Georgetown University Law Center
Continuing Legal Education

Advanced E-Discovery Institute:
Identifying Today's Problems
and Tomorrow's Solutions

November 12-13, 2009
Washington, DC

Negotiating E-Discovery in Government Civil Law Enforcement Pre-complaint Investigations

by

David Charles Shonka[1]
Principal Deputy General Counsel
Federal Trade Commission
Washington, D.C. 20580

[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 employee.

Negotiating E-Discovery in Government Civil Law Enforcement Pre-complaint Investigations

A. The Government's Civil Investigative Arsenal

Under Part V of the Federal Rules of Civil Procedure (Rules 26-37) and Rule 45 litigants in federal district court civil cases may use a broad assortment of tools for discovering information held by their opponents and by third parties; and courts have may apply a broad range of sanctions to compel, or at least encourage, cooperation. In contrast, the Federal Rules do not apply when the government seeks information in a pre-complaint investigation and to secure information the government must depend on statutory grants of authority. Absent voluntary cooperation or statutory authority, the government is powerless to collect information before filing any legal action.

The Federal Trade Commission, which has a rather 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 discover information in a pre-complaint investigation. At one end of the spectrum, the agency's statutes allow it to – and in practice the agency does – encourage voluntary cooperation in its investigations by issuing access letters,[2] which are unenforceable requests for information.[3] The Federal Trade Commission Act ("FTC Act") further encourages voluntary cooperation by assuring persons that the agency will provide information given "in place of compulsory process" the same level of confidential treatment that it provides to information it receives through compulsory process.[4]

On the other end of the spectrum, the agency is authorized to issue orders directing persons to submit "special reports" providing detailed information on their conduct and other matters.[5] Such orders are judicially enforceable,[6] and failure to comply may result in the imposition of civil penalties, which accrue daily.[7] In all its investigations, the agency also has the authority to issue civil investigation demands ("CIDs") that may compel the recipient to provide information through interrogatory-style questions, produce documentary materials, or

---

[2] 15 U.S.C. § 49.

[3] *See FTC v. Am. Tobacco Co.*, 264 U.S. 298 (1924).

[4] *See* 15 U.S.C. 57b-2(f); 16 C.F.R. § 4.10(a)(8)(ii).

[5] 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).

[6] 15 U.S.C. § 49.

[7] 15 U.S.C. § 50.

appear and give testimony at investigational hearings;[8] and 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.[9] FTC CIDs and subpoenas are both judicially enforceable and those who do not comply with a court's enforcement order may face contempt charges.[10]

The premerger notification statute (the HSR Act)[11] 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 and until they provide either all the requested information or a detailed statement of reasons why they cannot provide the information.[12] 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,[13] an action to rescind the transaction if it has been consummated,[14] or a suit for substantial civil penalties, which accrue daily.[15]

As the FTC's example shows, by and large the government has the tools it needs to conduct its pre-complaint law enforcement investigations and it has had those tools for some time. Access letters and subpoenas have been in the FTC's tool box since the very beginning. It gained its CID authority in consumer protection cases in 1980 and in 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, 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

---

[8] 15 U.S.C. § 57b-1.

[9] 15 U.S.C. § 49.

[10] 15 U.S.C. §§ 49, 57b-1(h).

[11] 15 U.S.C. § 18a

[12] *See* 18 U.S.C. § 18a(e); 16 C.F.R. § 803.3.

[13] 15 U.S.C. § 18a(g)(2).

[14] *See FTC v. Elders Grain, Inc.*, 868 F.2d 901 (7th Cir. 1989) (granting rescission on the merits).

[15] 15 U.S.C. § 18a(g)(1).

hundred boxes of documents. Today, FTC merger investigations may yield terabytes of information.[16]

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 the government justify its intrusions into private decision making with solid public interest justifications. 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*[17] 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 once may have been able to prove a law violation in merger cases by simply showing an undue increase in four or eight firm concentration ratios,[18] or even that a very large firm was acquiring a very small one,[19] today the government must produce solid economic evidence showing in advance that a merger is actually likely to harm competition if consummated.[20] This requires sophisticated economic analysis and modeling. This evidentiary burden requires the government to collect substantial amounts of data and information from the merging parties.[21]

---

[16]*Cf.,* Announcement by Deborah Platt Majoras, Chairman, Federal Trade Commission, *Reforms to the Merger Review Process* at 5-6 (February 16, 2006) [hereafter referred to as "*Reforms to Merger Review*";] *available at* http://www.ftc.gov/os/2006/02/mergerreviewprocess.pdf.

[17]*United States v. General Dynamics, Inc.*, 415 U.S. 486 (1974).

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

[19]*See, e.g., United States v. Aluminum Co. of America*, 377 U.S. 271, 278-81 (1964).

[20]*See, e.g., FTC v. H.J. Heinz Co.*, 246 F.3d 708, 716-18 (D.C. Cir. 2001).

[21]*See, e.g., FTC v. Staples, Inc.*, 979 F. Supp. 1066 (D.D.C. 1997). One aspect of a recent case illustrates this point well. In March, 2005, the FTC sued Blockbuster, Inc. seeking to enjoin its 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 in response to one sub-specification of the Commission's information request 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. Thus, 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 ¶ 17, *FTC v. Blockbuster, Inc.*, No. 1:05CV00463 (D.D.C., March 4, 2005); *available*

Second, the quantity of potential evidence is much greater today than it was twenty years ago. Virtually everyone with any decision making authority in today's business environment has at least a desktop computer at hand and readily uses email and digitally recorded voice mail to communicate with superiors, co-workers, underlings, and outside parties. Email, voice mail, instant messages, text messages, word processing, spreadsheets, presentations, and data compilations move freely and quickly through an enterprise, and in various forms are preserved, archived, and backed up in the process. Sometimes employees work around the information structure of the enterprise and carry or transmit data and information off-site. Thus, important and information may be widely dispersed through corporate networks, home computers, corporate web sites, blogs, and portable media such as thumb drives, cell phones, PDAs, and so forth. In the not-too-distant past, those determined to engage in questionable acts could hope to avoid detection by the simple expedient of circulating on first-name basis 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 computers make such evasion all but impossible – provided government investigators get their hands on the right computers, archives, or backup tapes. Of course, in order to retrieve all relevant electronic evidence and identify all those with knowledge of it, the government must cast a broad net; and this need in turn results in substantial discovery demands directed against investigative targets.

B. 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 arms'-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 uncovers something. Third, others co-operate by engaging in early and frequent discussions with investigators to determine what the government needs; providing the necessary materials on time; and pro-actively working with the government to address its concerns in a fashion that allows the target to put the investigation behind it and move on.

Practitioners of the first two methods may well be seeking to protect what they consider to be privileged or legitimate but highly confidential business material, or simply trying to advocate their strongly-held view of the merits from the outset. Nothing in the third method, of course, precludes appropriate consideration of these issues. However, those in the first two camps may be taking a big and risky bet that the government will back off, either from exhaustion or intimidation, and not pursue an investigation thoroughly if the target plays hard ball. On balance, this seems to be an untenable bet, and one that could end up costing the target much more in the long run as it consumes human and capital resources while the investigation

---

at http://www.ftc.gov/os/caselist/blockbuster/050304compblockbuster.pdf.

methodically progresses through each new lead the investigators uncover.[22] As noted in Part A, *supra*, the government generally has the means to obtain the information it needs.

The third option, that of full co-operation, all but guarantees that the government will find and deal with any law violation that it uncovers. Nonetheless, it promises several distinct advantages to the target, not the least of which is an opportunity to focus and narrow the government's inquiry to the precise matters that concern it and a consequent speedy and relatively inexpensive resolution of the matter. The balance of this paper identifies some of the things a target can do to ensure such an outcome.

C. Practical Means of Narrowing and Limiting Law Enforcement Investigations

One overarching principle underlies most law enforcement investigations. It is this:

> **The government does not know the organizational structure of its target corporations, or their filing systems, or the manner in which electronic information is collected, distributed, analyzed, used, kept, and destroyed**.

Its investigators must accordingly shape their requests for documents and information with that principle in mind. Therefore, their instructions on where to search for responsive files and information 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.[23]

Similarly, their instructions for producing computer files tend to look like this:

> The term "computer files" includes information stored in, or accessible through, computer or other information retrieval systems. Thus, the company should produce documents that exist in machine-readable form, including documents stored in personal

---

[22]Note too that, while the Federal Rules may sometimes require the requesting party to bear part of the cost of discovery (Fed. R. Civ. P. 26(b)(4)(C)), cost-shifting mechanisms are not consistently available to civil investigative targets, or even to third parties. *See e.g., FTC v. Texaco, Inc.*, 555 F.2d 862, 882 (D.C. Cir.) (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).

[23]FTC Model *Request for Additional Information and Documentary Material*, Instruction A, *available at* http://www.ftc.gov/bc/modelguide.htm.

> computers, portable computers, workstations, minicomputers, mainframes, servers, backup disks and tapes, archive disks and tapes, and other forms of offline storage, whether on or off company premises. Electronic mail messages should also be provided, even if only available on backup or archive tapes or disks. Computer files shall be printed and produced in hard copy or produced in machine-readable form (provided that Commission representatives determine prior to submission that it would be in a format that allows the agency to use the computer files), together with instructions and all other materials necessary to use or interpret the data.[24]

Or this:

> The term "document" means and includes all materials and information, including electronically stored information, discoverable under the Federal Rules of Civil Procedure.

In short, the target must search every desk, person and file drawer, even in its affiliates' offices as well as every computer, server, compact or floppy disc, blackberry, phone mail system, and other device that stores or holds electronic information.

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, the recipient should open an immediate dialogue with the investigators. Such a dialogue would address the following five subjects: (1) the scope of the search, (2) data retrieval issues, including email and phone mail, (3) timing, (4) the retention and disposition of legacy systems, archives, and back up tapes, (5) privilege logs, and (6) materials outside the United States.

1. Implementing a Litigation Hold / Directing Preservation

At common law, the duty to preserve evidence attaches when a person with ownership, custody, or control over the evidence should reasonably anticipate that the evidence may be needed for a matter that is or may be in litigation. Under Fed. R. Civ. P. 37 a party who fails to preserve relevant evidence may face substantial sanctions including the entry of a default judgment against the wrongdoer or the imposition of substantial costs. The government does not, of course, have Rule 37 sanctions available to it – at least until after it files a case – but, as discussed in Part A, *supra*, it does have means of enforcing its pre-complaint discovery demands. Perhaps most significant is the fact that obstruction of a federal investigation is a crime. 18 U.S.C. § 1501, et seq.

Potential criminal liability thus makes it especially important that parties take immediate steps to preserve information and materials promptly upon having notice of a government inquiry. Even when the party does not expect a government inquiry to lead to litigation, the party should take immediate steps to preserve information. This is so, both because the

[24] *Id.*, Instruction C.

government has the right, in principle, to conduct investigations even if it is only trying to satisfy itself that there is no law violation taking place, and in many situations it has the authority to "investigate" matters, if only for purpose of preparing a study or a report. In short, the government may undertake investigations even if it not doing so with an eye toward filing a law enforcement action and parties who ignore or, worse yet, "dispose" of information responsive to even an "informal" government inquiry do so at their peril.

That said, the principles that govern document and information retention in a government investigation are the same principles that govern such retention in the civil litigation: Parties are to take prompt and reasonable, not herculean, steps at preservation and must, to the extent possible, stop the routine destruction and disposition of responsive materials. As in civil litigation, this means identifying the sources and custodians of relevant information, informing them of their obligation to preserve relevant information and materials, and then following up to ensure that they are complying.

2. Preparation: Assessing the Landscape / Developing A Plan

The second step counsel must take in dealing with a government inquiry is to develop a realistic discovery and disclosure plan to present to the investigators. In general, files belong to one of two groups. Either they are corporate files found in centralized storage places or media, or they are personal files found in file drawers, desk top computers, blackberries or other wireless or remote devices (*e.g.*, the phone company's voice mail system for each cell phone), and other decentralized places or media. These groups shape negotiations about the scope of the search.

The subject matter of the investigation defines the corporate files that need to be searched. Accordingly, the best avenue open to counsel for limiting the search for these records is to identify the precise issues that are of concern and all sources of relevant information. Once counsel defines and understands the issues, he or she can draw distinctions between the corporate files 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.

Personal files present a much different problem. Regardless of the issues, the target must search each person's entire set of files to separate the relevant from the irrelevant and the privileged relevant from the unprivileged relevant. Accordingly, the cost of searching any particular person's files is pretty much fixed. The key for counsel is to limit the number of people whose files must be searched. This requires a thorough understanding of both the formal and informal organizational structure and the way in which people and offices communicate and interact. Once counsel understands the structure, he or she can identify the personnel who have direct knowledge of the relevant issues, those who have no knowledge (even though it may appear otherwise to an outsider), and those who are only incidentally aware. Once counsel has identified the relevant knowledgeable people, he or she should consider undertaking some sample searches that might be used to illustrate how the search plan will work.

Counsel should take a similar approach in assessing the target's electronic files, bearing in mind that some electronic files must be produced electronically. 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.[25]

Thus, counsel must first determine which data sets are pertinent to the investigation, then develop a full understanding of how the target collects, maintains, and uses that data as well as the software used to maintain and analyze it. In developing the discovery plan, counsel should seriously consider preparing several data samples that he or she can use to demonstrate the types of information the target uses and the capabilities of its systems and software to sort and analyze electronic information.

Digital messages and draft word processing documents are like escaped laboratory rats. While email and other digital communications (text messages, voice mail, instant messages, blogs, and social networking, to name only some) are probably the primary means of communication in today's corporate environment and draft documents allow wide input into final written materials, both digital messages and word processing drafts have an uncanny ability to show up in unexpected times and places. They can also be expensive to deal with. If an investigator's demand for them is not limited, they must each be corralled, counted, sorted for responsiveness, and reviewed for privilege, and if privileged, logged. The question, then, is how to limit the search for responsive documents. As indicated above, the best way is to limit the number of people whose files must be searched. A second method – one that works not only for email and word processing, but for other electronic information as well – is either to limit the search terms to correctly identifying the relevant concepts. Of course, to be effective, searches must apply terms or concepts that are actually used by the target or that fit the inquiry. To this end, counsel should compile a glossary of company and industry terminology; then test it with sample searches.

Next, counsel should assess the time periods that may be relevant for each set of documents and data. A reduction in the time frame that must be searched can result in a substantial savings in cost. For example, the FTC reports that in merger investigations that sought documents for a three-year period, approximately 25 % of the documents produced were

---

[25] *Statement of the Federal Trade Commission's Bureau of Competition On Guidelines for Merger Investigations* [hereafter referred to as *"Bureau of Competition Guidelines"*] at 4, *available at* www.ftc.gov/os/2002/12/bcguidelines021211.htm.

more than two years old.[26] Obviously, a reduction in the time period covered by an investigation can result in substantial savings in search, review, and production costs to the target. However, counsel should be mindful that a one-size-fits-all approach may not fit all document searches, even within the same investigation. For example, some sales data may not make sense unless they can be viewed over several seasonal cycles. Similarly, it may be appropriate to take a longer look back into the individual emails of some employees. Counsel should bear this in mind when developing a discovery plan and be prepared to draw rational lines when seeking to limit discovery periods.

After counsel has identified the appropriate files and persons within the target's organization and the appropriate time frames for searching each, he or she can develop a systematic plan and methodology for searching the appropriate files.[27] Depending on the case and circumstance, that plan might very well include a suggestion that the investigation proceed in a layered fashion whereby the target would first produce "core" files and the government may agree to give those files at least a preliminary look before determining whether it wants additional information.[28]

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. 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*[29] 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. In matters where the parties can anticipate an investigation, this may mean meeting before the investigation is formally opened.

---

[26]*Reforms to Merger Review, supra,* note 16, at 19.

[27]Beyond what has already been discussed, 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 the target will issue appropriate instructions to its employees as soon as it identifies files that may be relevant or responsive to the inquiry.

[28]The FTC's policy in premerger investigations is to limit, except in the most complex mergers, 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 16, at 9-11.

[29]*Available at* www.ftc.gov/be/ftcbebp.pdf.

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

- Present the search plan that counsel has prepared and provide sample search results so the investigators can assess the plan and methodology.

- Make one or more knowledgeable people readily (and if necessary, repeatedly) accessible 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.

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

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

- 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 subject matter of the investigation, the parties and their consultants should discuss their own economic or financial analyses with (and suggest appropriate analyses to) the investigators. In doing so, the parties should provide back up data and information to enable the investigators to test the parties' data, programs, and results.

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

4. Privilege and Privacy Review

Also, early in the investigation the parties should discuss privilege and privacy issues with the investigators. Where appropriate, these discussions should include two issues: waivers and privilege logs. In some situations, parties are willing to waive privilege claims and allow investigators to review at least some of their privileged materials.[30] At the same time, some agencies, including the FTC, have policies of returning privileged documents that are produced unintentionally.[31] 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 is essential to investigators who need sufficient detail to determine whether documents are being withheld properly. An agreement concerning the preparation of a partial log can potentially save the target time and money while meeting the needs of the investigators. For example, under certain specific conditions the FTC will allow a party to submit 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. The FTC staff may then designate a subset of the custodians whose files must be fully logged. Of course, if the case proceeds to litigation, the FTC reserves the right to demand a full privilege log in court discovery.[32]

Because Federal Rule of Evidence 502 is not an evidentiary rule at all, but a rule that governs the disclosure of privileged information in court proceedings or "to a federal office or agency," it potentially offers some prospect for relieve from detailed privilege review in the context of law enforcement investigations. In brief, the Rule applies to work product and attorney client materials and provides that the voluntary disclosure of such information results only in a waiver of the information disclosed (Rule 502(a)) and the involuntary disclosure of such information results in no waiver at all (Rule 502(b)). The Rule further provides that agreements relating to the disclosure of information are binding only on the parties to the

---

[30]This paper does not discuss the implications of such waivers and does not consider, at all, whether they result in waivers as to third parties.

[31] "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 23, at 6-7 (footnote omitted).

[32]*Reforms to Merger Review, supra* note 16, at 25-26.

agreement (Rule 502(e)); but such agreements will bind non-parties if they are the subject of a court order (Rule 502(d)). Together, Rule 502(d) and (e) suggest there is room for the government and private parties to negotiate claw back or quick peek agreements that might facilitate privilege review in government investigations. Although such agreements must of necessity 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 in the context of government investigations. Alternatively, in appropriate cases the government might file "friendly" subpoena enforcement actions for the purpose of asking a court to "ratify" a pre-complaint claw back or quick peek agreement under its Rule 502(d) authority.

5. Legacy Systems, Archives, and Backup Tapes

While the Federal Rules will usually excuse a litigant from retrieving and producing materials, such as those found on legacy systems, some archives, and on backup tapes, when they are not reasonably accessible because of undue burden or cost,[33] that excuse is not available to targets of law enforcement investigations. 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 information from such 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."[34] However, the FTC also recognizes that backup tapes often are not configured for routine document review since they are intended solely for disaster recovery or archiving purposes and that review of backup tapes "is expensive and may be duplicative."[35]

In order to balance the potential cost to private parties of reviewing disaster recovery tapes against the potential benefit to the government (and the public) in securing missing 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."[36] Given this policy, the negotiating point between the government and private parties, at least initially, is not whether backed up material has to be produced. Rather, the question is which tapes must be preserved pending the government's determination that they must be searched.

---

[33]Fed. R. Civ. P. 26(b)(2).

[34]*Bureau of Competition Guidelines, supra* note 23, at 5.

[35]*Id.*

[36]*Reforms to Merger Review, supra* note 16, 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.[37]

Thus, a party may not be obligated to preserve all backup tapes, but only a small subset, which may need to be reviewed in the event the FTC 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 can be made only after the target and its IT personnel have met with agency investigators and IT personnel "to discuss information about the archives and backup systems."[38]

6. International Matters

In today's economy civil law enforcement investigations may be global, with multiple jurisdictions running parallel investigations. Not surprisingly, the law enforcement agencies increasingly recognize the advantages of cooperation among themselves.[39] In the FTC, this takes the form of numerous agreements and memoranda between the Commission and foreign law enforcement authorities on both antitrust and consumer protection matters.[40] This cooperation has the potential to benefit not only the law enforcement agencies and the public, but also the target of the investigation. On the one hand, the agencies have "an interest in reaching, as possible, consistent, or at least non-conflicting, outcomes."[41] 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.

However, the benefits of international cooperation depend to a large extent 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

---

[37] *Id.*

[38] *Bureau of Competition Guidelines, supra* note 23, at 5.

[39] *See e.g., Antitrust Enforcement Guidelines for International Operations,* issued by U.S. Department of Justice and the Federal Trade Commission ¶¶ 2.91, 2.92 (April 1995), *available at* http://www.usdoj.gov/atr/public/guidelines/internat.htm.

[40] *See* http://www.ftc.gov/bc/international/coopagree.htm.

[41] *Best Practices on Cooperation in Merger Investigations* ¶ 1, *available at* http://www.ftc.gov/opa/2002/10/mergerbestpractices.htm.

otherwise be barred from sharing. 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.[42]

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 scarce time and resources reviewing irrelevant documents and data compilations. It is a rare case when 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 engage in discussions with parties who demonstrate a willingness to be candid and honest. If the target of an investigation knows in advance that its conduct is the sort that would ordinarily result in a direction to take some sort of corrective action, the target's best course is likely to be to "come clean," get all the facts out, and to resolve the question as quickly as possible. Conversely, if the target 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 no action is warranted and the investigation can be closed. In either circumstance, cooperation will yield a faster, less expensive, result than engaging in pitched battles or taking a hands-off, let's-see-if-they-can-find-it approach.

The key to successfully navigating a client through a government investigation in a civil matter 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. Candid and honest discussions and full cooperation can potentially hasten the investigative process and reduce the costs of the investigation to the target.

[42] *Id.* ¶¶ 3-7.