SHEPPARD MULLIN
SHEPPARD MULLIN RICHTER & HAMPTON LLP
Government Contracts Law BLOG
For the latest updates on laws affecting government contracts

Government Contracts Blog

Posted at 9:43 AM on March 19, 2010 by Sheppard Mullin

The Fourth Amendment Trumps Unbridled Government Searches Of Electronic Data

(And What Companies Should Know To Protect Their Interests)

There are few things worse for a business than starting the day with FBI agents at the door demanding to search the files and computers with a search warrant in hand. Matters have not improved for businesses in the last ten years. Courts have struggled with balancing the government's interest in discovering evidence of a crime before it is possibly destroyed by the target of a criminal investigation, and the Fourth Amendment right against unreasonable searches and seizures. This balancing of competing priorities is even more difficult now that the majority of business records are in electronic format, which makes an on site review for material covered by the search warrant virtually impossible. Consequently, the government has been obtaining search warrants that allow entire computer files and email communications to be copied, and then seized in their entirety by the government. Needless to say, such an unbridled search without reasonable constraints is tantamount to a "general warrant" that is expressly prohibited by the Fourth Amendment.

A. The Government Has Been An Advocate For Law Enforcement Efforts, Not For Safeguarding Fourth Amendment Rights.

The government has taken the position that once the search warrant has been issued, courts cannot manage how the government conducts the search.[1] The government has strenuously opposed courts conditioning search warrants on the government providing search protocols for the review of electronic data, and has also resisted providing courts with a time range in which the search will be completed.[2] The government has also tried to defend, albeit unsuccessfully, a search of electronic data that went far beyond the scope of the search warrant. In *United States v. Carey*, the government was authorized to search for documents concerning the distribution and sale of controlled substances.[3] When the government case agent opened one attachment and found child pornography, he made the unilateral decision to expand the criminal investigation of Carey by opening attachments for five hours in the hopes of finding more evidence of Carey being criminally liable for the possession of child pornography. This expanded search is tantamount to a warrantless search, and, yet, the government tried to defend its actions when Carey moved to suppress the evidence of child pornography.

Indeed, the government's training materials encourage DOJ attorneys to oppose any court mandated restrictions on how the search warrant is executed as a matter of office policy. The DOJ Manual recognizes that there are "significant constitutional restrictions," but, rather than provide real guidance on how to carefully comply with the Fourth Amendment in the area of seizures of electronic data (and allow for judicial oversight), the DOJ Manual cavalierly states that "[u]nreasonable conduct can be remedied after the fact, including, as a 'last resort,' with suppression of evidence."[4] The DOJ Manual also dedicates several pages to the government resisting court imposed guidelines, and entitles the section, "Do Not Place Limitations on the Forensic Techniques That May Be Used To Search."[5]

Thus, the government cannot be entrusted with safeguarding the constitutional rights of persons who are the targets of a search. Fortunately, courts are increasingly willing to step in and establish guidelines as a condition to issuing a search warrant. The courts are acting appropriately, and have been compelled to do so following some egregious abuses of the search warrant process.

B.Federal Courts Have Increasingly Set Guidelines For Searching Electronic Data With The Ninth Circuit *En Banc* Setting Forth Bright Line Guidance in *Comprehensive Drug Testing, Inc.*

Most recently, in *United States v. Comprehensive Drug Testing, Inc.* ("*CDT*"), the Ninth Circuit *en banc* affirmed orders for the return of seized property in a highly publicized case concerning the illegal use of steroids in professional baseball.[6] More significantly, the Ninth Circuit issued clear guidelines for the search and seizure of electronic data, and, thereby, continued what courts have done in the past when large quantities of data are being searched,[7] namely, establishing much needed guidelines for the search and seizure of electronic data to ensure compliance with the Fourth Amendment.

CDT was decided in the context of the steroid scandal commonly referred to as the "BALCO" case in which the United States Attorney for the Northern District Court of California was investigating the Bay Area Lab Cooperative ("BALCO"), which was suspected of providing steroids to major league baseball players. The Major League Baseball Players Association agreed to drug testing of the players after receiving assurances that the results would be remain anonymous and confidential. CDT administered the drug testing program, and maintained a list of the players and their test results.

When the government learned that ten players had tested positive, the government obtained a search warrant in the Central District of California authorizing the search of the Long Beach facility of Comprehensive Drug Testing, Inc. The warrant limited the items to be seized to the drug testing records of the ten specific major league baseball players as to whom the government had probable cause. When the warrant was executed, however, the government seized and reviewed computer records of hundreds of other players. Information that was clearly protected by the players' constitutional right to privacy was used by the government to get further subpoenas. As one district judge described it, the government demonstrated a "callous disregard for the rights of those persons whose records were seized and searched outside the warrant."[8]

The initial warrant in *CDT* was issued subject to certain conditions. First, the *CDT* warrant

authorized the seizure of entire computer files only if "computer personnel" determined that seizable data could not be segregated on-site. Second, the *CDT* warrant authorized the government to hold onto the computer files for no more than 60 days within which time "computer personnel" would determine what data fell within the scope of the warrant. Without further authorization from the court, all non-seizable data had to be returned within the 60 day period. Even though the DOJ Manual admonishes attorneys to abide by conditions in the warrant or risk evidence being suppressed, the government failed to do so in *CDT*.[9]

In *CDT*, the government ignored the mandates set forth in the search warrant, did not segregate the seizable information from the non-seizable, and never returned any of the computer files. Instead, the government used its wide reaching seizure of computer files to execute additional search warrants, as well as subpoenas, demanding production of the documents the government already seized. The Ninth Circuit *en banc* commented on how egregious the government acted in a highly publicized case for which a reasonable person would expect the government to act more carefully to avoid discovery sanctions. Several district court judges involved in the case below also "commented that they felt misled or manipulated by the government's apparent strategy of moving from district to district and judicial officer to judicial officer in pursuit of the same information, and without fully disclosing its efforts elsewhere."[10]

Motions for the return of the seized material (as well as a motion to quash the subpoenas) were filed by Comprehensive Drug Testing, Inc. The district courts found that the government consciously disregarded the limitations set forth in the search warrants and ordered the return of the property. The Ninth Circuit held that the government could not maintain possession of data when the government acted with conscious disregard of the limitations in a search warrant. *CDT* also made it more clear that courts can impose these sanctions without applying the *Ramsden* balancing test.[11]

C.*CDT* Guidelines for Search Warrants and Electronic Data.

The Ninth Circuit also set forth safeguards for the execution of search warrants on electronically stored data, and recommended (as opposed to compelling) that courts follow them:

1. Magistrates should insist that the government waive reliance on the "plain view" doctrine that the government has tried to use in the past as the basis for not returning electronic data beyond the scope of the initial search warrant.

2. The electronic data should be reviewed by specialized computer personnel or an independent third party when the government is performing the initial segregation of data covered by the warrant. If the segregation process is done by government computer personnel, the warrant application must state that the computer personnel will not disclose to the investigators any information other than that which is covered by the warrant.

3. The government must disclose to the magistrate, who is considering the application for a search warrant, the actual risks of the target destroying the electronic data, as well as

prior efforts to seize that information in other judicial forums.

4. The government's search protocol must be designed to uncover only the information for which it has probable cause, and only that information may be examined by the government agents and attorneys.

5. The government must destroy or, alternatively, return the non-responsive data if the target of the search can lawfully possess it.

The *CDT* decision has been described as offering *Miranda*-style guidelines on how to protect Fourth Amendment privacy rights while conducting computer searches.[12]

Just as the DOJ Manual is opposed to courts setting guidelines for the search of electronic data, the government has been equally adamant in objecting to the *CDT* opinion. In a rarely used motion, the government is seeking a full rehearing *en banc* by the entire court of the Ninth Circuit.

The government's stated fear that *CDT* will have a chilling effect on law enforcement efforts does not seem to be a realistic concern. While the government's response is consistent with the law enforcement bias of the government, it should not be allowed to circumvent constitutional protections. The government also reacted strongly when *United States v. Booker* was decided.[13] In *Booker*, the United States Supreme Court held that the Federal Sentencing Guidelines are subject to the jury trial requirements of the Sixth Amendment, and, therefore, district courts cannot be compelled to follow the Guidelines for sentencing purposes. In response to *Booker*, the government proposed emergency measures in Congress to "save" the guidelines.[14] Congress declined to do so.

D. What Companies Should Take From *CDT*.

The good news is that companies have some recourse if the government seizes electronic data beyond the scope of the search warrant. Federal courts will enforce the conditions of a search warrant. When the government acts in disregard of the conditions for the search and seizure of electronic data, the target of the search should act promptly to demand a return of all material that is outside the scope of the search warrant. If the government does not comply with this request, then the target company should file a motion for return of property under Rule 41(g) of the Federal Rules of Civil Procedure.

Further, the target company should assert the privacy rights of third parties who have email communications or other confidential information on work computers. These third party employees are generally held to have a reasonable expectation of privacy in their work computer.[15] Companies should be careful not to extinguish their employees' rights of privacy by using opening pages or other notices on the work computers that state the employees have no expectation of privacy in their work computers. It should be sufficient for a company to give employees' notice that the company reserves the right to monitor their computer use on company-owned computers, and to sanction employees who misuse their computers, without

extinguishing the right to privacy which can be asserted should the government seek discovery of that electronic data. However, the language of any such notice to employees should be coordinated with labor and employment counsel for the company in order to ensure that the company is not hindered in its ability to sanction employees who misuse their work computers.

Companies should also proactively challenge government subpoenas for the search of electronic data, and ask courts to require the government to comply with the *CDT* guidelines. In addition, companies should ask courts to modify subpoenas that do not include reasonable time periods for the government to return non-responsive electronic data. Companies should also move to quash subpoenas that do not make a specific showing that the target's computer has data related to the alleged crime.[16]

Companies should also consult with experienced white collar legal counsel concerning other aspects of the government's criminal investigation in order to protect the interests of the company, and advance its long term goals.

Authored By:

Charles L. Kreindler
(213) 617-4188
ckreindler@sheppardmullin.com

and

Michelle Sherman
(213) 617-5405
msherman@sheppardmullin.com

---

[1] *In the Matter of the 3817 W. West End*, 321 F. Supp. 2d 953, 961 (N.D. Ill. 2004). "The government's core objection to providing a search protocol is that the Court is powerless to require it."

[2] *In the Matter of Premises Known as 1406 N. 2nd Avenue*, 2006 WL 709036, *2-3 (W.D. Mich. March 17, 2006) (the FBI agent initially refused to give even one year as the time needed to search the seized computer media, or any time estimate whatsoever).

[3] *United States v. Carey*, 172 F.3d 1268, 1276 (10th Cir. 1999) (reversed the district court's denial of the motion to suppress, and held that the detective's "seizure of the evidence upon which the charge of conviction was based was a consequence of an unconstitutional general search…").

[4] DOJ Manual at 80.

[5] *Id.* at 79.

[6] *United States v. Comprehensive Drug Testing, Inc.*, 579 F.3d 989 (9th Cir. 2009) (*en banc*).

[7] *See*, *e.g.*, *United States v. Tamura*, 694 F.2d 591 (9th Cir. 1982).

[8] *CDT*, 579 F.3d at 997.

[9] DOJ Manual at 82.

[10] *CDT*, 579 F.3d at 1004.

[11] *Id*. at 1003. The Ninth Circuit has previously held that illegally seized property should be returned when the party moving for relief has been aggrieved by an unlawful seizure, which is precisely the situation when the government illegally retains non-responsive, electronic data. *See In re Grand Jury Investigation Concerning SSDI*, 130 F.3d 853 (9th Cir. 1997).

Thus, the target of an investigation does not need to show that the pre-indictment search justifies the court exercising its discretionary jurisdiction to decide a Federal Rule of Civil Procedure 41(g) motion for return of property as would be required under the *Ramsden* balancing test. *Ramsden v. United States*, 2 F.3d 322, 325 (9th Cir. 1993). The *Ramsden* factors include: 1) whether the Government displayed a callous disregard for the constitutional rights of the movant; 2) whether the movant has an individual interest and need for the property he wants returned; 3) whether the movant would be irreparably injured by denying return of the property; and 4) whether the movant has an adequate remedy at law for the redress of his grievance.

[12] David Kravets, *Obama Wants Computer Privacy Ruling Overturned*, Associated Press, November 25, 2009.

[13] *United States v. Booker*, 543 U.S. 220 (2005).

[14] *Judiciary Asks Congress to Tread Carefully with Sentencing*, The Third Branch, Vol. 38, Number 4 – April 2006. (William W. Mercer, Principal Associate Deputy Attorney General at the Department of Justice, "urged the [House Judiciary] subcommittee [on Crime, Terrorism, and Homeland Security] and Congress 'to fully examine the current sentencing practice as well as the short- and likely long-term impact of *Booker* and then to act to reinstitute mandatory sentencing in the federal criminal justice system.'").

[15] *United States v. Ziegler*, 474 F.3d 1184 (9th Cir. 2007).

[16] *Cf. In re Application for Search Warrant*, Mag. No. 09-320 (D.D.C. June 3, 2009 (Facciola M.J.)) in which a magistrate judge known for his e-discovery expertise denied the government's request for a search warrant to seize computer data because the government had not made a sufficiently specific showing that the computer was related to the alleged crime.