2013 WL 1729765
Only the Westlaw citation is currently available.
United States District Court,
S.D. Texas,
Houston Division.

In re WARRANT TO SEARCH A TARGET
COMPUTER AT PREMISES UNKNOWN.

No. H–13–234M. | April 22, 2013.

Opinion

MEMORANDUM AND ORDER

STEPHEN WM SMITH, United States Magistrate Judge.

 *1 The Government has applied for a Rule 41 search and seizure warrant targeting a computer allegedly used to violate federal bank fraud, identity theft, and computer security laws. Unknown persons are said to have committed these crimes using a particular email account via an unknown computer at an unknown location. The search would be accomplished by surreptitiously installing software designed not only to extract certain stored electronic records but also to generate user photographs and location information over a 30 day period. In other words, the Government seeks a warrant to hack a computer suspected of criminal use. For various reasons explained below, the application is denied.

Background

In early 2013, unidentified persons gained unauthorized access to the personal email account of John Doe, an individual residing within the Southern District of Texas, and used that email address to access his local bank account. The Internet Protocol (IP) address of the computer accessing Doe's account resolves to a foreign country. After Doe discovered the breach and took steps to secure his email account, another email account nearly identical to Doe's—the address differed by a single letter—was used to attempt a sizeable wire transfer from Doe's local bank to a foreign bank account. The FBI has commenced an investigation, leading to this search warrant request. At this point in the investigation, the location of the suspects and their computer is unknown.

The Government does not seek a garden-variety search warrant. Its application requests authorization to surreptitiously install data extraction software on the Target Computer. Once installed, the software has the capacity to search the computer's hard drive, random access memory, and other storage media; to activate the computer's built-in camera; to generate latitude and longitude coordinates for the computer's location; and to transmit the extracted data to FBI agents within this district.

Using this software, the government seeks to obtain the following information:

(1) records existing on the Target Computer at the time the software is installed, including:

• records of Internet Protocol addresses used; records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" Web pages, search terms that the user entered into any Internet search engine, and records of user-typed Web addresses;

• records evidencing the use of the Internet Protocol addresses to communicate with the [victim's bank's] e-mail servers;

• evidence of who used, owned, or controlled the TARGET COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs registry entries, configuration file, saved user names and passwords, documents, browsing history, user profiles, e-mail contents, e-mail contacts, "chat," messaging logs, photographs, and correspondence;

• evidence of software that would allow others to control the TARGET

 *2 COMPUTER;

• evidence of times the TARGET COMPUTER was used; and

• records of applications run.

(2) prospective data obtained during a 30–day monitoring period, including:

• accounting entries reflecting the identification of new fraud victims;

• photographs (with no audio) taken using the TARGET COMPUTER's built-in camera after the installation of the NEW SOFTWARE, sufficient to identify the location of the TARGET COMPUTER and identify persons using the TARGET COMPUTER;

• information about the TARGET COMPUTER's physical location, including latitude and longitude calculations the NEW SOFTWARE causes the TARGET COMPUTER to make;

• records of applications run.

Aff. Attach. B.[1]

Analysis

The Government contends that its novel request[2] is authorized by Rule 41. In the Court's view, this claim raises a number of questions, including: (1) whether the territorial limits of a Rule 41 search warrant are satisfied; (2) whether the particularity requirements of the Fourth Amendment have been met; and (3) whether the Fourth Amendment requirements for video camera surveillance have been shown. Each issue is discussed in turn.

1. Rule 41(b) Territorial Limit

Rule 41(b) sets out five alternative territorial limits on a magistrate judge's authority to issue a warrant. The government's application does not satisfy any of them.

The rule's first subsection, the only one expressly invoked by the Government's application, allows a "magistrate judge with authority in the district ... to issue a warrant to search for and seize a person or property located within the district." FED.R.CRIM.P. 41(b)(1). Even though the Government readily admits that the current location of the Target Computer is unknown, it asserts that this subsection authorizes the warrant "because information obtained from the Target Computer will first be examined in this judicial district." Aff. ¶ 20. Under the Government's theory, because its agents need not leave the district to obtain and view the information gathered from the Target Computer, the information effectively becomes "property located within the district." This rationale does not withstand scrutiny.

It is true that Rule 41(a)(2)(A) defines "property" to include "information," and the Supreme Court has long held that "property" under Rule 41 includes intangible property such as computer data. *See United States v. New York Tel. Co.,* 434 U.S. 159, 170, 98 S.Ct. 364, 54 L.Ed.2d 376 (1977). For purposes of search and seizure law, many courts have analogized computers to large containers filled with information.[3] *See United States v. Roberts,* 86 F.Supp.2d 678, 688 (S.D.Tex.2000); *United States v. Barth,* 26 F.Supp.2d 929, 936–37 (W.D.Tex.1998); *United States v. David,* 756 F.Supp. 1385, 1390 (D.Nev.2009)(holding that a computer notebook "is indistinguishable from any other closed container" for the purpose of Fourth Amendment analysis). By the Government's logic, a Rule 41 warrant would permit FBI agents to roam the world in search of a container of contraband, so long as the container is not opened until the agents haul it off to the issuing district. The court has found no case willing to stretch the territorial limits of Rule 41(b)(1) so far.

*3 The "search" for which the Government seeks authorization is actually two-fold: (1) a search for the Target Computer itself, and (2) a search for digital information stored on (or generated by) that computer. Neither search will take place within this district, so far as the Government's application shows. Contrary to the current metaphor often used by Internet-based service providers, digital information is not actually stored in clouds; it resides on a computer or some other form of electronic media that has a physical location.[4] Before that digital information can be accessed by the Government's computers in this district, a search of the Target Computer must be made. That search takes place, not in the airy nothing of cyberspace, but in physical space with a local habitation and a name. Since the current location of the Target Computer is unknown, it necessarily follows that the current location of the information on the Target Computer is also unknown. This means that the Government's application cannot satisfy the territorial limits of Rule 41(b)(1).

This interpretation of (b)(1) is bolstered by comparison to the territorial limit of subsection (b)(2), which expressly deals with a transient target. This subsection allows an extraterritorial search or seizure of moveable property "if it is located within the district when the warrant is issued but might move or be moved outside the district before the warrant is executed." FED.R.CRIM.P. 41(b)(2). Note that (b)(2) does not authorize a warrant in the converse situation—that is, for property *outside* the district when the warrant is issued, but brought back *inside* the district before the warrant

is executed. A moment's reflection reveals why this is so. If such warrants were allowed, there would effectively be no territorial limit for warrants involving personal property, because such property is moveable and can always be transported to the issuing district, regardless of where it might initially be found. [5]

The other subsections of Rule 41(b) likewise offer no support for the Government's application. Subsection (b)(3), dealing with an investigation of domestic or international terrorism, authorizes a search by a magistrate judge with authority in "any district in which activities related to the terrorism may have occurred," whether the property is within or outside that district. This case does not involve a terrorism investigation.

Subsection (b)(4) deals with a tracking device warrant, and its provisions echo those of (b)(2), allowing the device to be monitored outside the district, provided the device is installed within the district. FED.R.CRIM.P. 41(b)(4). There is a plausible argument that the installation of software contemplated here falls within the statutory definition of a tracking device, [6] because the software will activate the computer's camera over a period of time and capture latitude/longitude coordinates of the computer's physical location. But the Government's application would fail nevertheless, because there is no showing that the installation of the "tracking device" (i.e. the software) would take place within this district. To the contrary, the software would be installed on a computer whose location could be anywhere on the planet. [7]

 *4 The only remaining possibility is (b)(5), which authorizes a magistrate judge "in any district where activities related to the crime may have occurred" to issue a warrant for property that may be outside the jurisdiction of any state or district, but within a U .S. territory, possession, commonwealth, or premises used by a U.S. diplomatic or consular mission. FED.R.CRIM.P. 41(b)(5). The application does indicate that Doe's local bank account was improperly accessed, thereby satisfying (b)(5)'s initial condition. However, the remaining territorial hurdle of this subsection is not satisfied, because there is no evidence the Target Computer will be found on U.S.-controlled territory or premises.

2. Fourth Amendment particularity requirement

The Fourth Amendment prescribes that "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*." This particularity requirement arose out of the Founders' experience with abusive general warrants. *See Steagald v. United States,* 451 U.S. 204, 220, 101 S.Ct. 1642, 68 L.Ed.2d 38 (1981); *see generally* William J. Cuddihy, *The Fourth Amendment: Origins and Original Meaning* 602–1791 (2009).

As previously noted, the warrant sought here would authorize two different searches: a search *for* the computer used as an instrumentality of crime, and a search *of* that computer for evidence of criminal activity. Because the latter search presumes the success of the initial search for the Target Computer, it is appropriate to begin the particularity inquiry with that initial search.

The Government's application contains little or no explanation of how the Target Computer will be found. Presumably, the Government would contact the Target Computer via the counterfeit email address, on the assumption that only the actual culprits would have access to that email account. Even if this assumption proved correct, it would not necessarily mean that the government has made contact with the end-point Target Computer at which the culprits are sitting. It is not unusual for those engaged in illegal computer activity to "spoof" Internet Protocol addresses as a way of disguising their actual on-line presence; in such a case the Government's search might be routed through one or more "innocent" computers on its way to the Target Computer. [8] The Government's application offers nothing but indirect and conclusory assurance that its search technique will avoid infecting innocent computers or devices:

> Further, the method in which the software is added to the TARGET COMPUTER is designed to ensure that the [persons] committing the illegal activity will be the only individuals subject to said technology.

Aff.¶ 17. [9] This "method" of software installation is nowhere explained. [10] Nor does the Government explain how it will ensure that only those "committing the illegal activity will be ... subject to the technology." What if the Target Computer is located in a public library, an Internet café, or a workplace accessible to others? What if the computer is used by family or friends uninvolved in the illegal scheme? What if the counterfeit email address is used for legitimate reasons by others unconnected to the criminal conspiracy? What if the

email address is accessed by more than one computer, or by a cell phone and other digital devices? There may well be sufficient answers to these questions, but the Government's application does not supply them.

*5 The court concludes that the revised supporting affidavit does not satisfy the Fourth Amendment's particularity requirement for the requested search warrant for the Target Computer.

3. Constitutional standards for video camera surveillance

As explained above, the Government's data extraction software will activate the Target Computer's built-in-camera and snap photographs sufficient to identify the persons using the computer. The Government couches its description of this technique in terms of "photo monitoring," as opposed to video surveillance, but this is a distinction without a difference. In between snapping photographs, the Government will have real time access to the camera's video feed. That access amounts to video surveillance.

The Fifth Circuit has described video surveillance as "a potentially indiscriminate and most intrusive method of surveillance ." *United States v. Cuevas–Sanchez,* 821 F.2d 248, 250 (5th Cir.1987). In that case the court adopted constitutional standards for such surveillance by borrowing from the statute permitting wiretaps—Title III of the Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. §§ 2510–2520. *Id.,* citing *United States v. Biasucci,* 786 F.2d 504 (2nd Cir.), *cert. denied,* 479 U.S. 827 (1986). Under those standards, a search warrant authorizing video surveillance must demonstrate not only probable cause to believe that evidence of a crime will be captured, but also should include: (1) a factual statement that alternative investigative methods have been tried and failed or reasonably appear to be unlikely to succeed if tried or would be too dangerous; (2) a particular description of the type of communication sought to be intercepted, and a statement of the particular offense to which it relates; (3) a statement of the duration of the order, which shall not be longer than is necessary to achieve the objective of the authorization nor, in any event, longer than 30 days, (though extensions are possible); and (4) a statement of the steps to be taken to assure that the surveillance will be minimized to effectuate only the purposes for which the order is issued. *Cuevas–Sanchez,* 821 F.2d at 252.

The Government's application fails to meet the first and fourth of these criteria, *i.e.* inadequate alternatives and minimization. Regarding the inadequacy of alternative investigative techniques, the Government offers only a conclusory statement:

> Investigative methods that might be alternatives to the use of a camera attached to the TARGET COMPUTER reasonably appear to be unlikely to succeed if tried or would be too dangerous.

Aff. ¶ 14. The Government makes no attempt to explain why this is so. In fact, contemporaneous with this warrant application, the Government also sought and obtained an order under 18 U.S.C. § 2703 directing the Internet service provider to turn over all records related to the counterfeit email account, including the contents of stored communications. To support that application, an FBI agent swore that the ISP's records would likely reveal information about the "identities and whereabouts" of the users of this account. Yet the same agent now swears that no other technique is likely to succeed. The Government cannot have it both ways. *See Cuevas–Sanchez,* 821 F.2d at 250 ("A juxtaposition of such contentions trifles with the Court.") (citation omitted).

*6 As for minimization, the Government has offered little more than vague assurances:

> Steps will be taken to assure that data gathered through the technique will be minimized to effectuate only the purposes for which the warrant is issued. The software is not designed to search for, capture, relay, or distribute personal information or a broad scope of data. The software is designed to capture limited amounts of data, the minimal necessary information to identify the location of the TARGET COMPUTER and the user of TARGET COMPUTER.

Aff. ¶ 17. The steps taken to minimize over-collection of data are left to the court's imagination. The statement that the software is designed to capture only limited amounts of data—"the minimal necessary information needed to identify the location of the Target Computer and the user"— does mitigate the risk of a general search somewhat, but that assurance is fatally undermined by the breadth of

data authorized for extraction in the proposed warrant. *See* Aff. Attach. B, described *supra* at p. 2–3. Software that can retrieve this volume of information—Internet browser history, search terms, e-mail contents and contacts, "chat", instant messaging logs, photographs, correspondence, and records of applications run, among other things—is not fairly described as capturing "only limited amounts of data." Finally, given the unsupported assertion that the software will not be installed on "innocent" computers or devices, there remains a non-trivial possibility that the remote camera surveillance may well transmit images of persons not involved in the illegal activity under investigation.

For these reasons, the Government has not satisfied the Fourth Amendment warrant standards for video surveillance.

Conclusion

The court finds that the Government's warrant request is not supported by the application presented. This is not to say that such a potent investigative technique could never be authorized under Rule 41. And there may well be a good reason to update the territorial limits of that rule in light of advancing computer search technology. But the extremely intrusive nature of such a search requires careful adherence to the strictures of Rule 41 as currently written, not to mention the binding Fourth Amendment precedent for video surveillance in this circuit. For these reasons, the requested search and seizure warrant is denied.

Footnotes

1   At the Government's request, the warrant application has been sealed to avoid jeopardizing the ongoing investigation. This opinion will not be sealed because it deals with a question of law at a level of generality which could not impair the investigation.

2   This appears to be a matter of first impression in this (or any other) circuit. The Court has found no published opinion dealing with such an application, although in 2007 a magistrate judge is known to have issued a warrant authorizing a similar investigative technique to track the source of e-mailed bomb threats against a Washington state high school. *See* Application and Affidavit for Search Warrant, In the Matter of the Search of Any Computer Accessing Electronic Message(s) Directed to Administrator(s) of MySpace Account "Timberlinebombinfo" and Opening Messages Delivered to That Account by the Government at 2, No. MJ07–5114 (W.D. Wash. June 12, 2007), available at http://www.politechbot.com/d ocs/fbi.cipav.sanders.affidavit.071607.pdf.

3   Some scholars have challenged the aptness of the container metaphor, noting that the ever-growing storage capacity of an ordinary hard drive more closely resembles a library than a filing cabinet. *See* Paul Ohm, *Massive Hard Drives, General Warrants, and the Power of Magistrate Judges,* 97 Virginia Law Review In Brief 1, 5–6 (2011).

4   *See generally* H. Marshall Jarrett et al., *U.S. Dep't of Justice, Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* 84–85 (2009), available at http:// www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf.

5   This situation should be distinguished from an anticipatory warrant, which may be issued upon a showing of (1) a fair probability that contraband or evidence of a crime will be found in a particular place if a triggering condition occurs, and (2) probable cause to believe the triggering condition will occur. *United States v. Grubbs,* 547 U.S. 90, 96–97, 126 S.Ct. 1494, 164 L.Ed.2d 195 (2006). Here the "triggering condition" is the installation of software which will "extract" (i.e.seize) the computer data and transmit it to this district. This "triggering condition" is itself a search or seizure that separately requires a warrant.

6   *See* 18 U.S.C. § 3117(b)("an electronic or mechanical device which permits the tracking of the movement of a person or object").

7   According to the Government's application, the Target Computer's last known internet protocol address resolved to a country in Southeast Asia.

8   *See* Neal K. Katyal, *Criminal Law in Cyberspace,* 149 U. Pa. L.Rev. 1003, 1028 (2001).

9   The quoted passage is from the revised affidavit submitted by the FBI agent in response to the court's expressed concerns about the lack of particularity in the initial affidavit.

10   In response to a FOIA request several years ago, the FBI publicly released information about a Web-based surveillance tool called "Computer and Internet Protocol Address Verifier" (CIPAV). *See* https:// www.eff.org/ deeplinks/2011/04/new-fbi-documents-show-depth-government. Although apparently in routine use as a law enforcement tool, the court has found no reported case discussing CIPAV in the context of a Rule 41 search warrant (or any other context, for that matter).