AN A.S. PRATT PUBLICATION
SEPTEMBER 2017
VOL. 3 • NO. 7

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

United States v. Ulbricht: Dread Pirate Roberts Pushes the Envelope of the Fourth Amendment

By Jay D. Kenigsberg*

The author of this article discusses a recent decision by the U.S. Court of Appeals for the Second Circuit affirming a judgment of conviction and sentence to life imprisonment against Ross William Ulbricht for transactions arising out of his creation and operation of Silk Road, an online illegal drugs and services website that used Bitcoins for payment. The Second Circuit rejected Ulbricht's Fourth Amendment arguments.

In *U.S. v. Ulbricht*,[1] Ross William Ulbricht appealed from a judgment of conviction and sentence to life imprisonment entered in the U.S. District Court for the Southern District of New York. In February 2015, a jury convicted Ulbricht on seven counts arising from his creation and operation of Silk Road under the username Dread Pirate Roberts ("DPR"), a pseudonym of a pirate in the novel and film *The Princess Bride* that is periodically passed on from one individual to another. Ulbricht challenged his conviction on several grounds, including that the district court erred in denying his motion to suppress evidence obtained in violation of the Fourth Amendment. The U.S. Court of Appeals for the Second Circuit rejected that claim and affirmed Ulbricht's conviction and sentence in all respects. In doing so, however, the court sent a signal that our legislative and judicial systems may have reached a watershed moment in the permissible scope of Fourth Amendment searches given the current state of modern technology.

BACKGROUND

Silk Road was to illegal drugs and computer hacking software what Amazon is to detergent and best sellers. Between 2011 and 2013, thousands of vendors used Silk Road to sell approximately $183 million worth of illegal drugs and services. Those transactions exclusively used Bitcoins, a well-known digital currency. Although Bitcoins are transferred between anonymous Bitcoin accounts, the currency is traceable because the transaction history of each individual Bitcoin is logged on the blockchain. The blockchain uses distributed ledger technology to prevent a person from spending the same Bitcoin twice, thus allowing Bitcoin to act as a form of currency completely decentralized from nation states or central banks. Ulbricht accessed the blockchain from his laptop to engage in illicit transactions and also to assure the Silk Road community that posts on the site from DPR were actually from

* Jay D. Kenigsberg is a partner at Rivkin Radler LLP representing major domestic insurance carriers in a wide variety of coverage disputes, including actions involving pollution liability, individual disability, and Employee Retirement Income Security Act claims. He may be contacted at jay.kenigsberg@rivkin.com.

[1] 2017 U.S. App. LEXIS 9517 (2nd Cir. May 31, 2017).

him (by using public and private keys). This presented a rather unique challenge for government agents – how to tie Ulbricht to DPR based entirely upon digital evidence stored on a laptop linked to the blockchain?

In 2011, two separate divisions of the Department of Justice – the U.S. Attorney's Offices for the District of Maryland and for the Southern District of New York – became interested in Silk Road after international packages containing drugs were intercepted at Chicago's O'Hare airport. Law enforcement agents knew that the person using DPR as a Silk Road username created and managed the site, but DPR's actual identity was unknown. The investigation into the identity of DPR and the ultimate naming of Ulbricht as the man behind the username relied on evidence gathered from five "pen/trap" orders authorizing law enforcement agents to collect internet protocol ("IP") address data for internet traffic on Ulbricht's home wireless router and from warrants that authorized the search and seizure of his laptop as well as his Facebook and Google accounts. The evidence gathered through these devices included chat logs, journal entries, the Silk Road database and spreadsheets cataloguing the servers that hosted Silk Road expenses and profits associated with the site. This information led the government to seize approximately $18 million worth of Bitcoins from the electronic wallet on Ulbricht's laptop. By analyzing the transaction history through blockchain records, the government determined that about 89 percent of the Bitcoins on Ulbricht's computer came from Silk Road servers located in Iceland. The old adage remains true in the digital world: follow the money, even if that "money" exists only in the form of computer code.

Although the court's opinion acknowledges that pen/trap orders are based on a statute drafted with only telephone technology in mind and that computer searches pose "special problems," the court was not prepared to articulate any special limitations on digital searches under the Fourth Amendment simply because this case involved modern technology. However, the court recognized that a future case (presumably one with significant digital evidence requiring a high level forensic investigation) may require this court to do just that.

THE PEN/TRAP ACT

The five pen registers and trace devices used by the government were obtained pursuant to the Pen/Trap Act, 18 U.S.C. Section 3122(a)(1). Pen registers and trace devices "shall not include the contents of any communication."[2] The statute does not require a search warrant or the showing required to obtain a search warrant. Instead, the statute requires only that the application contain a certification that the information likely to be obtained is "relevant to an ongoing criminal investigation."[3] In this case, the pen registers and trace devices were authorized to identify the source and

[2] *Id.* Section 3127(3).
[3] *Id.* Section 3122(b)(2).

destination (IP) addresses, along with the dates, times, durations, ports of transmission, and any Transmission Control Protocol ("TCP") connection data associated with the electronic communications sent from Ulbricht's home wireless router and laptop. According to the government, this information was "akin to data captured by traditional telephonic pen registers and trap and trace devices."

THE FOURTH AMENDMENT ARGUMENTS

Ulbricht took a different view. He argued that the pen/trap orders violated his Fourth Amendment rights because he had a reasonable expectation of privacy in the IP address routing information that the orders allowed the government to collect. He noted that questions have been raised about whether some aspects of modern technology "which entrust great quantities of significant personal information to third party vendors" making extensive government surveillance possible calls for a re-evaluation of the third-party disclosure doctrine established by *Smith v. Maryland*.[4] In *Smith*, the U.S. Supreme Court held that a "person has no legitimate expectation of privacy in information he voluntarily turns over to third parties," including phone numbers dialed in making a telephone call and captured by a pen register.[5] The rationale behind this determination was that phone users "typically know that they must convey numerical information to the phone company; that the phone company has facilities for recording this information; and that the phone company does in fact record this information for a variety of legitimate purposes.[6] Ulbricht argued that the pen/trap orders may monitor a communication's content by tracking metadata. This argument was rejected by the court because Ulbricht did not identify what metadata the government might have or collected that gave the government information concerning the content of his communications.

Ulbricht's main argument, however, was that the pen/trap orders violated the Fourth Amendment because the government obtained the orders without a warrant. According to the court, the "cornerstone of the modern law of searches is the principle that, to mount a successful Fourth Amendment challenge, a defendant must demonstrate that he personally has an expectation of privacy in the place searched."[7] Thus, a "Fourth Amendment search does not occur unless the search invades an object or area in which one has a subjective expectation of privacy that society is prepared to accept as objectively reasonable." [8] The court looked to cases from other circuits and acknowledged that internet users should know that information they convey is provided to and used by internet service providers for the purpose of directing routing information and that "IP addresses . . . are voluntarily turned over in order to direct the third party's servers."[9]

---

[4] 442 US 735, 743-44. 99 S.Ct. 2577, 61 L. Ed. 2d 220 (1979).
[5] *Id.*
[6] *Id.* at 743.
[7] *United States v. Haqq*, 278 F.3d 44, 47 (2d Cir. 2002).
[8] *United States v. Hayes*, 551 F.3d 138, 143 (2d Cir. 2008).
[9] *United States v. Christie*, 624 F.3d 558, 574 (3d Cir. 2010).

THE COURT'S DECISION

The court concluded that the recording of IP address information and similar routing data, which reveal the existence of connections between communications devices without disclosing the content of the communications "are precisely analogous to the capture of telephone numbers at issue in *Smith*." According to the court, "That is why the orders here fit comfortably within the language of a statute drafted with the earlier technology in mind." The court recognized that novel or more intrusive surveillance techniques "might present future questions concerning the scope of the third-party disclosure doctrine" but that was not the case presented here by the pen/trap orders obtained by the government. The court saw no constitutional difference between monitoring home phone dialing information and IP address routing data. According to the opinion, electronic methods of communication do not "raise novel issues distinct from those long since resolved in the context of telephone communication, with which society has lived for the nearly forty years since *Smith* was decided." The Second Circuit joins the U.S. Courts of Appeals for the Third, Fourth, Sixth, and Ninth Circuits in agreeing that third-party information relating to the sending and routing of electronic communications does not receive Fourth Amendment protection.

Ulbricht also argued that the search warrants that were issued authorizing the search and seizure of his laptop and Facebook and Google accounts violated the Fourth Amendment's particularity requirement. The Fourth Amendment explicitly commands that warrants must be based on probable cause and must "particularly describe the place to be searched, and the persons or things seized."[10] The court stated that a general search of electronic data is a "potent threat" to privacy because hard drives and e-mail accounts may be "akin to a residence in terms of the scope and quantity of private information they may contain."[11] Search warrants covering digital data may contain some ambiguity, but law enforcement agents must do the best that could be reasonably expected under the circumstances.[12]

Here, the laptop warrant referenced the crimes charged against Ulbricht, which included narcotics trafficking, computer hacking, money laundering, and murder-for-hire offenses. The affidavit in support of the warrant also described the workings of Silk Road and the role Dread Pirate Roberts played in its operation and the information supporting a finding that there was probable cause to believe that Ulbricht and DPR were the same person. The warrant had divided the information to be searched into two categories, the first concerned Silk Road evidence on the laptop, including Bitcoin wallet files and transactions with Bitcoin exchangers, and information concerning any financial accounts where Silk Road funds may be stored. The

[10] U.S. Const. amend IV.
[11] *Citing*, *United States v. Galpin*, 720 F.3d 436, 446 (2d Cir. 2013).
[12] *Id.*

second category of information concerned evidence corroborating the identification of Ulbricht as Dread Pirate Roberts.

The court concluded that Ulbricht's arguments against the laptop warrant did not contest the warrant's basic compliance with the Fourth Amendment's particularity requirement. Rather, Ulbricht based his arguments on the intrusive nature of computer searches. Specifically, Ulbricht questioned the protocols that the laptop warrant instructed officers to use in executing the search which allowed the reading of the first few pages of a file, searching for hidden files, using key word searches through all electronic storage areas and the reviewing of file directories. The court found a fundamental flaw in these arguments – they confuse a warrant's breadth with a lack of particularity. For example, a warrant may allow the search of a suspected drug dealer's entire home where there is probable cause to believe that evidence relevant to that activity may be found anywhere in the residence. Similarly, where criminal activity pervades an entire business, seizure of all the records of the business is appropriate. The court was sensitive to the difficulties associated with preserving a criminal defendant's privacy while searching through his electronic data and computer hard drives. In this case, Ulbricht used his laptop to commit the charged offenses by operating Silk Road. Thus, the targeted crimes were committed largely through computers and the warrant's application provided an ample basis for the issuing judge to conclude that evidence related to Silk Road and Ulbricht's use of the DPR name likely permeated Ulbricht's computer.

CONCLUSION

Despite the unusual nature of the crimes charged in this case and the uniqueness of the evidence that tied Ulbricht to Silk Road and DPR, including the blockchain records of his Bitcoin transactions, the court declined to rethink the well-settled Fourth Amendment principles that the laptop warrant might implicate. The court was, however, mindful of the fact that the rapid pace of technology may require a reevaluation of Fourth Amendment principles. The court stated: "A future case may require this Court to articulate special limitations on digital searches to effectuate the Fourth Amendment's particularity or reasonableness requirements. Such a case is not before us."

That time, however, may be rapidly approaching. As a steady stream of investment funds flow into blockchain research in the financial and insurance worlds, the use of distributed ledgers to enforce contractual arrangements and to pay for goods and services through cryptocurrency will be on the rise. Those transactions will be digitally stored and programmers will inevitably embed greater amounts of data within the blockchain itself, which in turn will force law enforcement agents to keep pace with these developments through more precise forensic investigations. The day has arrived when investigative techniques can unlock a trove of information embedded within

data, thus distinguishing technological searches from those that targeted telephones and physical residences over the past 40 years. The transactional nature of digital contracts and the means to effectuate those transactions only within the digital space is a signal to legislative bodies and the courts to reassess the expectation of privacy we may all have in the digital world. The Second Circuit may have been unprepared to take that leap in *Ulbricht*, but the court certainly recognized the significance of its decision in light of modern technology. The "future case" it alluded to is probably on its docket at this very moment.