*, the government searched the CDT's offices for evidence that ten major league baseball players were taking banned performance enhancing drugs.[158] When executing the search, government agents viewed and seized electronic files containing the drug testing results of hundreds of major league players and many other people, in addition to records relating to the ten players that were the subject of the warrant.[159] The government argued that the seizure of this evidence was proper because it fell within the "plain view" exception to the warrant requirement.[160] The Ninth Circuit disagreed.[161]

---

[151] Lily R. Robinson, *Courting Chaos: Conflicting Guidance from Courts Highlights the Need for Clearer Rules to Govern the Search and Seizure of Digital Evidence*, 12 YALE J. L. & TECH. 311, 337 (Spring 2009-2010) (discussing case law).
[152] 464 F. Supp. 2d 1027 (D. Nev. 2006).
[153] *Id.* at 1037.
[154] 454 F.3d 511 (6th Cir. 2006).
[155] *Id.* at 523; *see also In re* Search Warrant for Law Offices, 153 F.R.D. 55, 59 (S.D.N.Y. 1994) ("[T]his court notes that reliance on the implementation of a Chinese Wall, especially in the context of a criminal prosecution, is highly questionable, and should be discouraged."); United States v. Neill, 952 F. Supp. 834, 841 n.14 (D.D.C. 1997) (criticizing taint teams as an "unwise . . . policy decision").
[156] *See* Lily R. Robinson, *supra* note 151, at 335-36.
[157] 621 F.3d 1162 (9th Cir. 2010).
[158] *Id.* at 1166.
[159] *Id.*
[160] *Id.* at 1176. The plain view doctrine states that "law enforcement officers may seize evidence in plain view, provided that they have not violated the Fourth Amendment in arriving at the spot from which the observation of the evidence is made." Kentucky v. King, --- U.S. ---, 131 S. Ct. 1849, 1858 (2011).

It reasoned:

> By necessity, government efforts to locate particular files will require examining a great many other files to exclude the possibility that the sought-after data are concealed there. . . . Once a file is examined, however, the government may claim (as it did in this case) that its contents are in plain view and, if incriminating, the government can keep it. Authorization to search *some* computer files therefore automatically becomes authorization to search all files in the same sub-directory, and all files in an enveloping directory, a neighboring hard drive, a nearby computer or nearby storage media. Where computers are not near each other, but connected electronically, the original search might justify examining files in computers many miles away, on a theory that incriminating electronic data could have been shuttled and concealed there. . . . We recognize that over-seizing is an inherent part of an electronic search process and proceed on the assumption that, when it comes to the seizure of electronic records, this will be far more common than in the days of paper records. . . . [However], [t]he process of segregating electronic data that is seizable from that which is not must not become a vehicle for the government to gain access to data which it has no probable cause to collect.[162]

Other courts have suggested that the government has greater discretion. As the Third Circuit explained, because "it is clear that because criminals—can and often do—hide, mislabel, or manipulate files to conceal criminal activity, a broad, expansive search [of electronic media] may be required."[163] Therefore, in some cases "there may be no practical substitute for actually looking in many (perhaps all) folders and sometimes at the documents contained within those folders."[164]

Courts recognize that the constitutional propriety of electronic search and seizure must be analyzed through "the Fourth Amendment's bedrock principle of reasonableness on a case-by-case basis."[165] But there is still substantial dispute as to what is reasonable in the electronic arena. In general, "[a]s the description of . . . places and things [to be searched and seized]

---

[161] Comprehensive Drug Testing, Inc., 621 F.3d at 1176.
[162] *Id.* at 1176-77.
[163] United States v. Stabile, 633 F.3d 219, 237 (3d Cir. 2011).
[164] United States v. Burgess, 576 F.3d 1078, 1094 (10th Cir. 2009); *see also* United States v. Mann, 592 F.3d 779, 782 (7th Cir. 2010) (noting that electronic data may be "manipulated to hide their true contents."); United States v. Hill, 459 F.3d 966, 978 (9th Cir. 2006) (noting that incriminating evidence "can be hidden in all manner of files. . . . Criminals will do all they can to conceal contraband, including the simple expedient of changing the names and extensions of files to disguise their content from the casual observer.").
[165] United States v. Richards, 659 F.3d 527, 538 (6th Cir. 2011).

becomes more general, the method by which the search is executed become[s] more important—the search method must be tailored to meet [the] allowed ends."[166] In addition, several courts recommend that law enforcement officers "us[e] a search protocol to structure the search with an analysis of the file structure, followed by a search for suspicious file folders, and then looking for files and types of files most likely to contain the objects of the search by doing keyword searches."[167] Therefore, the government takes a considerable, and often unjustifiable, risk when it broadly applies the plain view doctrine or does not respect a company's privileged communications when searing and seizing electronic information.

e. Post-Search

After the search is over, an agent must give a company representative a receipt for the property seized during the search.[168] The agents must also promptly return a copy of the warrant to the authorizing magistrate judge and file a copy of the receipt with the court.[169] In addition, "upon the conclusion of the search, the agents [will often] serve a [grand jury] subpoena *duces tecum* on the company requiring the production of documents covered by the search warrant and any additional documents needed by the grand jury."[170]

B. Responding to a Search Warrant from the Antitrust Division

As the foregoing discussion should indicate, a company cannot stop a search once agents show up in the lobby with a warrant. Instead, the focus should be on minimizing the disruption to day-to-day business operations, reducing the stress and fear of employees, dealing with reputational fallout, and establishing a credible position with the Antitrust Division. A company that finds itself unprepared for the execution of a search warrant starts with a significant disadvantage, and may find it difficult to accomplish even one of these goals. There is simply no substitute for training and preparedness prior to the execution of a search warrant.

---

[166] Burgess, 576 F.3d at 1094.
[167] Stabile, 633 F.3d at 239.
[168] FED. R. CRIM. P. 41(f)(1)(D).
[169] FED. R. CRIM. P. 41(f)(1)(B), (D).
[170] Antitrust Division Manual, *supra* note 111, at III-91.

1. The Rapid Response Team

Companies should designate and train a rapid response team before a search warrant is executed. Generally speaking, a company should designate four types of responders: (1) Designated Managers, (2) Administrative Representatives, (3) Attorney Representatives, and (4) IT Specialists. The roles of these team members are described below.[171]

- **Designated Managers**. One or more members of the management team and/or legal department at each office should be prepared to handle initial interactions with the FBI. These exchanges are particularly important because they set the tone for the search.[172]

- **Administrative Representatives**. A number of employees should be trained to interact with the government agents as they execute their search. Ideally, there should be one Administrative Representative per FBI agent, although that may not be realistic in most office settings. Administrative Representatives should be trained not to interfere with or obstruct the search. Instead, they should shadow a designated agent and take detailed notes regarding the documents searched and seized, employees whose documents were searched, and how the search was executed.[173]

- **Attorney Representatives**. A member of the company's legal department (or, in locations where the legal department is not present, its designee) should be trained to invoke privilege over areas of the office and computer systems that are likely to contain privileged documents. Attorney Representatives should also be prepared to document this invocation as well as the FBI agents' responses. Attorney Representatives should also be trained to alert outside counsel or the general counsel immediately in the event that agents seize privileged materials.

- **IT Specialists**. An employee from the information technology department at each office should be trained to deal with grand jury subpoenas and search warrants. IT Specialists should be prepared to discuss the company's document retention policies and disable automatic deletion policies on short notice.[174]

Each of these employees and outside counsel will have different tasks during the search.

- **Designated Managers**.

    1) Call the legal department immediately. Designated Managers and all employees should contact the legal department immediately if a search warrant is executed, and outside

[171] The roles and responsibilities of these employees and outside counsel on the day of a search are summarized in Appendix B.
[172] *See* James M. Griffin & Brian R. Meiners, *supra* note 110, a 10.
[173] *Id.*
[174] *Id.*

counsel should be informed about the search immediately. Until legal counsel arrives, keep an open line of communication between in-house counsel, outside counsel, and the search site so there is no delay in dealing with issues that come up during the search.

2) Obtain a copy of the search warrant. Request a copy of the search warrant, copying it, and forwarding it to counsel.[175]

3) Ask for the name and contact information of key government employees. The Designated Manager should request the name and contact information of the lead agent executing the search warrant and the Antitrust Division attorney that is in charge of the investigation. This information should be immediately forwarded to in-house and outside counsel.[176]

4) Deal with Non-Essential Employees. Before a search warrant is executed, the company should develop a policy for how it will handle employees that are not essential to the search warrant response. There are several options. Experience teaches that one of the more advisable approaches is as follows:

   - Senior management should notify the employees that a search warrant is being executed.

   - Inform the employees of their rights before and during the search.[177] If an FBI agent does not allow the company to inform its employees of their legal rights, this should be carefully noted and outside counsel should be informed immediately. These rights include:

     - An employee does not have to speak with any government agent;[178]

     - An employee can set limits on what he or she will discuss with the government;[179]

     - An employee has the right to have legal counsel present during any interview with a government agent;[180]

     - Unless the FBI agents object, an administrative representative will attend any on-site meeting the employee has with FBI agents and take notes;

     - Unless government agents say otherwise, an employee is free to go at any time;[181]

---

[175] James M. Griffin & Brian R. Meiners, *supra* note 110, at 11; *see also* Ray V. Hartwell, III, *supra* note 117, at 8.
[176] Ray V. Hartwell, III, *supra* note 117, at 8.
[177] W. Thomas McGough, Jr., *Search and Seizure in the United States: Surviving a Search Warrant*, 10 ANTITRUST 6, 7 (Spring 1996).
[178] Cecil A. Lynn III, *You've Been Served: Corporate Response to Grand Jury Subpoenas & Search Warrants for Electronically Stored Information*, 9 SEDONA CONF. J. 183, 191 (Fall 2008).
[179] However, as noted above, *Salinas* suggests that there may be important consequences to placing limits on an interview without invoking the protection against self-incrimination. 133 S. Ct. at 2174.
[180] Ray V. Hartwell, III, *supra* note 117, at 11.
[181] W. Thomas McGough, Jr., *supra* note 177, at 9.

- Employees should not speak with the press or discuss the search warrant on social media;[182]

- Employees should be courteous to the FBI agents, should not use abusive language, and should not resist their search;[183]

- Employees should not attempt to destroy, delete, or hide any documents or electronically stored information;[184] and

- Employees should not discuss the subject matter of the investigation between themselves.[185]

- Unless the government instructs otherwise, senior management should ask all non-essential employees to leave the office until further notice.

- If the company decides to dismiss non-essential employees until the search ends, outside counsel should explain this policy to the Antitrust Division.[186]

- To the extent employees will remain at the office, the company should consider the extent to which employees should assist government agents during the search. On the one hand, not assisting the government could result in normal business operations being disrupted for considerably longer while government agents search for materials specified in the search warrant. On the other hand, FBI agents could misinterpret assistance from employees as consent to search beyond the scope of the warrant. Therefore, if employees provide assistance to government agents during the search, they should first ask the FBI agent to identify the items that they are looking for before providing assistance. Employees should not provide government agents with documents outside the scope of the search warrant; this could also be viewed as consent to search beyond the scope of the warrant.[187]

- **Administrative Representatives**.

1) Document Warrant Execution. Administrative representatives should carefully document how the FBI executes the search warrant. This can be done either by taking notes or videotaping the execution of the search warrant.[188]

2) Create an Inventory. During the execution of the search, administrative representatives should keep their own separate inventory of the documents and information seized by the

[182] Ray V. Hartwell, III, *supra* note 117, at 12.
[183] *Id*.
[184] Cecil A. Lynn III, *supra* note 178, at 184.
[185] Ray V. Hartwell, III, *supra* note 117, at 13.
[186] *Id.* at 12.
[187] James M. Griffin & Brian R. Meiners, *supra* note 110, at 13-14.
[188] Ray V. Hartwell, III, *supra* note 117, at 9; James M. Griffin & Brian R. Meiners, *supra* note 110, at 11-12.

FBI. After the search, this inventory should be compared to the one prepared by the FBI to determine if there are any discrepancies or omissions.[189]

- **Attorney Representatives**.

1) Call outside counsel immediately. When a search is executed, a company should *immediately* call its outside counsel, even if that firm does not handle antitrust matters. (Of course, the better course is to engage outside antitrust counsel before a problem ever arises to help develop and implement an antitrust compliance program and search warrant response protocol.[190]) The designated manager may have already contacted counsel, but it makes sense to have built in redundancies to ensure that this critical step is not overlooked.

2) Review the search warrant. Carefully review the warrant to make sure it is technically correct. If the name of the company or its address is incorrect, counsel should request that the FBI agents halt the search until a proper search warrant has been obtained. Counsel should carefully note any refusal of this request.[191]

3) Invoke Attorney-Client Privilege. Where appropriate, the Attorney Representatives should invoke the attorney-client privilege over paper and electronic files that are likely to contain privileged material. Attorney Representatives should document the FBI's response to the invocation of privilege, and communicate this to outside counsel as soon as possible.

4) Prepare a Reactive Press Statement. Outside counsel and the legal department should determine whether it is necessary to issue a reactive media statement. If so, inside counsel and outside counsel should work with the company's communications team to prepare a statement in case there are press inquiries regarding the search. In some cases, a person may need to be prepared to answer questions from major customers.

- **IT Specialists**.

1) Ask that an FBI Specialist be Present. While an FBI technical specialist is not required to take part in a search,[192] the presence of these specialists can reduce business disruptions.[193]

2) Request that FBI Image Electronic Media. Because "forensic analysis of a hard drive (or other computer media) takes too long to perform on-site during the initial execution of a

[189] Ray V. Hartwell, III, *supra* note 117, at 10.
[190] *Id.* at 13 ("establish a communication system in order to ensure that issues that arise during the search are resolved in a quick and efficient manner.").
[191] *See* Ray V. Hartwell, III, *supra* note 117, at 8-9.
[192] Cecil A. Lynn III, *supra* note 178, at 192.
[193] Forro Precision, Inc. v. Int'l Bus. Machs. Corp., 673 F.2d 1045, 1054 (9th Cir. 1982) ("such assistance may be more necessary to the police in the context of a search, where technical knowledge may be wanting").

search warrant,"[194] the FBI will often seize or image electronic media during its search.[195] IT Specialists should request that the FBI image electronic media, so that the FBI does not take the electronic equipment offsite for further forensic analysis.[196]

3) Ask about the Search Protocol for Electronically Stored Information. Although the Antitrust Division is likely to oppose it,[197] some magistrates will require the government to include a search protocol for electronically stored information in the warrant.[198] The search protocol will contain the methods that the government intends to use when searching and seizing electronic information to ensure that the search is bound by the terms of the warrant.[199] Generally, the search protocol will describe (1) the electronic information that the government intends to seize, and (2) the methods that the government will use to locate this information without reviewing all of the company's electronic information.[200] If such a search protocol exists, the IT Specialist should obtain it and send a copy of it to in-house and outside counsel, who should review whether the protocol adequately protects privileged materials and trade secrets.[201] The IT Specialist should also note any instances where the FBI fails to comply with the search protocol.

4) Inform the Government about Documents that are Hosted on Servers Outside of the Jurisdiction. Magistrate judges only have the power to authorize the seizure of property, including electronic information, in their particular judicial district.[202] As a practical matter, this can severely restrict the government's ability to seize electronic information when it is stored in servers throughout the country. For instance, if the FBI executes a search warrant on a financial services company located in Manhattan, the warrant cannot authorize FBI agents to seize electronic information hosted on company servers in New Jersey, or even Brooklyn. As a result, the IT Specialist should ask the FBI whether they have obtained multiple warrants. In addition, the IT Specialist should inform FBI agents when they are searching or seizing information hosted on out-of-state servers, and document the FBI's reaction.

5) Document the Electronic Search. IT Specialists should be prepared to take detailed notes

---

[194] H. MARSHALL JARRETT, *supra* note 86, at 86.
[195] *Id.*
[196] *Id.* ("This process has two steps: *imaging*, in which the entire hard drive is copied, and *analysis*, in which the copy of the hard drive is culled for records that are responsive to the warrant.").
[197] *Id.* at 79 (advising that FBI agents "should *not* commit . . . to any particular 'protocol' for reviewing the media to find evidence that falls within the scope of the warrant.").
[198] *Id.* at 80 ("A few magistrate judges issue warrants to search computers only subject to limitations on the way the seized media may later be examined."). Arguably, these protocols are critical to ensuring that a search of electronic information does not become "a limitless search." Cecil A. Lynn III, *supra* note 178, at 193; *see also* United States v. Carey, 172 F.3d 1268, 1273 (10th Cir. 1999) (officer overstepped bounds of search warrant for drug evidence by searching suspect's laptop for child pornography for four hours).
[199] Cecil A. Lynn III, *supra* note 178, at 193; *see also In re* Search of 3817 W. West End, First Floor, Chicago, Illinois 60621, 321 F. Supp. 2d 953, 955 (N.D. Ill. 2004) (court required use of a search protocol "to avoid generally rummaging through all information on the computer, much of which would be irrelevant to the alleged criminal activity.").
[200] Cecil A. Lynn III, *supra* note 178, at 194.
[201] *Id.* at 194-95.
[202] FED. R. CRIM. P. 41(b)(1), (a)(2)(A).

regarding the search methods used by the FBI agents, the employees whose files were searched, and whether the agents attempted to remotely access documents hosted at other offices or outside the United States.[203]

6) Prepare a Detailed Inventory. IT Specialists should keep a detailed inventory of the exact types of electronic information imaged and/or seized by the FBI.[204] The FBI is only required to "describ[e] the physical storage media that were seized or copied" in its inventory.[205] Because these simple descriptions can omit important information about which employee's electronic media was searched and seized, how much data was seized from each employee, and the likely time period that the electronic records cover, it is important for IT Specialists to create their own inventory.

7) Disable Automatic Deletion Features and Preserve Electronically Stored Information. The failure to preserve electronic information can lead to a criminal prosecution for obstruction of justice under the Sarbanes-Oxley Act.[206] After the FBI leaves, IT Specialists should immediately disable any automatic deletion settings on company servers or email systems. IT Specialists should also work with in-house and outside counsel to ensure that all relevant electronic information is preserved, either by imaging hard drives and servers, or other forensically sound means.[207]

All of these procedures are intended to minimize the disruption from a search, decrease the risk that the company will make the problem worse with ill-advised statements or behaviors while the search is being executed, and ensure that outside counsel will be alerted to the search at the earliest possible moment. Once outside counsel becomes aware of the search, they too have a critical role to play. We summarize below some of the steps that outside counsel should immediately undertake upon learning of a search.

1) Ask for a brief delay. The FBI is likely to ignore it, but it cannot hurt for outside counsel to ask the agents to delay the search until counsel arrives. Inform the FBI that the company maintains privileged files at the search site that should not be reviewed by law enforcement.[208]

2) Call the lead attorney at the Antitrust Division. Outside counsel should contact the

[203] While the issue has not been litigated, it seems unlikely that FBI agents can access documents hosted on foreign servers when executing a domestic search warrant. *See, e.g.*, JAMES H. MUTCHNIK, ET AL., GRASPING AT CLOUDS: DOCUMENTS HOSTED OVERSEAS AND GRAND JURY SUBPOENAS 6-7 (2012). In addition, most warrants only grant FBI agents "authority to . . . search for and seize a person or property located within the district." FED. R. CRIM. P. 41(b)(1). Therefore, agents may need to seek an additional warrant to search and seize documents stored at other U.S. offices.
[204] Cecil A. Lynn III, *supra* note 178, at 195-96.
[205] FED. R. CRIM. P. 41(f).
[206] Cecil A. Lynn III, *supra* note 178, at 184; *see also* 18 U.S.C. § 1512(c).
[207] Cecil A. Lynn III, *supra* note 178, at 184.
[208] *See* Ray V. Hartwell, III, *supra* note 117, at 8.

Antitrust Division attorney that is leading the investigation. As in all things, first impressions matter. Early strident comments or uninformed denials of wrongdoing should be avoided, as they can taint the relationship.[209] Rather, it is best to take no position on the merits of the Antitrust Division's claims. When speaking with the Antitrust Division, outside counsel should do the following:

- Inform the Antitrust Division that the company is represented by outside counsel and provide appropriate contact information.

- Confirm that the company will cooperate with the search, but that it does not consent to any searches beyond the scope of the warrant.[210]

- Propose that the company preserve and produce all relevant, non-privileged documents in lieu of the search.[211]

- Raise the seizure of trade secrets and privileged communications with the Antitrust Division. Offer to negotiate a protocol for dealing with trade secrets and privileged information. To manage business disruptions and preserve the attorney-client privilege, suggest that the information seized be segregated for a preliminary privilege review by outside counsel.[212]

- Discuss procedures that could help minimize the disruption of the company's business operations, such as imaging hard drives rather than seizing them.[213]

- Request that the agents refrain from interviewing employees without counsel present.[214] It is expected and reasonable for employees to provide minimal assistance to FBI agents during the search, but counsel should request being present when more detailed questioning occurs. If the Antitrust Division denies this request, it should be noted in detail.[215]

- Counsel should inquire whether another company has already received corporate leniency, or if "the door is still open."[216]

- Outside counsel should inquire exactly which products are the subject of the investigation, and whether there is an opportunity for an amnesty plus application in any related products.[217]

- Ask for a copy of the affidavit supporting the search warrant. This document was

[209] *See* James M. Griffin & Brian R. Meiners, *supra* note 110, at 13.
[210] *Id.* at 14.
[211] *See* Ray V. Hartwell, III, *supra* note 117, at 9.
[212] *See id.* at 9, 10.
[213] *Id.* at 9.
[214] *Id.* at 11; *see also* James M. Griffin & Brian R. Meiners, *supra* note 110, at 13.
[215] Ray V. Hartwell, III, *supra* note 117, at 11.
[216] *Id.* at 13.
[217] *Id.* at 9.

likely filed under seal. It probably contains important information regarding the identity of the amnesty applicant, key meetings or communications, and employees at the company that have criminal exposure. Unfortunately, the Antitrust Division probably will not provide it, but there are times the Division might find it advantageous to disclose it.[218]

- Ask for a reverse proffer from the Antitrust Division for a later date, so that counsel can learn additional information regarding the scope of the investigation and key areas of criminal exposure.[219]

2. Preparing for Drop-in Interview

Before the search, the company should also prepare senior employees for the possibility of a drop-in interview or an interview during the search.[220] Preparations should include:[221]

- All employees should understand their rights. Employees have every right to decline an interview without counsel. FBI agents will not be surprised or offended by an employee's decision to defer an interview until counsel is present.[222]

- The employee should ask for the name of each agent/attorney taking the interview and for copies of their business cards.[223]

- Unless the government says otherwise, the employee can leave the interview at any time.[224]

- The employee should not consent to a search of their home, unless the government has a warrant.[225]

IV. The FBI Has Left the Building: Where Do We Go From Here?

The FBI agents appear to be taking the last of the labeled bankers' boxes out of the office. The FBI computer technician has finished imagining employee hard drives. The lead agent approaches you, thanks you for your compliance, and hands you two documents: an inventory of the items seized and a grand jury subpoena for the seized documents and additional documents and information. It sinks in that you will be dealing with this investigation for a long time.

* * *

[218] *See* Cecil A. Lynn III, *supra* note 178, at 191.
[219] *Id.*
[220] Ray V. Hartwell, III, *supra* note 117, at 6.
[221] Appendix C of the memorandum contains a succinct checklist of the steps that a company can take to prepare for drop-in interviews.
[222] Ray V. Hartwell, III, *supra* note 117, at 6.
[223] *Id.* at 6.
[224] *Id.* at 6.
[225] *Id.* at 6.

How the execution of a search warrant is handled is just the first in a series of key decisions that will need to be made over the next several months and even years during the investigation. In order to assist the company and its employees in making these decisions, outside counsel needs to (1) effectively communicate with the Antitrust Division, (2) quickly master the facts, and (3) work with the client and the global defense team to advise the company on the best strategy going forward.

Counsel should build on the experience with the Antitrust Division during the execution of the search warrant to establish a reliable and credible working relationship with the Division on behalf of the company.[226] This credibility is important, particularly if the company discovers that it has information about a separate conspiracy that could entitle the company to amnesty plus protections.[227]

At the earliest opportunity, outside counsel must begin investigating the government's allegations.[228] Counsel should try to learn as much about the government's claims as possible by reviewing the notes of the administrative representatives, debriefing employees that were interviewed by the FBI, meeting with the Antitrust Division, and possibly filing a motion to unseal the affidavit that established probable cause to search the company.[229] In addition, counsel should begin reviewing documents, electronically stored information, and other business records for (a) evidence of the alleged conspiracy, (b) evidence of innocence and possible defenses, and (c) evidence of other, separate conspiracies that might entitle the company to amnesty-plus protection.[230] This process will begin with drafting a legal hold notice and working with company counsel and IT personnel to pull data and documents from relevant employees/custodians.[231]

Outside counsel should also interview relevant employees. When interviewing

[226] *Id.* at 13.
[227] *Id.* at 13.
[228] *Id.* at 16.
[229] *Id.* at 16-17.
[230] *Id.* at 18.
[231] *See* Cecil A. Lynn III, *supra* note 178, at 184-85.

employees, counsel should be careful to begin with the now-familiar *Upjohn* warning.[232] If applicable, counsel should remind the employee that they are required to comply with the internal investigation by virtue of their employment agreement with the company.[233] If employees ask questions that call for legal advice, they should be told that company counsel cannot provide legal advice to individual employees.[234]

At the same time, counsel will need to consider which employees need separate legal representation, when it should be provided, and whether the company is prepared (or obligated) to pay for it.[235] Once individual counsel is retained by these employees, company counsel should consider creating a joint defense relationship with these attorneys.[236] In most cases, it will be advisable to have a written joint defense agreement.[237]

If the company is being investigated in other jurisdictions, outside counsel should also establish communications with the company's global defense team.[238] It is common for competition agencies to conduct dawn raids in multiple jurisdictions at the same time that a search warrant is being executed in the U.S.[239] As a result, U.S. counsel will need to coordinate with counsel in other jurisdictions while conducting their internal investigations, presenting information to the company, the board of directors, and then to antitrust enforcers in affected jurisdictions, many of which have different procedural rules and enforcement regimes.

V. Conclusion

The representation of a company facing this array of potential issues is a potentially daunting task. The best way to deal with them is to put in place a carefully designed antitrust compliance program that minimizes the likelihood of the company becoming involved in a

---

[232] *See* Ray V. Hartwell, III, *supra* note 117, at 19.
[233] *Id.* at 20.
[234] *Id.* at 20.
[235] *See id.* at 21-22.
[236] *Id.* at 22.
[237] *See id.* at 23.
[238] *Id.* at 13.
[239] *See, e.g.*, Antitrust Div., U.S. Dep't of Justice, *Division Update: Spring 2013* (2013) (noting that in 2012, the Antitrust Division "enhanced its relationships and increased interactions with other competition agencies," including competition agencies in Australia, Brazil, Canada, Colombia, the European Union, Germany, Japan, Mexico, South Africa, and the U.K.), http://www.justice.gov/atr/public/division-update/2013/international-program.html.

criminal investigation. If a search or investigation does happen, important judgments will have to be made quickly, but prior, thoughtful preparation should leave the company well positioned to make informed decisions. Proper training is essential to lessening the impact to a company's operations, reputation, and standing with its employees, customers, and the public.

APPENDIX A: CORPORATE COMPLIANCE CHECK LIST

- □ Review and update corporate antitrust compliance statements, codes of ethics, and codes of conduct
- □ Publish and distribute an antitrust compliance handbook
- □ Employees must certify in writing that they will comply with the company's antitrust policy
- □ Require employees to attend a training course on the company's antitrust policy
- □ Provide specific training and written guidance on pricing decisions and competitive intelligence
- □ Consider separating employees with pricing authority from those that may interact with competitors
- □ Create an internal reporting structure
- □ Consider retaining outside counsel to perform an audit or spot-check of antitrust compliance

APPENDIX B: SEARCH WARRANT RESPONSE CHECK LIST

Rapid Response Team Checklist

Attorney Representatives

- □ Call outside counsel immediately
- □ Review the search warrant to ensure that it is technically correct
- □ Invoke the attorney-client privilege for areas of the office and electronic media that are likely to contain privileged information
- □ Discuss any search protocol contained in the warrant with the IT Specialist(s)
- □ Assist Designated Managers in dealing with non-essential employees
- □ Assist in preparing a reactive press statement

Outside Counsel

- □ Ask for a brief delay
- □ Review the search warrant to ensure that it is technically correct
- □ Call the attorney at the Antitrust Division who is responsible for the investigation. Discuss the basis for investigation, seizure of electronic documents, privilege review of seized documents, avoiding disruption of company's ongoing business operations, whether corporate leniency is still available, that the FBI not interview employees and consider asking for a copy of the affidavit supporting the search warrant.
- □ Discuss any search protocol contained in the warrant with the IT Specialist(s)
- □ Determine if a reactive press statement is necessary and assist in preparing it. Be prepared to deal with media and customer inquiries.

Designated Managers

- □ Call the legal department immediately
- □ Obtain a copy of the search warrant and distribute it to in-house and outside counsel
- □ Ask for the name and contact information of key government employees (FBI and lead Antitrust Division investigator)
- □ Inform employees of the search and their rights, and dismiss non-essential employees until

the search has ended

Administrative Representatives

- □ Document the execution of the search warrant
- □ Create an inventory of the items seized by the government

IT Specialists

- □ Ask for an FBI technical specialist to be present
- □ Request that the FBI image electronic media
- □ Ask for a copy of any search protocol for electronically stored information
- □ Inform the government about information hosted on servers outside the jurisdiction
- □ Document the electronic search
- □ Prepare a detailed inventory
- □ Disable automatic deletion features and preserve electronically stored information after the documents are seized and inventoried by the FBI

APPENDIX C: DROP-IN INTERVIEW PREPARATION CHECK LIST

- □ Inform employees of their rights in advance
- □ Employee should ask for the name and title of each agent/attorney attempting to take a drop-in interview
- □ Inform employee that they are free to terminate the interview at any time
- □ Employee should not consent to a search of their home, unless the government has a search warrant