The Sedona Conference Journal

Volume 15 2014

Responding to the Government's Civil Investigations

David C. Shonka

Recommended Citation:

David C. Shonka, *Responding to the Government's Civil Investigations*, 15 SEDONA CONF. J. 1 (2014).

For this and additional publications see: https://thesedonaconference.org/publications

The Sedona Conference Journal® (ISSN 1530-4981) is published on an annual basis, containing selections from the preceding year's Conferences and Working Group efforts.
The Journal is available on a complementary basis to courthouses and public law libraries and by subscription to others ($45; $30 for Conference participants and Working Group members).
Send us an email (info@sedonaconference.org) or call (1-602-258-4910) to order or for further information. Check our website for further information about our Conferences, Working Groups, and publications: www.thesedonaconference.org.

Comments (strongly encouraged) and requests to reproduce all or portions of this issue should be directed to:
The Sedona Conference, 5150 North 16th Street, Suite A-215,
Phoenix, AZ 85016 or call 1-602-258-4910; fax 602-258-2499; email info@sedonaconference.org.

The Sedona Conference Journal® designed by MargoBDesign.com – mbraman@sedona.net

Cite items in this volume to "15 Sedona Conf. J. _____ (2014)."

RESPONDING TO THE GOVERNMENT'S CIVIL INVESTIGATIONS

David C. Shonka[1]
Federal Trade Commission
Washington, D.C.

INTRODUCTION

Litigators often say that litigation is more about storytelling than it is about the facts. The goal is to put together a coherent, plausible, and sympathetic story that will grab the attention and interest of the audience and compel a conclusion favorable to the litigator's client. In contrast, government investigations are not about storytelling. They are about facts and the opinions and conclusions that can be drawn from the facts. More specifically, they are about obtaining a complete set of facts. Incomplete facts can lead to incorrect decisions. Incomplete facts can just as easily lead to law enforcement actions being filed that should not be filed as they can lead to important cases that should be filed not being filed. Either of these outcomes can be very expensive for the government, the parties, taxpayers, and the general public interest. This paper is about civil law enforcement investigations, the way the government conducts them, and the ways in which the parties to an investigation might appropriately deal with them.

A. Basics of Government Investigations

Government investigations are not like civil litigation. With respect to gathering facts, they differ from litigation in three major respects. First, only one party in an investigation gets to ask for documents and question witnesses. The government investigates so that it alone might collect information and decide whether to close an inquiry (as it does in most cases) or pursue further action, usually in the form of an administrative or judicial proceeding.

Second, investigations usually are conducted before any cause of action is identified, any claim or defense is asserted, or any court complaint is filed and served. This means the Federal Rules of Civil Procedure do not apply and discovery is not limited by the same notions of relevance that apply in litigation. While litigating parties may seek information relevant to a claim or defense of a party, the government may seek any information that is reasonably related to the scope of its investigation.[2]

---

1 The views expressed herein are solely those of the author and do not represent the views of the Federal Trade Commission, any individual Commissioner, or any other Commission employee. Preliminary versions of this article were presented at the 6th and 9th Annual Georgetown Advanced eDiscovery Institute programs held on December 12, 2009 and December 5, 2012 respectively, and at the Practicing Law Institute: Government Investigations 2014 program held on March 26, 2014. The author appreciates the opportunity for dialogue that these venues permitted. The author also thanks Jeane A. Thomas, Crowell & Moring, LLP, for her very substantial suggestions and insights, especially with respect to the perspective of the private practitioner, and Jonathan Hill, FTC attorney, for his close attention to the paper and helpful suggestions for making certain points more precise. That said, any errors in this paper are solely those of the author.

2 *E.g., FTC v. Invention Submission Corp.*, 965 F.2d 1086, 1089-90 (D.C. Cir. 1992).

Third, in contrast to litigation, which is usually triggered by an event resulting in one party having a claim against another, government investigations may be triggered by anything that piques the government's curiosity. They may be triggered by news stories, consumer complaints, requests from Congress, leaks from informants, first-hand observations by government employees, self-reporting, or any number of other sources. An agency "can investigate merely on suspicion that the law is being violated, or even just because it wants assurance that it is not."[3]

In those relatively few instances in which government investigations end up in court (generally because the government has sued to secure compliance), the courts have consistently recognized that the scope of issues that they may consider "must be narrow, because of the important governmental interest in the expeditious investigation of possible unlawful activity."[4] Although the court's function in such proceedings is "neither minor nor ministerial,"[5] it is "strictly limited" to determining whether the inquiry is "within the authority of the agency, the demand is not too indefinite and the information sought is reasonably relevant" [and] 'the disclosure sought [is] not [] unreasonable."[6] Significantly, a government request is not unreasonably burdensome unless it "threatens to unduly disrupt or seriously hinder normal business operations."[7]

B. The Government's Civil Investigative Arsenal

Under Part V of the Federal Rules of Civil Procedure (Rules 26-37) and Rule 45, litigants have several paths for discovering information; and courts may apply a broad range of sanctions to compel, or at least encourage, cooperation. In contrast, the government in its investigations must depend on statutory grants of authority to obtain information. Absent voluntary cooperation or statutory grants of authority, the government is powerless to collect information before filing any legal action.

The Federal Trade Commission ("FTC"), which has a full range of information-gathering resources at its disposal, is a good example of both the breadth and limits of the government's ability to gather information in a pre-complaint investigation. At one end of the spectrum, the agency's statutes allow it to – and in practice it does – encourage voluntary cooperation by issuing access letters,[8] which are unenforceable requests for information.[9] In this regard, the, FTC Act protects the information from public disclosure. It provides that the agency will afford information given "in place of compulsory . . . process" the same level of confidential treatment that it provides to information it receives through compulsory process.[10]

On the other end of the spectrum, the agency may compel parties to give information. For example, the FTC may issue orders directing persons to submit "special reports" providing detailed information about their conduct and other matters.[11] Such orders are judicially enforceable,[12] and failure to comply may result in the imposition of

3 *FTC v. Texaco, Inc.,* 555 F.2d 862, 872 (D.C. Cir. 1977) (*en banc*) (quoting *United States v. Morton Salt Co.*, 338 U.S. 632, 642-43 (1950).
4 *Texaco,* 555 F.2d at 872.
5 *Okla. Press Publ'g Co. v. Walling*, 327 U.S. 186, 217 n.57 (1946).
6 *Morton Salt Co.*, 338 U.S. at 652-53 (1950); *Texaco*, 555 F.2d at 872.
7 *Texaco*, 555 F.2d at 882; *Invention Submission Corp.,* 965 F.2d at 1090.
8 15 U.S.C. §§ 46(a), 49; *see also* FTC Rule 2.4, 16 C.F.R. § 2.4.
9 *See FTC v. Am. Tobacco Co.,* 264 U.S. 298 (1924).
10 *See* 15 U.S.C. § 57b-2(f); FTC Rule 4.10(a)(8)(ii), 16 C.F.R. § 4.10(a)(8)(ii).
11 15 U.S.C. § 46(b). The Commission's authority to order such reports is limited to investigations that do not involve unfair or deceptive acts or practices. 15 U.S.C. § 57b-1(b).
12 15 U.S.C. § 49.

civil penalties, which accrue daily.[13] In all its investigations, the agency also has the authority to issue civil investigative demands ("CIDs") that may compel the recipient to provide information through interrogatory-style questions, produce documentary materials, or appear and give testimony at investigational hearings.[14] In its antitrust investigations, the agency additionally has the power to issue administrative subpoenas to compel the production of documents or the giving of testimony at investigational hearings almost anywhere in the country.[15] FTC CIDs and subpoenas are both judicially enforceable, and those who do not comply with a court's enforcement order may face contempt charges.[16]

Other federal agencies have additional powers to gather information. For example, the Consumer Financial Protection Bureau ("CFPB") has supervisory authority that provides it with immediate access to certain records maintained by entities it regulates.[17] Similarly, the Securities and Exchange Commission ("SEC") requires certain entities subject to its jurisdiction to file financial and other reports, and to maintain certain records that the agency may see at any time.[18] That agency also asserts the authority to issue "forthwith subpoenas."[19] Similarly, the Department of Labor and the Environmental Protection Agency both mandate the retention of various records; and in some instances the failure to maintain the records can result in fines or even imprisonment.[20]

The premerger notification statute, the Hart-Scott-Rodino Act ("HSR Act"),[21] lies somewhere between "voluntary" and "compulsory." On the one hand, the HSR Act authorizes the antitrust agencies to request detailed information relating to covered transactions. On the other hand, the parties are not required to respond to the requests – although they are forbidden to consummate their transaction unless they observe a statutory waiting period after providing either all the requested information or a detailed statement of reasons why they cannot provide the information.[22] Failure to comply with the HSR reporting and waiting-period requirement may trigger a court action to enjoin the transaction until there has been compliance,[23] an action to rescind the transaction if it has been consummated,[24] or a suit for substantial civil penalties, which accrue daily.[25] As these examples show, the government has the tools it needs to conduct its investigations, and it has had those tools for some time.

Access letters and subpoenas have been in the FTC's toolbox since the very beginning. It gained its CID authority in consumer protection cases in 1980 and in

13 15 U.S.C. § 50.
14 15 U.S.C. § 57b-1.
15 15 U.S.C. § 49.
16 15 U.S.C. §§ 49, 57b-1(h). *See, e.g.,* Stipulation for Entry of Order, *FTC v. Western Union Co.,* No. 13-mc-00131 AKH (S.D.N.Y. Dec. 9, 2013), ECF No. 67. Other agencies have also successfully sought civil contempt against parties who disobeyed court orders. *See, e.g.,* Contempt Order, *SEC v. Coronati,* No. 13-Misc.-372-P1(S.D.N.Y. Jan. 17, 2014), ECF No. 19.
17 *See* 12 U.S.C. §§ 5512(b)(1), 5514(a)(1)(C); 5514(b)(7); 12 C.F.R. pt. 1091.
18 *See, e.g.*, 15 U.S.C. §§ 78m, 78q; 17 C.F.R. §§ 230.401-.498, 240.12b-1 to -37.
19 For a discussion of "forthwith subpoenas," *see* John Reed Stark, *When to Say When: Handling Emerging Technology-Related SEC Enforcement Tactics*, 45 SEC. REG. & L. REP. (BNA) 1737 (Sept. 23, 2013), *available at* http://www.strozfriedberg.com/wp-content/uploads/2013/09/When-to-Say-When-Handling-Emerging-Technology-Related-SEC-Enforcement-Tactics_BloombergBNA_Stark.pdf.
20 *See, e.g.,* 29 C.F.R. pt. 516; 40 C.F.R. §§ 141.31-.35. For a summary of some Department of Labor and EPA record keeping requirements, *see Wages: Record Keeping & Reporting*, U.S. DEPARTMENT OF LABOR, http://www.dol.gov/dol/topic/wages/wagesrecordkeeping.htm (last visited July 16, 2014); Office of Water, Envtl. Prot. Agency, EPA 816-F-06-033, Record Keeping Rules: A Quick Reference Guide (2006), *available at* http://www.epa.gov/ogwdw/smallsystems/pdfs/guide_smallsystems_records_08-25-06.pdf;.
21 15 U.S.C. § 18a.
22 *See* 18 U.S.C. § 18a(e); 16 C.F.R. § 803.3.
23 15 U.S.C. § 18a(g)(2).
24 *See, e.g.*, *FTC v. Elders Grain, Inc.*, 868 F.2d 901 (7th Cir. 1989) (granting rescission on the merits).
25 15 U.S.C. § 18a(g)(1).

competition cases in 1994; and the HSR Act has been in effect since 1978. While the FTC's investigative tools have remained constant since 1994,[26] FTC antitrust investigations have grown in size and complexity. In the mid-1990s, very few cases involved document productions exceeding one million pages, and significant major merger investigations might have resulted in the production of a couple hundred boxes of documents.[27] Today, FTC merger investigations may yield terabytes of information.

While some may argue that these numbers evince the growth of intrusive government regulation, two facts account for the government's increased demand for information. First, the public, the courts, and the Congress all (correctly) demand that solid public interest justifications underpin any government intrusions into private decision-making. In matters involving private economic activity, this means agencies must base regulatory actions on evidence showing, in one form or another, that the public benefit from regulation is sufficient – or at least probable enough – to offset any private harm that may follow from the regulation. The Supreme Court's 1974 *General Dynamics* [28] decision is illustrative. That decision foreshadowed the end of the government's ability to prove a Clayton Act violation with simple evidence showing that a given merger would result in highly concentrated markets. While the government formerly could prove a violation in merger cases by simply showing an undue increase in four- or eight-firm concentration ratios,[29] or even that a very large firm was acquiring a very small one,[30] today the government must produce solid economic evidence showing that a merger may substantially lessen competition if consummated.[31] This often requires sophisticated economic analysis and modeling. This evidentiary burden requires the government to collect substantial data and information from the merging parties and other persons.[32]

Second, the quantity of potential evidence is vastly greater today than it was in the past. Virtually everyone with any decision-making authority in today's business environment has an array of electronic devices and social media tools readily at hand and uses them to transact business and communicate with superiors, co-workers, subordinates, and outside parties. Email, voice mail, instant messages, text messages, tweets, word processing, spreadsheets, presentations, and data compilations move freely and quickly through (and outside) an enterprise, and in various forms may be modified, preserved, replicated, and archived in the process. Sometimes employees work around the information structure of the enterprise and carry or transmit data and information off-site. In addition, companies and their employees are increasingly using "cloud"-based providers for hosting and processing data, as well as social networking sites, which are all hosted by third parties. Further, organizations increasingly allow employees to conduct business on any device they choose, rather than restricting them to company-owned equipment – a phenomenon

---

26 The SAFEWEB Act expanded the Commission's ability to secure and share information in some circumstances with foreign governments, but did not *per se* enlarge the tools at the FTC's disposal. *See* 15 U.S.C. § 46(j).

27 *Cf.,* Announcement by Deborah Platt Majoras, Chairman, Federal Trade Commission, Reforms to the Merger Review Process 5-6 (Feb. 16, 2006) [hereafter referred to as "Reforms to Merger Review"], *available at* http://www.ftc.gov/sites/default/files/attachments/mergers/mergerreviewprocess.pdf.

28 *United States v. General Dynamics Corp.,* 415 U.S. 486 (1974).

29 *See, e.g., United States v. Philadelphia Nat'l Bank,* 374 U.S. 321 (1963).

30 *See, e.g., United States v. Aluminum Co. of Am.,* 377 U.S. 271, 278-81 (1964).

31 *See, e.g., FTC v. Whole Foods Market, Inc.,* 548 F.3d 1028 (D.C. Cir. 2008); *FTC v. H.J. Heinz Co.,* 246 F.3d 708, 716-18 (D.C. Cir. 2001).

32 *See, e.g., FTC v. Staples, Inc.,* 970 F. Supp. 1066 (D.D.C. 1997). The FTC's lawsuit against Blockbuster further illustrates this point. In March, 2005, the FTC sued to enjoin Blockbuster's acquisition of Hollywood Entertainment Corp., on the ground that it had not complied with the premerger notification reporting and waiting period requirements. The Commission's complaint alleged, among other things, that Blockbuster had provided data for only approximately 400 of the company's 4,600 stores and that, at the time of the complaint, Blockbuster had only recently corrected the problem. The Commission alleged, "[t]he original data disk produced by Blockbuster contained 2.8 megabytes of data and had approximately 65,000 data rows [while the corrected disk] contained 96 megabytes of data and approximately 873,000 data rows." Complaint at § 17, *FTC v. Blockbuster, Inc.*, No. 1:05CV00463 (D.D.C. Mar. 4, 2005), ECF No. 1, *available at* http://www.ftc.gov/sites/default/files/documents/cases/2005/03/050304compblockbuster.pdf.

known as "bring your own device." Thus, important information can be widely dispersed through corporate networks, third-party servers, company- and privately-owned devices, electronic media storage (such as thumb drives and CD-ROMS), and Internet websites.

In the not-too-distant past, those engaging in questionable acts could hope to avoid detection by the simple expedient of circulating undated, unsigned memos with no letterhead. Even if discovered, ownership, distribution, and authorship of such documents was easy to deny, or at least not recall. Today's digital world makes such evasion all but impossible – provided government investigators get their hands on the right devices or sources. Of course, in order to retrieve all the relevant electronic evidence and identify those with knowledge of it, the government must cast a broad net; and this need often results in substantial demands on investigative targets and others.

C. How Government Investigations Begin

Parties typically have little opportunity to shape a government investigation at its very earliest stages. Information that triggers an investigation may come from many different sources, ranging from news reports to consumer complaints, leaked information, Congressional inquiries, or even reports or information that parties themselves file with the government. Just as the sources that trigger an investigation vary widely, so do the procedures that various agencies follow in opening an investigation. For example, in some agencies, such as the EPA, CFTC, and SEC, investigators are delegated broad discretion in choosing whether to follow a "hot tip." In contrast, agencies such as the FTC exercise top-down control over the process, while others, such as the CFPB, fall in between.[33]

Statutory requirements shape the process used at the FTC. Accordingly, FTC staff may conduct only a limited inquiry to see whether an alleged act or practice warrants closer examination. Assuming staff thinks a matter is worth investigating, the agency's attorneys must prepare a written recommendation that the Commission open a full investigation and authorize staff to use compulsory process. These "process memos" are not cursory. Staff must identify the target, or potential targets, of the inquiry, the conduct that is of concern, the ways in which that conduct may violate any law that the Commission enforces, the sort of evidence the staff believes it will need to collect to determine whether there may be a law violation, the possible legal and factual defenses the targets may use to counter any legal challenge, and how staff plans to proceed with the investigation. The Commission then opens a formal investigation only if a majority of voting Commissioners approve it, at which time the Commission will issue a Resolution Authorizing Compulsory Process. The Resolution identifies the target or potential targets of the investigation, the conduct that is being investigated, and the legal basis for the inquiry.

Notably, the Resolution is not the Commission's last contact with the matter. Although the staff is responsible for drawing up the specifications for each subpoena and CID, they have no authority to actually issue compulsory process. By law, all compulsory process issued by the Commission must be signed by an individual Commissioner. This means that staff must prepare the papers and submit them to the Commissioner assigned to the matter, who in turn must review and sign them before they may be served by the Commission's Secretary.

33 The CFPB's Rules of Practice specify that only an Assistant Director or Deputy Assistant Director of the Office of Enforcement has authority to initiate investigations and issue process. 12 C.F.R. §§ 1080.4, 1080.6(a). The Rules further limit the authority to close investigations to the Assistant Director or Deputy Assistant Director. *Id.* § 1080.11.

No matter how government investigations may begin, civil law enforcement investigations typically fall into two categories: those that the parties cannot anticipate because they are not aware of the government's concerns about a matter, and those that they can anticipate because the parties are engaging in activities that are likely to trigger an inquiry. In the former situation, the parties usually have little or no opportunity to shape the government's inquiry because the groundwork for the inquiry is laid before the investigation officially begins. However, parties who can anticipate an investigation and who are willing to engage the government proactively – sometimes even before any event can trigger an inquiry – do have an opportunity to shape the investigation, by discussing matters that they believe may raise particular concerns. Parties who are candid and cooperative in this early engagement have a unique potential to focus and limit the scope of an inquiry. Indeed, some practitioners boast of their "track record" in "working things out" before agencies even open inquiries.

D. Options for Responding to Government Civil Investigations

Targets of government investigations seem to employ one of three methods in responding. First, some resist by delaying every response, seemingly nitpicking over every document request, construing every request narrowly, and litigating – or threatening court challenges – at every opportunity. Second, some take an arm's-length approach. They volunteer nothing, leave the government to figure out what it needs, and surrender only what is requested when threatened with enforcement. They engage in dialogue with the government only when, and if, the government starts the conversation. Third, others cooperate by engaging in early and frequent discussions with investigators to determine what the government needs, providing the requested materials on time, and proactively working with the government to find the best way to address its concerns.

The difficulty with the first two approaches is that it is impossible for the government investigator, who is trained to identify suspicious activities, to distinguish between those who have something to hide, those who have nothing to hide but are clueless about the process, and those who are merely taking a "make-them-work-for-it" approach. Admittedly, practitioners who take either of the first two approaches to civil investigations may well be seeking to protect privileged or legitimate but highly confidential business material, or simply trying to advocate their strongly held view of the merits from the outset. However, the approach entails a big and risky bet that government investigators will back off, either from exhaustion or intimidation, and not pursue an investigation thoroughly if the target plays hardball. On balance, this seems like placing a substantial bet that could cost the client dearly in the long run, as the client consumes human and capital resources while the investigation methodically grinds through each new lead the investigators uncover.[34] As noted in Parts A and B, *supra*, the government generally has the means to obtain the information it needs.

The third option, that of full cooperation, does not preclude a practitioner from maintaining an arm's-length relationship with the government and fully and vigorously representing a client's interests. Cooperation does not require social interactions, but it does require honesty and candor. Admittedly, the approach all but guarantees that the government will find any relevant information and deal with any law violation that it

34 Note too, that, while courts sometimes require the requesting party in litigation to bear part of the cost of discovery (Fed. R. Civ. P. 26(b)(4)(C)), cost-shifting mechanisms are rarely available to civil investigative targets, or even to third parties. *See, e.g., Texaco*, 555 F.2d at 882 (enforcement of compulsory process will not be denied on grounds of burdensomeness and breadth, absent a showing that "compliance threatens to unduly disrupt or seriously hinder normal operations of a business"), *cert. denied,* 431 U.S. 914 (1977).

uncovers. Nonetheless, cooperation offers several distinct advantages to the target. Even when it cannot lead to leniency, it at least gives the target an opportunity to focus and narrow the government's inquiry, with a consequent speedy and relatively less expensive resolution of the matter.[35] The balance of this paper identifies some of the things a target can do to ensure such an outcome.

E. Practical Means of Narrowing and Limiting Law Enforcement Investigations

Two overarching facts greatly influence the course of many law enforcement investigations. They are these:

First:

> **The government typically does not know the organizational structure of any specific corporation, or the manner in which it creates, distributes, analyzes, uses, retains, and destroys records.**

Second:

> **Government investigators are often required to complete investigations promptly, often within rigid deadlines, and without making repeated demands for information.**

Investigators must keep these facts in mind when shaping their requests for documents and information. Therefore, their instructions regarding the definition of the "target," and the scope of the expected search for responsive information, may look something like this:

> The corporation includes its domestic and foreign parents, predecessors, divisions, subsidiaries, affiliates, partnerships and joint ventures, and all directors, officers, employees, agents and representatives of the foregoing. The terms "subsidiary," "affiliate" and "joint venture" refer to any person in which there is partial (25 percent or more) or total ownership or control between the company and any other person.[36]

In short, the instructions tell a party that to comply fully it must search every desk, person and file drawer, even in its affiliates' offices, as well as every computer, server, cloud-based source, notebook, smartphone, phone mail system, tablet, and other device that may hold responsive information.

The instructions for producing computer files are similarly comprehensive, specifying whether files must be submitted in native format, in image format with extracted text and metadata, image format accompanied by OCR, or some combination thereof. The instructions also identify the metadata fields that must be submitted, the use of de-

35 In some circumstances, cooperation can even lead to less burdensome remedial orders, or even no order at all. *See* Sec. & Exch. Comm'n, Accounting and Auditing Enforcement Release No. 1470, Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934 and Commission Statement on the Relationship to Agency Enforcement Decisions (Oct. 23, 2001), *available at* http://www.sec.gov/litigation/investreport/34-44969.htm.

36 *See* Premerger Notification Office, Fed. Trade Comm'n, Hart-Scott-Rodino Premerger Notification Program Introductory Guide III: Model Request for Additional Information and Documentary Material (Second Request) 10 (June 2010), *available at* http://www.ftc.gov/sites/default/files/attachments/premerger-introductory-guides/guide3.pdf.

duplication or email threading software, the criteria for submitting data, such as data in Excel spreadsheets, and the media to be used in submitted productions.[37]

Unless the recipient of an investigative demand is prepared to face the potential consequences of conducting an inadequate search or of having important evidence obliterated, its lawyers should immediately talk to the investigators. That conversation should address, at minimum, the following six subjects: (1) the scope of the search, both as to time and as to custodians; (2) data preservation and retrieval issues, including email, phone mail, tweets and instant messages, social media, and cloud sources; (3) the retention and disposition of legacy systems, archives, and backup tapes; (4) privilege logs; (5) materials located outside the United States; and (6) the timing and staging of production.

1. Implementing a Litigation Hold / Directing Preservation

The first step that a party must take upon learning of an investigation is to implement a litigation hold. At common law, the duty to preserve evidence attaches when a person with possession, custody, or control over the evidence reasonably anticipates litigation in which that evidence may be relevant. Under Fed. R. Civ. P. 37, a party who fails to produce relevant evidence may face substantial sanctions including the entry of a default judgment against the wrongdoer or the imposition of substantial costs. The government, during an investigation, does not, of course, have Rule 37 sanctions available to it – at least not until after it files a case – but, as discussed in Part A, *supra*, it does have means of enforcing its pre-complaint discovery demands and, in some instances, of extracting penalties for non-compliance. Laying aside those instances in which fines and penalties are more or less automatic,[38] the most significant tools are the ability to seek civil contempt against parties who do not obey court orders enforcing process,[39] and the ability to charge obstruction as a crime.[40]

The potential for civil and criminal liability shows the importance of parties taking immediate steps to preserve information and materials when they have notice of an actual or contemplated government inquiry. Even when the party does not expect a government inquiry to lead to litigation, the party must preserve relevant information. This is so because the government has the right to conduct investigations, even if it is only "seeking assurance" that the law is not being violated. Also, in many situations, it has the authority to "investigate" matters, for the purpose of preparing a study or a report.[41] In short, law suits and sanctions are not always the object of investigations. Parties who ignore or, worse yet, "dispose" of information responsive to even an "informal" inquiry do so at their peril.

The principles that govern retention in investigations are the same principles that govern retention in the civil litigation: parties are to take prompt and reasonable, not herculean, steps to preserve and to stop the routine destruction and disposition of relevant materials. This requires identifying the custodians of relevant information, informing them of their obligation to preserve relevant information and materials, and following up to ensure that they are complying. It also means identifying all other sources of potentially relevant electronic information and implementing procedures to ensure that such information will not be destroyed.

---

37 *Id.* at 13-14.
38 For example, Section 21(c) of the Securities Exchange Act, 15 U.S.C. § 78u(c), potentially makes it a misdemeanor, punishable by fines and imprisonment, to wilfully disobey an SEC subpoena.
39 Indeed, civil contempt can sometimes result in imprisonment. *See, e.g., Coronati, supra* note 16.
40 18 U.S.C. §§ 1505, 1506, 1509, 1519, 1520.
41 *E.g., Morton Salt Co.,* 338 U.S. 632.

2. Preparation: Assessing the Landscape / Developing A Plan

The second step in dealing with a government inquiry is to develop a realistic discovery and disclosure plan. In general, files belong to one of two groups. Either they are "corporate" files found in centralized storage places (such as shared network folders or workspaces, databases, or cloud-based storage applications), or they are "custodian-based" files that are either (1) network-based files that are readily associated with particular custodians (such as email or voicemail) or (2) files maintained off-network in localized sources (such as file drawers, personal computers, smartphones or portable media (tablets and flash drives)). These groups, and the type and volume of accessible data within each group, shape negotiations about the scope of the search and ultimate production.

The subject matter of the investigation and the period it covers define the boundaries of the search. Accordingly, the way to limit the search is to talk to the investigators about the issues that are of concern and the periods and sources of relevant information that will need to be produced. To do this effectively, counsel need to know the structure and content of corporate data and any special costs or burdens associated with retrieving those files. Once counsel defines and understands the scope of what may be relevant, he or she can draw distinctions between the corporate sources that are essential, those that are marginal and might not need to be searched or reviewed if the essential files are sufficient to satisfy the government's needs, and those that are irrelevant or only arguably relevant.

Custodian-based files present a different problem. Regardless of the issues, the ultimate production of such data requires a search of each custodian's files to separate the relevant from the irrelevant and the privileged relevant from the non-privileged relevant. Even with the use of technology-assisted review and other efficiency-enhancing technologies and processes, this is a very expensive and labor-intensive effort. Thus, one important key to minimizing cost and burden is to limit the number of custodians. This requires a thorough understanding of both the formal and informal organizational structure, the allocation of job responsibilities, and the way in which people and offices communicate and interact. With that knowledge, counsel can identify the personnel who have direct knowledge of the relevant issues, those who have no knowledge (even though to an outsider it may appear otherwise), and those who are somewhere in the middle. After making these determinations, counsel may propose a list of custodians and undertake some sample searches to show how the search plan will work. He or she might also be able to propose a staged production, where key custodian files are produced first and files from other "relevant but not critical" custodians are deferred.

Counsel also must bear in mind that some electronic files most likely must be produced in native form. As the Federal Trade Commission has noted:

> [P]rinted versions of Microsoft Excel spreadsheets are inherently inadequate, because they do not include cell contents, comments, and formulas. Similarly, many programs generate conflicts when their files are printed on popular printers; such conflicts may, for example, eliminate or change underlined or bolded characters, or result in the failure to show the existence of attachments. Further, electronic documents contain "metadata" – embedded data that does not print with the document, but

> which includes vital information such a bibliographic data about the document and the names of the recipients of "blind" copies on emails.[42]

Thus, counsel must first determine which data sets are relevant to the investigation, then learn how the client collects, maintains, and uses that data as well as any software used to maintain and analyze it. In developing the response plan, counsel should consider preparing data samples to demonstrate the types of information the target maintains and the capabilities of its systems and software to sort and analyze electronic information.

Email and other digital communications are the primary means of communication today. They also enable wide input into final written materials. As a result, digital messages, their attachments, and draft documents all have an uncanny ability to show up in unexpected times and places. They can be expensive to deal with because of their enormous volume. If an investigator's demand for them is not limited, they must all be collected, processed, analyzed and reviewed for responsiveness and privilege, and if privileged, logged.

Besides limiting the number of custodians whose files must be searched, a second method – one that works not only for email and word processing documents, but for other electronic information as well – is to use one or more advanced technology options that utilize computer software to assist in determining "relevance" based on user-selected criteria, or "seed sets." These applications, sometimes referred to as "technology-assisted review," may be extremely effective and efficient when properly used and verified. Other techniques, such as the use of search terms, concept clustering, de-duplication, near duplication, and email threading, can also yield efficiencies. Each variation of each technology is different, and the results are greatly influenced by the human process used to employ the technology. Thus, early in the planning stage counsel should design his or her project management workflow, including which specific technology applications will be used. Not all government investigators may want to know the details of the target's processes and technologies, but targets are increasingly finding themselves being asked such questions. For example, the Department of Justice Antitrust Division usually requires a fulsome disclosure about methodology before agreeing to a party's use of technology assisted review. In contrast, the FTC tends to seek such information much later in the investigation, and only if it thinks a production has been deficient. Ultimately, in presenting any technological approach to government investigators, candor and transparency will be critical to acceptance of the final production.

Next, counsel should assess the periods that may be relevant for each set of relevant documents and data. A reduction in the period that must be searched can result in a substantial savings. For example, the FTC reports that in merger investigations that sought documents for a three-year period, approximately 25% of the documents produced were more than two years old.[43] Obviously, a reduction in the period covered by an investigation can result in substantial savings in search, review, and production costs. However, counsel should be mindful that a one-size-fits-all approach may not be appropriate for all searches, even within the same investigation. For example, some sales data may make sense only when viewed over several seasonal cycles. Similarly, it may be appropriate to take a longer look back into the individual emails of some employees, while a shorter period may be appropriate for others. Counsel should draw rational lines when seeking to limit discovery periods.

---

42 Fed. Trade Comm'n, Statement of the Federal Trade Commission's Bureau of Competition On Guidelines for Merger Investigations 4 [hereafter referred to as "Bureau of Competition Guidelines"], available at, http://www.ftc.gov/system/files/documents/public_events/114015/ftc_statement_on_guidelines_for_merger_investigations_12-22-02_2.pdf.

43 Reforms to Merger Review, *supra* note 27, at 19.

After counsel has identified the appropriate files and custodians, and the appropriate periods for searching each, he or she can develop a systematic plan and methodology for searching and producing relevant information from those files.[44] Depending on the case and circumstance, that plan might include a suggestion that the investigation proceed in a layered fashion, whereby the target first produces "core" files, and the government agrees to give those files at least a preliminary look before determining whether to require additional information.[45]

3. Presenting the Plan

The third step in dealing with the inquiry is to convince the investigators to accept the discovery plan, or something close to it. Here it is important to know the Rules of Practice of the agency conducting the investigation. While all agencies encourage parties to meet and confer with investigators, some require it.[46] Similarly, the FTC's Reforms To Merger Review; Bureau of Competition Guidelines; and it's Bureau of Economics' Best Practices for Data, and Economics and Financial Analyses in Antitrust Investigations[47] identify several steps that counsel may take to streamline and facilitate complex investigations. These steps may be synthesized as follows:

- Meet with the investigators as soon as possible. When the parties anticipate an investigation, this may mean meeting before the investigation is formally opened.

- Provide the investigators with organization charts or equivalent materials so they can identify the parties' employees and their positions.

- Provide the investigators with brief written descriptions of the responsibilities of each person the investigators identify as a person whose files might be searched.

- Present the discovery plan and ideally provide sample search results so the investigators can assess the plan and methodology.

- Make one or more knowledgeable people readily (and repeatedly) available to the investigators. These people should be knowledgeable about the issues and be able to assist the investigators in identifying people whose files must be searched.

- Discuss with the investigators the types and forms of electronic data the parties maintain and provide data samples to assist them in determining what data and data compilations are available.

---

44 The mechanics of document preservation instructions and litigation holds are beyond the scope of this paper; but implicit in this paper is the assumption that a party will issue appropriate instructions to its employees as soon as it identifies files that may be relevant or responsive to the inquiry.

45 Except in the most complex mergers, the FTC's policy in premerger investigations is to limit to 35 the number of persons whose files must be searched. Notably, if a person is in the "search group," the search must extend to those who maintain his or her files as well as that person's "personal assistants, secretary, or person with the same or similar responsibilities." Also, that limitation is subject to receiving full cooperation from the merging party in identifying the appropriate files to search. *See* Reforms to Merger Review, *supra* note 27, at 9-11.

46 *See* FTC Rule 2.7(k), 16 C.F.R. 2.7(k). In contrast to the FTC, the SEC's Rules neither require a meet and confer nor provide a means to ask the agency to quash or modify an administrative subpoena. Nonetheless, that agency encourages parties to meet with staff and discuss any and all issues relating to compliance.

47 *Economics Best Practices*, FEDERAL TRADE COMMISSION, http://www.ftc.gov/about-ftc/bureaus-offices/bureau-economics/best-practices (last visited July 16, 2014).

- Make available to the investigators one or more people thoroughly knowledgeable about the parties' computer systems and software and the way in which the parties collect, store, maintain, analyze, and use the data and other electronic information that is relevant to the investigation.

- Where appropriate to the investigation, discuss the parties' own economic or financial analyses with (and suggest appropriate analyses to) the investigators. In doing so, the parties should provide backup data and information to enable the investigators to test the parties' data, programs, and results.

- Consider submitting "white papers" that address the issues and provide a sound analysis of the issues from the parties' perspective.

The goal is to provide the government with the relevant information it needs to finish its investigation, while limiting the cost and burden for the target, particularly with respect to the production of information that may be unnecessary, duplicative, or only tangentially relevant. Phased or prioritized discovery can often achieve these goals, particularly when combined with a good faith effort to address the government's concerns through voluntary submissions on the merits.

4. Privilege Issues

Counsel for parties should discuss two privilege-related issues with the investigators: waivers and privilege logs. In some situations, parties are willing to knowingly waive privilege claims and allow investigators to review at least some of their privileged materials.[48] At the same time, some agencies, including the FTC, have policies or practices of returning privileged documents that are truly produced unintentionally.[49] If parties intend to waive any privilege claims, they should make this clear at the outset so the investigators are able to distinguish between the documents they may review and those they must set aside to determine if they should be returned.

Complete privilege logs can be time-consuming and expensive to produce. Yet, the information in such logs is essential to investigators who need to determine whether documents are being withheld improperly. An agreement concerning the preparation of a partial log can save time and money while meeting the needs of the investigators. For example, a party may suggest submitting a partial privilege log in which it merely identifies each person who has custody of documents claimed to be privileged and the number of documents each such person holds. In response, the investigators might then designate a smaller subset of custodians whose files must be fully logged. Of course, in this scenario the agency would reserve the right to demand a full privilege log should the matter proceed to litigation.[50]

---

48 This paper does not discuss the scope or implications of such intentional waivers and does not consider, at all, whether they result in waivers as to third parties.

49 *See, e.g.*, Commission Rule 2.11(d)(1)(ii), 16 C.F.R. § 2.11(d)(1)(ii). Similarly, in the merger context the Commission has said: "By 'inadvertent production' [the FTC] refer[s] to the established body of case law that defines truly inadvertent production as a mistake that occurs despite the existence and use of reasonable procedures to screen out privileged materials. This situation differs from production that occurs because of negligence so significant that – taking into account the totality of the circumstances, including the extent and timing of production – it may still constitute a waiver." Bureau of Competition Guidelines, *supra* note 42, at 3 (footnote omitted).

50 Reforms to Merger Review, *supra* note 27, at 25-26. In this regard, the FTC's Rule 2.11(b) makes clear the agency's willingness to explore meaningful alternatives to the production of full privilege logs. *See* 16 C.F.R. § 2.11(b).

With respect to both waiver and the potential for reducing the privilege review/logging burden, civil litigants can rely on the protections of Federal Rule of Evidence 502. That Rule governs the disclosure of privileged information in court proceedings or "to a federal office or agency," and potentially offers some prospect for relief from detailed privilege review in the context of law enforcement investigations. In brief, the Rule applies to work product materials and attorney-client communications. It provides that the voluntary disclosure of such information usually results only in a waiver of the information disclosed (Rule 502(a)) and the involuntary disclosure of such information results in no waiver (Rule 502(b)), if certain criteria are met. The Rule further provides that agreements relating to the disclosure of privileged information (often referred to as "claw back agreements") are binding only on the parties to the agreement (Rule 502(e)); but such agreements will bind non-parties if the agreements are incorporated into court orders (Rule 502(d)).

Although Rule 502 leaves a gap with respect to pre-litigation agreements, such as those reached in a government investigation, Rule 502(d) and (e) suggest there is room for the government and private parties to negotiate claw back or quick peek agreements to facilitate privilege review during investigations. Although such agreements would necessarily be reached before any court complaint is filed, courts in any subsequent proceedings – either in law enforcement actions or in unrelated actions seeking access to the information provided to the government – would do well to give effect to the purpose of Rule 502 and hold that such agreements do not constitute subject matter waivers. Alternatively, in appropriate cases the government might file a subpoena enforcement action and simultaneously ask the court to "So Order" a settlement that incorporates a claw back or quick peek agreement under its Rule 502(d) authority. Here too, the FTC's Rule 2.11(d) closely tracks Rule 502 and signals the agency's willingness to work with parties on these issues.

5. Legacy Systems, Archives, and Backup Tapes

If the government suspects a law violation, and its investigators believe that some electronic information has been recently deleted, it will be keenly interested in obtaining information from alternative sources. As the FTC's Bureau of Competition has stated, "in our experience, in some cases the search of even a small portion of the parties' archive and backup systems produces valuable information that is helpful to the staff's investigation."[51] However, the FTC also recognizes that backup tapes are not always configured for routine document collection when they are intended solely for disaster recovery or archiving purposes and that review of backup tapes "is expensive and may be duplicative."[52]

To balance the potential cost to private parties of reviewing disaster recovery tapes or other non-accessible sources against the potential benefit to the government (and the public) in securing relevant evidence, the FTC's policy in merger cases is to "require a party to produce documents contained on backup tapes only when responsive documents are not available through other more accessible sources."[53] However, if a party uses backup tapes as its sole means of preserving material subject to a litigation hold or relevant to the investigation, it should expect the FTC to demand that the backup tapes be searched for relevant information. The question, at least initially, is not whether such material must be produced. Rather, the question is whether and how such information must be preserved, pending a determination that information, or some subset thereof, must be searched.

51 Bureau of Competition Guidelines, *supra* note 42, at § 6(c).
52 *Id.*
53 Reforms to Merger Review, *supra* note 27, at 24.

Here too the FTC's merger review policy statement offers a solution that might be applied in other civil investigations:

> [A] party may elect to preserve backup tapes for only two calendar days identified by staff, and . . . . [i]f a party's document storage system does not permit designation of backup tapes for two specific calendar days, staff will work with the party to designate a comparable set of backup tapes that the party must preserve.[54]

Investigators might not demand that a party preserve all backup tapes, but only a small subset, which may need to be reviewed in the event the staff determines there are significant gaps in the materials obtained from other sources. However, a party may not unilaterally decide which backup tapes to preserve and which to recycle. That determination is for the agency to make after the party and the agency investigators have met "to discuss information about the archives and backup systems."[55] This is yet another topic for the dialogue between the government and the counsel, and there can be significant benefits in resolving questions about the preservation of backup tapes and other inaccessible sources, particularly with respect to reducing costs and future litigation risks.

6. Parallel Investigations and International Matters

Private conduct will sometimes interest more than one federal agency, may raise concerns with various state agencies, and will frequently get the attention of foreign authorities as well. In other words, multiple law enforcement agencies and jurisdictions may conduct parallel investigations. Not surprisingly, law enforcement agencies increasingly recognize the advantages of cooperating with one another.[56] Such cooperation may take the form of sharing information with other federal agencies, granting states access to various federal files, and agreements and memoranda of understanding between the various agencies and foreign law enforcement authorities.[57] This cooperation has the potential to benefit everyone. On the one hand, the agencies have "an interest in reaching, insofar as possible, consistent, or at least non-conflicting, outcomes."[58] On the other hand, the parties benefit from speedier resolution of all matters; reduced discovery costs resulting from agency sharing; and less risk of facing conflicting (i.e., mutually exclusive) regulatory requirements.

Notably, the benefits of international cooperation depend largely on the willingness of the investigative target to cooperate in the investigation. Such cooperation may include the granting of waivers to allow the jurisdictions to share information they might otherwise be barred from sharing.[59] It may also require the parties to engage in multilateral negotiations to coordinate the production of responsive materials and synchronize the investigations so all jurisdictions conclude their investigations at more or less the same time.

---

54 *Id.*

55 Bureau of Competition Guidelines, *supra* note 42, at § 6(c).

56 *See, e.g.*, U.S. Dept. of Justice & Fed. Trade Comm'n, Antitrust Enforcement Guidelines for International Operations §§ 2.91, 2.92 (April 1995), *available at* http://www.usdoj.gov/atr/public/guidelines/internat.htm.

57 *See, e.g., International Competition and Consumer Protection Cooperation Agreements*, U.S. DEPARTMENT OF JUSTICE, http://www.ftc.gov/policy/international/international-cooperation-agreements (last visited July 16, 2014). An interesting example of international cooperation is the US SAFEWEB Act, which allows the FTC to assist non-US law enforcement agencies under certain conditions. *See In re FTC*, 13-mc-524-MJG, 2014 U.S. Dist. LEXIS 106214 (D. Md. Aug. 4, 2014) (enforcing an FTC Application under 28 U.S.C. § 1782 to obtain information on behalf of the Canadian Competition Bureau).

58 US-EU Merger Working Group, Best Practices on Cooperation in Merger Investigations § 1 (Oct. 2011), *available at* http://www.ftc.gov/system/files/documents/public_statements/310481/111014eumerger.pdf.

59 *Id.* §§ 3-7. In this regard, the antitrust agencies have jointly published a Model Waiver of Confidentiality for international civil matters, along with a set of Frequently Asked Questions, to assist parties in determining how and when to waive confidentiality with the enforcement agencies. *See International Waivers of Confidentiality in FTC Antitrust Investigations*, FEDERAL TRADE COMMISSION, http://ftc.gov/policy/international/international-competition/international-waivers (last visited July 16, 2014).

CONCLUSION

Because investigators approach each matter on a case-by-case basis, there are no hard and fast rules to inform counsel on which step or combination of steps will succeed in any particular investigation. Nonetheless, the government is generally not anxious to spend time and resources reviewing irrelevant documents and data compilations. It is a rare civil investigation in which the government absolutely must have unlimited access to all the materials conceivably responsive to its original requests. Even in those cases, it is generally willing to talk meaningfully with parties who demonstrate candor and honesty. If a party knows that its conduct will likely result in an order to take corrective action, its best course is likely to "come clean," get all the facts out, and resolve the issue as quickly as possible. Conversely, if it honestly thinks the government's investigation is misdirected and unnecessary, the best way to address that is to lay out the facts and let the government satisfy itself that the investigation can be closed. In either circumstance, cooperation will yield a faster, less expensive result than engaging in pitched battles or taking a "make-them-work-for-it" approach.

The key to successfully navigating a client through a government civil investigation lies in understanding the government's law enforcement concerns and objectives; devising a comprehensive plan for conveying necessary information to the government; and then meeting with the investigators early and frequently throughout the process. Candor and transparency will hasten the process and minimize costs.