BEWARE OF GOVERNMENT AGENTS BEARING TROJAN HORSES

*Brian L. Owsley**

I. INTRODUCTION

The Government has increasingly sought, with some success,

permission to access the targeted computers of suspects in criminal investigations. Specifically, the applications for search warrants request authority to use a Trojan device to invade a computer in order to gather all manner of information. The most powerful of these devices "can covertly download files, photographs and stored e-mails, or even gather real-time images by activating cameras connected to computers."[1] These Trojan devices are known by a number of different names: data extraction software, network investigative technique ("NIT"), port reader, harvesting program, remote search, CIPAV for Computer and Internet Protocol Address Verifier, or IPAV for Internet Protocol Address Verifier.[2] One of the principal benefits of these types of devices is that they assist law enforcement officials in locating individuals who are using proxy servers or anonymizing their internet activities in order to hide their identities linked to the crimes they perpetrate via the internet.[3]

In a two-year period, the FBI used such devices around the United States in at least sixteen major cities, including Buffalo, Charlotte, Cleveland, Denver, El Paso, Honolulu, Houston, Las Vegas, Los Angeles, Miami, New Orleans, Omaha, Pittsburgh, Philadelphia, Phoenix, and St. Louis.[4] Some within the FBI have argued that the use

---

* Brian L. Owsley, Visiting Assistant Professor, Texas Tech University School of Law; B.A., University of Notre Dame; J.D., Columbia University School of Law; M.I.A., Columbia University School of International and Public Affairs. From 2005 until 2013, the author served as a United States Magistrate Judge for the United States District Court for the Southern District of Texas. This Article was written in the author's private capacity. No official support or endorsement by the United States District Court for the Southern District of Texas or any other division of the federal judiciary is intended or should be inferred.

1. Craig Timberg & Ellen Nakashima, *FBI's Search for 'Mo,' Suspect in Bomb Threats, Highlights Use of Malware for Surveillance*, WASH. POST (Dec. 6, 2013), http://www.washingtonpost.com/business/technology/2013/12/06/352ba174-5397-11e3-9e2c-e1d01116fd98_story.html; *see also* Laura K. Donohue, *FISA Reform*, 10 I/S: J. L. & POL'Y FOR INFO. SOC'Y 599, 623 (2014) ("Network investigative techniques . . . allow the FBI to covertly download files, photographs, and stored emails, or even to activate cameras located on computers, allowing the government to obtain real-time images.").

2. *See* Yale Law School Information Society Project, Law Enforcement and Hacking Conference, LIVESTREAM (Feb. 18, 2014), http://new.livestream.com /yalelaw/LawEnforcementAndHacking (discussion by Laura Donahue); Declan McCullagh, *FBI Pressures Internet Providers to Install Surveillance Software*, CNET (Aug. 2, 2013, 12:26 PM), http://www.cnet.com/news/fbi-pressures-internet-providers-to-install-surveillance-software/; Kevin Poulsen, *Documents: FBI Spyware Has Been Snaring Extortionists, Hackers for Years*, WIRED (Apr. 16, 2009, 9:33 PM), http://www.wired.com/2009/04/fbi-spyware-pro/.

3. Poulsen, *supra* note 2.

4. *See, e.g.*, ELEC. FRONTIER FOUND., https://www.eff.org/files/filenode/cipav/FBI_CIPAV-10.pdf (last visited Mar. 8, 2015); *see also* Jennifer Lynch, *New FBI Documents Provide Details on Government's Surveillance Spyware*, ELEC. FRONTIER FOUND. (Apr. 29, 2011), www.eff.org/deeplinks/2011/04/new-fbi-documents-show-depth-government.

of these devices does not require any judicial authorization.[5]

These various devices are "designed to infiltrate a target's computer and gather a wide range of information, which it secretly sends to an FBI server in eastern Virginia."[6] Much of how the Government uses this type of technology is secret; however, the software has been designed to collect several types of data after infiltrating a computer.[7] Specifically, when the Government is able to use this type of software it may obtain a computer's internet protocol ("IP") address,[8] Media Access Control address, a list of any open ports, a list of any running programs, the operating system along with the version and its serial number, the type and version of the internet browser, the most recently visited URL, the register computer name and company, and the currently logged-in user name.[9]

Imagine being the parent of a child who has engaged in some type of criminal activity involving computers and an email account. The investigating federal agency learns some information, including an email address. Based on this information, an agent applies for a search warrant from the nearest federal magistrate judge to send an electronic surveillance device via the known email address to a computer to obtain additional information. Of course, this information may lead back to the parent's computer and compromise that individual's personal and financial records. Additionally, because the federal agency performs the search based on known information such as an email address, the targeting device may be used on any computer to which the individual with the targeted email address logs on. Such computers could include the computers of family, friends, and even public-access computers at libraries or schools.

This Article addresses the use of Trojan devices by the Government to legally search computers potentially around the world. Although the Government does seek judicial authorization for these techniques based

5. Email message dated Aug. 24, 2005, ELEC. FRONTIER FOUND., https://www.eff.org/files/FBI_CIPAV-14-p36.pdf (last visited Mar. 8, 2015); Lynch, *supra* note 4.

6. Poulsen, *supra* note 2.

7. Kevin Poulsen, *FBI's Secret Spyware Tracks Down Teen Who Made Bomb Threats*, SECLISTS.ORG (July 19, 2007, 12:33 AM), http://seclists.org/isn/2007/Jul/78; Lynch, *supra* note 4.

8. An "Internet Protocol number" is "[t]he unique identification of the location of an end-user's computer, the IP address serves as a routing address for email and other data sent to that computer over the internet from other end-users." Register.com, Inc. v. Verio, Inc., 356 F.3d 393, 407 (2d Cir. 2004). "Every computer connected to the Internet has a unique Internet Protocol ("IP") address, . . . which are long strings of numbers, such as 64.233.161.147." Liberty Media Holdings, LLC v. Letyagin, 925 F. Supp. 2d 1114, 1116 n.2 (D. Nev. 2013); *see also* Orin S. Kerr, *Digital Evidence and the New Criminal Procedure*, 105 COLUM. L. REV. 279, 284 (2005) ("An IP address is the internet equivalent of a telephone number").

9. Poulsen, *supra* note 7; Lynch, *supra* note 4.

on a search warrant, there are still concerns about whether the applications meet constitutional standards as well as Rule 41 of the Federal Rules of Criminal Procedure ("Rule 41").

The use of these Trojan devices has not been addressed in current scholarship meaningfully; therefore, this Article focuses on when and how authorization of search warrant applications for these techniques are appropriate. Part II addresses the implications of the standards enunciated in the Fourth Amendment and Rule 41 in ascertaining whether a search warrant should be issued. Next, Part III discusses four search warrant applications seeking authorization for the techniques discussed in Part II and analyzes whether the search warrants were appropriate. Finally, in Part IV, the Article concludes by addressing the privacy concerns that put these search methods in direct opposition with both constitutional protections and procedural requirements for search warrants. The Article proposes solutions to avoid the overreaching and invasive concerns that the use of Trojan device search methods can create.

II. THE FOURTH AMENDMENT AND RULE 41 CIRCUMSCRIBE THE PARAMETERS IN WHICH APPLICATIONS FOR TROJAN DEVICES ARE PERMITTED

The Government has sought to use these Trojan devices pursuant to a search warrant as compared to other types of electronic surveillance in which the Government has attempted to avoid obtaining a warrant.[10] The framers of the Constitution instilled within the Fourth Amendment "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[11] Additionally, the Fourth Amendment establishes that "no Warrants shall issue, but upon probable cause."[12] Finally, in seeking a search warrant, the agent must describe with particularity "the places to be searched, and the persons or things to be seized."[13]

Rule 41 defines the parameters by which the Government could

10. *See generally* Brian L. Owsley, *The Fourth Amendment Implications of the Government's Use of Cell Tower Dumps in its Electronic Surveillance*, 16 U. PA. J. CONST. L. 1, 15-16 (2013) [hereinafter Owsley, *Cell Tower Dumps*] (discussing the Government's practice of seeking cell tower dumps pursuant to 18 U.S.C. § 2703(d) because it is a lesser standard than Rule 41); Brian L. Owsley, *TriggerFish, StingRays, and Fourth Amendment Fishing Expeditions*, 66 HASTINGS L.J. 183, 199-200 (2014) (discussing the Government's practice of seeking orders authorizing cell site simulators pursuant to the federal pen register statute because it has a very low standard).

11. U.S. CONST. amend. IV.

12. *Id.*

13. *Id.*

obtain a search warrant or other seizures based on a probable cause standard consistent with the Fourth Amendment.[14] Moreover, this rule establishes that a warrant may be issued to obtain "evidence of a crime" or "property designed for use, intended for use, or used in committing a crime."[15] Given that the typical position in each of these warrant applications is that a computer and an email address were being used to perpetrate various crimes, the applications all satisfy Rule 41(c). However, the problem for the Government, and the tension within the case examples that demonstrates at least one was incorrectly decided, is that Rule 41 is not as expansive as the Government would like. Specifically, Rule 41(b) outlines a number of bases in which a magistrate judge has the authority to issue a warrant:

> (1) a magistrate judge with authority in the district—or if none is reasonably available, a judge of a state court of record in the district—has authority to issue a warrant to search for and seize a person or property located within the district;
>
> (2) a magistrate judge with authority in the district has authority to issue a warrant for a person or property outside the district if the person or property is located within the district when the warrant is issued but might move or be moved outside the district before the warrant is executed;
>
> (3) a magistrate judge—in an investigation of domestic terrorism or international terrorism—with authority in any district in which activities related to the terrorism may have occurred has authority to issue a warrant for a person or property within or outside that district;
>
> (4) a magistrate judge with authority in the district has authority to issue a warrant to install within the district a tracking device; the warrant may authorize use of the device to track the movement of a person or property located within the district, outside the district, or both; and
>
> (5) a magistrate judge having authority in any district where activities related to the crime may have occurred, or in the District of Columbia, may issue a warrant for property that is located outside the jurisdiction of any state or district, but within any of the following:
>
> (A) a United States territory, possession, or commonwealth;
>
> (B) the premises—no matter who owns them—of a United States diplomatic or consular mission in a foreign state, including any

14. *See generally* FED. R. CRIM. P. 41.
15. FED. R. CRIM. P. 41(c).

> appurtenant building, part of a building, or land used for the mission's purposes; or
>
> (C) a residence and any appurtenant land owned or leased by the United States and used by United States personnel assigned to a United States diplomatic or consular mission in a foreign state.[16]

In other words, the rule outlines five ways in which magistrate judges have authority to issue search warrants. This subsection of Rule 41 is especially significant given that, in each of the applications regarding Trojan devices, the Government requests the issuance of a search warrant. The issue that arises is whether the issuance of a search warrant is appropriate in a given application.

The first one—subsection (b)(1)—is the most straightforward, indeed virtually axiomatic. A magistrate judge may authorize the search or seizure of property within the district in which the judge sits.[17] The relevant question for the magistrate judge to entertain regarding this subsection is not where the crime occurred, but where the search is to take place.[18] As one commentator explained, "traditionally warrants have only been allowed to search for property in that district."[19]

Subsection (b)(2) is a variation of the first subsection in that it concerns property to be searched or seized within the district even though the property may no longer be in the district at the time the warrant is executed.[20] Thus, while historically there were only a few narrow exceptions that permitted search warrants regarding property outside the magistrate judge's district, those exceptions have been broadened in recent years.[21]

Indeed, most decisions focus on situations in which Rule 41(b)(2) is inapplicable. For example, in *United States v. Glover*, the FBI was

16. FED. R. CRIM. P. 41(b).

17. *See* United States v. Chipps, 410 F.3d 438, 446 (8th Cir. 2005); *see also* United States v. Kernell, No. 3:08-CR-142, 2010 WL 1408437, at *2 (E.D. Tenn. Apr. 2, 2010) ("Rule 41(b) . . . limits a Magistrate Judge's authority to issue warrants only for property within the district."); United States v. Hernandez, No. 3:08-CR-142, 2008 WL 4748576, at *16 (D. Minn. Oct. 28, 2008) ("the jurisdiction of a United States Magistrate Judge which, as a general proposition, is limited to the District in which he or she sits").

18. *See* United States v. McVicker, No. 3:11-CR-00101-SI, 2012 WL 860412, at *2 (D. Or. Mar. 13, 2012).

19. Orin S. Kerr, *The Modest Role of the Warrant Clause in National Security Investigations*, 88 TEX. L. REV. 1669, 1680 (2010) [hereinafter Kerr, *The Modest Role of the Warrant Clause*]; *accord* Orin S. Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 STAN. L. REV. 1005, 1014 (2010) [hereinafter Kerr, *Applying the Fourth Amendment*].

20. *See* United States v. Glover, 736 F.3d 509, 515 (D.C. Cir. 2013); *see also* United States v. Krueger, 998 F. Supp. 2d 1032, 1035 (D. Kan. 2014); *In re* Emachines Computer Model No. S1940, No. C-12-740M, 2012 WL 3259897, at *1-2 (S.D. Tex. July 19, 2012).

21. Kerr, *Applying the Fourth Amendment*, *supra* note 19, at 1014 n.29.

investigating the defendant for distribution of PCP and heroin when it sought and obtained a warrant from a federal judge in the District of Columbia to place a recording device in Glover's truck.[22] Although it was clear at the time of the search warrant application that this truck was parked in the Baltimore area, the warrant nonetheless authorized the agents to enter the truck outside of the District of Columbia.[23] Subsequently, Glover was recorded in this truck discussing his narcotics trafficking business, which led to his arrest and conviction.[24] On appeal, Glover challenged the warrant authorizing the recording device placed in his truck in Maryland.[25] In response, the Government argued "that it is perfectly permissible for a district judge to authorize the placement of such an electronic listening device on a vehicle *anywhere in the United States*."[26] Ultimately, the court concluded that Rule 41(b)(2) was "crystal clear" in that the warrant violated the rule such that any evidence based on the recording device must be excluded.[27]

Similarly, in *United States v. Krueger*, a federal agent was investigating information that the defendant was engaged in the possession and distribution of child pornography.[28] In the course of his investigation, the agent determined that Krueger resided in Emporia, Kansas, for which he in turn was able to get a search warrant issued by a magistrate judge sitting in Wichita, Kansas.[29] During execution of the warrant, the agent learned that Krueger and his computer were in Oklahoma City, Oklahoma.[30] The agent then prepared a second search warrant application, indicating that the computer was in Oklahoma, but nonetheless seeking authorization from a Kansas magistrate judge to seize and search Krueger's computer in Oklahoma.[31] Indeed, the computer was initially seized but not searched in part because of concerns about the warrant issued by the Kansas magistrate judge.[32] In a

22. *Glover*, 736 F.3d at 510.

23. *Id.*; United States v. Vann, No. 07-CR-247(JMR/RLE), 2007 WL 4321969, at *22 (D. Minn. Dec. 6, 2007) (magistrate judge in Minnesota issued a search warrant for a house in Superior, Wisconsin); *see also* United States v. Jones, 132 S. Ct. 945, 948 (U.S. 2012) (a warrant authorizing a GPS tracking device was authorized in the District of Columbia, but executed in Maryland).

24. *Glover*, 736 F.3d at 511.

25. *Id.* at 512.

26. *Id.* (emphasis in original).

27. *Id.* at 515; *Vann*, 2007 WL 4321969, at *22 (magistrate judge in Minnesota had no authority to issue a search warrant for a house in Superior, Wisconsin); *see also Jones*, 132 S. Ct. at 949, 953 (the installation of the GPS tracking device constituted a Fourth Amendment search that required a minimum degree of protection be afforded to the subject of the search).

28. United States v. Krueger, 998 F. Supp. 2d 1032, 1033-34 (D. Kan. 2014).

29. *Id.* at 1034.

30. *Id.*

31. *Id.*

32. *Id.*

motion to suppress, the defendant argued that the second warrant concerning Oklahoma violates Rule 41(b).[33] The Government argued that "the property could have been moved at the time the warrant was requested" so that it satisfied Rule 41(b)(2) and that the rule was ambiguous.[34] The district court rejected these arguments, finding that the warrant was void ab initio and suppressing the evidence from the defendant's computer as well as his statements.[35]

Regarding subsection (b)(3), Congress enacted the USA Patriot Act in 2001,[36] which empowered magistrate judges to authorize search warrants related to both domestic and international terrorism regardless of whether the property to be searched or seized is within the district.[37] Additionally, the Act defined domestic terrorism in order to provide further guidance.[38]

Next, subsection (b)(4) allows magistrate judges to authorize the installation of a tracking device inside a district which would then track the movement of the targeted individual or property inside or outside of that district. This subsection resulted from an amendment to the Federal Rules of Criminal Procedure in 2006.[39] Courts had previously concluded that a warrant was not necessary if the tracking device is installed on a public street on the exterior of a vehicle.[40] However, following the Supreme Court's decision in *Jones*, a warrant was deemed required.[41]

Finally, in 2008, the Federal Rules of Criminal Procedure were again amended to include subsection (b)(5), providing a fifth basis for magistrate judges to authorize search warrants: warrants for crimes outside the district's jurisdiction, but in areas over which the United

33. *Id*. at 1035.

34. *Id.*

35. *Id.* at 1036-37; *see also In re* Emachines Computer Model No. S1940, No. C-12-740M, 2012 WL 3259897, at *1-2 (S.D. Tex. July 19, 2012) (rejecting a search warrant in the Southern District of Texas pursuant to Rule 41(b)(2) for a computer that had been removed from that district and taken to the Western District of Texas).

36. USA Patriot Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001).

37. *Id.* § 219; United States v. Vilar, No. S305CR621KMK, 2007 WL 1075041, at *52 n.33 (S.D.N.Y. Apr. 4, 2007); *see also* Gerald G. Ashdown, *The Blueing of America: The Bridge Between The War On Drugs And The War On Terrorism*, 67 U. PITT. L. REV. 753, 789-90 (2006).

38. USA Patriot Act of 2001 § 802 (codified at 18 U.S.C. § 2331(5) (2012)); *see also id.* § 2331(1) (defining international terrorism).

39. United States v. Asghedom, 992 F. Supp. 2d 1167,1168 (N.D. Ala. 2014); United States v. Hersman, No. 2:13-cr-00002, 2013 WL 1966047, at *8 (S.D. W.Va. May 10, 2013); *see also* 18 U.S.C. § 3117(a) ("a court is empowered to issue a warrant or other order for the installation of a mobile tracking device, such order may authorize the use of that device within the jurisdiction of the court, and outside that jurisdiction if the device is installed in that jurisdiction").

40. United States v. Smith, 387 F. App'x 918, 920-21 (11th Cir. 2010) (per curiam).

41. *Asghedom*, 992 F. Supp. 2d at 1170-71 (discussing United States v. Jones, 132 S. Ct. 945 (U.S. 2012)).

States exercises control.[42] This area ranges from territories of the United States such as Guam or the Virgin Islands to the various American diplomatic and consular buildings around the world.

III. BOTH RULE 41 AND THE FOURTH AMENDMENT RAISE QUESTIONS ABOUT WHETHER THE GOVERNMENT'S SEARCH WARRANT APPLICATIONS FOR TROJAN DEVICES SHOULD SO READILY BE GRANTED

Although there are anecdotal reports of dozens of applications by federal agents using Trojan devices, there are not nearly as many examples available for analysis. No doubt, the paucity of examples is partly because the FBI wants to keep the use of this technology from public knowledge.[43] Moreover, these applications are sealed when filed, and often judges do not unseal such applications.[44] To the extent that the Government is putting more judicial records online, any searches would be thwarted by the limited availability of sealed records in electronic databases.[45] Consequently, without knowing specific file numbers, anyone researching these types of applications must manually search through the dockets of each federal courthouse in the hopes of finding some record that would by its meager caption or description indicate it is an application for a Trojan device.

Alternatively, a researcher or an investigator could attempt to use the Freedom of Information Act ("FOIA")[46] to obtain information regarding such applications. However, such requests are not likely to bear much fruit. Quite likely, the Government would assert that such

42. Kerr, *The Modest Role of the Warrant Clause*, *supra* note 19, at 1680-81; *see also* David A. Schlueter, *Criminal Procedure Rules Pending Public Comment*, 21 CRIM. JUST. 45, 45-46 (2007) ("The proposed addition of new Rule 41(b)(5) is intended to fill a perceived gap in the authority of magistrate judges to issue search warrants for property located outside the United States but within the jurisdictional control of the United States.").

43. *See* Declan McCullagh, *FBI Remotely Installs Spyware to Trace Bomb Threat*, CNET (July 18, 2007, 9:42 AM), http://www.cnet.com/news/fbi-remotely-installs-spyware-to-trace-bomb-threat/; Application and Affidavit for Search Warrant at 5, *In re* Any Computer Accessing Electronic Message(s) Directed to Administrator(s) of MySpace Account "Timberlinebombinfo" and Opening Message(s) Delivered to That Account by the Government, No. 07-mj-5114 (W.D. Wash. June 12, 2007) [hereinafter In re *"Timberlinebombinfo" Application*].

44. *See generally* Brian L. Owsley, *To Unseal or Not to Unseal: The Judiciary's Role in Preventing Transparency in Electronic Surveillance Applications and Orders*, 5 CALIF. L. REV. CIRCUIT 259 (2014).

45. The E-Government Act of 2002 was enacted mandating that the federal government, including the judiciary, make information electronically available to the public. Pub. L. 107-347, § 205, 115 Stat. 2899 (2002); *see also* 44 U.S.C. § 3501 (2012).

46. 5 U.S.C. § 552 (2012).

information is exempt from FOIA for national security reasons.[47] This exemption would be available in any case involving terrorism. Alternatively, the FBI could argue that the law enforcement exemption would apply regarding its investigations and electronic surveillance techniques.[48]

That leaves us with just a few exemplars of the use of these devices. As becomes evident, the federal government makes many similar representations, explanations, and descriptions regarding Trojan devices.

A. The Western District of Washington

1. Facts and Circumstances

In June 2007, an agent with the FBI investigating a series of bomb threats against a Lacey, Washington high school filed a search warrant seeking authorization to install a Trojan device on any computer accessing a MySpace account.[49] Specifically, the agent alleged that he had probable cause to use a CIPAV on the MySpace "Timberlinebombinfo" account as well as several email addresses.[50]

The agent explained the technology by noting that "a CIPAV utilizes standard Internet computer commands commonly used commercially over local area networks (LANs) and the Internet to request that an activating computer respond to the CIPAV by sending network level messages, and/or other variables, and/or registry information, over the Internet to a computer controlled by the FBI."[51] He further cautioned that "[t]he exact nature of these commands, processes, capabilities and their configuration is classified as a law enforcement sensitive investigative technique, the disclosure of which would likely jeopardize other on-going investigations and/or future use of the technique."[52] Finally, he described the information that would likely be

47. *Id.* § 552(b)(1); *accord* Students Against Genocide v. Dep't of State, 257 F.3d 828, 833 (D.C. Cir. 2001); *see also* Milner v. Dep't of Navy, 131 S. Ct. 1259, 1271 (U.S. 2011) (citing 5 U.S.C. § 552(b)(1)) ("[T]he Government has other tools at hand to shield national security information and other sensitive materials. Most notably, Exemption 1 of FOIA prevents access to classified documents."); *see also* In re "*Timberlinebombinfo" Application*, *supra* note 43, at 5.

48. 5 U.S.C. § 552(b)(7)(E); *accord* Citizens for Responsibility and Ethics in Washington v. U.S. Dep't of Justice, 746 F.3d 1082, 1101-02 (D.C. Cir. 2014); Public Employees for Envt'l Responsibility v. U.S. Section, Int'l Boundary and Water Comm'n, U.S.-Mex., 740 F.3d 195, 202 (D.C. Cir. 2014).

49. In re "*Timberlinebombinfo" Application*, *supra* note 43; *see generally* Paul Ohm, *Good Enough Privacy*, 2008 U. CHI. LEGAL F. 1, 26-28 (2008) (discussing the case).

50. In re "*Timberlinebombinfo" Application*, *supra* note 43, at 4.

51. *Id.* at 4-5.

52. *Id.* at 5.

obtained by the use of the CIPAV: "the computer's true assigned IP address, MAC address, open communications ports, list of running programs, operating system (type, version, and serial number), internet browser and version, language encoding, registered computer name, registered company name, current logged-in user name, and Uniform Resource Locator (URL) that the target computer was previously connected to."[53]

On May 30, 2007, school officials evacuated Timberline High School in Lacey, Washington, after discovering a handwritten bomb threat note.[54] On June 4, 2007, they received an email from dougbriggs123@gmail.com indicating that "I will be blowing up your school Monday, June 4, 2007. There are 4 bombs planted throughout timberline high school. One in the math hall, library hall, main office and one portable. The bombs will go off in 5 minute intervals at 9:15 AM."[55] The sender further threatened that "[t]he email server of your district will be offline starting at 8:45 am," and subsequently the school district experienced a Denial-of-Service attack.[56] As a result, school officials evacuated Timberline High School.[57]

The next day, Timberline High School officials received an email from dougbrigs@gmail.com with another bomb threat:

> Now that the school is scared from yesturdays [sic] fake bomb threat it's now time to get serious. One in a gym locker, the girls. It's in a locker hidden under a pile of clothes. The other four I will only say the general location. One in the Language Hall, One in the math hall, One underneath a portable taped with strong ducktape [sic]. This bomb will go off if any vibrations are felt. And the last one, Is in a locker. It is enclosed in a soundproof package, and litteraly [sic] undetectable. I have used a variety of chemicals to make the bombs. They are all different kinds. They will go off at 10:15AM. Through remote detonation. Good Luck.[58]

Additionally, the message challenged and taunted the reader about the lack of success in gathering information about yesterday's threat. Specifically, it indicated that the email account was created in Italy and

53. *Id.*; Nate Anderson, *FBI Uses Spyware to Bust Bomb Threat Hoaxster*, ARS TECHNICA (July 18, 2007, 11:34 AM), http://arstechnica.com/security/2007/07/fbi-uses-virus-to-bust-bomb-threat-hoaxster/; *see also* Poulsen, *supra* note 7; Lynch, *supra* note 4.

54. In re "*Timberlinebombinfo" Application*, *supra* note 43, at 6.

55. *Id.* at 6-7. The dougbriggs123@gmail.com account was created on June 3, 2007, with the IP address of 80.76.80.103. *Id.* at 10-11.

56. In re "*Timberlinebombinfo" Application*, *supra* note 43, at 7.

57. *Id.*

58. *Id.*

the sender unidentifiable.[59] Later that day, school officials received another email from dougbriggs234@gmail.com:

> Hello Again. Seeing as how you're too stupid to trace the email back lets [sic] get serious." [The UNSUB(s) mentions 6 bombs set to detonate between 10:45-11:15 AM, and adds] Seriously, you are not going to catch me. So just give up. Maybe you should hire Bill Gates to tell you that it is coming from Italy. HAHAHA Oh wait I already told you that. So stop pretending to be "tracing it" because I have already told you it's coming from Italy. That is where trace will stop so just stop trying. [60]

Based on these two emails, school officials evacuated the high school that day.

On June 6, 2007, the Timberline High School principal received an email from dougbriggs911@gmail.com telling him to "ENJOY YOUR LIFE ENDING."[61] That same day, a second email from this account explicitly threatened the school as well as taunted those who were seeking his identity:

> Well hello Timberline, today is June 6, 2007 and I"M [sic] just emailing you today to say that school will blow up and that's final! There are 2 bombs this time (Iran [sic] short on money to buy things at home depot). They will go off at exactly 10:45:00 AM. One is located on a portable. And the other is somewhere else. Keep trying to 'trace' this email. The only thing you will be able to track is that it came from Italy. There is no other information that leads it back to the United States in any way so get over it. You should hire Bill Gates to track it for you. Also, stop advising teachers to no [sic] show this email to classmates. Everyone would be ammused [sic] by this email and I might stop if you do. Funny how I can trick you all into thinking that I included my name to show that it isn't me, because who the hell would put their name? . . . .[62]

Again, school officials evacuated the high school that day.

On June 7, 2007, another threat was sent to the school by email from thisisfromitaly@gmail.com: "There are 3 bombs planted in the school and they're all different kinds. I have premade these weeks in advance and tested the timers to make sure they work to the exact millisecond. Locking the doors is a good plan, but too late."[63] Based on

59. *Id.*
60. *Id.* at 8.
61. *Id.*
62. *Id.*
63. *Id.* at 8-9.

this threat, Timberline High School was evacuated again.

On June 7, 2007, the agent alleged that the subject of the investigation posed three threatening messages in the comments section of a local online newspaper. After the newspaper removed them, they were posted again before the newspaper disabled the comments section.[64] These threats came from IP address 192.135.29.30, which was associated with the National Institute of Nuclear Physics in Italy.[65]

Additionally on June 7, 2007, the county sheriff's office advised the Lacey Police Department about an individual who complained of receiving a MySpace invitation from the "Timberlineinfo" MySpace profile wanting her to post "htttp://bombermails.hypephp.com" on her MySpace page.[66] If she failed to do as requested, she was warned that her name would be associated with future bomb threats.[67] The parent of a Timberline High School student also called about a similar request and threat that her son received.[68] In total, 33 students reported similar requests and threats, but none of them ultimately had any useful information.[69]

Two of the individuals who received a MySpace invitation from "Timberlineinfo" accepted the invitation and then received an instant message from screen name "Alexspi3ring_09."[70] When one of the individuals sent a message regarding more information about the bomb threats, the instant messages from the sender stopped.[71] Alex Spiering was a student at Timberline High School at that time and used to have a MySpace webpage with the same graphics as those used in the instant messages.[72]

On June 8, 2007, district school officials received two separate bomb threats from Timberline.Sucks@gmail.com.[73] Consequently, Timberline High School was evacuated.

The IP for dougbriggs123@gmail.com and the "Timberlinebombinfo" MySpace account were both the same: 80.76.80.103.[74] This IP address was associated with an Italian internet

64. *Id.* at 9.
65. *Id.* at 12.
66. *Id.* at 9.
67. *Id.*
68. *Id.*
69. *Id.*
70. *Id.* at 9-10.
71. *Id.* at 10.
72. *Id.*
73. *Id.*
74. *Id.* at 10-12.

provider.[75]

On June 12, 2007, a federal magistrate judge authorized the search warrant for the MySpace account "Timberlinebombinfo."[76] The next day, the FBI executed the CIPAV on the targeted computer via the internet and obtained a CD-ROM worth of data.[77] Within a couple of days, based on the Government's use of a CIPAV, a tenth-grader was arrested and charged with making the bomb threats.[78] This person, who was fifteen-years-old at the time of arrest, pled guilty to making bomb threats, harassment, and identity theft for which he received ninety days in a juvenile facility.[79]

2. The Court's Rationale

Although in hindsight it is apparent that the computer was within the Western District of Washington when the warrant was issued, there was no evidence in the application to establish this fact; thus, neither Rule 41(b)(1) or Rule 41(b)(2) applied in this case.[80] Similarly, the agent was not requesting a tracking device, so Rule 41(b)(4) did not apply.[81] Finally, Rule 41(b)(5) did not apply because it was not alleged that the computer was on United States territory or property.[82]

That left just Rule 41(b)(3) as the territorial basis for any search warrant. Although the application did not mention this subsection, it did explain that the warrant sought information for a criminal investigation into both an interstate transmission of a communication containing a threat to injure a person as well as the use of a computer to cause a threat to public safety.[83] The making of bomb threats constitutes terrorism.[84] Here, the application met the territorial requirement based on an investigation of terrorism so that the specific location of the computer was legally irrelevant.

75. *Id.* at 11.

76. In re "*Timberlinebombinfo" Application*, *supra* note 43.

77. Anderson, *supra* note 53.

78. Seattle Times Staff, *Lacey 10th-grader Arrested in Threats to Bomb School*, SEATTLE TIMES (June 14, 2007, 4:01 PM), http://seattletimes.com/html/localnews/2003747761_webthreats14m.html.

79. McCullagh, *supra* note 43.

80. *See generally* In re "*Timberlinebombinfo" Application*, *supra* note 43.

81. *Id.*

82. *Id.*

83. *Id.* at ¶¶ 4, 5, 16.

84. *See, e.g.*, United States v. Garey, 546 F.3d 1359, 1361 (11th Cir. 2008) (per curiam).

B. The District of Colorado

1. Facts and Circumstances

In October 2012, a federal agent with the Bureau of Alcohol, Tobacco, Firearms and Explosives sought a search warrant from a United States magistrate judge in the District of Colorado.[85] Specifically, the agent sought to search "the computer activating the network investigative technique ('NIT') that may assist in identifying the computer, its location, other information about the computer, and the user of the computer."[86] In the application, he requested a long list of information, including the targeted computer's IP address; its media access control address; its open communication ports; the names of programs it was operating, including the name and version of the web browser; the type of operating system run by the computer; its time zone information; its language encoding and default language; wire and wireless internet network connection information; user name and accounts; and previously used URLs.[87]

The special agent testified that the initial contact with the subject of the investigation took place on July 22, 2012, when he telephoned the Arapahoe County Sheriff's Office with a bomb threat.[88] Specifically, the caller, who identified himself as Andrew Ryan and spoke with an accent, sought the release of James Holmes[89] from custody.[90] He threatened to blow up the Arapahoe County Jail with a bomb made of ammonium nitrate if James Holmes was not released.[91] The deputy sheriffs determined that the caller was using a voice over internet connection with telephone number (760) 705-8888.[92] Because of the poor quality of the internet connection as well as the subject's accent, the deputy

85. Application for a Search Warrant, *In re* Network Investigative Technique ("NIT") for email address texas.slayer@yahoo.com, No. 1:12-sw-05685-KMT (D. Colo. Oct. 9, 2012) [hereinafter In re *NIT for texas.slayer@yahoo.com*]; Steven M. Bellovin et al., *Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet*, 12 NW. J. TECH. & INTELL. PROP. 1, 83 (2014) (characterizing this as the first time that the FBI sought a search warrant for a CIPAV).

86. Application for a Search Warrant, *supra* note 85, at Attachment A.

87. *Id.* at Attachment B.

88. *Id.* at 3 (Affidavit of Craig Roegner, ¶ 4 [hereinafter Roegner]).

89. James Holmes is the suspect charged with killing twelve people in an Aurora, Colorado, movie theater on July 20, 2012. *See* Jack Healy, *Mental Evaluations Endorse Insanity Plea in Colorado Shootings, Defense Says*, N.Y. TIMES (May 13, 2013), www.nytimes.com/2013/05/14/us/james-holmes-aurora-shooting-suspect-enters-insanity-plea.html?_r=0.

90. Roegner, supra note 88, ¶ 4; *see also* Yale Law School Information Society Project, *supra* note 2 (discussion by Laura Donahue).

91. Roegner, supra note 88, ¶ 4.

92. *Id.*

sheriffs conducted a written conversation with the caller through the email account soozanvf@gmail.com.[93]

Over the next several days, a person, who spoke with an accent identifying himself as Andrew Ryan, contacted the Arapahoe County Sheriff's Department threatening to blow up the county jail if James Holmes was not released. These calls were made using telephone number (760) 705-8888.[94] Moreover, deputies received similar threats from the email account soozanvf@gmail.com.[95]

On July 25, 2012, a person, who spoke with an accent identifying himself as Andrew Ryan, contacted the Arapahoe County Sheriff's Department using telephone number (760) 705-8888 and informed them that he and his associates had shot and killed three people at the Cherry Creek Reservoir in Arapahoe County and left them in the reservoir.[96] A search ultimately revealed no victims.

On July 30, 2012, the Greenwood Village Police Department received a telephone call about a bomb threat to blow up a Doubletree Hotel. A police officer was sent to the hotel because the person making the threats was still on the phone. When the officer arrived, he spoke on the telephone with a man who had an accent also identifying himself as Andrew Ryan. This caller told the officer that he had placed bombs made with ammonium nitrate in the hotel to blow it up if James Holmes was not released.[97] While the officer was talking with the caller, he heard another person telling the caller how many bombs were in the hotel and how much time remained before they exploded. After evacuating the hotel, a search did not reveal any bombs. However, this time, the caller used phone number (877) 573-9800, which was a Voice Over Internet Protocol server phone number.[98]

On the morning of July 31, 2012, a person, who spoke with an accent again identifying himself as Andrew Ryan, contacted the Denver International Airport. He claimed that he and his friends had placed bombs on airplanes and in the baggage area, threatening to blow up the airport if James Holmes was not released.[99] Caller identification revealed that the telephone call was made from (760) 705-8888, which

93. *Id.*
94. *Id.* ¶¶ 6-7.
95. *Id.* ¶ 5.
96. *Id.* ¶ 8.
97. *Id.* ¶ 9.
98. *Id.* ¶ 10.
99. *Id.* ¶ 12; *see also* Will C. Holden, *Denver International Airport Confirms Non-specific Bomb Threat*, FOX 31 DENVER (July 31, 2012, 2:11 PM), http://kdvr.com/2012/07/31/denver-international-airport-confirms-non-specific-bomb-threat/.

was assigned to the Google Voice G-mail system.[100]

On the afternoon of August 14, 2012, a telephone call to officials with the county jail in Aurora, Colorado, warned of a bomb threat. The caller identified himself as Alex Anderson and threatened to put ammonium nitrate bombs around Aurora if James Holmes was not released. This call was again made using telephone number (760) 705-8888 through the Google voice system.[101]

On the evening of September 12, 2012, a person, identifying himself as Jason, called the Denver International Airport to report that an ammonium nitrate bomb was checked onto United Flight 6318 to Fargo, North Dakota, and was set to detonate upon arrival. He further indicated that he was affiliated with Al Qaeda and was going to blow up the airplane in response to American military actions. This call also was made using telephone number (760) 705-8888 through the Google voice system.[102]

On September 9, 2012, a person emailed some photographs to a Denver police sergeant from soozanvf@gmail.com, including one of an Iranian man in a military uniform. The sender told the sergeant that his name was Mohammed.[103] On September 16, 2012, Mohammed again contacted the sergeant indicating that he had made bomb threats to the University of Texas and North Dakota State University. He further explained that because his soozanvf@gmail.com had been disabled by Google, he could now be reached at Texas.Slayer@yahoo.com.[104] The sergeant received several emails from this new account in which Mohammed admitted to making bomb threats against numerous universities and airports across the United States.[105]

On October 9, 2012, the magistrate judge authorized a search warrant for the Network Investigative Technique of the email address for Texas.Slayer@yahoo.com.[106] On October 19, 2012, the federal agent filed an application for an amended search warrant in order to "better clarif[y] how the NIT will function."[107] These clarifications sought to explain more clearly how the device authorized by the search warrant would be used.[108] Moreover, the affidavit contained some handwritten

100. Roegner, *supra* note 88, ¶ 12.

101. *Id.* ¶ 15.

102. *Id.* ¶ 17.

103. *Id.* ¶ 16; *see also* Yale Law School Information Society Project, *supra* note 2 (discussion by Laura Donahue); Timberg & Nakashima, *supra* note 1.

104. Roegner, *supra* note 88, ¶ 18.

105. *Id.* ¶¶ 22-23.

106. Search Warrant, In re *NIT for texas.slayer@yahoo.com*, No. 1:12-sw-05685-KMT.

107. Roegner, *supra* note 88, ¶ 4.

108. *Id.* ¶¶ 17 n.1, 20 n.2, 21 nn.3-4.

addenda by the agent. For example, he noted that the "crime being investigated is an offense involving international or domestic terrorism [so that the] warrant is sought under Fed. R. Crim. P. 41(b)(3)."[109] Moreover, he assured the magistrate judge that the warrant "does not seek live content of any email messages."[110] On October 19, 2012, the magistrate judge authorized the amended search warrant for the Network Investigative Technique of the email address for "Texas.Slayer@yahoo.com."[111]

On October 29, 2012, a task force officer filed an application for a second amended search warrant in order to correct typographical errors in the first two applications.[112] That same day, the magistrate judge authorized the second amended search warrant for the Network Investigative Technique of the email address for Texas.Slayer@yahoo.com.[113]

On December 11, 2012, a task force officer filed an application for a third amended search warrant in order to "deploy a newly designed NIT after execution of the original NIT was aborted because it was determined that the original NIT was not viable as first designed."[114] On that same day, the magistrate judge authorized the third amended search warrant for the Network Investigative Technique of the email address for Texas.Slayer@yahoo.com.[115]

On December 14, 2012, the NIT was executed by sending a link to Texas.Slayer@yahoo.com. The federal agent indicated that the NIT was only partially successful in that the program in the link did not execute as designed.[116] Nonetheless, the search resulted in information that implicated two IP addresses located in Iran.[117]

109. *Id.* ¶ 19; *see also* FED. R. CRIM. P. 41(b)(3).

110. Roegner, *supra* note 88, ¶ 20.

111. Amended Search Warrant, In re *NIT for texas.slayer@yahoo.com*, No. 1:12-sw-05685-KMT.

112. Second Amended Application for a Search Warrant, In re *NIT for texas.slayer@yahoo.com*, No. 1:12-sw-05685-KMT (Affidavit of William Gallegos, ¶ 5).

113. Second Amended Search Warrant, In re *NIT for texas.slayer@yahoo.com*, No. 1:12-sw-05685-KMT.

114. Third Amended Application for a Search Warrant, In re *NIT for texas.slayer@yahoo.com*, No. 1:12-sw-05685-KMT (Affidavit of William Gallegos, ¶ 6) [hereinafter Gallegos].

115. Third Amended Search Warrant, In re *NIT for texas.slayer@yahoo.com*, No. 1:12-sw-05685-KMT.

116. Return, In re *NIT for texas.slayer@yahoo.com*, No. 1:12-sw-05685-KMT; Timberg & Nakashima, *supra* note 1.

117. *See* sources cited *supra* note 116.

2. The Court's Rationale

In the application concerning bomb threats by Mohammed seeking the release of James Holmes, the magistrate judge did not issue any decision but simply signed the search warrant, authorizing the use of the NIT. The federal agent specifically indicated that the warrant was sought pursuant to Rule 41(b)(3) because the underlying criminal offense involved terrorism.[118] In other words, the FBI acknowledged that only subsection (b)(3) established the requisite territorial standard.

Looking at the applicability of Rule 41(b)(3), the agent provided a significant amount of information related to the crimes involving bomb threats and hoaxes. Moreover, in analyzing the particularity requirement, this same information was beneficial in finding that standard was satisfied. Indeed, there was enough evidence within the application to support a finding of probable cause justifying the search for the computer because it was involved in criminal activity as well as a search of the computer using the NIT to obtain evidence of the crime.[119]

C. The Western District of Texas

1. Facts and Circumstances

On December 18, 2012, a federal agent with the FBI sought a search warrant from a United States magistrate judge in the Western District of Texas.[120] Specifically, he wanted to utilize an NIT in order to send communications to the targeted computer through an email address to "help identify the computer, its location, other information about the computer, and the user of the computer."[121] In the application, he requested a long list of information, including the targeted computer's IP address; its media access control address; its open communication ports; the names of programs it is operating, including the name and version of the web browser; the type of operating system run by the computer; its time zone information; its language encoding and default language; wire and wireless internet network connection information; user name and accounts; and previously used URLs.[122]

118. Roegner, *supra* note 88, ¶ 19; Gallegos, *supra* note 114, ¶ 32.

119. *See In re* Warrant to Search a Target Computer at Premises Unknown, 958 F. Supp. 2d 753, 758-59 (S.D. Tex. 2013).

120. Application for a Search Warrant, *In re* Network Investigative Technique (NIT) for Email Address 512SocialMedia@gmail.com, No. 1:12-mj-748 (W.D. Tex. Dec. 18, 2012) [hereinafter In re *NIT for 512SocialMedia@gmail.com*].

121. *Id.* at 7 (Affidavit of Justin Noble, ¶ 6 [hereinafter Noble]).

122. *Id.* at Attachment B.

In support of the application, the agent asserted there was probable cause to believe that the email address 512SocialMedia@gmail.com was being used by Donald Lee Phelps, a fugitive from federal custody.[123] Specifically, Phelps was wanted for allegedly defrauding financial institutions.[124]

Starting in 2005, Phelps was alleged to have assumed the identity of his girlfriend's estranged husband who was serving in the United States military in Iraq at that time.[125] First, he obtained a Florida state-issued identification card in the husband's name after altering a Texas driver's license. In turn, he used the newly-obtained Florida ID to open an account with a credit union and to get a job at a credit union.[126] Eventually, he wrote checks from this account for various expenses as well as obtained credit cards and loans in his stolen identity. On October 16, 2007, a federal arrest warrant was issued for Phelps for bank fraud.[127]

On November 14, 2012, a confidential informant provided law enforcement officers with a cell phone number for Phelps.[128] This person explained that Phelps had been living in the Austin, Texas, area for about five years. Using the assumed name of James Bridges, Phelps operated a business named Extreme Social Media and worked as a computer programmer. The confidential informant regularly spoke with Phelps on the cell phone number that was provided to law enforcement.[129]

On November 20, 2012, a federal magistrate judge signed a search warrant that authorized federal agents to track Phelps based on the cell phone number provided by the confidential informant. The next day, they tracked the cell phone to a hotel in San Antonio, Texas. When agents arrived at the hotel, employees identified Phelps from a photograph as a guest of the hotel who had checked out of his room earlier that day. Phelps had registered using a different false name, Jack Rady, and paid cash for his room.[130]

On December 3, 2012, the FBI learned that Phelps was using the email address JBridges007@gmail.com. The next day, the IP address was obtained from Google for that email address. It was further

123. Noble, *supra* note 121, ¶ 1.
124. *Id.* ¶ 4.
125. *Id.*; Timberg & Nakashima, *supra* note 1.
126. Noble, *supra* note 121, ¶ 4.
127. *Id.*
128. *Id.* ¶ 5.
129. *Id.* ¶ 6.
130. *Id.* ¶ 7.

discovered that Phelps was using an IP anonymizer known as "HideMyAss.com" to hide the IP address that he was actually using to access his email account.[131]

On December 10, 2012, a second confidential informant provided the 512SocialMedia@gmail.com as an email address used by Phelps.[132] This person was able to identify a photograph of Phelps.[133] Moreover, that person also provided an account number at Amplify Credit Union that Phelps was using.[134] This credit union account was the account for Extreme Social Media, the business operated by Phelps. Although this account was overdrawn, someone accessed it through the internet on December 8, 2012, from a computer using "HideMyAss.com" to hide the user's true IP address.[135]

On December 18, 2012, a magistrate judge signed the search warrant authorizing the NIT for 512SocialMedia@gmail.com.[136] On December 20, 2012, federal agents conducted the search.[137] The search warrant return revealed an IP address that was controlled by a provider in Austin, Texas.[138] The device was tracked to a computer, and the NIT revealed the computer was a Hewlett-Packard using Windows 7 Home Premium with 3561 MB of total Random Access Memory, with 959 MB of remaining for use, and a total of 589,663 MB on the hard disk, with 512,540 MB remaining.[139] Additionally, it revealed information about the central processing unit as well as extensive application lists of various software.[140]

Ultimately, Phelps was apprehended in Alabama and indicted for bank fraud and aggravated identity theft in the Northern District of Florida. On April 3, 2012, he pleaded guilty to both charges and was sentenced to five years in custody on July 17, 2012.[141]

131. *Id.* ¶ 8.

132. *Id.* ¶ 9.

133. *Id.* ¶ 11.

134. *Id.* ¶ 9.

135. *Id.* ¶ 11.

136. Search Warrant, In re *NIT for 512SocialMedia@gmail.com*, No. 1:12-mj-748 (W.D. Tex. Dec. 18, 2012).

137. Return at 2, In re *NIT for 512SocialMedia@gmail.com*, No. 1:12-mj-748.

138. *Id.* at 3.

139. *Id.* at 4.

140. *Id.*

141. Press Release, FBI, Jacksonville Division, Former Gainesville Resident Sentenced for Bank Fraud and Identity Theft (July 18, 2013), *available at* http://www.fbi.gov/jacksonville/press-releases/2013/former-gainesville-resident-sentenced-for-bank-fraud-and-identity-theft; Timberg & Nakashima, *supra* note 1.

2. The Court's Rationale

In the application for the search warrant targeting Donald Phelps' email address, the magistrate judge again did not issue any written decision, but simply signed the form authorizing the use of the NIT. Here, the underlying criminal offense was bank fraud.[142] In other words, the agent did not allege anything that would establish a claim of terrorism.[143] Thus, the territorial limitation that existed in the Colorado example did not exist here.

The application provided no evidence that the computer was within the district at the time the search warrant was sought. Consequently, Rule 41(b)(1) did not provide a basis for granting the application.[144] Similarly, because there was no evidence of the computer's location, Rule 41(b)(2) was also inapplicable because location within the district at the time the warrant was issued was a requirement.[145] Because the application did not seek authorization for a tracking device, Rule 41(b)(4) did not provide any basis for the issuance of a warrant.[146] Lastly, Rule 41(b)(5) was inapplicable because the computer was not located in a United States territory or diplomatic building.

Thus, without even addressing the particularity requirement, there is a strong argument that this warrant was improvidently granted. Of course, it does not appear that the warrant's issuance played any part in the capture of Donald Phelps, so there was no incentive for him to challenge it after his arrest.

D. The Southern District of Texas

1. Facts and Circumstances

In early 2013, an FBI agent sought a search warrant to target an unknown computer that allegedly was involved in violating federal laws regarding bank fraud, computer security, and identity theft. Specifically, the agent sought "to surreptitiously install data extraction software on the Target Computer [that will then] search the computer's hard drive, random access memory, and other storage media; . . . activate the computer's built-in camera; . . . generate latitude and longitude

142. Noble, *supra* note 121, ¶ 4.

143. *Id.*

144. *See* United States v. Chipps, 410 F.3d 438, 446 (8th Cir. 2005); United States v. Kernell, No. 3:08-CR-142, 2010 WL 1408437, at *2 (E.D. Tenn. Apr. 2, 2010).

145. *See* United States v. Glover, 736 F.3d 509, 515; United States v. Krueger, 998 F. Supp. 2d 1032, 1035 (D. Kan. 2014).

146. *See* United States v. Asghedom, 992 F. Supp. 2d 1167, 1174-75 (N.D. Ala. 2014).

coordinates for the computer's location; and . . . transmit the data to FBI agents within this district" for a monitoring period of thirty days.[147] He requested this warrant in order to obtain a list of information from the Target Computer, including "records of Internet Protocol addresses used"; "records of internet activity"; "records evidencing the use of the Internet Protocol addresses to communicate with the [victim's bank's] email servers"; "evidence of who used, owned, or controlled the TARGET COMPUTER" during the alleged criminal activity; and "evidence of times that the TARGET COMPUTER was used."[148] Additionally, because the warrant sought monitoring to continue forward for thirty days from the time that the surveillance device was installed, the application also asked for prospective data, including "accounting entries reflecting the identification of new fraud victims"; "photographs . . . taken using the TARGET COMPUTER's built-in camera . . . to identify the location of the TARGET COMPUTER and identify persons using" it; and "information about the TARGET COMPUTER's physical location, including latitude and longitude calculations."[149] Essentially, the application sought authorization for the device to enable them, through the computer, to take a photograph of the computer user. This would give the agents not only facial recognition, but longitude and latitude information for the computer that would enable law enforcement officials to pinpoint geographical location.[150]

In support of the application, the agent testified that an individual's personal email account and the victim's local bank account were improperly accessed.[151] The IP address for the computer that accessed this victim's account was located in a foreign country.[152] Once the victim took measures to secure his email account, a second email account with an email address nearly identical to the victim's personal email address was created. This second email address differed from the

147. *In re* Warrant to Search a Target Computer at Premises Unknown, 958 F. Supp. 2d 753, 755 (S.D. Tex. 2013); *see also* Yale Law School Information Society Project, *supra* note 2 (discussion by Magistrate Judge Stephen Smith).

148. *In re* Warrant to Search a Target Computer at Premises Unknown, 958 F. Supp. 2d at 755-56; *see also* Gus Hosein & Caroline Wilson Palow, *Modern Safeguards for Modern Surveillance: An Analysis of Innovations in Communications Surveillance Techniques*, 74 OHIO ST. L.J. 1071, 1089-90 (2013).

149. *In re* Warrant to Search a Target Computer at Premises Unknown, 958 F. Supp. 2d at 756; *see also* Bellovin et al., *supra* note 85, at 83.

150. *See* Yale Law School Information Society Project, *supra* note 2 (discussion by Magistrate Judge Stephen Smith).

151. *In re* Warrant to Search a Target Computer at Premises Unknown, 958 F. Supp. 2d at 755.

152. *Id.*

victim's by only one letter.[153] Using this second email address, an attempt was made to wire transfer the victim's money from his local bank to a foreign bank.[154]

2. The Court's Rationale

In this application concerning bank fraud, the magistrate judge denied the search warrant in a written opinion. In denying the warrant, the judge provided three bases to support his decision: the lack of a territorial limit pursuant to Rule 41(b); the Fourth Amendment particularity requirement; and concerns about the constitutional standards for video camera surveillance.[155]

Because of the indiscriminate and intrusive nature of video surveillance, the Fifth Circuit has adopted a heightened standard based in part on the standard for wiretaps.[156] Specifically, the magistrate judge explained four additional factors beyond probable cause that were necessary:

> 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.[157]

In applying this standard, the court concluded the application failed to establish that the Government had taken all necessary alternative approaches to obtain such information.[158] Moreover, it explained that there was no explanation of the measures that would be taken to minimize the intrusive effect so as to obtain only what was sought in the

153. *Id.*

154. *Id.*

155. *See id.* at 756-61.

156. *Id.* at 759-60; *see also* United States v. Cuevas-Sanchez, 821 F.2d 248, 250 (5th Cir. 1987); 18 U.S.C. §§ 2510-20 (2012).

157. *In re* Warrant to Search a Target Computer at Premises Unknown, 958 F. Supp. 2d at 760 (citing *Cuevas-Sanchez*, 821 F.2d at 252).

158. *Id.*

search warrant.[159]

The magistrate judge also found that the Government had failed to satisfy the Fourth Amendment's particularity requirement.[160] First, he noted that the application failed to explain how the device would search for and contact the targeted computer, in part because use of the software and how it functions was not discussed.[161] Additionally, the decision addressed that the application failed to indicate how any search of the computer would reveal any evidence of criminal activity.[162] Specifically, the judge questioned the location of the computer, indicating that it could be in a public place such as a library, internet café, a job site, or alternatively could be used by family or friends such that people uninvolved with the alleged criminal activity could be swept up into the search and have their personal information compromised.[163]

Most germane to our discussion, the magistrate judge analyzed the applicability of the five bases in Rule 41 authorizing judges to issue search warrants.[164] He concluded that none of the five subsections provided a basis for issuing a warrant. Although the application explicitly relied upon Rule 41(b)(1), it also acknowledged there was no evidence that the targeted computer was within the Southern District of Texas.[165] Notwithstanding the lack of knowledge about the computer's location, the Government argued "that subsection authorizes the warrant 'because information obtained from the Target Computer will first be examined in this judicial district.'"[166] The court rejected this position because it would essentially provide a basis for any computer search around the world provided the "information" was not accessed until it was retrieved and brought back into the district where the warrant was issued.[167] Furthermore, the judge explained that there were two searches at issue: the search for the computer itself as well as the search for the information stored on the computer.[168] Because neither of these searches was done within the district, there was no basis for authorizing a warrant

159. *Id.* at 760-61; *see also* Hosein & Palow, *supra* note 148, at 1090.

160. *In re* Warrant to Search a Target Computer at Premises Unknown, 958 F. Supp. 2d at 758-59.

161. *Id.* at 759.

162. *Id.*; *see also* Bellovin et al., *supra* note 85, at 83 ("Arguably, two different court orders should be obtained.").

163. *In re* Warrant to Search a Target Computer at Premises Unknown, 958 F. Supp. 2d at 759; *see also* Hosein & Palow, *supra* note 148, at 1090.

164. *In re* Warrant to Search a Target Computer at Premises Unknown, 958 F. Supp. 2d at 756-58.

165. *Id.* at 756.

166. *Id.*

167. *Id.* at 756-57.

168. *Id.* at 757.

pursuant to Rule 41(b)(1).[169]

Next, the magistrate judge focused on Rule 41(b)(2), concluding that this subsection was inapplicable. The Court held this section does not authorize the search of an object located outside the district when the search warrant is issued and then brought into the district.[170] Instead, it authorizes the opposite. To allow otherwise would be to essentially allow a search of anything that ultimately could be located and brought into the district.[171]

Finally, the judge rejected the three remaining bases. The criminal investigation did not involve terrorism, therefore Rule 41(b)(3) was inapplicable.[172] Even if the court allowed an argument that the Trojan device would be a tracking device, because it seeks to locate the computer, the Government still could not establish "that the installation of the 'tracking device' (i.e. the software) would take place within this district."[173] Therefore, Rule 41(b)(4) did not provide a basis for issuing a search warrant. Because the application did not establish that the computer was within property or territory controlled by the United States, Rule 41(b)(5) was also inapplicable.[174]

E. The District of Nebraska

1. Facts and Circumstances

The FBI was investigating a child pornography ring in which the participants were using "The Onion Router" ("Tor") software in order to shield their identities on a bulletin board operating from Bellevue, Nebraska, where they distributed child pornography and discussed sexual abuse of children.[175] "Tor involves the application of layers of encryption (nested like layers of an onion) to anonymize communication by sending the original data to its destination without revealing the source IP address making it impossible to trace the communications back through the network to the actual user who sent the communication."[176]

---

169. *Id.*
170. *Id.*
171. *Id.*
172. *Id.* at 758.
173. *Id.*
174. *Id.*
175. United States v. Pierce, Nos. 8:13CR106, 8:13CR107, & 8:13CR108, 2014 WL 5173035, at *3 (D. Neb. Oct. 14, 2014).
176. *Id.*; *see also* Fed. Trade Comm'n v. Asia Pac. Telecom, Inc., 788 F. Supp. 2d 779, 786-87 (N.D. Ill. 2011) ("[T]he Tor Project functions by rerouting a user's online activity through an international network of servers, allowing the user to reach an online destination through one of

Because the IP addresses of those involved in the child pornography bulletin board were unknown, the FBI sought a search warrant to install a network investigative technique on the bulletin board.[177] A court authorized the use of a network investigative technique between November 16, 2012, and December 2, 2012, on the bulletin board so that each time someone accessed any of the bulletin board, the device would cause the person's computer to send data to an FBI computer, which would assist agents in determining the identity of each computer.[178] Based on the use of this device, "the FBI was able to identify a computer's actual IP address and the date and time Website A was accessed together with a date and time of accession with a unique session identifier to distinguish the accession."[179] The discovery of these IP addresses was the first step that led to administrative subpoenas, additional search warrants, indictments, and arrests.

The various defendants filed motions to suppress information obtained through the network investigative techniques authorized by the search warrants. For purposes of each motion, the government stipulated that the use of the device constituted a Fourth Amendment search on each computer, which were located in the defendants' various residences.[180] After a hearing, a magistrate judge recommended that each of the motions to suppress be denied.[181] The district judge adopted this recommendation.[182]

2. The Court's Rationale

Regarding the search warrants for the defendants indicted for child pornography offenses, this example actually involved defendants seeking to suppress evidence obtained through the FBI's use of a network investigative technique. Based on the charge of child pornography, there was nothing to indicate that the charged offenses involve terrorism. Consequently, the territorial limitation based on Rule 41(b)(3) was inapplicable.

There were over fifteen defendants, and it was unclear where they resided at the time they engaged in accessing or distributing child pornography. However, because the identity of each defendant was

---

many 'exit nodes.' The user's destination site then records the exit node's IP address rather than the user's true IP address, making it very difficult to trace the user's true identity.")

177. *Pierce*, 2014 WL 5173035, at *3.

178. *Id.*

179. *Id.*

180. *Id.* at *8.

181. *Id.*at *10.

182. *Id.*at *6.

unknown at the time the order authorizing the network investigative technique was sought, there was no basis for granting the search warrant pursuant to Rule 41(b)(1). Although the computer operating the child pornography bulletin board was located in Bellevue, Nebraska, at the time of the applications, there was no information to establish any of the defendants' computers were located within the district. Therefore, Rule 41(b)(2) was also inapplicable.

Because the application did not seek authorization for a tracking device, Rule 41(b)(4) was inapplicable.[183] Finally, Rule 41(b)(5) was inapplicable because the computer was not located in a United States territory or diplomatic building. Therefore, regardless of the particularity issue, a good argument exists here that the search warrants had no basis for issuance pursuant to Rule 41(b).

IV. ALTHOUGH THE ISSUANCE OF WARRANTS FOR TROJAN DEVICES IS PERMISSIBLE, IT IS IMPORTANT TO BE CAUTIOUS WHEN DOING SO

In presenting applications for authorization of Trojan devices, the Government likely has alternatives to get electronic data related to its criminal investigation. With a known email address, a federal agent may apply for a "pen register" and "trap and trace" device.[184] Regarding a telephone call, a pen register captures the outgoing information, whereas a trap and trace device captures the incoming information.[185] For an application concerning an email, the Government may obtain the addresses to and from for any messages sent, "the IP addresses of the websites visited," as well as "the total amount of data transmitted to or from an account."[186] The benefit to the Government is that the standard to obtain such information is very low and there is virtually no discretion on the part of the magistrate judge if the following threshold is met: "if the court finds that the attorney for the Government has certified to the court that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation."[187] Information

183. *See* United States v. Asghedom, 992 F. Supp. 2d 1167, 1174-75 (N.D. Ala. 2014).

184. *See* 18 U.S.C. §§ 3121-27 (2012).

185. *Compare id.* § 3127(3) *with id.* § 3127(4); *see also* Owsley, *Cell Tower Dumps*, *supra* note 10, at 16 (discussing the differences between pen registers and trap and trace devices).

186. United States v. Forrester, 512 F.3d 500, 510 (9th Cir. 2008); United States v. Hazelwood, No. 1:10 CR 150, 2011 WL 2553265, at *7 (N.D. Ohio June 28, 2011).

187. 18 U.S.C. § 3123(a)(1); *see also id.* § 3122(b)(2) (the Government's application must include "a certification by the applicant that the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by that agency"). One judge has characterized the court's role as simply a rubber stamp for these applications. *In re* Order Authorizing the Installation and Use of a Pen Register and Trap and Trace Device, 846 F. Supp. 1555, 1563 (M.D. Fla 1994) ("Since it is virtually impossible to botch the simple certification, the court under the Act seemingly

obtained from these applications may be used to further the criminal investigation as well as possibly provide the basis for a search warrant, including one that may seek to execute a Trojan device.

Furthermore, during the course of its criminal investigation, the Government may also file an application in order to get various subscriber information related to the email address from the provider.[188] An application pursuant to § 2703 of the United States Code would enable the Government to obtain the cell phone or internet subscriber's name, date of birth, address, the starting date and length of email service, as well as potentially any financial information provided as a subscriber.[189] Although the standard is not as low as that for a pen register, it is still lower than the probable cause standard required for a search warrant:

> A court order for disclosure . . . may be issued by any court that is a court of competent jurisdiction and shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation.[190]

Again, any information obtained from these applications may be used to further a criminal investigation as well as possibly provide the basis for a search warrant, including one that may seek to execute a Trojan device.

In addition to the fact that the applications for these types of devices do not fit squarely within Rule 41 because of the nature of both computers and the internet, there are other concerns raised by these devices. For example, when executed, these devices will seize everything on the computer even though much may be unrelated to the crime being investigated or to any criminal offense at all. Moreover, the information seized may potentially be that of an innocent third party. In both situations, there needs to be an acknowledgment not only that irrelevant information may be caught up in the search, but that such information must be protected and not kept by the Government.

---

provides nothing more than a rubber stamp.").

188. *See* 18 U.S.C. § 2703.

189. *Id.* § 2703(c)(2); Owsley, *Cell Tower Dumps*, *supra* note 10, at 16; *In re* § 2703(d) Order; 10GJ3793, 787 F. Supp. 2d 430, 436 (E.D. Va. 2011); *In re* Application of the United States of America for an Order Pursuant to 18 U.S.C. § 2703(d), 157 F. Supp. 2d 286, 288 (S.D.N.Y. 2001).

190. 18 U.S.C. § 2703(d); *see also In re* Application of the United States for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 620 F.3d 304, 315 (3d Cir. 2010) ("the legislative history provides ample support for the proposition that the standard is an intermediate one that is less stringent than probable cause"); Owsley, *Cell Tower Dumps*, *supra* note 10, at 15-16; Peter P. Swire, *Katz is Dead. Long Live Katz*, 102 MICH. L. REV. 904, 910 (2004).

In 2006, Rule 41 was revised in order to explicitly authorize magistrate judges to issue warrants for tracking devices, which was twenty years after the enactment of the Electronic Communications Privacy Act authorized tracking devices.[191] The Judicial Conference's Committee on Rules of Practice and Procedure could propose a new rule addressing how warrants should be issued for Trojan devices.[192] Recently, the Department of Justice proposed a change to Rule 41 to authorize search warrants for Trojan devices in all types of criminal investigations.[193] The proposed change specifically creates a new subsection to search electronically stored information:

> (b) Authority to Issue a Warrant. At the request of a federal law enforcement officer or an attorney for the government:
>
> * * * * *
>
> (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 use remote access to search electronic storage media and to seize or copy electronically stored information located within or outside the district if:
>
> (A) the district where the media or information is located has been concealed through technological means; or
>
> (B) in an investigation of a violation of 18 U.S.C. § 1030(a)(5), the media are protected computers that have been damaged without authorization and are located in five or more districts.[194]

If adopted, the proposed rule would likely go into effect. As divided by partisanship as Congress has been recently, it is unlikely that Congress would even be able to reject any rule that the Supreme Court adopted.[195]

The technology involved in this generation of Trojan devices

191. Electronic Communications Privacy Act, Pub. L. 99-508, 100 Stat. 1859 (1986).

192. *See* Rules Enabling Act, 28 U.S.C. §§ 2071-77 (2012); *see also Laws and Procedures Governing the Work of the Rules Committees*, UNITED STATES COURTS, http://www.uscourts.gov/RulesAndPolicies/rules/about-rulemaking/laws-procedures-governing-work-rules.aspx (last visited Mar. 7, 2015).

193. Ellen Nakashima, *FBI Wants Easier Process to Hack Suspects' Computers*, WASH. POST (May 9, 2014), http://www.washingtonpost.com/world/national-security/fbi-wants-easier-process-to-hack-suspects-computers/2014/05/09/f30c37b0-d78d-11e3-8a78-8fe50322a72c_story.html; *see also* Committee on Rules of Practice and Procedure, Meeting Minutes (May 29-30, 2014), *available at* http://www.uscourts.gov/uscourts/RulesAndPolicies/rules/Agenda%20Books/Standing/ST2014-05.pdf; Advisory Committee on Criminal Rules, Meeting Minutes (Apr. 7-8, 2014), *available at* http://cryptome.org/2014/03/doj-hacker-attack.pdf.

194. Committee on Rules of Practice and Procedure, *supra* note 193, at 499; Advisory Committee on Criminal Rules, supra note 193, at 499.

195. *See* Owsley, *Cell Tower Dumps*, *supra* note 10, at 42-43.

utilized by the Government has far exceeded Congressional expectations and understanding when the Electronic Communications Privacy Act was enacted in 1986 and even when the Patriot Act was enacted in 2001.[196] Professor Susan Freiwald has explained that Congress typically does not amend statutes concerning electronic surveillance and privacy matters until the federal courts strenuously raise the issue.[197] Given this structural problem, coupled with bipartisan intransigence, it is unlikely Congress can solve this matter even if the courts push for it.

To the extent that these types of applications are permissible based on a showing of probable cause consistent with the Fourth Amendment as well as satisfaction of Rule 41's requirements, the Government must still address the concerns about how to handle documents and information from third parties as well as non-relevant personal material from the subjects of the investigation. Therefore, courts should begin fashioning some type of protocol whenever the issuance of a search warrant for a Trojan device is authorized by law.[198] For example, in obtaining a search warrant for a cell tower dump, a court ordered the Government to "return any and all original records and copies, whether hardcopy or in electronic format or storage, to the Provider, which are determined to be not relevant to the Investigative Agency's investigation."[199] As another court explained regarding a search warrant application for a suspect's Facebook account, it will require "that some safeguards must be put in place to prevent the government from collecting and keeping indefinitely information to which it has no right."[200] Indeed, Magistrate Judge John Facciola, presiding in federal court in the District of Columbia, has issued several published decisions in response to applications for search warrants, requiring the Government to establish and adhere to a protocol to safeguard personal

196. *See* Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311, 344 (2012).

197. Susan Freiwald, *Cell Phone Location Data and the Fourth Amendment: A Question of Law, Not Fact*, 70 MD. L. REV. 681, 687 (2011).

198. *See In re* Application of the United States for an Order Pursuant to 18 U.S.C. § 2703(d), 964 F. Supp. 2d 674, 678 (S.D. Tex. 2013) ("Although the use of a court-sanctioned cell tower dump invariably leads to such information being provided to the Government, in order to receive such data, the Government at a minimum should have a protocol to address how to handle this sensitive private information."); *In re* Application of the United States of America for an Order Pursuant to 18 U.S.C. § 2703(d) Directing Providers to Provide Historical Cell Site Location Records, 930 F. Supp. 2d 698, 702 (S.D. Tex. 2012) (same); *see also* Owsley, *Cell Tower Dumps*, *supra* note 10, at 46 (recommending a protocol be designed for courts authorizing cell tower dumps).

199. *In re* Cellular Telephone Towers, 945 F. Supp. 2d 769, 771 (S.D. Tex. 2013).

200. *In re* Information Associated with the Facebook Account Identified by the Username Aaron.Alexis that is Stored at Premises Controlled by Facebook, Inc., 21 F. Supp. 3d 1, 9 (D.D.C. 2013).

information to which it is not entitled.[201]

Any application that would be granted consistent with the Fourth Amendment and Rule 41 would also have to outline a protocol with which the federal officers must comply regarding information or documents obtained. First, the Government must be barred from keeping any third party's information that is unrelated to the criminal investigation. Any hard copies regarding this information would have to be destroyed, and any electronic records would have to be deleted. Of course, if the criminal investigators could actually demonstrate that the third party was a co-conspirator in the criminal conduct, then the documents and information need not be destroyed.

Second, the law enforcement officials must differentiate between information relevant to the subject of the investigation on the targeted computer and non-relevant materials, such as personal photos and financial information that does not evidence any criminal activity. Any hard copies of the latter materials must be destroyed, while any electronic records must be deleted.

V. CONCLUSION

There are both dangers and benefits that come with the Government's use of Trojan devices. There is a danger that such devices will collect information not meant to be obtained from innocent third parties. However, one benefit is that these devices enable the Government to catch criminals that may have evaded them in the past. Other good news about the government's use of Trojan devices is that the government seeks a search warrant when using the devices, which it often does not do in other applications for electronic surveillance. The problem, however, is that some magistrate judges, in reviewing the Trojan device applications, are not closely hewing to the requirements of Rule 41(b) and are granting these applications where the rule should not allow them.

Ultimately, judges reviewing applications for search warrants must be diligent in ensuring that the standards are satisfied before granting them. Moreover, judges must account for the likelihood that third party data may be swept up within any search and develop appropriate protocols to safeguard innocent individual's privacy. This measure is necessary to ensure that, while the Government pursues criminals, the

201. *In re* Apple iPhone, IMEI 013888003738427, 31 F. Supp. 3d 159, at *5-7 (D.D.C. 2014) (application seeking authorization to search a cell phone); *In re* ODYS LOOX Plus Tablet, Serial Number 4707213703415, in Custody of United States Postal Inspection Serv., 28 F. Supp. 3d 40, 46 (D.D.C. 2014) (application seeking authorization to search a computer).

rights of the American people are not violated.