Recent Case Report

Date posted: October 4, 2010

U.S. v. Comprehensive Drug Testing, Inc.

(9th Cir. En Banc 2010) __ F.3d. __ [2010 WL 3529247]

Issue

While executing a warrant to search a legitimate business for computer data pertaining to certain clients, did federal agents comply with a court-ordered procedure designed to prevent the inspection and seizure of data pertaining to other clients?

Facts

In the course of an investigation into steroid use by Major League Baseball players, federal agents learned that, pursuant to a collective bargaining agreement, all players were required to submit urine samples that were tested for steroids. The program was administered by Comprehensive Drug Testing, Inc. (CDT), and the test results were stored on CDT's computers in Long Beach.

When agents learned that ten players had tested positive, they sought a warrant to search CDT's computers for test data pertaining to those players. The affidavit also contained an explanation of the difficulties in searching computers:

> [C]omputer files can be disguised in any number of ingenious ways, the simplest of which is to give files a misleading name (pesto.recipe in lieu of blackmail.photos) or a false extension (.doc in lieu of .jpg or .gz). In addition the data might be erased or hidden; there might be booby traps that destroy or alter data if certain procedures are not scrupulously followed.

Because of these problems and the difficulty in searching an untold (but probably huge) number of computer files at the site, the affiant requested authorization to, in the words of the court, remove "pretty much any computer equipment found at CDT's Long Beach facility, along with any data storage devices, manuals, logs or related materials."[1]

A federal magistrate issued the warrant but refused to authorize such a broad seizure of computer data and equipment unless the agents complied with a procedure that was "designed to ensure that data beyond the scope of the warrant would not fall into the hands of the investigating agents."[2] Specifically, the warrant required that it be executed in the following manner:

---

[1] **NOTE**: The court pointed out that, while the affidavit "made a strong generic case that the data in question could not be thoroughly examined or segregated on the spot," it pointed out that the affiant's fears that files may be hidden or booby trapped was misplaced because CDT "is after all a legitimate business not suspected of any wrongdoing."

[2] **NOTE**: The court noted that the procedure was based on the Ninth Circuit's decision in *U.S.* v. *Tamura* (9th Cir. 1982) 694 F.2d 592 and pointed out that "[t]he point of the *Tamura* procedures is to maintain the privacy of materials that are intermingled with seizable materials, and to avoid turning a limited search for particular information into a general search of office file systems and computer databases."

1. The agents who execute the warrant must be accompanied by "computer personnel," a term defined as "law enforcement personnel trained in searching and seizing computer data," (hereinafter, "computer specialist").
2. The computer specialist must begin by inspecting the computer files to determine if the drug test results of the ten named players could be obtained on-site "in a reasonable amount of time and without jeopardizing the ability to preserve the data."
3. If the computer specialist determined that an on-site search was impractical, the computer specialist—"not the case agents"—was authorized "to examine all the data on location to determine how much had to be seized to ensure the integrity of the search."
4. The agents were then instructed to remove the necessary data to a "controlled environment, such as a law enforcement laboratory," where the computer specialist was authorized to do the following:
    (a) Take steps to "recover or restore hidden or erased data."
    (b) Separate the computer data into two groups: (1) data pertaining to the ten players listed in the warrant, and (2) all other data.
5. The data pertaining to the ten players was to be given to the case agent, while the other data would remain quarantined. (The warrant stated that, within a "reasonable period of time," but not more than 60 days after the warrant was executed, agents were required to return all unseizable data to CDT.)
6. The case agent was then permitted to search the data for information that was relevant to the criminal investigation.

When the warrant was executed, the computer specialist determined that it would be unnecessary to seize all files because the relevant data had apparently been stored in files located in one directory—the "Tracey" directory. But because the Tracey directory also included "information and test results involving hundreds of other baseball players and athletes engaged in other professional sports," the computer specialist determined that it could not be searched and segregated on-site. So he copied the directory and took it to a secure facility pursuant to the magistrate's instructions. But, contrary to those instructions, the copy of the directory was then "turned over to the case agent, and the specialist did nothing further to segregate the target data from that which was swept up simply because it was nearby or commingled."[3]

When CDT and the MLB Players Association learned what had happened, they filed a motion for the return of the non-quarantined data on grounds that the government had failed to comply with the procedural requirements set forth in the warrant. At the conclusion of the hearing, the court ruled that the government "completely ignored" the requirements and, moreover, had "demonstrated a callous disregard for the rights of those persons whose records were seized and searched outside the warrant." Consequently, the court granted the motion, and the government appealed to the Ninth Circuit.

[3] **NOTE**: The government later admitted that "the idea behind taking the copy of the Tracey Directory was to take it and later on briefly peruse it to see if there was anything above and beyond that which was authorized for seizure in the initial warrant."

Discussion

The government argued that the motions should have been denied because, although agents had inspected a lot of data pertaining to players and others who were not listed in the warrant, this data was properly seized under the plain view rule. Among other things, the plain view rule provides that officers who are executing a search warrant may seize any unlisted evidence they happen to discover if (1) they viewed the evidence while conducting a lawful search for listed evidence; (2) they had probable cause to believe it was, in fact, evidence of a crime; and (3) such probable cause existed at the time they first viewed the evidence; i.e., they did not develop probable cause as the result of a further inspection.

The court ruled, however, that the agents were not conducting a lawful search when they first saw the unlisted data because, contrary to the magistrate's explicit instructions, there "no effort by a dedicated computer specialist to separate data for which the government had probable cause from everything else in the Tracey Directory." Furthermore, the person who initially inspected all the files at the CDT offices was the case agent, and he immediately "rooted out" the testing records for "hundreds of players in Major League Baseball (and a great many other people)."

Consequently, because the unlisted records were not legally seized under the plain view rule, the court ruled that the district court judges properly ordered the government to return the unlisted data to CDT.

Comments

Three things should be noted. First, officers who are searching computers often have legitimate concerns that files may be mislabeled, hidden, encrypted, erased, or booby trapped. But these concerns are usually present only when officers are searching computers that belong to suspects or others who may have a motive to undermine the investigation. But when, as here, the computer is owned and operated by a legitimate business that is not suspected of any wrongdoing, a court may find that wholesale seizures of computer files or equipment are unwarranted, at least unless officers can point to specific facts indicating that a threat to the data is a reasonable possibility. The court probably had this in mind when it observed that, when agents arrived at the facility, CDT personnel offered "to provide all information pertaining to the ten identified baseball players," but their offer was "brushed aside." (As noted earlier, the affidavit in this case contained an explanation of the dangers of searching computers. But, as the court pointed out, "[t]he record reflects no forensic lab analysis.")

Second, the court acknowledged that it is often necessary for officers to search every computer file they seize pursuant to a warrant because "[t]here is no way to be sure exactly what an electronic file contains without somehow examining its contents." But it added that such "over-seizing" makes it difficult to ensure that computer searches are carefully circumscribed because "[a]uthorization to search *some* computer files therefore automatically becomes authorization to search all files in the same sub-directory, and all files in an enveloping directory, a neighboring hard drive, a nearby computer or nearby storage media"—and maybe even networked computer files. For these reasons, the court encouraged officers and judges to institute procedures, such as those set forth by the magistrate in this case to "avoid turning a limited search for particular information into a general search of office file systems and computer databases."

Third, this is actually the second en banc decision in this case. The first one was filed in 2009—and it generated controversy throughout the country because, as we reported in the Fall 2009 edition, the court purported to "impose sweeping restrictions on the manner in which *all* warrants to search computers are issued an executed." For example, it announced that computer searches must be conducted by disinterested observers; and it instructed the lower courts to "insist that the government waive reliance upon the plain view doctrine in digital evidence cases," thus ensuring that all unlisted evidence will be suppressed even if was obtained inadvertently in the course of a lawful search. Those requirements were eliminated in the second decision. POV