The Sedona Conference Journal

Volume 9 2008

You've Been Served: Corporate Response to Grand Jury Subpoenas & Search Warrants for Electronically Stored Information

Cecil A. Lynn III

Recommended Citation: Cecil A. Lynn III, *You've Been Served: Corporate Response to Grand Jury Subpoenas & Search Warrants for Electronically Stored Information*, 9 SEDONA CONF. J. 183 (2008).

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

YOU'VE BEEN SERVED: CORPORATE RESPONSE TO GRAND JURY SUBPOENAS & SEARCH WARRANTS FOR ELECTRONICALLY STORED INFORMATION

Cecil A. Lynn III[1]
Ryley, Carlock & Applewhite
Phoenix, AZ

Over the past few years, prosecutions of corporations and corporate defendants have seemingly risen as obscure plea agreements[2] taken with little fanfare have given way to splashy jury trials complete with a full entourage of media coverage. The seeming proliferation of prosecutions actually comes from a rather small number of high-profile cases involving well-known companies such as Arthur Andersen and Enron. As the government continues to crack down on actual and perceived corporate excess, corporate legal departments more and more find themselves caught up in investigations sparked by disgruntled employees, whistle-blowers and administrative agencies. These investigations coupled with the resulting prosecution of corporate officers can stress a corporate legal department as it seeks to cooperate with the investigation while still safeguarding the corporation, its employees and officers.

This article takes a look at the general constitutional principles related to grand jury subpoenas and search warrants demanding electronically stored information. It offers practical suggestions for responding to the government's queries that seek to maximize the level of cooperation while still ensuring constitutional safeguards are observed to the extent possible to protect the rights and responsibilities of the corporation. While not intended to be an exhaustive summary of available options, this article is a starting point for discussion and further dialogue.

I. FOURTH AMENDMENT PROTECTION FOR CORPORATIONS

The Fourth Amendment protects persons, houses, papers, and effects against unreasonable searches and seizures.[3] An unreasonable search is one conducted without a proper warrant when no consent, exigent circumstances, or other articulated exception applies.[4] Although the Fourth Amendment protects businesses[5], corporations are "artificial beings" that exists only by exercise of law[6] and are not entitled to many of the guarantees found in the Constitution that apply to persons.[7] For example, a corporation has no Fifth Amendment privilege against self-incrimination[8] or a right to privacy.[9]

---

1 Cecil Lynn is an attorney at Ryley, Carlock & Applewhite, A Professional Association. He is a recognized thought leader in the area of electronic discovery and speaks and publishes on a wide variety of e-discovery topics. He is an active member of the Sedona Conference® and enjoys a very diverse practice which includes representing clients on issues related to intellectual property, employment, and white-collar crime. The author wishes to thank E. Gary Grundy for his extensive research and invaluable assistance with this article.

2 Corporate cooperation with state and federal prosecutors and regulators is increasingly more common in criminal and enforcement litigation. A promise of "fully continuing and complete cooperation" is bartered for the prosecutor's promise to forego prosecution or dismiss the charges without prejudice. *Stolt-Nielson v. United States*, 442 F.3d 177 (3d Cir. 2006), *cert denied*., 127 S.Ct. 494 (2006)

3 Specifically, the Fourth Amendment provides, "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

4 This article focuses on subpoenas and search warrants; accordingly warrantless searches are outside the scope of consideration.

5 *G.M. Leasing Corp. v. United States*, 429 U.S. 338, 339, 97 S.Ct. 619, 622 (1977).

6 *Dartmouth College v. Woodward*, 17 U.S. 518, 636, 4 L.Ed. 629 (1819).

7 *First Nat'l Bank of Boston v. Bellotti*, 435 U.S. 765, 779, n. 14, 98 S.Ct. 1407, 55 L.Ed.2d 707 (1978).

8 *Wilson v. United States*, 221 U.S. 361, 31 S.Ct. 538, 55 L.Ed. 771 (1911).

9 *United States v. Morton Salt Co.,* 338 U.S. 632, 70 S.Ct. 357, 94 L.Ed. 401 (1950).

II. SUBPOENAS DUCES TECUM

A grand jury's power to investigate criminal law violations is very broad.[10] Rule 17 of the Federal Rules of Criminal Procedure gives the grand jury considerable discretion to order a witness to produce books, papers, documents, data, or other items designated in a subpoena.[11] Unlike search warrants, there is no probable cause requirement inherent in the grand jury's issuance of a subpoena since the purpose of the subpoena is to aid in the determination of whether probable cause exists in a particular case.[12] Probable cause is also not required to support an administrative subpoena.[13]

The rule imposes no limits on the methods or means of procuring evidence, and generally requires the person served with the subpoena to either surrender the identified items or seek to quash the subpoena when compliance would be unreasonable or oppressive.[14] Likewise, courts will enforce an administrative agency's subpoena for corporate records if the demands contained within are "sufficiently limited in scope, relevant in purpose, and specific in directive so that compliance will not be unreasonably burdensome."[15]

In the context of subpoenas *duces tecum*, the courts have held that reasonableness has three components: (1) the subpoena can seek only the production of things relevant to the investigation being pursued;[16] (2) the subpoena must specify the items to be produced with reasonable particularity;[17] and (3) the subpoena may only request documents covering a reasonable period of time.[18] Of course, determining whether the requests outlined in the subpoena are reasonable may be a difficult task if the corporation is not aware of the government's purpose in seeking the requested information. Grand juries have wide latitude and operate in relative secrecy.[19]

III. CONSIDERATIONS IN NEGOTIATING THE SCOPE OF A SUBPOENA

1. Preserve All Potentially Relevant Electronically Stored Information.

Once a corporation receives a subpoena requesting electronic data it has an obligation to preserve the information and halt the routine destruction of information relevant to the subpoena.[20] The failure to preserve may lead to potential criminal action for obstruction of justice under the Sarbanes-Oxley Act of 2002 ("SOX") which was created, in part, to increase the government's ability to prosecute and convict corporate officers and their agents who destroy documents.[21]

SOX amended 18 U.S.C. Section 1512(c) to increase penalties for those who "corruptly" alter, destroy or conceal information with the intent to impair the integrity or availability of the information.[22] In addition, SOX added Section 1519 making it a crime to knowingly destroy, alter or falsify records with the intent to impede, obstruct or influence an ongoing or contemplated federal

10 *United States v. Calandra*, 414 U.S. 338, 343, 94 S.Ct. 613, 617, 38 L.Ed.2d 561 (1974).
11 Similarly, Rule 17(c) governs trial subpoenas. *United States v. R.W. Prof. Leasing Services Corp*., 228 F.R.D 158, 162 (E.D.N.Y. 2005)(unlike grand jury subpoenas and civil discovery, a criminal defendant has the burden of showing that the documents sought are both relevant and admissible at the time of the attempted procurement).
12 *United States v. R. Enterprises, Inc*., 498 U.S. 292, 297, 111 S.Ct. 722, 726 (1991).
13 *Doe v. United States* (*In re Admin. Subpoena*), 253 F.3d 256, 262-65 (6th Cir. 2001)(applying "reasonable relevance" test).
14 Fed. R. Crim. P. 17(c)(2).
15 *Becker v. Kroll*, 494 F.3d. 904, 916 (10th Cir. 2007). *See also Oklahoma Press Pub. Co. v. Walling*, 327 U.S. 186, 209, 66 S.Ct. 494, 90 L.Ed. 614, 166 A.L.R. 531 (1946). *In re Grand Jury Subpoena Duces Tecum to Provision Salesmen and Distributors Union, Local 627,* 203 F. Supp. 575, 577 (D.C.N.Y. 1961).
16 *Oklahoma Press Pub.*, 327 U.S. at 208-209.
17 *Braswell v. United States,* 487 U.S. 99,106,108 S.Ct. 2284, 2288 (1988). *See also Hale v. Hinkle*, 201 U.S. 43, 77, 26 S.Ct. 370, 50 L.Ed. 652 (1960), *Overruled in part* by *Murphy Waterfront Com'n of New York Harbor*, 378 U.S. 52, 84 S.Ct. 1594 (1964).
18 *Id*. (subpoena requiring production of records from date of company inception held invalid).
19 Fed. R. Crim P. 6(e)(2).
20 *See e.g., United States v. Comprehensive Drug Testing, Inc*., 513 F.3d 1085, 1090 (9th Cir. 2008)(government agreed to extend subpoena return date after it received assurances that documents would neither be destroyed nor altered).
21 *See* Sections 802 and 1102 of the Sarbanes-Oxley Act.
22 *See* 18 U.S.C. Section 1512(c). Although some district courts have addressed the meaning of "corruptly" in Section 1512 (c) since 2005), there is no consensus. *See e.g., US v. Makham,* 2005 WL 3533263 at *96 (D. Ore. Dec 23, 2005) (applying *Andersen* definition of "corruptly" to all sections of Section 1512; *United States v. Hey,* 2005 WL 1039388 at *5 (E.D. Mich. April 29, 2005) (convicting defendant under Section 1512 (c)(2) without discussing the definition "corruptly"). *United States v. Ortiz*, 367 F. Supp. 2d 536, 541 (S.D.N.Y. 2005) (finding that the government need not prove that the defendant's conduct was "likely to affect" the official proceeding or the defendant knew that her conduct was "likely to affect" the official proceeding).
23 *See* 18 U.S.C. 1519.

investigation.[23] Prior to the amendment of Section 1512, a person who obstructed justice, but did not influence or intimidate another, was immune from prosecution. The SOX revision now eliminates the requirement that the obstructionist "corruptly persuade" another.[24]

Section 1519 does not require a willful or corrupt state of mind, nor does it require the impediment of a pending investigation. Literally read, the statute could lead to conviction of a defendant who destroys documents even in the absence of any grand jury or administrative proceeding and where the defendant is wholly unaware of the existence of an investigation. In this regard, Section 1519 seemingly conflicts with the Supreme Court's prior pronouncement that the act of destroying documents itself is not a crime.[25] Yet, recent cases dealing with Section 1519 have not addressed the issue.[26]

2. Ascertain Whether the Corporation, its Officers, or Employees are Targets of the Investigation.

Given the wide range of issues presented in responding to a subpoena, corporate counsel should seek the advice and guidance of outside counsel who is familiar with both the inner-workings of grand jury and administrative proceedings as well as the intricacies inherent in the collection and production of electronically stored information. Moreover, as the corporation may be a target of the investigation, outside counsel should be retained to communicate with the government and protect the corporation's interest while it complies with the grand jury subpoena. The corporation should find out as much information as it can about the investigation as well as those being targeted, as the target could very well be a corporate officer or employee for whom the corporation will be providing a legal defense.[27]

As noted above, grand jury proceedings are secret. While generally a grand jury witness is not bound by secrecy,[28] the person may be obligated to refrain from contacting the target regarding the subpoena.[29] Indeed, the subpoena may include a specific request that the target not be notified of the pending investigation, the existence of a subpoena, the nature of any information subpoenaed, and any testimony before the grand jury.[30] This "veil of secrecy" would not prevent the witness from discussing their testimony with counsel or select personnel within its organization about the subpoena.[31] However, such a gag order could make it difficult to explain to targeted officers or employees why the corporation suddenly needs to take possession of their laptops, PDAs, or home computers.

3. Determine Whether Compliance With the Subpoena is Possible Given the Amount of Requested Material as Compared to the Allotted Time.

If a subpoena is overly broad or if compliance would be difficult by the return date, counsel should notify the government to discuss alternatives or extensions.[32] The reasonableness of the return date will depend on how long it will take the corporation to locate, review, copy, and

---

24 *See id.*

25 *Arthur Andersen, LLP v. United States*, 544 U.S. 696, 704, 125 S.Ct. 2129, 2135, 161 L.Ed.2d 1008 (2005)(holding jury instruction failed to properly convey the requisite "consciousness of wrongdoing" to sustain a conviction under 18 U.S.C. Section 1512(b)); *see also United States v. Aguilar*, 515 U.S. 593, 599, 115 S.Ct. 2357 (1995)("[I]f the defendant lacks knowledge that his actions are likely to affect the judicial proceeding . . . he lacks the requisite intent to obstruct.")

26 *See e.g., United States v. Wortman*, 488 F.3d 752 (7th Cir. 2007)(Court affirmed 18 U.S.C. Section 1519) (conviction of defendant who broke a computer CD containing child pornography after FBI agent told her not to touch it and there was evidence defendant accompanied her boyfriend to find CD knowing he wanted to destroy incriminating evidence); *United States v. Ionia Management S.A.*, 526 F. Supp. 2d 319 (D.Conn 2007).

27 *See e.g., United States v. Stein*, 495 F. Supp. 2d 390 (S.D.N.Y. 2007) (*Stein III*) (holding government's inducement of corporate employer's cutoff of defense costs for its employees was part of a pattern of government misconduct in violation of employees' right to substantive due process). *See also (Stein II),* 440 F. Supp. 2d 315 (S.D.N.Y. 2006) The Court spoke to the implications of these deferred prosecution agreements and how coercion played into prosecutorial misconduct. In *Stein II*, the Court found that an individual claiming that a statement was coerced in violation of 5th Amendment rights against self incrimination must adduce evidence both that (1) the individual subjectively believed he or she had no real choice but to speak and (2) that a reasonable person in that the position would have felt the same way." *Id* at 328. Here the court found seven of the nine defendants were not products of coercion, *Id*. at 330.

28 *See* Fed. R. Crim. P. 6(e)(2)(B).

29 *See e.g.,* 12 U.S.C. Section 3413(i)(Financial Privacy Act contains a provision giving courts the authority to order a financial institution on which a grand jury subpoena for customer records has been served to refrain from notifying the customer of the existence of the subpoena or information that has been furnished to the grand jury).

30 *See In re Grand Jury Subpoena Duces Tecum*, 797 F.2d 676, 677 (8th Cir. 1986)

31 *Id.*

32 *See In re Grand Jury Subpoenas* Dated *December 10th*, 926 F.2d 847, 851 (9th Cir. 1991)("As a result of negotiations with the United States Attorney, the firm designated the areas which fell within the warrant [and] firm personnel were allowed to identify the relevant documents and place them in a sealed package without examination by agents.")

33 *See Becker,* 494 F.3d at 917 (subpoena for medical records that demanded immediate compliance was valid because the requested records were readily available and were able to be copied and returned to the doctor's office in one day).

produce the subpoenaed materials.[33] One factor the court looks at to assess the respective burden on the subpoena holder is whether the holder made reasonable efforts to reach an accommodation with the government.[34]

For example, in *In re Subpoena Duces Tecum (Dwight L. Bailey, M.D.)*, a physician and his employer, a professional health care organization, moved to quash an administrative subpoena issued by the U.S. Attorney that sought the production of the doctor's personal and financial files, claims-processing files, and more than 15,000 patient files consisting of approximately 750,000 to 1.25 million pages of materials.[35] The court quashed the subpoena with respect to the doctor's personal and financial files and the government offered to allow the health care organization to retain patient files and claim-processing files, subject to the U.S. Attorney's ability to call and review particular files if needed. The doctor and his employer rebuffed the U.S. Attorney's offer and incurred $40,000 in expenses related to "labor, equipment, and supply costs" copying the documents.[36] The court rejected the claimed expenses, holding that as a condition of maintaining the position that the subpoena was overly broad and oppressive, the doctor and employer would have had to explain why the government's accommodation was unacceptable.[37]

4. Meet and Confer with Government Specifically Relating to Electronically Stored Information.

Corporate counsel should review the subpoena with outside counsel to ascertain what specific electronic information is being requested and to determine the relative burden of producing the information. If the subpoena requests electronically stored communications, counsel should begin a dialogue with the subpoena issuer to establish production procedures. Reaching out to the government also provides an opportunity to establish the company's good faith efforts to comply with the subpoena and demonstrates its willingness to cooperate. The appropriate introduction with government officials responsible for serving the subpoena *duces tecum* should be about the preservation of information requested in the subpoena. If information has been destroyed or deleted prior to receiving the subpoena, it should be documented and disclosed. Likewise, the government should be apprised when the sole source of potentially relevant information resides on media that may not be reasonably accessible due to undue cost or burden.

In federal civil cases, parties are required to meet and confer regarding issues related to the preservation and disclosure of electronically stored information, including the formats in which it should be produced and any issues related to claims of privilege or protection of trial preparation materials.[38] While there is no equivalent rule related to criminal procedure, Rule 26(f) of the Federal Rules of Civil Procedure provides an essential checklist to use when speaking with law enforcement about the breadth and scope of the subpoena *duces tecum*. Unfortunately, unlike in the civil context, there is no obligation of disclosure on the government's part, so the conversation may ultimately be only one-sided. However, the effort is invaluable and demonstrates a good faith attempt to educate the government about the company's limitations and the subpoena's burden prior to the corporation seeking to quash or modify the subpoena.

One critical topic of discussion with the government relates to the format in which documents are to be produced once the subpoena holder collects them. A native production may be more cost efficient, but such a production lacks redaction or Bates stamp capabilities. On the other hand, production of electronic information as static images may cost more and take more time to produce.

As Magistrate Judge John Facciola recently noted, in criminal cases there is no rule to guide the courts in determining whether the documents have been produced in an appropriate format.[39]

---

34 *See Morton Salt*, 338 U.S. at 653. ("Before the courts will hold an order seeking information reports to be arbitrarily excessive, they may expect the supplicant to have made reasonable efforts . . . to obtain reasonable conditions").
35 228 F.3d 341 (4th Cir. 2000).
36 *Id* at 345.
37 *Id* at 351.
38 *See* Fed. R. Civ. P. 26(f)(3) & (4).
39 *United States v. O'Keefe*, 2008 WL 449729, at *4 (D.D.C. 2008).

However, Rule 34 of the Federal Rules of Civil Procedure specifically addresses the form of production of electronic documents and can provide guidance in producing electronically stored information in response to a grand jury subpoena. Judge Facciola observed, "It is far better to use these rules than reinvent the wheel when the production of documents in criminal and civil cases raise the same problems."[40] Consistent with Rule 34, if the subpoena lacks instructions on the format for the production of electronically stored information, a corporation should produce the information in the form in which it is ordinarily maintained or in a reasonably usable format.[41]

5. Resist Calls for the Production of the Virtual "File Cabinet" Where Targeted Search and Collection Efforts Work Better for the Corporation and the Government.

A grand jury subpoena should be narrowly tailored to require only the production of information actually pertinent to the investigation.[42] Using the analogy of a file cabinet, courts have cautioned against blanket production when only specific identifiable files are relevant.[43] Counsel must carefully read the subpoena to determine whether the corporation can provide the requested information by the specified return date and at what cost and burden. Particular attention should be paid to the specificity of the request for information. The request should give sufficient enough detail to enable the corporation to determine the location and existence of information. In addition, the subpoena must give the corporation sufficient notice of its preservation obligation. Vague or overly broad assertions for categories of documents or blanket requests for computers, hard drives of other storage media may be completely unnecessary and require clarification.

In re Twenty-Fourth Statewide Investigating Grand Jury, Lancaster Newspapers, Inc. was served with two subpoenas commanding it to produce four workstations and two hard drives.[44] The newspaper complained that the subpoenas were overly broad because they required the production of information not relevant to the grand jury investigation and sought privileged and constitutionally protected material.[45] The newspaper filed motions to quash both subpoenas. The court denied both motions, but ordered the attorney general to limit the examination of the hard drives to review of historical information concerning internet access, and admonished the examiners not to view or access unrelated files or other content on the hard drives.

In response to the newspaper's application for review challenging the production ordered by the trial court, the Pennsylvania Supreme Court held the subpoenas were overly broad, stating:

> [A] careful balancing of the respective interests involved leads us to the conclusion that this particular method of disclosure is unduly intrusive in the circumstances presented. Notably, part of the reason that the Fourth Amendment is of limited application in the setting of grand jury subpoenas is that the appearance at grand jury proceedings is not regarded as a search or seizure. [citation omitted]. The extraction by the executive branch of entire "filing cabinets" from a witness and/or subject of investigation, however, tests the limits of credulity in the attempt to maintain the understanding that no search or seizure is involved.[46]

A corporation should determine whether less restrictive alternatives are available that would achieve the resulting production of responsive information. For example, in certain instances, the information may be collectable using file names, keyword searches, date range restrictions or automated tools.

The subpoena does not have to specify the search terms or methodology, but it needs to be specific enough that the corporation does not need to turn over entire volumes of storage media. The

40 *Id.*
41 Fed. R. Civ. P. 34(b)(E)(ii).
42 *In re Grand Jury Subpoena Duces Tecum*, 846 F. Supp. 11, 13 (S.D.N.Y. 1994).
43 *Id.; see also In re Twenty-Fourth Statewide Investigating Grand Jury*, 589 Pa. 89, 104, 907 A.2d 505 (S.Ct. Penn 2006).
44 *In re Twenty-Fourth Statewide Investigating Grand Jury*, 589 Pa. at 92-93.
45 Specifically, the newspaper raised the First Amendment, the First Amendment Privacy Protection Act, and the Pennsylvania Shield Law.
46 *In re Twenty-Fourth Statewide Investigating Grand Jury*, 589 Pa. at. 104-105 (court recommended a search warrant if collection of hard drives was necessary).

true nature of the government's request may be difficult to ascertain if the subpoenaed corporation is not familiar with the grand jury investigation or does not understand the relevance of the information, but an effort should be made to obtain clarification and to narrow the scope of the requested information to avoid overproduction.

6. Take Adequate Steps to Ensure the Corporation Does Not Produce Privileged and Protected Materials.

A blanket production of hard drives or other storage media also raises privilege concerns. Given the secret nature of grand jury proceedings, subpoenas are generally not quashed on the grounds that they would require the production of confidential or trade secret information. However, the production of privileged information could have far-reaching and unintended results. Thus far, only the Eighth Circuit recognizes the notion of limited or "selective waiver" to protect attorney-client communications previously disclosed to the government.[47] The Fourth Circuit has applied the selective waiver comment to protect opinion work product, but rejected its application for non-opinion work product.[48] With very few exceptions, courts have not been supportive of arguments that production of protected materials pursuant to a government subpoena did not effectively waive the attorney-client privilege as to third parties in litigation.[49]

An early draft of proposed Federal Rule of Evidence 502 incorporated language that would recognize the doctrine of selective waiver, stating that a person or entity generally waives privilege by disclosing protected information "unless that disclosure is made to a federal, state, or local governmental agency during an investigation by that agency...." The Senate approved a bill adding Rule 502 to the Federal Rules of Evidence. However, the selective waiver language was dropped from the bill before it reached the Senate.[50]

In the absence of clear guidance on the issue, corporations should confer with the government to ensure that any production excludes privileged information. In 2006, the Department of Justice placed new restrictions on a prosecutor's ability to seek the production of privileged materials from corporations. The so-called "McNulty Memorandum" provides detailed instructions for prosecutors investigating corporate misconduct with an eye toward prosecution.[51] Its advice is instructive in the context of compliance with subpoenas requesting privileged information. The McNulty Memorandum states that "[p]rosecutors may only request waiver of attorney-client or work product protections when there is a legitimate need for the privileged information to fulfill their law enforcement obligations." [52] In ascertaining the legitimacy of the need, prosecutors are required to determine whether the information can be obtained using alternative means that do not require waiver. Although the overarching theme of the memo is cooperation with the government's efforts to prosecute the corporation providing the information, the government may be more willing to discuss options when the corporation is a witness rather than the target of the investigation.

In *United States v. Martha Stewart*, the grand jury investigating the defendant, founder of Martha Stewart Living Omnimedia ("MSLO"), for improper sale of ImClone Systems, Inc. stock, issued a subpoena to MSLO seeking all computers used by Martha Stewart.[53] Compliance with the request would have potentially revealed emails protected as attorney-client communications. MLSO reached a compromise with the government whereby the company produced the requested files and computers to the grand jury, and the government agreed that it would not review the files until MSLO identified which documents were responsive to the subpoena.[54] MSLO also agreed to provide

47 *Diversified Indus., Inc. v. Meredith*, 572 F.2d 596 (8th Cir. 1978)(*en banc*).
48 *In re Martin Marietta Corp.*, 856 F.2d 619, 623 (4th Cir. 1988).
49 *See e.g., Permian Corp. v. United States,* 665 F.2d 1214, 1220 (D.C. Cir. 1981); *In re Weiss*, 596 F.2d 1185 (4th Cir. 1979); *In re John Doe Corp.*, 675 F.2d 482 (2d Cir. 1982); *Genentech, Inc. v. U.S. Int'l Trade Comm.*, 122 F.3d 1409 (Fed. Cir. 1997); *Westinghouse Elec. Corp. v. Republic of the Philippines*, 951 F.2d 1414 (3d Cir. 1991); *United States v. Massachusetts Inst. Tech*, 129 F.3d 681 (1st Cir. 1997*); In re Columbia/HCA Healthcare Corp. Billing Litigation*, 293 F.3d 289 (6th Cir. 2002).
50 *See* S.2450 *available at* http://www.uscourts.gov/rules/S2450.pdf as of March 23, 2008.
51 *See* "Federal Prosecution of Business Organizations" Memorandum from the Deputy Attorney General Paul J. McNulty, *available at* http://www.usdoj.gov/dag/speeches/2006/mcnulty_memo.pdf as of March 23, 2008.
52 *Id.*
53 *In re Regal Petroleum Products Co.,* 287 F. Supp. 2d 461 (S.D.N.Y. 2003).
54 *Id.* at 463.

a privilege log. The government agreed that it would not review any produced files that were not specifically listed on the log of responsive documents without first consulting MSLO.[55] However, after Stewart was indicted, she objected to the production of her privileged emails.[56]

Likewise, a subpoenaed corporation should create a privilege log and resist the disclosure of privileged material until an agreement can be reached with the government.[57] The agreement should specify that the government will not review materials identified on the corporation's privilege log without court intervention.[58] If the government rejects this accommodation, a corporation should consider filing a motion to quash the subpoena to prevent disclosure of the protected material.

7. Recognize that if the Cost of Subpoena Compliance is Oppressive, The Court May Order The Government to Copy and Review the Material in Lieu of Cost Shifting.

While a court in exercising its power under Rule 17(c) of the Federal Rules of Criminal Procedure may modify a subpoena to require the government to pay the costs of compliance,[59] the general rule is that a witness or recipient of a subpoena *duces tecum* is required to bear such costs.[60] As Rule 17(c) provides relief only when compliance is "unreasonable or oppressive," the general presumption is that associated costs are ordinary consequences of the witness's "public obligation to provide evidence."[61]

The Advisory Committee Note for Rule 17(c) states that the rule is substantially similar to Rule 45(b) of the Federal Rules of Civil Procedure.[62] When the Advisory Committee Notes were drafted, Rule 45 gave the court the power to quash or modify a subpoena *duces tecum* if it was "unreasonable or oppressive." Rule 45 has subsequently been amended and the subject language omitted. Rule 45 now places an affirmative obligation on subpoena issuers to avoid imposing undue burden or expense on a person subject to the subpoena.[63] Under Rule 45, a subpoenaed party is given the option to move to quash the subpoena as unduly burdensome or to file a timely objection.[64] Once an objection if filed, the party seeking production must move to compel and demonstrate that the cost of compliance would not subject the subpoenaed person to "significant expense."[65]

But whether the standard is "significant expense" or "unreasonable or oppressive," the bar for shifting the expense of subpoena compliance to the government may be very high even when factoring in the overall costs of copying hard drives or other media, recovering deleted information on active and inactive media (e.g., backup tapes for disaster recovery), and translating any recovered information to a reasonably usable format. Claims of oppressiveness generally rest on the cost and disruption associated with the collection and production of large quantities of documents.[66] Yet, courts have been reluctant to order the government to pay the cost of subpoena compliance and instead may seek to have the government take over the legwork involved in producing and reviewing subpoenaed materials.[67]

For example, in *In re Grand Jury Proceedings*, the grand jury subpoenaed information stored on 250 rolls of microfilm.[68] The bank sought to shift the cost of compliance by estimating that there were a total of 40,200 items on each microfilm, that it would take eight hours to review every item on one roll of film, and thus that it would take a trained employee a year to review. The court denied the

55 *Id.*
56 *Id.*
57 *In re Grand Jury Subpoena*, 274 F.3d 563, 575-576 (1st Cir. 2001).
58 *See United States v. Rigas*, 281 F. Supp. 2d 733 (S.D.N.Y. 2003)
59 *In re Grand Jury No. 76-3 (MIA) Subpoena Duces Tecum*, 555 F.2d 1306, 1308 (5th Cir. 1977).
60 *Matter of Midland Asphalt Corp.*, 616 F. Supp. 223, 225 (N.Y. Dist. Ct. 1985); *In re Grand Jury Investigation*, 459 F. Supp. 1335 (E.D. Pa. 1978); *In re Grand Jury Subpoena Duces Tecum*, 405 F. Supp. 1192, 1198 (N.D.Ga. 1975); *In re Grand Jury No. 76-3*, 555 F.2d at 1307-1308.
61 *See Hurtado v. United States*, 410 U.S. 578, 589, 93 S.Ct. 1157, 35 L.Ed.2d 508 (1973)("It is beyond dispute that there is in fact a public obligation to provide evidence . . . and that this obligation persists no matter how financially burdensome it may be . . . The personal sacrifice involved is a part of the necessary contribution of the individual to the welfare of the public.")
62 *In re Grand Jury No. 76-3*, 555 F.2d at 1308.
63 Fed. R. Civ. P. 45(c)(1).
64 *Cf* Fed. R. Civ. P. 45(c)(3)(A) and 45(c)(2)(B).
65 Fed. R. Civ. P. 45(c)(2)(B)(ii).
66 *In re August, 1993 Regular Grand Jury*, 854 F. Supp. 1392 (S.D. Ind. 1993); *In re Grand Jury Subpoena Served on PHE, Inc.*, 790 F. Supp. 1310 (W.D.Ky. 1992); *In re Grand Jury Subpoena Issued to First Nat'l Bank of Maryland*, 436 F. Supp. 46 (D.Md. 1977).
67 *In re Grand Jury Proceedings* 636 F.2d at 83, n.2.
68 *Id.*

bank's motion to quash and ordered it to produce the requested materials at its own expense, or at its option, to allow three grand jury agents to view and copy the relevant files at government expense. The bank elected to produce the records itself and hired an independent company to make an initial review of the microfilm.

Counsel should evaluate the cost of production to determine whether the cost of compliance with the subpoena requires significant expense. In determining what constitutes an unreasonable or significant expense, the court will first determine what it would cost to produce the original documents requested for the government's inspection or use.[69] Traditionally with paper productions, the court considered copying costs only when providing originals was a "practical impossibility." Courts have attempted to alleviate the burden of copying documents by having the government search through the electronic information and identify specifically what documents are needed in furtherance of the investigation.[70] In such cases, the government's role is similar to that in a search warrant. However this approach, while undoubtedly more cost effective than converting electronically stored information from its native format into static images, would not remedy the privilege-waiver problems inherent in the government's review.[71]

8. Consider Using Neutral Third Party to Collect Data

A corporation must make a determination whether to have its internal information technology personnel collect relevant electronic data or whether to outsource the function to a vendor. Corporations tend to want to save money by collecting the data internally. However, regardless of who collects the data, adequate steps must be taken to ensure it is done in a forensically sound manner. If the collection will include data that has been modified, deleted, or encrypted, a third party forensic specialist is better suited for the task.

Having a neutral third party collect data may also be a useful bargaining chip with the government over the scope of the collection and the timing of the return. Further, use of a neutral party can be seen as an additional sign of good faith and prevent allegations of intentional miscollection or spoliation.[72]

IV. SEARCH WARRANTS

Many of the considerations that go into responding to a subpoena *duces tecum* are relevant to issues related to complying with a warrant to search for electronic information. The major difference between the two is timing and the element of surprise. While service of a subpoena generally grants the corporation ample time to comply,[73] a search warrant allows government agents to enter a corporation and execute a search warrant without prior warning.[74] Once inside, the government's right to examine everything in the premises is limited only by the constraints of the warrant.[75] Unlike subpoenas, which can be quashed, a corporation has no lawful way to prevent the execution of a search warrant or the potential disruption that may result.[76] It is relatively rare for government agents to hold off execution of a warrant to allow a legal challenge. However, it is also rare for the government to resort to a search warrant on a non-target without attempting to obtain the information through less obtrusive means.[77]

Because the execution of a warrant is an immediate and substantial invasion of privacy, one can only be issued after a judicial determination that probable cause exists and that the search

69 *In re Grand Jury No. 76-3*, 555 F.2d at 1307-1308.
70 *See In re Subpoena Duces Tecum*, 228 F.3d 341, 351 (4th Cir. 2000).
71 *In re Grand Jury No. 76-3*, 555 F.2d at 1307-1308.
72 *Rigas*, 281 F. Supp. 2d at 733 (defendant's employer hired Price Waterhouse Coopers to copy 26 hard drives used by corporate employees during the time period requested on the grand jury subpoena).
73 *But see In re Grand Jury Subpoenas*, 926 F.2d at 854 (court held that subpoenas served at same time as execution of search warrant does not turn subpoena into the "functional equivalent" of a warrant).
74 *United States v. SDI Future Health, Inc.*, 2006 WL 4457335 at *16 (D. Nev. 2006).
75 *Grand Jury Subpoenas*, 926 F.2d at 854.
76 *Id.*
77 *Comprehensive Drug Testing*, 473 F.3d at 933; *Cf. Steve Jackson Games, Inc. v. United States Secret Service*, 816 F. Supp. 432, 437 (W.D. Tex 1993)(court chastises government and lead agent for not attempting to enlist corporation's cooperation prior to executing search warrant) (*aff'd* 36 F.3d 457 (5th Cir. 1994)).

complies with the particularity requirement of the Fourth Amendment.[78] The Fourth Amendment makes "general searches under [a warrant] impossible and prevents seizure of one thing under a warrant describing another."[79] A search warrant must state with reasonable particularity what items are being targeted for search and seizure, or in the alternative, what criminal activity is suspected of having been committed.[80] While the level of specificity may vary depending upon the circumstances of the case and the type of items involved, vague or ambiguous assertions may cause the warrant to become an impermissible general search warrant.[81]

The scope of the warrant is also limited by the probable cause on which the warrant is based.[82] Like the particularity requirement, this "breadth" requirement prevents a "general, exploratory rummaging in the person's belongings."[83] The courts interpret breadth as requiring probable cause to seize the particular items named in the warrant.[84] A warrant that exceeds the scope of the probable cause shown in the affidavit is subject to invalidation.[85]

The mechanics of search warrant execution are relatively straightforward. An officer executing a warrant must: (1) give a copy of the warrant and a receipt for property taken to the person from whom (or from whose premises) the property was taken; or (2) leave a copy of the warrant and receipt at the place where the officer took the property.[86] The manner and tone of the officers in executing the warrant will generally depend upon whether the corporation is the intended target of the investigation.

V. CONSIDERATIONS WHEN A CORPORATION IS SERVED WITH A SEARCH WARRANT

When law enforcement authorities enter a company with a search warrant in hand, the appropriate contact persons should be alerted immediately. The so-called "knock and announce" rule[87] generally is not an issue in executing search warrants on corporations during business hours;[88] however, a search warrant executed on a locked office building at night would need to comply with the knock and announce requirement.[89]

1. Follow Company's Internal Guidelines for Compliance with Search Warrant.

A corporation should have established procedures for dealing with search warrants. These guidelines should specifically address concerns related to the seizure of electronically stored information. The corporation's legal department should have a point person assigned to handle all issues related to search warrants. This representative should coordinate with information technology ("IT") and records managers to develop contingency plans in the event law enforcement seeks to search electronic records or seize equipment. If the company does not have internal guidelines for search warrant compliance, it should work with its outside counsel to develop a set of rules that maximize protection of the corporation while still emphasizing cooperation with law enforcement to the extent possible.

Employees should be advised that a search warrant relates to the search and seizure of physical evidence and cannot be used to compel employee interviews. While employees should be instructed to cooperate with the investigation, they are under no obligation to talk to the agents conducting the search. However, the corporation must be careful to avoid instructing its employees

78 *In re Subpoena Duces Tecum*, 228 F.3d at 348.
79 *United States v. Bridges*, 344 F.2d 1010, 1016 (9th Cir. 2003).
80 *Id.* at 1016-1017.
81 *United States v. Bright*, 630 F.2d 804, 812 (5th Cir. 1980)("Generic classifications in a warrant are acceptable only when a more precise description is not available").
82 *United States v. Towne*, 997 F.2d 537, 544 (9th Cir. 1993).
83 *Andresen v. Maryland*, 427 U.S. 463, 480, 96 S.Ct. 2737, 2748, 49 L.Ed.2d 627 (1976).
84 *See e.g., In re Grand Jury Subpoenas*, 926 F.2d 847.
85 *United States v. Washington*, 797 F.2d 1461, 1472 (9th Cir. 1986)("where a business is searched for records, specificity is required to ensure that only the records which evidence crime will be seized and other papers will remain private").
86 Fed. R. Crim. P. 41(f)(3).
87 18 U.S.C. Section 3109 (federal officer permitted to break a window or door of a house in order to gain entry to execute a search warrant only if, after notice of authority and purpose, entrance is refused).
88 *United States v. Little* 753 F.2d 1420, 1435-1436 (9th Cir. 1985).
89 *United States v. Phillips*, 497 F.2d 1131, 1133-1134 (9th Cir. 1974).

not to talk to law enforcement as this may be viewed as an obstruction of justice. The company should determine whether it will provide legal counsel to employees and notify employees of the company's policy in that regard.

A corporate representative (preferably from the legal department) should serve as the liaison for law enforcement executing the warrant. Employees likely impacted by the warrant (records management and IT) should be instructed to be cooperative. An agent may ask that employees leave the premises or stay away from the general vicinity of the area searched. If practical, these employees can remain in a conference room or may be sent home if the search is expected to take all day. Once the search starts, employees may need to get permission from the lead agent conducting the search in order to leave the premises.[90]

While it is best the corporate legal representative and outside counsel both be present for the search, it may not always be possible as the warrant may be executed in a different city or state than the corporation's headquarters. Thus, it is of critical importance to have a contingency plan mapped out for all corporate locations.

2. Obtain a Copy of the Search Warrant and Read it Carefully

Law enforcement officials will generally assign a team to coordinate and execute a search warrant on a corporation. The team may consist of a case agent, the prosecutor, and a technical specialist or expert. The lead case agent will usually ask to speak to the person in charge. Any receptionist or lobby personnel should be instructed to contact the designated representative from the legal department. The representative will be entitled to a copy of the warrant and should take time to read it thoroughly.

The warrant should be very specific and describe, in as much detail as possible, the areas to be searched and the items or information authorized to be seized.[91] The warrant may include a search protocol for the search and potential seizure of electronically stored information along with instructions for the technical expert assisting in the search.[92] However, the government may deviate from the protocol so long as in executing the warrant, it limits itself to the particular descriptions contained in the warrant.[93]

In speaking with the lead agent, the corporate representative should get the sense that the government search strategy is to pursue the quickest, least intrusive, and most direct route to secure the described evidence. If the corporation has multiple locations, the agents should be asked whether the government has also issued a warrant for another corporate location. If the government is aware that information is stored in a different city, it is possible other agents are simultaneously executing a similar warrant in another corporate office.[94]

While technical specialists are not required to execute a search, their presence can benefit the corporation.[95] This specialist is generally tasked with reviewing the computer equipment and storage media to determine whether there are any immediate preservation issues and whether the search can be done at the corporation within a reasonable period of time.[96] If an on-site search is impractical, the technician will either make a forensically sound copy of the computer storage devices or take possession of such devices for later review and analysis. In many cases, a search warrant for electronic information authorizes seizure of computers and storage media where experts have a controlled environment.

---

90 *See United States v. P.A. Landers, Inc.*, 2006 WL 3103087 at *1 (D. Mass. 2006).
91 *See e.g., United States v. Tylman*, 2007 WL 2669567 at *2 (C.D. Ill. 2007)(first warrant executed by agents failed to list items to be seized while second warrant sought items to be seized on a property located 100 miles away).
92 *See e.g., In re Search of 3817 W. West End*, 321 F. Supp. 2d 953, 958 (N.D. Ill. 2004).
93 *United States v. Fumo*, 2007 WL 3232112, at *6 (E.D. Pa. 2007).
94 *See e.g., Comprehensive Drug Testing*, 473 F.3d at 933.
95 *See e.g., Forro Precision, Inc. v. IBM*, 673 F.2d 1045, 1054 (9th Cir. 1982); *United States v. Tamura*, 694 F.2d 591, 596 n.4 (9th Cir. 1982).
96 *Comprehensive Drug Testing*, 473 F.3d at 933.

3. Contact Outside Counsel and Ask the Lead Agent to Wait for the Attorney's Arrival Before Commencing with the Search

As noted above, in the context of complying with a subpoena, the corporation should seek the advice of a lawyer with experience with search warrant procedure. Fax the lawyer a copy of the search warrant immediately so that she can determine any potential deficiencies and, if appropriate, make arrangements to travel to the search location. Any conversations the lawyer has with company personnel should be conducted outside the presence of law enforcement to preserve the attorney-client communication privilege.

If the lawyer's office is not far away, ask the agent to await the lawyer's arrival before beginning the search. The agent responsible for serving the subpoena may be willing to delay the search long enough for the company to reach outside counsel if the agent is assured there is no danger of destruction of potential evidence in the meantime (i.e., that evidence is not about to be removed, altered, or destroyed.)[97] However, if the corporation or corporate officer is the target of the investigation, law enforcement may execute the warrant immediately.

4. Be Cooperative But Do Not Consent to the Search

The attitude of the agents may be influenced by corporation's willingness to cooperate with the investigation. Corporate representatives should do so to the extent the agents' actions are within the scope of the search warrant. Company employees are not required to talk to law enforcement and may be advised of their right not to do so. However, a corporate representative has no authority to prohibit its employee from talking to a law enforcement officer executing a warrant. Often when searching for electronic information, law enforcement may call upon a member of the corporation's IT department to assist in locating specific files or electronic data. IT personnel may also be tasked with accessing data from the company's servers that may be password protected.

While the corporate employees should be cooperative and assist law enforcement in locating relevant files or electronically stored information, the employee must be careful not to consent to the search as the employee's actions may cure a defective warrant or improper search. Absent consent or other exceptions, an agent will need to obtain a warrant to search an area or look for an item outside the scope of the initial search warrant.[98] Therefore, it is best that the legal representative be present to assist employees when the agent requests information regarding electronic information.[99]

5. Determine Whether the Agents Have a Search Protocol for Electronically Stored Information

A search warrant seeking computer information should call for a specific search for information pertaining to specific criminal activity. Without specific guidance regarding the limitations of the warrant, a search of electronic information may fall dangerously close to a limitless search.[100] Accordingly, when seeking a search warrant, the court may require the government to submit a protocol outlining the methods it intends to use to ensure the proposed search is reasonably tailored to find documents related to criminal activity.[101] The protocol is intended to provide the court sufficient assurances that the search will not be a random one or constitute a general examination of documents unrelated to the investigation.[102]

---

97 *See United States v. Reed*, 935 F.2d 641, 642 (4th Cir. 1991).
98 *See United States v. Foote*, 2002 WL 1856996 (D. Kan. 2002).
99 *United States v. Vilar,* 2007 WL 1075041 (S.D.N.Y. 2007) advises against the "catch all" warrant and emphasizes the 4th Amendment "particularity" requirement. In *Vilar,* the District Court found parts of the warrant and subpoena lacked particularity offending the 4th Amendment and so broad that a "well trained officer would have known that the search was illegal despite the magistrates authorization." (*Vilar* at 24, quoting *United States v. Leon,* 468 U.S. 897, 922 (1984)).
100 *United States v. Carey*, 172 F.3d 1268, 1273 (10th Cir. 1999)(officer overstepped boundaries of search warrant for drug evidence when he searched for child pornography for four hours collecting hundreds of images); *cf. United States v. Walser*, 275 F.3d 981, 986-87 (10th Cir. 2001)(finding no Fourth Amendment violation when officer searched for electronic data related to drugs and opened single file containing child pornography, stopped search, and then returned to magistrate for second warrant to search for child pornography).
101 *In re Search of 3817 W. West End*, 321 F. Supp. 2d at 955-956 (concluding that government must provide search protocol to satisfy Fourth Amendment particularity requirement).
102 *Id.*

A protocol generally describes (1) the information that government seeks to seize from the computer, and (2) the methods used to locate that information without generally reviewing all information on the computer. The protocol may also disclose whether agents intend to search the computer and make electronic copies of specific files or to duplicate entire storage devices for later off-site review. There is no one-size-fits-all protocol. Rather, it should be tailored to the specific needs of the investigation. For example, certain cases may have no reasonable need for graphics files, which can be excluded in the protocol.[103] Effective search protocols may also limit searches via a particular date range, specific key words, location, or particular user. The absence of such information can also render the warrant defective. For example, in invalidating a search warrant related to a health care fraud investigation, the court in *SDI Future Health,* was critical of several categories of records that contained no date range or other criteria that would limit the breadth of the search to a specific criminal activity.[104] Instead, the warrant sought information from 34 categories of records, including all "documents relating to non-privileged internal memorandum and E-mail," "documents related to personnel and payroll records," and "documents related to non-privileged correspondence with consultants."[105] The court held these categories and ten others, failed to meet the Fourth Amendment's particularity requirement.[106]

In some cases, the government has vigorously argued against the need for a search protocol.[107] One court called the government's position "disingenuous" in light of the fact that the Department of Justice manual *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations, July 2002* encourages the government to provide a specific explanation of the search methodology it intends to use when searching electronic information.[108] However, recent cases have rejected this position and have adopted the government's assertion that the search methodology is best left to the agents serving the warrant.[109] The rationale is based, at least in part, on the fact that the prosecutors drafting the warrant – and officers tasked with serving it – may have no knowledge of the particular form in which the potential evidence is maintained which would require the agents to search the all computer files, digital media and storage devices.[110]

Irrespective of the protocol, if large amounts of electronically stored information are to be searched, time restraints and technical limitations may dictate that the data be actually reviewed off-site.[111] In such cases, the government may make a mirror image of hard drives or storage devices, thus effectively seizing the information.[112] The agents will then take the duplicate copies to an off-site facility for review.[113]

Whether the warrant includes a protocol or the search includes a technical expert, the more specific and targeted the collection, the easier it may be for personnel to assist law enforcement and still limit disruption to the day-to-day operations of the company. Moreover, the existence of formal procedures related to the search and seizure of a company's electronic information can lessen the potential for "invasion of materials protected by the attorney-client privilege."[114]

6. Determine Whether Search Warrant and/or Protocol Adequately Protect Attorney-Client Privileged Documents or Other Protected Information.

The potential waiver of attorney-client privilege regarding material requires that law enforcement utilize techniques to minimize the risk of seizure of privileged or otherwise protected materials. These procedures should be articulated in the search warrant affidavit and search protocol.

---

103 *See id.* at 956.
104 2006 WL 4457335 at *27.
105 *Id.*
106 *Id.* at 42.
107 *See e.g., In re Search of 3817 W. West End*, 321 F. Supp. 2d at 959 n.3; *In re Search of Premises Known as 1406 N. 2nd Ave.*, 2006 WL 709036 at *6 (W.D. Mich. 2006).
108 *In re 1406 N. 2nd Ave.*, 2006 WL 709036 at *6, n.3.
109 *See e.g., United States v. Tylman*, 2007 WL 2669567 at *12-13; *United States v. Gocha,* 2007 WL 2379721 (N.D. Iowa 2007); and *United States v. Summage*, 481 F.3d 1075 (8th Cir. 2007).
110 *U.S. v. Gocha*, 2007 WL 2379721 at *7.
111 *Id* at *13 (Court noted that on-site inspection would be impractical and "would almost certainly be more intrusive into the privacy of the computer owners; it could take weeks to complete [the search] process in a case with a large volume of documents, while the computers in this case were removed, imaged, and returned within a few business days.")
112 *See United States v. Hill*, 459 F.3d 966, 974-75 (9th Cir.2006).
113 *In* re *Search of 3817 W. West End*, 321 F. Supp. 2d at 961.
114 *United States v. Hunter*, 13 F. Supp. 2d 574, 578 (D. Vt. 1998).

The corporate representative should quickly identify the location of potentially privileged or protected materials so that they can be segregated from the search and discuss with the agents what procedures are in place to protect this information. If the company's outside lawyer is available, she may be able to speak to the prosecutor further about the review of such information. The corporation may have other confidential information that is subject to protection. In *SDI Future Health* the court expressed concern about the handling of patient records and required that the warrant contain instructions that would ensure greater protection for the confidentiality of patient information.[115]

If the search warrant seeks matters related to First Amendment activities such as publishing, including Internet postings and blogs, the execution of the warrant may violate the Privacy Protection Act ("PPA"). Under the PPA, it is unlawful for the government to search or seize materials when the materials are work product prepared in anticipation of communicating such materials to the public where the materials include the "mental impressions, conclusions or theories" of the author and the materials are possessed for the purpose of communicating the material to the public by a person "reasonably believed to have a purpose to disseminate to the public . . . some form of public communication."[116] While a violation of this section cannot result in suppression of evidence in a criminal case, the PPA authorizes civil damages against the government.[117] However, the incidental seizure of material protected under the PPA may not subject the government to liability.[118]

Once the potentially privileged or protected information has been segregated, the government has several options to determine whether the data is in fact protected. The agents may use "taint teams" consisting of agents and a prosecutor who are not otherwise connected with the investigation to review the documents for privilege. Documents that are identified as such are withheld from the prosecutor.[119] The government may also submit the documents for *in camera* inspection or for review by a special master. However, given the fact that the search can potentially encompass millions of files, judges are reluctant to conduct *in camera* reviews.[120] For example, in *United States v. Jackson*, the court applied a four-part test in rejecting the use of a taint team and instead appointing a special master to review potentially privileged materials.[121]

If the taint team determines that information is protected by the attorney-client privilege or work product doctrine, the information should not be reviewed by the prosecutor but rather returned to the defendant.[122] Counsel should be pay particular attention to any information collected and reviewed by the government and inspect each document at the earliest opportunity.[123] Since production pursuant to a warrant is not voluntary, a defendant is given the opportunity to object and seek the return of his protected documents.[124] However, a defendant's failure to timely object to the disclosure of protected materials may effectively waive the protection.[125]

7. *Proactively Monitor Search and Double-Check the Agent's Receipt of Inventory*

The corporate representative should carefully monitor the search at all times to not only ensure that employees are cooperating, but also to make an accurate record of the agents' activities during the search. It is permissible to videotape the agents as they conduct their search; in fact, the agents themselves may videotape their activities.[126] Videotapes may prove invaluable if there is a later challenge to the reasonableness of the search.[127]

---

115 *SDI Future Health*, 2006 WL 4457335 at *38.
116 42 U.S.C. Section 2000aa.
117 *See Davis v. Gracey*, 111 F.3d. 1472 (10th Cir. 1997); *United States Secret Service,* 36 F.3d at 460.
118 *Guest v. Leis*, 255 F.3d 325 (6th Cir. 2001).
119 *United States v. Woody*, 2008 WL 504097, at *3 (W.D.N.C. Feb. 20, 2008).
120 *Id.*
121 *United States v. Jackson*, 2007 WL 3230140 (D.D.C. 2007)(In evaluating the appropriateness of taint teams, the court evaluated: (1) whether exigent circumstances exist in which government officials have already obtained the physical control of potentially privileged documents; (2) whether the defendant challenges the lawfulness of the acquisition of the documents to be reviewed; (3) the volume of documents at issue; and (4) the appearance of fairness.
122 *See United States v. Ary*, 518 F.3d 775, 780 (10th Cir. Mar. 4, 2008)
123 Counsel should determine whether the prosecutor is willing to grant informal access to the information prior to the Government's Rule 16 disclosures.
124 *United States v. de la Jara*, 973 F.2d 746, 749 (9th Cir. 1992).
125 *Id.* (court found waiver when defendant waited 6 weeks after Rule 16 disclosures to file a motion to suppress protected documents).
126 *See SDI*, 2006 WL 4457335 at *8.
127 *See U.S. v. Tylman*, 2007 WL 2669567 at *4-5.

When the agents are done with the search, the lead agent will give the corporate representative a list of all documents and information searched and seized during the execution of the warrant and a detailed receipt for property.[128] The representative should check the receipt against the company's records and if possible resolve any discrepancies before the agent leaves. If the discrepancy cannot be reconciled, the representative should make a note on the agent's copy of the receipt.

A corporation aggrieved by an unlawful search and seizure may file a motion seeking the return of the seized property[129] including all property removed along with all notes made by government agents during the seizure. [130] If the corporation is indicted, it could also request that the evidence be suppressed.[131]

VI. CONCLUSION

Corporate counsel are often caught off-guard by subpoenas and search warrants that demand voluminous electronic information, with little or no advance warning and a short timetable for compliance. Even when the warrant or subpoena does not implicate the corporation as a "target", compliance may still be difficult or impractical depending upon the requested information and the corresponding demand on corporate resources required to respond or comply. A corporation that has a plan in place before the subpoena is served or the warrant executed most likely will be in the best position to cooperate with law enforcement while safeguarding the limited protections offered to corporations by the Constitution.

128 Fed. R. Crim P. 41(f)(1)(B) and (C).
129 Fed. R. Crim. P. 41(g) Motion to Return Property
130 *Tattered Cover, Inc. v. City of Thornton*, 44 P.3d 1044 (Co. Sup. Ct. 2002).
131 *United States v. Gantt*, 194 F.3d 987, 994 (9th Cir. 1999)(requiring the defendant show a "deliberate disregard" for the Fourth Amendment).