U.S. v. Ulbricht

(2nd Cir. 2017) 858 F.3d 71

Issue

When officers write search warrants for electronic communications or data, how much specificity is required when they describe the information to be seized?

Facts

This is the case about the audacious "Silk Road" website which, between 2011-2013 operated on the Darknet.[1] According to the court, Silk Road was a "massive, anonymous criminal marketplace" on which users could buy and sell drugs, illegal weapons, false IDs, computer hacking software, and other contraband; and they could pay for it anonymously via a digital currency called Bitcoin.

The suspected creator and operator of Silk Road was Ross Ulbricht, a young physicist and fearless libertarian, whose user name was Dread Pirate Roberts or DPR. In 2012, federal investigators in New York and Maryland began the seemingly impossible task of gathering information about the site and the mysterious person who ran it. Eventually, they developed a strong case against Ulbricht but, in order to obtain a conviction they needed to catch him in the act of working on the site as an administrator—and they must do so before he was able to activate an emergency

Their opportunity arose in 2013 when investigators followed Ulbricht as he walked into a branch of the San Francisco Public Library. He was carrying his laptop, and the investigators were aware that many people who conduct illegal internet operations often do so at libraries and coffee shops because they are often able to sit in locations where others cannot see their monitors. Shortly after Ulbricht sat down, opened his laptop and began using it, investigators stationed outside determined that DPR had just logged into Silk Road as an administrator. This provided them with the proof they needed, so they rushed him, and they did it so fast that they prevented him from encrypting the data or permanently locking the laptop.

After seizing the laptop, investigators obtained a warrant to search it and, during the search, found "overwhelming evidence" that Ulbricht created and continued to administer Silk Road. Also on the laptop, they found evidence that the site had processed transactions totaling approximately $183 million. Prosecutors used this evidence at trial and Ulbricht was convicted of, among other things, engaging in a continuing criminal enterprise and conspiring to obtain unauthorized access to a computer for the purpose of furthering the enterprise. He was sentenced to life in prison.

Discussion

On appeal, Ulbricht argued that the evidence discovered in his laptop should have been suppressed because the warrant did not adequately describe the digital information

[1] **What is "The Darknet"?** The Darknet is "a special network on the Internet designed to make it practically impossible to physically locate the computers hosing or accessing websites on the network." *Ulbricht* at fn.2. Users of The Darknet "deliberately hide from the prying eyes of the searchable Web. They cloak themselves in obscurity with specialized software that guarantees encryption and anonymity between users, as well as protocols or domains that the average webizen will never stumble across." *PC World*, August 2, 2013.

that the investigators were authorized to search for and seize. For example, he objected to the following descriptions:

- "[A]ny communications or writings by Ulbricht, which may reflect linguistic patterns or idiosyncrasies associated with DPR."
- "[A]ny evidence concerning any computer equipment, software, or user names by Ulbricht."
- "[A]ny evidence concerning Ulbricht's technical expertise concerning [the Darknet], Bitcoins, and other computer programming issues."

Ulbricht was correct that search warrants must contain a "particular" description of the places to be searched and the evidence to be seized.[2] As might be expected, however, it is impossible to provide much guidance for determining what constitutes a "particular" description. Instead, the courts usually say something nebulous such as the description must impose a "meaningful restriction" on what officers may search for and seize.[3] While this requirement seldom causes problems, when officers want to search for physical evidence such as illegal drugs and weapons, it may be a big problem when they want to search for information and data stored in a computer or other electronic communications device. This is because, as the court in *Ulbricht* pointed out, "officers cannot readily anticipate how a suspect will store information related to the charged crimes. Files and documents can easily be given misleading or coded names, and words that might be expected to occur in pertinent documents can be encrypted."

Were the descriptions contained in the Silk Road warrants sufficiently particular? The court ruled they were because the affiant—who was obviously well-trained for the job—utilized at least four methods of describing evidence that he or she had never seen. Those methods were as follows:

(1) **SEARCH PROTOCOLS**: A affidavit may contain a "search protocol" in which the affiant describes a certain procedure by which officers can identify seizable evidence. If the judge issues the warrant, officers will be authorized to utilize this procedure. For example, a search protocol for a computer might require "an analysis of the file structure, next looking for suspicious file folders, then looking for files and types of files most likely to contain the objects of the search by doing keyword searches."[4]

In *Ulbricht*, the affiant included three such protocols. First, the agents were authorized to start with a "key word" search in which they utilized a software program that examines all of the files, looking for certain words that are indicative of, or otherwise related to, seizable information. Second, they were instructed that, when they found such a file, they must begin by "cursorily reading the first few" pages to make sure that it contains relevant information. Third, in order to link Ulbricht to Silk Road, they were authorized "to compare Ulbricht's writings to DPR's posts to confirm that they were the same person, by identifying both linguistic patters and distinctive shared political or economic view."

---

[2] See *U.S. v. SDI Future Health, Inc.* (9th Cir. 2009) 568 F.3d 684, 702 ["Particularity means that the warrant must make clear to the executing officer exactly what it is that he or she is authorized to search for and seize."].

[3] See *Burrows v. Superior Court* (1974) 13 Cal.3d 238, 249; *Andresen v. Maryland* (1976) 427 U.S. 463, 480; *Maryland v. Garrison* (1987) 480 U.S. 79, 84; *Lo-Ji Sales, Inc. v. New York* (1979) 442 U.S. 319, 325.

[4] *U.S. v. Burgess* (10th Cir. 2009) 576 F.3d 1078, 1094.

(2) **INCORPORATION BY REFERENCE**: An affiant may also be able to provide a more complete description of communications and data by incorporating the entire search warrant affidavit into the warrant; e.g., "Attached hereto and incorporated by reference is the affidavit in support of this warrant." This was done in *Ulbricht* and the court pointed out that "[b]y incorporating the affidavit by reference, the Laptop Warrant lists the charged crimes, describes the place to be searched, and designates the information to be seized in connection with the specified offenses."

(3) **"PERMEATED WITH FRAUD" RULE**: It sometimes happens that a business is so corrupt—so "permeated with fraud"—that there is a fair probability that all or substantially all of the documents stored in its computers constitute relevant evidence. When this happens, the description of the evidence may be quite broad, and may even permit officers to search for and seize *all* stored communications and data.[5] Because the affidavit established that Silk Road was the quintessential "permeated with fraud" operation, the court ruled there was an "ample basis for the issuing magistrate judge to conclude that evidence related to Silk Road and Ulbricht's uses of the DPR username likely permeated Ulbricht's computer."

(4) **INCLUDING REASONABLY AVAILABLE INFORMATION**: Finally, the courts will permit a more general description if it reasonably appeared that the affiant provided as much descriptive information as he or she could be expected to provide under the circumstances.[6] As the court explained in *U.S. v. Young*, "Courts tend to tolerate a greater degree of ambiguity where law enforcement agents have done the best that could reasonably be expected under the circumstances, have acquired all the descriptive facts which a reasonable investigation could be expected to cover, and have insured that all those facts were included in the warrant."[7] This was a factor in *Ulbricht* because the court pointed out that the agents "did the best that could reasonably be expected under the circumstances," and that they "acquired all the descriptive facts which a reasonable investigation could be expected to cover, and had insured that all those facts were included in the warrant."

---

[5] See *U.S. v. Smith* (9th Cir. 2005) 424 F.3d 992, 1006 ["a warrant authorizing the seizure of essentially all business records may be justified when there is probable cause to believe that fraud permeated the entire business operation"]; *In re Grand Jury Investigation* (9th Cir. 1997) 130 F.3d 853, 856 ["a generalized seizure of business documents may be justified if the government establishes probable cause to believe that the entire business is merely a scheme to defraud or that all of the business's records are likely to evidence criminal activity"]; *People v. Hepner* (1994) 21 Cal.App.4th 761, 778 [medical practice in which about 90% of patient files were of fraud was "permeated with fraud"].

[6] See *People v. Robinson* (2010) 47 Cal.4th 1104, 1132 ["the specificity required varies depending on the circumstances of the case and the type of items involved"]; *People v. Smith* (1986) 180 Cal.App.3d 72, 89 ["the requirement of reasonable particularity is a flexible concept, reflecting the degree of detail known by the affiant and presented to the magistrate. While a general description may be sufficient where probable cause is shown and a more specific identification is impossible, greater specificity is required in a case where the identity of the objects is known."]; *U.S. v. Reyes* (10th Cir. 1986) 798 F.2d 380, 383 ["[I]n the age of modern technology and commercial availability of various forms of items, the warrant could not be expected to describe with exactitude the precise form the records would take."]; *U.S. v. Holzman* (9th Cir. 1989) 871 F.2d 1496, 1509 ["Because the police reasonably could not list all of the names included on [credit] cards used during the fraud, a generic description was sufficient."].

[7] (2nd Cir. 1984) 745 F.2d 733, 759.

For these reasons, the court ruled that the agents' description of the communications and data in Ulbricht's laptop was sufficient, and it affirmed Ulbricht's conviction and sentence . POV

Date posted: June 8, 2017
Date modified: June 26, 2017