U.S. Department of Justice

Criminal Division

13-CR-B

Assistant Attorney General *Washington, D.C. 20530*

September 18, 2013

The Honorable Reena Raggi
Chair, Advisory Committee on the Criminal Rules
704S United States Courthouse
225 Cadman Plaza East
Brooklyn, NY 11201-1818

Dear Judge Raggi:

The Department of Justice recommends an amendment to Rule 41 of the Federal Rules of Criminal Procedure to update the provisions relating to the territorial limits for searches of electronic storage media. The amendment would establish a court-supervised framework through which law enforcement can successfully investigate and prosecute sophisticated Internet crimes, by authorizing a court in a district where activities related to a crime have occurred to issue a warrant – to be executed via remote access – for electronic storage media and electronically stored information located within or outside that district. The proposed amendment would better enable law enforcement to investigate and prosecute botnets and crimes involving Internet anonymizing technologies, both which pose substantial threats to members of the public.

Background

Rule 41(b) of the Federal Rules of Criminal Procedure authorizes magistrate judges to issue search warrants. In most circumstances, search warrants issue for property that is located within the judge's district. Currently, Rule 41(b) authorizes out-of-district search warrants for: (1) property in the district when the warrant is issued that might be moved outside the district before the warrant is executed; (2) tracking devices, which may be monitored outside the district if installed within the district; (3) investigations of domestic or international terrorism; and (4) property located in a United States territory or a United States diplomatic or consular mission.

Rule 41(b) does not directly address the special circumstances that arise when officers execute search warrants, via remote access, over modern communications networks such as the Internet. Rule 41 should be amended to address two increasingly common situations: (1) where the warrant sufficiently describes the computer to be searched but the district within which that computer is located is unknown, and (2) where the investigation requires law enforcement to coordinate searches of numerous computers in numerous districts.

The first of these circumstances – where investigators can identify the target computer, but not the district in which it is located – is occurring with greater frequency in recent years. Criminals are increasingly using sophisticated anonymizing technologies when they engage in crime over the Internet. For example, a fraudster exchanging email with an intended victim or a child abuser sharing child pornography over the Internet may use proxy services designed to hide his or her true IP address. Proxy services function as intermediaries for Internet communications: when one communicates through an anonymizing proxy service, the communications pass through the proxy, and the recipient of the communications receives the proxy's IP address, rather than the originator's true IP address. There is a substantial public interest in catching and prosecuting criminals who use anonymizing technologies, but locating them can be impossible for law enforcement absent the ability to conduct a remote search of the criminal's computer. Law enforcement may in some circumstances employ software that enables it through a remote search to determine the true IP address or other identifying information associated with the criminal's computer.

Yet even when investigators can satisfy the Fourth Amendment's threshold for obtaining a warrant for the remote search – by describing the computer to be searched with particularity and demonstrating probable cause to believe that the evidence sought via the remote search will aid in a particular apprehension or conviction for a particular offense – a magistrate judge may decline to issue the requested warrant. For example, in a fraud investigation, one magistrate judge recently ruled that an application for a warrant for a remote search did not satisfy the territorial jurisdiction requirements of Rule 41. *See In re Warrant to Search a Target Computer at Premises Unknown,* ___ F. Supp. 2d ___, 2013 WL 1729765 (S.D. Tex. Apr. 22, 2013) (noting that "there may well be a good reason to update the territorial limits of that rule in light of advancing computer search technology").

Second, criminals are using multiple computers in many districts simultaneously as part of complex criminal schemes, and effective investigation and disruption of these schemes often requires remote access to Internet-connected computers in many different districts. For example, thefts in one district may be facilitated by sophisticated attacks launched from computers in multiple other districts. An increasingly common form of online crime involves the surreptitious infection of multiple computers with malicious software that makes them part of a "botnet" – a collection of compromised computers under the remote command and control of a criminal. Botnets may range in size from hundreds to millions of compromised computers, including home, business, and government systems. Botnets are a significant threat to the public: they are used to conduct large-scale denial of service attacks, steal personal and financial data, and distribute malware designed to invade the privacy of users of the host computers.

Effective investigations of these sophisticated crimes often require law enforcement to act in many judicial districts simultaneously. Under the current Rule 41, however, except in cases of domestic or international terrorism, investigators may need to coordinate with agents,

prosecutors, and magistrate judges in every judicial district in which the computers are known to be located to obtain warrants authorizing the remote access of those computers. For example, a large botnet investigation is likely to require action in all 94 districts, but coordinating 94 simultaneous warrants in the 94 districts would be impossible as a practical matter. At a minimum, requiring so many magistrate judges to review virtually identical probable cause affidavits wastes judicial and investigative resources and creates delays that may have adverse consequences for the investigation. Authorizing a court in a district where activities related to a crime have occurred to issue a warrant for electronic storage media within or outside the district would better align Rule 41 with the extent of constitutionally permissible warrants and remove an unnecessary obstruction currently impairing the ability of law enforcement to investigate botnets and other multi-district Internet crimes.

Thus, while the Fourth Amendment permits warrants to issue for remote access to electronic storage media or electronically stored information, Rule 41's language does not anticipate those types of warrants in all cases. Amendment is necessary to clarify the procedural rules that the government should follow when it wishes to apply for these types of warrant.

Language of Proposed Amendment

Our proposed amendment includes two parts. First, we propose adding the following language at the end of subsection (b):

> and (6) a magistrate judge with authority in any district where activities related to a crime may have occurred has authority to issue a warrant, to be executed via remote access, for electronic storage media or electronically stored information located within or outside that district.

Second, we propose adding the following language at the end of subsection (f)(1)(C):

> In a case involving a warrant for remote access to electronic storage media or electronically stored information, the officer executing the warrant must make reasonable efforts to serve a copy of the warrant on an owner or operator of the storage media. Service may be accomplished by any means, including electronic means, reasonably calculated to reach the owner or operator of the storage media. Upon request of the government, the magistrate judge may delay notice as provided in Rule 41(f)(3).

Discussion of Proposed Amendment

The proposed amendment authorizes a court with jurisdiction over the offense being investigated to issue a warrant to remotely search a computer if activities related to the crime under investigation have occurred in the court's district. In other circumstances, the Rules or federal law recognize that it can be appropriate to give magistrate judges nationwide authority to issue search warrants. For example, in terrorism investigations, the current Rule 41(b)(3) allows a magistrate judge "in any district in which activities related to the terrorism may have occurred" to issue a warrant "for a person or property within or outside that district." This approach is also similar to the current rule for a warrant requiring communication service providers to disclose electronic communications: a court with "jurisdiction over the offense being investigated" can issue such a warrant. *See* 18 U.S.C. §§ 2703(a) & 2711(3)(A)(I); *United States v. Bansal,* 663 F.3d 634, 662 (3d Cir. 2011); *United States v. Berkos*, 543 F.3d 392, 397-98 (7th Cir. 2008). Mobile tracking device warrants may authorize the use of tracking devices outside the jurisdiction of the court, so long as the device was installed in that jurisdiction. Fed. R. Crim. P. 41(b)(4); 18 U.S.C. § 3117(a). In the proposed amendment, the phrase "any district where activities related to a crime may have occurred" is the same as the language setting out the jurisdictional scope of Rule 41(b)(3).

The amendment provides that notice of the warrant may be accomplished by any means reasonably calculated to reach an owner or operator of the computer or – as stated in the amendment, which uses existing Rule 41 language – the "storage media or electronically stored information." In many cases, notice is likely to be accomplished electronically; law enforcement may not have a computer owner's name and street address to provide notice through traditional mechanisms. The amendment also requires that the executing officer make reasonable efforts to provide notice. This standard recognizes that in unusual cases, such as where the officer cannot reasonably determine the identity or whereabouts of the owner of the storage media, the officer may be unable to provide notice of the warrant. *Cf.* 18 U.S.C. § 3771(c)(1) (officers "shall make their best efforts to see that the crime victims are notified of … the rights described in subsection (a)").

In light of the presumption against international extraterritorial application, and consistent with the existing language of Rule 41(b)(3), this amendment does not purport to authorize courts to issue warrants that authorize the search of electronic storage media located in a foreign country or countries. The Fourth Amendment does not apply to searches of the property of non-United States persons outside the United States, *see United States v. Verdugo-Urquidez*, 494 U.S. 259, 261 (1990), and the Fourth Amendment's warrant requirement does not apply to searches of United States persons outside the United States. *See United States v. Stokes*, ___ F.3d ___, 2013 WL 3948949 at *8-*9 (7th Cir. Aug. 1, 2013); *In re Terrorist Bombings*, 552 F.3d 157, 170-71 (2d Cir. 2008). Instead, extraterritorial searches of United States persons are subject to the Fourth Amendment's "basic requirement of reasonableness." *Stokes*, 2013 WL 3948949 at

*9; *see also In re Terrorist Bombings*, 552 F.3d at 170 n.7. Under this proposed amendment, law enforcement could seek a warrant either where the electronic media to be searched are within the United States or where the location of the electronic media is unknown. In the latter case, should the media searched prove to be outside the United States, the warrant would have no extraterritorial effect, but the existence of the warrant would support the reasonableness of the search.

* * *

We believe that timely and thorough consideration of this proposed amendment by the Advisory Committee is appropriate. We therefore ask that the Committee act at its November meeting to establish a subcommittee to examine this important issue. Criminals are increasingly using sophisticated technologies that pose technical challenges to law enforcement, and remote searches of computers are often essential to the successful investigation of botnets and crimes involving Internet anonymizing technologies. Moreover, this proposal would ensure a court-supervised framework through which law enforcement could successfully investigate and prosecute such crimes.

We look forward to discussing this with you and the Committee.

Sincerely,

Mythili Raman

Mythili Raman
Acting Assistant Attorney General

cc: Professor Sara Sun Beale, Reporter
Professor Nancy J. King, Reporter