

No.

In the Supreme Court of the United States

ROSS WILLIAM ULBRICHT, PETITIONER

v.

UNITED STATES OF AMERICA

*ON PETITION FOR A WRIT OF CERTIORARI
TO THE UNITED STATES COURT OF APPEALS
FOR THE SECOND CIRCUIT*

PETITION FOR A WRIT OF CERTIORARI

KANNON K. SHANMUGAM
Counsel of Record
ALLISON JONES RUSHING
MASHA G. HANSFORD
MICHAEL J. MESTITZ
WILLIAMS & CONNOLLY LLP
725 Twelfth Street, N.W.
Washington, DC 20005
(202) 434-5000
kshanmugam@wc.com

QUESTIONS PRESENTED

1. Whether the warrantless seizure of an individual's Internet traffic information without probable cause violates the Fourth Amendment.
2. Whether the Sixth Amendment permits judges to find the facts necessary to support an otherwise unreasonable sentence.

TABLE OF CONTENTS

	Page
Opinions below	1
Jurisdiction	2
Constitutional provisions involved	2
Statement.....	2
Reasons for granting the petition.....	11
I. This Court should grant review to decide whether the Fourth Amendment protects an individual's Internet traffic information	11
A. The question presented is of exceptional importance and cannot be answered without this Court's review	11
B. The decision below is erroneous	17
1. Internet traffic information is not analogous to the telephone routing information gathered in <i>Smith v. Maryland</i>	17
2. Individuals have a reasonable expectation of privacy in their Internet traffic information.....	21
C. The question presented warrants review in this case.....	22
II. This Court should grant review to decide whether the Sixth Amendment permits a judge to find the facts necessary to support an otherwise unreasonable sentence	24
A. The question presented is an important one expressly reserved by this Court and subject to extensive debate by judges in the lower courts....	25
B. The decision below is erroneous	27
C. The question presented warrants review in this case.....	30
Conclusion.....	32

IV

	Page
Table of contents—continued:	
Appendix A	1a
Appendix B	3a
Appendix C	109a

TABLE OF AUTHORITIES

Cases:

<i>Alleyne v. United States</i> , 133 S. Ct. 2151 (2013).....	28
<i>Apprendi v. New Jersey</i> , 530 U.S. 466 (2000)	28, 29
<i>Batson v. Kentucky</i> , 476 U.S. 79 (1986)	28
<i>Blakely v. Washington</i> , 542 U.S. 296 (2004).....	28
<i>Carpenter v. United States</i> , cert. granted, No. 16-402 (argued Nov. 29, 2017).....	<i>passim</i>
<i>Hurst v. Florida</i> , 136 S. Ct. 616 (2016)	28
<i>Jones v. United States</i> , 135 S. Ct. 8 (2014)	24, 25, 26, 31
<i>Katz v. United States</i> , 389 U.S. 347 (1967)	20
<i>Packingham v. North Carolina</i> , 137 S. Ct. 1730 (2017)	18
<i>Peugh v. United States</i> , 133 S. Ct. 2072 (2013)	28, 29
<i>Riley v. California</i> , 134 S. Ct. 2473 (2014)	<i>passim</i>
<i>Rita v. United States</i> , 551 U.S. 338 (2007).....	2, 25
<i>Smith v. Maryland</i> , 442 U.S. 735 (1979).....	<i>passim</i>
<i>Southern Union Co. v. United States</i> , 567 U.S. 343 (2012).....	27
<i>United States v. Bell</i> , 808 F.3d 926 (D.C. Cir. 2015), cert. denied, 137 S. Ct. 37 (2016).....	27
<i>United States v. Briggs</i> , 820 F.3d 917 (8th Cir. 2016), cert. denied, 137 S. Ct. 617 (2017).....	26
<i>United States v. Bynum</i> , 604 F.3d 161 (4th Cir.), cert. denied, 560 U.S. 977 (2010).....	14
<i>United States v. Caira</i> , 833 F.3d 803 (7th Cir. 2016), petition for cert. pending, No. 16-6761 (filed Nov. 7, 2016)	13, 16, 23

	Page
Cases—continued:	
<i>United States v. Canania</i> , 352 F.3d 764 (8th Cir.), cert. denied, 555 U.S. 1037 (2008).....	27, 29
<i>United States v. Cassius</i> , 777 F.3d 1093 (10th Cir.), cert. denied, 135 S. Ct. 2909 (2015).....	26
<i>United States v. Christie</i> , 624 F.3d 558 (3d Cir. 2010), cert. denied, 562 U.S. 1236 (2011).....	14
<i>United States v. Di Re</i> , 332 U.S. 581 (1948)	20
<i>United States v. Faust</i> , 456 F.3d 1342 (11th Cir.), cert. denied, 549 U.S. 1046 (2006).....	27
<i>United States v. Forrester</i> , 512 F.3d 500 (9th Cir. 2008).....	14
<i>United States v. Jones</i> , 565 U.S. 400 (2012)	18, 20, 21
<i>United States v. Karo</i> , 468 U.S. 705 (1984)	19, 20
<i>United States v. Mercado</i> , 474 F.3d 654 (9th Cir. 2007), cert. denied, 552 U.S. 1297 (2008).....	27
<i>United States v. Miller</i> , 425 U.S. 435 (1976)	<i>passim</i>
<i>United States v. Sabillon-Umana</i> , 772 F.3d 1328 (10th Cir. 2014).....	26
<i>United States v. Settles</i> , 530 F.3d 920 (D.C. Cir. 2008), cert. denied, 555 U.S. 1140 (2009).....	26
<i>United States v. Stanley</i> , 753 F.3d 114 (3d Cir.), cert. denied, 135 S. Ct. 507 (2014).....	13, 14
<i>United States v. White</i> , 551 F.3d 381 (6th Cir. 2008), cert. denied, 556 U.S. 1215 (2009).....	27
Constitution and statutes:	
U.S. Const. Amend. IV	<i>passim</i>
U.S. Const. Amend. VI	<i>passim</i>

VI

	Page
Statutes—continued:	
Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848.....	5, 20, 23
18 U.S.C. 3122	5
28 U.S.C. 1254(1)	2
Miscellaneous:	
PC Magazine, <i>Definition of TCP/IP Port</i> <tinyurl.com/portdefinition> (last visited Dec. 22, 2017)	18
Pew Research Center, <i>Public Perceptions of Privacy and Security in the Post-Snowden Era</i> (Nov. 12, 2014) <tinyurl.com/privacystudy>	21
Pew Research Center, <i>Tech Adoption Climbs Among Older Adults</i> (May 17, 2017) <tinyurl.com/pewtechuse>	19
United States Sentencing Commission, <i>Life Sentences in the Federal System</i> (Feb. 2015) <tinyurl.com/ussclife>	31

In the Supreme Court of the United States

No.

ROSS WILLIAM ULBRICHT, PETITIONER

v.

UNITED STATES OF AMERICA

*ON PETITION FOR A WRIT OF CERTIORARI
TO THE UNITED STATES COURT OF APPEALS
FOR THE SECOND CIRCUIT*

PETITION FOR A WRIT OF CERTIORARI

Ross William Ulbricht respectfully petitions for a writ of certiorari to review the judgment of the United States Court of Appeals for the Second Circuit in this case.

OPINIONS BELOW

The opinion of the court of appeals (App., *infra*, 3a-108a) is reported at 858 F.3d 71. The district court's order denying petitioner's motion to suppress (App., *infra*, 109a-146a) is unreported.

JURISDICTION

The judgment of the court of appeals was entered on May 31, 2017. A petition for rehearing was denied on August 30, 2017. On November 21, 2017, Justice Ginsburg extended the time within which to file a petition for a writ of certiorari to and including December 28, 2017. The jurisdiction of this Court is invoked under 28 U.S.C. 1254(1).

CONSTITUTIONAL PROVISIONS INVOLVED

The Fourth Amendment to the United States Constitution provides in relevant part:

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause[.]

The Sixth Amendment to the United States Constitution provides in relevant part:

In all criminal prosecutions, the accused shall enjoy the right to a speedy and public trial, by an impartial jury[.]

STATEMENT

This case—one of the highest-profile federal criminal prosecutions in recent years—presents two important questions requiring the Court’s review. The first question is whether the warrantless seizure of an individual’s Internet traffic information without probable cause violates the Fourth Amendment. That question is closely related to the question the Court is currently considering in *Carpenter v. United States*, cert. granted, No. 16-402 (argued Nov. 29, 2017). The second question is whether the Sixth Amendment forbids a judge from finding facts necessary to support an otherwise unreasonable sentence. The Court left open that question a decade ago in *Rita v.*

United States, 551 U.S. 338 (2007). As to both questions, the courts of appeals have expressed serious doubts about the constitutionality of existing practices, but they perceive themselves to be bound by the Court’s precedents.

In this case, without a warrant or probable cause, the government seized petitioner’s private Internet traffic information and used that information to arrest and convict him of drug trafficking and related offenses. The district court then sentenced petitioner to life imprisonment without the possibility of parole—a sentence almost unheard of for a first-time offender charged with the offenses at issue. The district court imposed that sentence by resolving several disputed issues of fact; absent those judge-found facts, petitioner’s sentence would have been unreasonable.

The court of appeals affirmed. Although the court acknowledged that “questions have been raised” about the constitutionality of both practices, it considered itself bound to apply this Court’s precedents on those issues “until and unless” the Court intervenes. App., *infra*, 33a; see *id.* at 106a n.72. This case is an appropriate vehicle in which to provide much-needed clarity on critical and recurring questions of federal criminal law.

1. In 2009, petitioner, a 25-year-old committed libertarian with a master’s degree in materials science and engineering, began working to create an online marketplace that would allow users to buy goods anonymously and securely. Petitioner’s efforts culminated in 2011 in the creation of a website called the Silk Road, which allowed individual users to create anonymous accounts to buy and sell a range of goods and services. As petitioner later told the district court: “I remember clearly why I created the Silk Road. I had a desire to—I wanted to empower people to be able to make choices in their lives for themselves and to have privacy and anonymity.” C.A. App. 1507. Users

bought and sold a variety of illegal goods on the Silk Road website, including drugs, false identification documents, and computer hacking software. App., *infra*, 5a.

In 2012, the lead administrator of the Silk Road adopted the username “Dread Pirate Roberts,” a reference to the novel and film *The Princess Bride* (in which Dread Pirate Roberts was a pseudonym periodically passed from one individual to another). Petitioner contended at trial that he abandoned his interest in the Silk Road in 2011, but was lured back by a successor administrator toward the end of the site’s operation so that he would take the blame for the site. App., *infra*, 14a, 19a.

2. The government began investigating the Silk Road website in 2011 after it started to receive attention in the news media. The government initially targeted “several individuals” it suspected of being the Dread Pirate Roberts, including Mark Karpeles, a computer developer and a self-proclaimed hacker. According to the government, it began to focus on petitioner when it found an Internet post on one of Karpeles’ websites relating to the Silk Road. The post was made by a user associated with the e-mail address rossulbright@gmail.com. App., *infra*, 6a; Gov’t C.A. Br. 64-65; Tr. 1263, 1266-1267 (Jan. 26, 2015).

Using that e-mail address, the government was able to locate petitioner and eventually to monitor his Internet traffic and location. To begin with, the government identified a particular Internet Protocol (IP) address that regularly accessed petitioner’s e-mail account. An IP address is a unique number assigned to every device connected to the Internet. When a user visits a webpage, checks his e-mail, or performs any other action requiring an Internet connection, his computer or device communicates its IP address so the responding computer knows how to route the requested data. App., *infra*, 7a.

The government collected data about the Internet traffic to and from petitioner's IP address and identified his home address as 235 Monterey Boulevard in San Francisco, California. The government then secured an order authorizing a "pen register," along with a "trap and trace device," to be applied to the wireless router in petitioner's living room. A pen register is a device that records the dialing, routing, addressing, or signaling information transmitted by a particular device, such as a telephone, computer, or e-mail account. App., *infra*, 30a, 112a-114a; Gov't C.A. Br. 105-106.

In order to obtain an order authorizing a pen register under Title III of the Electronic Communications Privacy Act, the government is not required to show probable cause; instead, a government attorney need only certify that the information "likely to be obtained" by the pen register is "relevant" to an ongoing criminal investigation. 18 U.S.C. 3122. A trap and trace device is like a pen register, only it collects incoming (rather than outgoing) data. Together, the combination of a pen register and a trap and trace device is known as a "pen/trap."

The orders authorizing the pen/trap on the router in petitioner's home, like other pen/traps the government later employed, allowed the government to collect several categories of information associated with petitioner's Internet activity. Specifically, orders allowed the government to "identify the source and destination IP addresses, along with the dates, times, durations, ports of transmissions, and any Transmission Control Protocol (TCP) connection data[] associated with any electronic communication sent to or from" specified devices associated with petitioner, including his router and laptop. App., *infra*, 30a-31a (alteration, footnote, and citation omitted).

The pen/trap orders allowed the government to determine the IP addresses contacted by petitioner's router;

the time and duration of those connections; and the individual devices that were connecting to the Internet through the router. By identifying the “port of transmission” associated with petitioner’s Internet traffic, the pen/trap orders also allowed the government to determine what *type* of Internet traffic was occurring. As the government’s lead FBI investigator explained: “Computers use different ‘ports’ to handle different types of Internet traffic. For example, e-mail traffic is handled on certain ports while website traffic is handled on others. Port information thus reveals what type of traffic is reflected on a pen register[.]” D. Ct. Dkt. 57, at 9 (¶ 19 n.10) (Sept. 5, 2014) (declaration of Christopher Tarbell).

As a result of the pen/trap orders, the government was able to identify all of the individual devices that regularly connected with petitioner’s router, along with the traffic associated with those devices. In particular, the government determined that a particular laptop computer—petitioner’s personal laptop—routinely connected with the router. The government did so by identifying the media access control (MAC) address of the laptop—a unique number embedded in a device’s hardware that can be used to identify the device on any network to which it connects. After identifying the MAC address of petitioner’s laptop, the government could isolate the Internet traffic associated with that computer. App., *infra*, 30a-31a; D. Ct. Dkt. 57, at 9 (¶ 19 n.11).

Using that MAC address, the government secured yet another pen/trap order to collect data about any Internet communications sent to or from petitioner’s laptop. During this period, the government monitored petitioner’s Internet activity, including the times he logged on and off, to compare it with the Dread Pirate Roberts’ Internet activity. After two weeks of warrantless pen/trap surveillance, agents sought a warrant for petitioner’s arrest, as

well as warrants to search his home and laptop. Petitioner was subsequently arrested at a public library in San Francisco. App., *infra*, 12a, 112a-114a; Gov’t C.A. Br. 107-108.

3. A grand jury in the Southern District of New York indicted petitioner on numerous counts of drug trafficking and related offenses. Before trial, petitioner moved to suppress evidence gathered in the course of the government’s warrantless pen/trap surveillance, contending that the pen/trap orders were unlawful because a warrant was required. App., *infra*, 7a-8a, 31a.

The district court denied the motion. App., *infra*, 110a, 141a-142a. The court relied on this Court’s decision in *Smith v. Maryland*, 442 U.S. 735 (1979), which held that individuals have no Fourth Amendment privacy interest in phone numbers captured during a telephone call by a pen register. App., *infra*, 141a-142a. Based on that holding, the district court concluded that the “law is clear—and there is truly no room for debate—that the type of information” gathered by the pen/trap orders at issue here “was entirely appropriate for that type of order.” App., *infra*, 141a.¹

4. After a highly publicized trial, petitioner was convicted on all counts. Under the relevant statutes, petitioner’s convictions exposed him to a mandatory minimum sentence of 240 months in prison and a maximum sentence of life in prison. Under the Sentencing Guidelines, petitioner’s offenses and complete lack of criminal history should have led to a recommended Guidelines range substantially below that maximum.

¹ Although the district court also determined that petitioner had not demonstrated he possessed a sufficient interest in the information at issue, App., *infra*, 141a-142a & n.14, the government stipulated that petitioner had such an interest, and the court of appeals proceeded to address the constitutionality of the pen/trap orders, *id.* at 31a n.28.

At petitioner’s sentencing hearing, however, the district court resolved several disputed issues of fact by a preponderance of the evidence and applied several enhancements to petitioner’s offense level. The court imposed an increase for directing the use of violence, based on its determination that petitioner commissioned five murders (which were never committed) during his alleged time as the Dread Pirate Roberts. Petitioner was not charged for the alleged commissioning of murders; indeed, at trial, the government did not claim the murders actually occurred and stressed to the jury that it was “not required to make any findings about them.” Tr. 2159-2160 (Feb. 3, 2015). But the district court discussed the alleged commissioning of murders at length at sentencing and imposed an enhancement on that basis. App., *infra*, 26a-27a; C.A. App. 1464-1466, 1528-1529.

The district court also made findings resulting in an increase under the Guidelines for importing methamphetamine; an increase for maintaining premises for manufacturing or distributing a controlled substance; and an increase for distributing a drug quantity far in excess of the quantity found by the jury. Because the offense level resulting from these enhancements exceeded the maximum allowable level, the Guidelines “range” became a recommended sentence of life imprisonment. App., *infra*, 26a-27a; C.A. App. 1463-1470.

The district court also devoted extensive attention at sentencing to other conduct for which petitioner was never charged. In particular, the district court considered evidence of six drug-related deaths allegedly connected to Silk Road, including testimony from parents of two of the decedents. App., *infra*, 27a-28a; C.A. App. 1472-1496. Although the court noted that “[t]he defendant is not convicted of killing these people” and the evidence of the deaths was “not relevant to the offenses of conviction,” it

determined it could consider the deaths as “related conduct” on the theory that they were, “by a preponderance of the evidence * * * , in some way, related to the Silk Road.” C.A. App. 1472.

The defense objected to the district court’s factual findings. C.A. App. 1481. Petitioner also submitted almost one hundred letters attesting to his character, which the court called “profoundly moving,” “written by a vast, broad array of people * * * from every phase of your life,” and which showed “a man who was loved, who has built enduring and significant relationships over a lifetime and maintained them, * * * [who] displayed great kindness to many people.” *Id.* at 1534-1535. The government’s sentencing letter to the court nevertheless urged a “lengthy sentence,” citing the fact that petitioner’s “sentencing [was] being closely watched.” *Id.* at 1328.

Noting the “significant public interest in this case,” the district court sentenced petitioner (who was then 31 years old) to life imprisonment. The court also imposed a forfeiture order of \$184 million, representing the amount that allegedly passed through the Silk Road website. C.A. App. 1537-1539.

5. On appeal, petitioner argued, as is relevant here, that the district court erred in denying his motion to suppress the evidence from the pen/trap orders and that his life sentence was both procedurally and substantively unreasonable.

The court of appeals affirmed. App., *infra*, 3a-108a. As to the denial of petitioner’s motion to suppress, the court adopted the government’s assertion that the collected information about Internet traffic was “akin to data captured by traditional telephonic pen registers and trap and trace devices.” *Id.* at 31a (internal quotation marks and citation omitted). Relying on the so-called “third-party doctrine” developed in the context of telephone calls

in *Smith*, the court concluded that petitioner had no reasonable expectation of privacy in his Internet traffic information because he voluntarily conveyed it to his Internet service provider and to third-party servers. *Id.* at 32a-33a. Although the court acknowledged that “questions have been raised about whether some aspects of modern technology * * * call for a re-evaluation” of the rule of *Smith*, it nevertheless viewed itself as “bound * * * by [*Smith*] until and unless it is overruled by the Supreme Court.” *Id.* at 33a.

As to the reasonableness of the sentence, the court of appeals ultimately upheld the sentence, although it did “not reach [its] conclusion lightly.” App., *infra*, 107a. Even though a “life sentence for selling drugs alone would give pause,” the court of appeals differentiated this case from the typical drug-trafficking case based on the district court’s factual findings at sentencing. *Id.* at 100a-101a. In particular, the court reasoned that the district court’s finding that petitioner had “[c]ommission[ed] * * * murders significantly justified the life sentence,” rendering it substantively reasonable. *Id.* at 101a n.68; see *id.* at 102a.

The court of appeals likewise upheld petitioner’s sentence as procedurally reasonable, despite the district court’s decision to take into account the drug-related deaths. App., *infra*, 87a-97a. At the outset, the court of appeals stated that there was “no need” for the government to introduce such “emotionally inflammatory” evidence at sentencing, “let alone to hammer the point home with unavoidably emotional victim impact statements by parents of two of the decedents.” *Id.* at 91a. But the court of appeals ultimately concluded that the district court was permitted to consider the uncharged conduct, found by a

preponderance of evidence, as long as the facts did not increase the statutory maximum sentence for the crimes for which petitioner was found guilty. *Id.* at 92a-93a, 96a.

Petitioner and his amici cited various opinions by members of this Court suggesting that judicial factfinding violates a defendant's constitutional right to a jury trial where it renders reasonable an otherwise unreasonable sentence. Pet. C.A. Reply Br. 60-62; see, *e.g.*, Drug Policy Alliance C.A. Br. 14-15. But the court of appeals rejected petitioner's constitutional argument as having "no support in existing law." App., *infra*, 106a n.72. Although the court of appeals "might not have imposed the same sentence [itself] in the first instance" in this case, it determined that the district court's factual findings brought petitioner's sentence within a permissible range. *Id.* at 107a. Based on those findings, the court of appeals upheld what it described as the district court's exercise of its "power to condemn a young man to die in prison." *Id.* at 108a.

6. The court of appeals denied a petition for rehearing without recorded dissent. App., *infra*, 1a-2a.

REASONS FOR GRANTING THE PETITION

I. THIS COURT SHOULD GRANT REVIEW TO DECIDE WHETHER THE FOURTH AMENDMENT PROTECTS AN INDIVIDUAL'S INTERNET TRAFFIC INFORMATION

A. The Question Presented Is Of Exceptional Importance And Cannot Be Answered Without This Court's Review

This case presents the question whether the Fourth Amendment permits the government, without probable cause, to collect data generated by millions of individuals as an everyday incident of modern life: their Internet traffic information. The Court has previously granted certiorari to resolve similar questions about the interplay

between modern technology and Fourth Amendment privacy interests, see, *e.g.*, *Riley v. California*, 134 S. Ct. 2473 (2014), and it has done so again this Term, see, *e.g.*, *Carpenter v. United States*, cert. granted, No. 16-402 (argued Nov. 29, 2017). The Court should similarly grant certiorari to resolve the question presented in this case or, at a minimum, hold this case pending its decision in *Carpenter*, which may articulate principles applicable here.

1. Courts of appeals addressing the question presented here have largely felt constrained by this Court’s ill-fitting precedents from a generation ago concerning privacy interests in dialed telephone numbers revealed to, and physical papers held by, third parties. At the same time, the courts of appeals have signaled the need for this Court to address whether, and how, those precedents apply in the context of modern Internet technology.

The Fourth Amendment guarantees “[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures.” U.S. Const. Amend. IV. In *Smith v. Maryland*, 442 U.S. 735 (1979), this Court held that the Fourth Amendment did not forbid law enforcement from using a pen register to capture telephone numbers dialed by individual telephone users. See *id.* at 745-746. The Court reasoned that an individual’s expectation of privacy in the numbers he dialed was diminished because the individual “voluntarily conveyed” that information to the phone company. *Id.* at 744 (citation omitted). The Court doubted that “people in general entertain any actual expectation of privacy in the numbers they dial,” observing that an individual would have known that the phone company recorded those numbers because they would be listed on the individual’s bills. *Id.* at 742. In reaching its decision, the Court emphasized the pen register’s “limited capabilities,” noting that “a law enforcement official could not even determine from the

use of a pen register whether a communication existed” or “whether the call was even completed.” *Id.* at 741-742 (citation omitted). Similarly, in *United States v. Miller*, 425 U.S. 435 (1976), the Court relied in part on the notion of voluntary conveyance in holding that a bank customer lacked a Fourth Amendment privacy interest in papers held by a bank. See *id.* at 442-443.

Courts of appeals, including the court of appeals below, have applied *Smith* and *Miller* to reject individuals’ Fourth Amendment privacy interests in their Internet traffic information, even while calling on this Court for guidance on the question. In the decision below, for example, the court of appeals considered itself “bound” by *Smith* “until and unless it is overruled by the Supreme Court.” App., *infra*, 33a. Similarly, the Seventh Circuit has noted that, although “at least one Justice believes ‘it may be necessary’ to reconsider the third-party doctrine * * *, [u]ntil the Court says otherwise, [*Smith* and *Miller*] bind us.” *United States v. Cairra*, 833 F.3d 803, 809 (7th Cir. 2016) (citation omitted), petition for cert. pending, No. 16-6761 (filed Nov. 7, 2016).

The Third Circuit, in particular, has flagged the conundrum facing the lower courts. In *United States v. Stanley*, 753 F.3d 114, cert. denied, 135 S. Ct. 507 (2014), the defendant surreptitiously connected his computer to his neighbor’s wireless router and used his neighbor’s network to download child pornography. Although the Third Circuit held that the defendant could not claim any legitimate expectation of privacy in the information he transmitted while “wrongful[ly]” connected to his neighbor’s wireless network, it cautioned that the district court “went too far” in relying on *Smith* categorically to reject any privacy interest in the defendant’s wireless signal. *Stanley*, 753 F.3d at 120-123. The court reasoned that such an approach would “open a veritable Pandora’s Box

of Internet-related privacy concerns,” because “[t]he Internet, by its very nature, requires *all* users to transmit their signals to third parties.” *Id.* at 124.

To be sure, some courts have considered the question presented to be “constitutionally indistinguishable from [the question in] *Smith*,” *United States v. Forrester*, 512 F.3d 500, 510 (9th Cir. 2008), despite this Court’s admonition in a similar context that “any extension” of analog-era reasoning to digital data “has to rest on its own bottom.” *Riley*, 134 S. Ct. at 2489; see, e.g., *United States v. Christie*, 624 F.3d 558, 573-574 (3d Cir. 2010), cert. denied, 562 U.S. 1236 (2011); *United States v. Bynum*, 604 F.3d 161, 164 (4th Cir.), cert. denied, 560 U.S. 977 (2010). But those decisions only underscore the necessity of this Court’s intervention. Calling the Internet traffic information collected by pen/traps today “constitutionally indistinguishable” from the list of telephone numbers at issue in *Smith* is “like saying a ride on horseback is materially indistinguishable from a flight to the moon”: “[b]oth are ways of getting from point A to point B, but little else justifies lumping them together.” *Riley*, 134 S. Ct. at 2488. The Court should address the question presented and provide lower courts with guidance pertinent to the application of Fourth Amendment principles to modern Internet technology.

2. This Term, the Court is already considering a closely related question in *Carpenter*: namely, whether the warrantless seizure and search of historical cell phone records revealing the location and movements of a cell phone user is permitted by the Fourth Amendment. See Pet. at i, *Carpenter*, *supra*. This case presents an ideal opportunity for the Court to resolve a similar legal question concerning Internet traffic information in tandem with the question presented in *Carpenter*. Both *Carpenter* and this case turn on whether lower courts are correct

in applying the rationale of *Smith* and *Miller* to certain types of data transmitted to third parties. Indeed, in the decision below in this case, the court of appeals cited the Sixth Circuit's decision in *Carpenter* for the proposition that courts have not extended Fourth Amendment protection to information concerning IP addresses. App., *infra*, 34a.

This case is an appropriate companion case to *Carpenter* because the Internet traffic information at issue here is broader in important ways than the cell site location information at issue in *Carpenter*. In addition to allowing the government to determine when petitioner was accessing the Internet from the privacy of his own home, the information gathered by the pen/traps here permitted the government to determine the websites to which petitioner connected, the length of the connections, and the port of transmission of the data. As this Court has recognized, the collection of such Internet information could reveal “an individual’s private interests or concerns.” *Riley*, 134 S. Ct. at 2490.

Accordingly, a decision in the government’s favor in *Carpenter* is unlikely to resolve the question presented here, because *Carpenter* provides no opportunity for the Court to rule on Internet traffic information (such as information concerning IP addresses and ports of transmission). The Court’s decision in *Carpenter* thus may leave the lower courts without the specific guidance they need. Such a piecemeal approach would deprive law enforcement of “clear rules” regarding such data, and “it would take many cases and many years” for the federal courts of appeals to reevaluate and adjust their approach to Internet traffic information. *Riley*, 134 S. Ct. at 2497 (Alito, J., concurring in part and concurring in judgment). In that time, “the nature of the electronic devices” possessed

by “ordinary Americans * * * would continue to change.” *Ibid.*

It would be most efficient for the Court to resolve the question presented in this case now, while it is considering a related question in *Carpenter*. Such an approach would enable the Court’s decision in each case to be informed by the potential implications presented by the other.

3. At a minimum, the Court should hold this petition pending its decision in *Carpenter*. Notably, the Court appears to be holding another petition presenting a similar question concerning the Fourth Amendment interest in IP address information. See *United States v. Caira, supra* (No. 16-6761). In *Caira*, the government identified alleged criminal activity associated with a particular Hotmail address and issued an administrative subpoena to Microsoft, which owns the Hotmail domain. See 833 F.3d at 805. In response, Microsoft disclosed a list of IP addresses used to access the e-mail account. See *ibid.* Identifying one of the IP addresses, the government issued a second administrative subpoena to Comcast to identify the physical address associated with that IP address. See *ibid.* The defendant moved to suppress the evidence, arguing that he possessed a Fourth Amendment privacy interest in information concerning IP addresses, but the Seventh Circuit rejected the defendant’s claim by invoking *Smith* and *Miller*. See *id.* at 806-807.

In light of the Court’s apparent conclusion that *Caira* presents a similar enough question for that petition to be held pending *Carpenter*, this petition should at a minimum also be held. Both this case and *Caira* turn on whether information that may be collected incident to an individual’s Internet browsing activity, including information concerning IP addresses, is entitled to Fourth Amendment protection. And both courts of appeals relied centrally on *Smith* and *Miller* in rejecting the defendants’

arguments. If the Court does not grant certiorari outright in this case, therefore, it should at least hold the petition pending the resolution of *Carpenter*.

B. The Decision Below Is Erroneous

1. *Internet Traffic Information Is Not Analogous To The Telephone Routing Information Gathered In Smith v. Maryland*

In upholding the warrantless seizure at issue here, the court of appeals explained that collecting Internet traffic information (such as information concerning IP addresses and ports of transmission) was “precisely analogous to the capture of telephone numbers at issue in *Smith*.” App., *infra*, 33a. But *Smith* is distinguishable from this case in important respects and should not be extended to Internet traffic information. In *Smith*, the pen register that was applied to the defendant’s telephone had only “limited capabilities”: it could not tell the government “the purport of any communication between the caller and the recipient of the call, their identities, nor whether the call was even completed.” 442 U.S. at 741-742 (citation omitted). Here, by contrast, the pen/traps allowed the government to “identify the source and destination IP addresses, along with the dates, times, durations, ports of transmission, and any Transmission Control Protocol (“TCP”) connection data, associated with any electronic communications sent to or from” petitioner’s devices, including his laptop and his wireless router. App., *infra*, 30a-31a (alteration, footnote, and citation omitted). Each of these categories of data is significant individually; collectively, they far exceed the data collected by the pen register at issue in *Smith*.

a. To begin with, unlike in *Smith*, the government could identify the “purport of any communication” at issue

here, because it collected the ports of transmission of petitioner’s Internet activity. A “port” is a piece of information used to identify the purpose of a particular packet of data being transmitted between computers. D. Ct. Dkt. 57, at 9 (¶ 19 n.10); see PC Magazine, *Definition of TCP/IP Port* <tinyurl.com/portdefinition> (last visited Dec. 22, 2017). For example, if port numbers “80” or “443” appeared in connection with petitioner’s Internet activity, the government would know that petitioner was accessing a webpage. Similarly, if port numbers “25,” “110,” or “143” appeared, the government would know that petitioner was using an e-mail application.

b. More broadly, an individual’s Internet traffic information is far more sensitive than the telephone routing information at issue in *Smith*. As this Court has observed, “[a]n Internet search and browsing history * * * [can] reveal an individual’s private interests or concerns—perhaps a search for certain symptoms of disease, coupled with frequent visits to WebMD.” *Riley*, 134 S. Ct. at 2490. Extending *Smith* and *Miller* to Internet traffic information would allow the government to access significant information about an individual’s Internet habits without a warrant and without probable cause. For example, the government could learn that the individual regularly visits websites associated with a particular political party or sexual orientation, “enabl[ing] the Government to ascertain, more or less at will, [people’s] political and religious beliefs, sexual habits, and so on.” *United States v. Jones*, 565 U.S. 400, 416 (2012) (Sotomayor, J., concurring).

Individuals today use the Internet to apply for jobs, find love, answer questions, keep up with news and politics, and engage with one another on “websites integral to the fabric of our modern society and culture.” *Packingham v. North Carolina*, 137 S. Ct. 1730, 1738 (2017). Some 90% of U.S. adults today use the Internet, and 77% report

that they use it either “several times a day” or “almost constantly.” Pew Research Center, *Tech Adoption Climbs Among Older Adults* 7, 21 (May 17, 2017) <tinyurl.com/pewtechuse>.

In *Smith*, the government could not even determine whether a connection was completed. 442 U.S. at 741. Here, by contrast, the government’s data not only showed whether a connection “was * * * completed,” *ibid.*, but also for how long the connection lasted—far more detail than the pen register provided in *Smith*.

What is more, pen/traps revealing IP address information can also allow the government to identify an individual’s general location, as the government demonstrated at petitioner’s trial. See Tr. 102-103, 105-106 (Jan. 13, 2015). In addition, by placing pen/traps on petitioner’s laptop and wireless router, the government could determine when petitioner was using his laptop in his home by monitoring when petitioner’s laptop was connected to the Internet.

In that respect, the government turned petitioner’s laptop into an analogue of the tracking device at issue in *United States v. Karo*, 468 U.S. 705 (1984). In that case, the Court held that the government conducted an unconstitutional search when it monitored a signal from a tracking device in the defendant’s home without a warrant. *Id.* at 718. The Court observed that, even when a digital tracking device is accompanied by conventional surveillance, it implicates the Fourth Amendment because it confirms for the government that “a particular article is actually located at a particular time in the private residence” and that the article “remains on the premises”—information that the government “could not have otherwise obtained without a warrant.” *Id.* at 715. Here, as in *Karo*, the government should not be “free * * * to determine by means of an electronic device, without a warrant and

without probable cause or reasonable suspicion, whether a particular article—or a person, for that matter—is in an individual’s home at a particular time.” *Id.* at 716.

The significant breadth and sensitivity of Internet traffic information distinguishes this case from *Smith* and counsels in favor of Fourth Amendment protection. Extending *Smith* and *Miller* to Internet traffic information “entrust[s] to the Executive” tremendous power that is “amenable to misuse” and runs counter to “the Fourth Amendment’s goal to curb arbitrary exercises of police power and prevent ‘a too permeating police surveillance.’” *Jones*, 565 U.S. at 416-417 (Sotomayor, J., concurring) (quoting *United States v. Di Re*, 332 U.S. 581, 595 (1948)). When agents can gather an individual’s Internet traffic information upon only the minimal showing required by the Electronic Communications Privacy Act, little beyond their discretion constrains their ability to monitor citizens’ private lives. And an agent’s choice to exercise discretion is no substitute for clear limits imposed by an impartial magistrate. See *Katz v. United States*, 389 U.S. 347, 356-357 (1967).

c. In many cases, moreover, Internet traffic information is not shared voluntarily, because computers and other devices often connect to the Internet without requiring a user to act. Applications on those devices automatically connect to Internet servers and check for updates, fetch e-mail, or send data without users’ knowledge. That information can be valuable—for example, to establish that an individual has certain software installed on his computer. But it cannot be said to have been “voluntarily conveyed” to a third party. *Smith*, 442 U.S. at 744.

Even when a user voluntarily acts to enter an Internet address into his browser, the “voluntary” disclosure of that information is unlike the disclosure in *Smith*. There,

the Court reasoned, telephone customers knew that companies recorded the numbers they dialed because telephone customers could “see a list of their long-distance (toll) calls on their monthly bills.” 442 U.S. at 742. Internet service providers, by contrast, do not provide that information to their customers, nor do they routinely share information about ports of transmission.

2. *Individuals Have A Reasonable Expectation Of Privacy In Their Internet Traffic Information*

The court of appeals applied *Smith* and *Miller* to hold that conveying Internet traffic information to a third party destroyed any privacy interest in that information. But there is no reason to extend those decisions to the information at issue in this case. Internet users may not even understand that they are providing that sensitive and revealing information, much less that they are relinquishing any expectation of privacy by conveying it. As this Court recently cautioned, reflexively relying on “pre-digital analogue[s]” risks “a significant diminution of privacy.” *Riley*, 134 S. Ct. at 2493.

Individuals overwhelmingly consider their Internet browsing habits to be private. A 2014 Pew Research survey found that 70% of adults consider the websites they have visited to be “very sensitive” or “somewhat sensitive” information. Pew Research Center, *Public Perceptions of Privacy and Security in the Post-Snowden Era* 37 (Nov. 12, 2014) <tinyurl.com/privacystudy>. As Justice Sotomayor has noted, it is “doubt[ful] that people would accept without complaint the warrantless disclosure to the government of a list of every Web site they had visited in the last week, or month, or year.” *Jones*, 565 U.S. at 418 (concurring opinion). Yet that is precisely what can happen when the government places a pen/trap on individuals’ computers.

This problem, moreover, is no longer limited merely to Internet traffic from desktop and laptop computers; it applies with equal force to any Internet-enabled device that connects to a wireless network. If petitioner's smart-phone had been connected to his wireless network at home, the Internet traffic information from that phone would have traveled through his router and been captured by the government's pen/trap. To the extent that traffic associated with data sent to or from any of the many applications on a user's phone will be swept into the government's net, the court of appeals' holding implicates many of the concerns this Court has already addressed in *Riley*. See 134 S. Ct. at 2490 (describing "apps for alcohol, drug, and gambling addictions; apps for sharing prayer requests; apps for tracking pregnancy symptoms; apps for planning your budget; apps for every conceivable hobby or pastime; [and] apps for improving your romantic life"). Indeed, the government can readily identify which applications an individual has on his phone from the destination IP addresses of the data transmitted from those applications.

It is not difficult to conclude that individuals have a reasonable expectation of privacy that is cognizable under the Fourth Amendment in the highly personal information that may be revealed by a pen/trap collecting Internet traffic information. The government should not be free to collect that information without the constraint of a warrant or any showing of probable cause.

C. The Question Presented Warrants Review In This Case

This case presents a timely opportunity to consider the question presented on a well-developed record.

1. This case presents the constitutional question in an ideal context for addressing the relationship between

Smith and modern technology. The Internet traffic information gathered in this case was significant both in quantity and quality. The pen/trap orders permitted the government prospectively to collect petitioner's Internet traffic information for 60 days. See Pet. C.A. Br. 110. Ultimately, the government collected gigabytes of data on petitioner's Internet activity over a matter of weeks, and swept in tens of thousands of individual transmissions, if not more.

The pen/trap on petitioner's laptop, in particular, allowed the government to identify when petitioner was connected to the Internet, which websites petitioner accessed during his browsing session, and for how long. That information was much more invasive than, for example, the information collected in *Caira*, which was limited to historical records of IP addresses that had accessed a particular e-mail account (along with the physical address associated with the defendant's IP address). See 833 F.3d at 805. And this case offers the Court an opportunity to address the question presented in the context of the Electronic Communications Privacy Act, the statute governing the issuance of orders authorizing pen registers and trap and trace devices.

2. The question presented was also preserved at each stage of the proceedings below. In the district court, petitioner argued that "the information obtained through the [pen/trap orders] should have been the subject of a warrant application," and he specifically argued that *Smith* did not apply. App., *infra*, 141a-142a & n.14. And the court of appeals, recognizing that petitioner "made the same arguments" in the district court, addressed the question presented at length, ultimately concluding that it was bound by *Smith* to reject petitioner's claims "until and unless it is overruled by the Supreme Court." *Id.* at 31a n.28, 33a. The question presented is thus ripe for the

Court's review in this case, and the Court's guidance on that question is sorely needed.

II. THIS COURT SHOULD GRANT REVIEW TO DECIDE WHETHER THE SIXTH AMENDMENT PERMITS A JUDGE TO FIND THE FACTS NECESSARY TO SUPPORT AN OTHERWISE UNREASONABLE SENTENCE

This case also presents the unrelated, but equally important, question whether the Sixth Amendment permits judges, as opposed to juries, to find facts necessary to render a sentence reasonable. This Court has repeatedly “left [that question] for another day.” *Jones v. United States*, 135 S. Ct. 8, 8-9 (2014) (Scalia, J., dissenting from the denial of certiorari). And as in this case, the courts of appeals have interpreted the Court's silence as consent to the proposition that an otherwise unreasonable sentence supported by judicial factfinding is constitutional as long as it is within the statutory sentencing range—despite the contrary import of the Court's sentencing decisions.

“This has gone on long enough.” *Jones*, 135 S. Ct. at 9 (Scalia, J., dissenting from the denial of certiorari). And it is hard to imagine a better example of the consequences of runaway judicial factfinding than this case. Petitioner, a young man with no criminal history, was sentenced to life imprisonment without the possibility of parole for drug crimes that do not ordinarily carry that sentence, based substantially on numerous factual findings made by the sentencing judge by a preponderance of the evidence. The Court should finally resolve this long-unsettled question and put an end to unconstitutional sentences such as petitioner's.

A. The Question Presented Is An Important One Expressly Reserved By This Court And Subject To Extensive Debate By Judges In The Lower Courts

1. In *Rita v. United States*, 551 U.S. 338 (2007), this Court held that applying a presumption of reasonableness to within-Guidelines sentences is constitutional on the ground that the Sixth Amendment does not “automatically forbid” a judge from taking account of factual matters not determined by the jury. *Id.* at 352. Justice Scalia, joined by Justice Thomas, expressed concern that this scheme would lead to “constitutional violations” if a defendant’s sentence is “upheld as reasonable only because of the existence of judge-found facts.” *Id.* at 374 (opinion concurring in part and concurring in the judgment). In response, the Court stated that that question was “not presented by this case.” *Id.* at 353. Justice Stevens, joined by Justice Ginsburg, noted that “[s]uch a hypothetical case should be decided if and when it arises.” *Id.* at 366 (concurring opinion).

Seven years later, Justice Scalia, joined by Justices Thomas and Ginsburg, noted the pressing need for the Court to resolve the question. See *Jones*, 135 S. Ct. at 8-9 (opinion dissenting from the denial of certiorari). Justice Scalia observed that, ever since the question was reserved in *Rita*, the courts of appeals had “uniformly taken our continuing silence” on the question as “suggest[ing] that the Constitution *does* permit otherwise unreasonable sentences supported by judicial factfinding, so long as they are within the statutory range.” *Id.* at 9. Justice Scalia urged the Court to grant certiorari in an appropriate case in order to “put an end to the unbroken string of cases disregarding the Sixth Amendment—or to eliminate the Sixth Amendment difficulty by acknowledging that all sentences below the statutory maximum are substantively reasonable.” *Ibid.*

Shortly after Justice Scalia’s opinion in *Jones*, then-Judge Gorsuch similarly observed that “[i]t is far from certain whether the Constitution allows” a judge to increase a defendant’s sentence within the statutorily authorized range “based on facts the judge finds without the aid of a jury or the defendant’s consent.” *United States v. Sabillon-Umana*, 772 F.3d 1328, 1331 (10th Cir. 2014) (citing *Jones*). Three years later, however, that question remains unanswered by the Court, despite intervening opportunities to address it.

2. As several members of the Court have now recognized, the lower courts will continue to authorize sentences that would be unreasonable but for judge-found facts until this Court intervenes. In the decision below, the court of appeals rejected petitioner’s Sixth Amendment argument as having “no support in existing law.” App., *infra*, 106a n.72. And other courts have declined to adopt similar arguments in the absence of clearer guidance from this Court, despite admitting that “there is room for debate.” *United States v. Briggs*, 820 F.3d 917, 922 (8th Cir. 2016), cert. denied, 137 S. Ct. 617 (2017); *United States v. Cassius*, 777 F.3d 1093, 1099 n.4 (10th Cir.) (calling argument about judge-found sentencing facts “precluded by binding precedent” but citing *Jones*), cert. denied, 135 S. Ct. 2909 (2015); see also *United States v. Settles*, 530 F.3d 920, 923-924 (D.C. Cir. 2008) (noting that “we understand why defendants find it unfair for district courts to rely on acquitted conduct when imposing a sentence,” but ultimately relying on “binding precedent” to affirm the sentence), cert. denied, 555 U.S. 1140 (2009).

Numerous judges in the lower courts have urged a different approach or specifically importuned this Court to provide guidance, noting the importance of the question and the attendant uncertainty surrounding sentencing practices while the question remains open. See, *e.g.*,

United States v. White, 551 F.3d 381, 390 (6th Cir. 2008) (en banc) (Merritt, J., dissenting) (taking the position on behalf of six judges that, when judge-found enhancements increase the Guidelines range such that the sentence would be unreasonable absent those facts, “those judge-found facts are necessary for the lawful imposition of the sentence, thus violating the Sixth Amendment right to a jury trial”), cert. denied, 556 U.S. 1215 (2009); *United States v. Bell*, 808 F.3d 926, 932 (D.C. Cir. 2015) (per curiam) (Millett, J., concurring in denial of rehearing en banc) (noting that “only the Supreme Court can resolve the contradictions in the current state of the law”), cert. denied, 137 S. Ct. 37 (2016); *id.* at 927 (Kavanaugh, J., concurring in denial of rehearing en banc) (“shar[ing] Judge Millett’s overarching concern” and observing that a solution “would likely require” intervention by this Court).² The Court should accept the recurrent invitation to intervene and finally resolve the question presented.

B. The Decision Below Is Erroneous

The court of appeals erred when it concluded that petitioner’s Sixth Amendment argument had “no support” in existing law. App., *infra*, 107a n.72. In so concluding, the court of appeals ignored the development of this Court’s Sixth Amendment jurisprudence and the serious concerns raised by numerous members of this Court.

The Sixth Amendment was intended to preserve the “jury’s historic role as a bulwark between the State and the accused at the trial for an alleged offense.” *Southern*

² See also *United States v. Canania*, 532 F.3d 764, 776-778 (8th Cir.) (Bright, J., concurring), cert. denied, 555 U.S. 1037 (2008); *United States v. Mercado*, 474 F.3d 654, 663 (9th Cir. 2007) (Fletcher, J., dissenting), cert. denied, 552 U.S. 1297 (2008); *United States v. Faust*, 456 F.3d 1342, 1349 (11th Cir.) (Barkett, J., specially concurring), cert. denied, 549 U.S. 1046 (2006).

Union Co. v. United States, 567 U.S. 343, 350 (2012) (citation omitted). The Sixth Amendment’s guarantee of a trial by jury is a constitutional protection “of surpassing importance,” *Apprendi v. New Jersey*, 530 U.S. 466, 476–477 (2000), and it “has occupied a central position in our system of justice by safeguarding a person accused of a crime against the arbitrary exercise of power by prosecutor or judge,” *Batson v. Kentucky*, 476 U.S. 79, 86 (1986).

As is relevant here, the jury trial right is a “fundamental reservation” of jury power that ensures that a judge’s “authority to sentence derives *wholly* from the jury’s verdict.” *Blakely v. Washington*, 542 U.S. 296, 306 (2004) (emphasis added). In *Apprendi*, this Court held that “facts that increase the prescribed range of penalties to which a criminal defendant is exposed” must either be admitted by the defendant or submitted to a jury. 530 U.S. at 490; see *Blakely*, 542 U.S. at 303. The Court reaffirmed that principle in *Alleyne v. United States*, 133 S. Ct. 2151 (2013), explaining that, “[w]hen a finding of fact alters the legally prescribed punishment so as to aggravate it, the fact necessarily forms a constituent part of a new offense and must be submitted to the jury.” *Id.* at 2162. Most recently, in *Hurst v. Florida*, 136 S. Ct. 616 (2016), the Court declared Florida’s capital sentencing scheme unconstitutional under the Sixth Amendment because it permitted a judge, not a jury, to find the aggravating circumstances necessary to support a defendant’s sentence. *Id.* at 624.

The foregoing principles apply with equal force where, as here, judicial factfinding alters the Guidelines range and thereby encourages the court to impose a sentence that would otherwise be substantively unreasonable. Although the Sentencing Guidelines are no longer mandatory, they “remain the starting point for every sentencing calculation in the federal system.” *Peugh v. United*

States, 133 S. Ct. 2072, 2083 (2013). “[I]f the judge uses the sentencing range as the beginning point” for the sentencing decision, “*then the Guidelines are in a real sense the basis for the sentence*,” even if the ultimate sentence deviates from the Guidelines range. *Ibid.* (citation omitted). A sentencing court is not free to impose a sentence, even if it falls within the statutory range, without taking account of the Guidelines range and explaining any variance. To do otherwise constitutes procedural error and results in an unlawful sentence. See *ibid.*

In the absence of a decision by this Court squarely addressing the question presented, however, the Sixth Amendment right to trial by jury is being “lost * * * by erosion.” *Apprendi*, 530 U.S. at 483 (citation omitted). The government is now frequently permitted a “second bite at the apple” at sentencing when it presents a judge with conduct for which the defendant was acquitted or (as here) not even charged. That strategy—whereby the government relies on facts the jury either refused or had no opportunity to find—“entirely trivializes” the jury’s “principal fact-finding function.” *Canania*, 532 F.3d at 776 (Bright, J., concurring).

Even within the statutory range, there are sentences that would be unlawful but for a judge’s factfinding. Under this Court’s Sixth Amendment precedents, facts that justify an otherwise unreasonable sentence must be found by a jury or admitted by the defendant before they can be used to increase the defendant’s sentence. This Court should grant review and definitively hold that the practice of sustaining an otherwise unreasonable sentence through judicial factfinding is unconstitutional.

C. The Question Presented Warrants Review In This Case

This case is a particularly egregious example of judicial factfinding. Petitioner was convicted by the jury of distributing “one kilogram or more” of heroin, “five kilograms or more” of cocaine, “ten grams or more” of LSD, and “500 grams or more” of methamphetamine. D. Ct. Dkt. 183, at 1-3 (Feb. 5, 2015) (verdict form). Petitioner was not charged with, and the jury was never asked to render a verdict on, the alleged commissioning of murders connected to the Silk Road.

At sentencing, however, the district court made a number of factual findings—most significantly, that petitioner commissioned five murders and distributed a total quantity of drugs far in excess of that found by the jury. Those factual findings greatly increased petitioner’s Guidelines range. C.A. App. 1462-1470; App., *infra*, 26a-27a. The judge also made findings that six drug deaths were “in some way” related to the Silk Road, although those deaths similarly were not charged in the indictment or part of the jury’s verdict. C.A. App. 1472. In all, the district court’s factual findings resulted in enhancements that raised petitioner’s Guidelines sentencing range from a determinate range of no more than thirty years to a “range” of life imprisonment. App., *infra*, 26a-27a.

The court of appeals acknowledged as much: it confirmed that petitioner’s “high offense level” under the Guidelines “largely resulted” from the district court’s findings about the “quantity of drugs trafficked using Silk Road” as well as the enhancement for “directing the use of violence.” App., *infra*, 26a-27a. Although the court of appeals stated that “a life sentence for selling drugs alone would give us pause,” it ultimately found petitioner’s life sentence substantively reasonable because of the district court’s findings. *Id.* at 100a-101a & n.68.

Absent those findings, petitioner’s sentence of life imprisonment would plainly have been substantively unreasonable. As the Sentencing Commission has recognized, “[t]he drug trafficking guidelines specifically provide for a sentence of life imprisonment * * * only where death or serious bodily injury resulted from the use of the drug” and the defendant has prior convictions. United States Sentencing Commission, *Life Sentences in the Federal System* 3 (Feb. 2015) (footnote omitted) <tinyurl.com/ussclife>. In cases involving “very large” quantities of drugs and significant prior criminal history, “the sentencing range can include life imprisonment * * * only as the sanction at the top of the range.” *Ibid.* Here, however, petitioner is a young first-time offender who was never charged with causing any death or bodily injury. This case directly implicates the question presented, and it does so in the most acute of circumstances: a high-profile criminal prosecution that heaped intense scrutiny and pressure on the sentencing judge, resulting in a sentence of life imprisonment without parole for a first-time offender.

In this case, the sentencing judge’s factual findings elevated the Guidelines range from a determinate range of no more than thirty years to a “range” of life imprisonment, “condemn[ing] a young man to die in prison.” App., *infra*, 108a. The unconstitutional practice of judicial fact-finding “has gone on long enough.” *Jones*, 135 S. Ct. at 9 (Scalia, J., dissenting from the denial of certiorari). The Court should grant certiorari on that question, as well as the Fourth Amendment question, and review this consequential conviction and sentence on the merits.

CONCLUSION

The petition for a writ of certiorari should be granted.
Respectfully submitted.

KANNON K. SHANMUGAM
ALLISON JONES RUSHING
MASHA G. HANSFORD
MICHAEL J. MESTITZ
WILLIAMS & CONNOLLY LLP
725 Twelfth Street, N.W.
Washington, DC 20005
(202) 434-5000
kshanmugam@wc.com

DECEMBER 2017

APPENDIX

TABLE OF CONTENTS

Appendix A:	Court of appeals order, August 30, 2017	1a
Appendix B:	Court of appeals opinion, May 31, 2017	3a
Appendix C:	District court opinion and order, October 10, 2014.....	109a

APPENDIX A

UNITED STATES COURT OF APPEALS FOR THE SECOND CIRCUIT

At a stated term of the United States Court of Appeals for the Second Circuit, held at the Thurgood Marshall United States Courthouse, 40 Foley Square, in the City of New York, on the 30th day of August, two thousand seventeen.

United States of America,

Appellee,

ORDER

Docket No. 15-1815

v.

Ross William Ulbricht,
AKA Dread Pirate Roberts,
AKA Silk Road, AKA Sealed
Document 1, AKA DPR,

Defendant – Appellant.

Appellant, Ross William Ulbricht, filed a petition for panel rehearing, or, in the alternative, for rehearing *en banc*. The panel that determined the appeal has considered the request for panel rehearing, and the active

2a

members of the Court have considered the request for rehearing *en banc*.

IT IS HEREBY ORDERED that the petition is denied.

FOR THE COURT:
Catherine O'Hagan Wolfe, Clerk




APPENDIX B

UNITED STATES COURT OF APPEALS
FOR THE SECOND CIRCUIT

August Term, 2016
Docket No. 15-1815

UNITED STATES OF AMERICA,
APPELLEE,

v.

ROSS WILLIAM ULBRICHT, a/k/a DREAD
PIRATE ROBERTS, a/k/a SILK ROAD,
a/k/a SEALED DEFENDANT 1, a/k/a DPR,
DEFENDANT-APPELLANT.

Argued: October 6, 2016
Decided: May 31, 2017

Before NEWMAN, LYNCH, and DRONEY, Circuit
Judges.

OPINION

GERALD E. LYNCH, Circuit Judge.

Defendant Ross William Ulbricht appeals from a judgment of conviction and sentence to life imprisonment entered in the United States District Court for the Southern District of New York (Katherine B. Forrest, *J.*). A jury convicted Ulbricht of drug trafficking and other crimes associated with his creation and operation of Silk Road, an online marketplace whose users primarily purchased and sold illegal goods and services. He challenges several aspects of his conviction and sentence, arguing that (1) the district court erred in denying his motion to suppress evidence assertedly obtained in violation of the Fourth Amendment; (2) the district court committed numerous errors that deprived him of his right to a fair trial, and incorrectly denied his motion for a new trial; and (3) his life sentence is both procedurally and substantively unreasonable. Because we identify no reversible error, we **AFFIRM** Ulbricht’s conviction and sentence in all respects.

BACKGROUND

In February 2015, a jury convicted Ross William Ulbricht on seven counts arising from his creation and operation of Silk Road under the username Dread Pirate Roberts (“DPR”).¹ Silk Road was a massive, anonymous criminal marketplace that operated using the Tor Network,

¹ The seven crimes of conviction were: (1) distribution and aiding and abetting distribution of narcotics, 21 U.S.C. § 812, § 841(a)(1), § 841(b)(1)(A) and 18 U.S.C. § 2; (2) using the Internet to distribute narcotics, 21 U.S.C. § 812, § 841(h) and § 841(b)(1)(A); (3) conspiracy to distribute narcotics, 21 U.S.C. § 846; (4) engaging in a continuing criminal enterprise, 21 U.S.C. § 848(a); (5) conspiring to obtain unauthorized access to a computer for purposes of commercial advantage and private financial gain and in furtherance of other criminal and tortious acts, 18 U.S.C. § 1030(a)(2) and § 1030(b); (6) conspiring to

which renders Internet traffic through the Tor browser extremely difficult to trace.² Silk Road users principally bought and sold drugs, false identification documents, and computer hacking software. Transactions on Silk Road exclusively used Bitcoins, an anonymous but traceable digital currency.³ The site also contained a private message system, which allowed users to send messages to each other (similar to communicating via email), a public forum to discuss topics related to Silk Road, and a “wiki,” which is like an encyclopedia that users could access to receive advice about using the site. Silk Road customers and vendors could also access a support section of the website to seek help from the marketplace’s administrators when an issue arose.

traffic in fraudulent identification documents, 18 U.S.C. § 1028(f); and (7) conspiring to launder money, 18 U.S.C. § 1956(h).

² Tor is short for the “The Onion Router.” The Tor Network is “a special network on the Internet designed to make it practically impossible to physically locate the computers hosting or accessing websites on the network.” App’x 53. The Tor Network can be accessed via the Tor browser using software that anyone may obtain for free on the Internet.

³ Bitcoins allow vendors and customers to maintain their anonymity in the same way that cash does, by transferring Bitcoins between anonymous Bitcoin accounts, which do not contain any identifying information about the user of each account. The currency is “traceable” in that the transaction history of each individual Bitcoin is logged in what is called the blockchain. The blockchain prevents a person from spending the same Bitcoin twice, allowing Bitcoin to operate similarly to a traditional form of currency. Bitcoin is also a completely decentralized currency, operating free of nation states or central banks; anyone who downloads the Bitcoin software becomes part of the Bitcoin network. The blockchain is stored on that network, and the blockchain automatically “self-updates” when a Bitcoin transaction takes place. Tr. 160.

According to the government, between 2011 and 2013, thousands of vendors used Silk Road to sell approximately \$183 million worth of illegal drugs, as well as other goods and services. Ulbricht, acting as DPR, earned millions of dollars in profits from the commissions collected by Silk Road on purchases. In October 2013, the government arrested Ulbricht, seized the Silk Road servers, and shut down the site.

I. Silk Road Investigation

After Ulbricht created Silk Road in 2011, the site attracted the interest of at least two separate divisions of the Department of Justice:⁴ the United States Attorney's Offices for the District of Maryland and for the Southern District of New York. Throughout the investigations, law enforcement agents knew that the person using Dread Pirate Roberts as his or her Silk Road username had created and managed the site, but they did not know DPR's actual identity. In 2012 and 2013, agents from both offices investigated several individuals who the government suspected were operating Silk Road as DPR. Those individuals included Ulbricht, Anand Athavale, and Mark Karpeles. Ultimately, the New York office identified Ulbricht as DPR, but the Maryland office had investigated and later abandoned the theory that either Athavale or Karpeles might have been Dread Pirate Roberts.

Two aspects of the pre-arrest investigation into Ulbricht are particularly relevant to this appeal: (1) the pen/trap orders that the government obtained to monitor Internet Protocol ("IP") address traffic to and from various devices associated with Ulbricht; and (2) the corrupt

⁴ The government first learned of Silk Road and began investigating it in 2011 after international packages containing drugs were intercepted at Chicago's O'Hare airport.

behavior of two Baltimore agents who worked on the Silk Road investigation.

A. The Pen/Trap Orders

In September 2013, after Ulbricht became a primary suspect in the DPR investigation, the government obtained five “pen/trap” orders. *See* 18 U.S.C. §§ 3121-27 (“Pen/Trap Act”). The orders authorized law enforcement agents to collect IP address data for Internet traffic to and from Ulbricht’s home wireless router and other devices that regularly connected to Ulbricht’s home router. According to the government’s applications for the pen register and trap and trace device, “[e]very device on the Internet is identified by a unique number” called an IP address. S.A. 73.⁵ “This number is used to route information between devices, for example, between two computers.” *Id.* at 73-74. In other words, an “IP address is analogous to a telephone number” because “it indicates the online identity of the communicating device without revealing the communication’s content.” *Id.* at 74. Ulbricht does not dispute that description of how IP addresses function.

The pen/trap orders thus did not permit the government to access the content of Ulbricht’s communications, nor did the government “seek to obtain[] the contents of any communications.” *Id.* at 75. According to Ulbricht, the government’s use of his home Internet routing data violated the Fourth Amendment because it helped the government match Ulbricht’s online activity with DPR’s use of Silk Road. Ulbricht argues that he has a constitutional privacy interest in IP address traffic to and from his home

⁵ S.A. refers to the joint sealed appendix in this case. Portions of the sealed appendix quoted in this opinion are to that extent unsealed.

and that the government obtained the pen/trap orders without a warrant, which would have required probable cause.

B. Corrupt Agents Force and Bridges

One of the many other tactics that the government used to expose DPR's identity was to find low-level Silk Road administrators who helped DPR maintain the site, obtain their cooperation, take over their Silk Road usernames, and chat with DPR under those identities. The true owners of the administrator accounts would assist in the investigation by helping the government chat with DPR and access various aspects of the site. Government agents would also create their own new usernames and pose as drug dealers or buyers to purchase or sell narcotics and occasionally contact DPR directly. One of the government's principal trial witnesses, Special Agent Jared Der-Yeghiayan, used the former technique to chat with DPR under the name Cirrus. Cirrus had been a member of the Silk Road support staff before the government took over his account, and Der-Yeghiayan frequently used Silk Road's messaging system to communicate with DPR and other administrators as Cirrus. Cirrus also gave the government access to the staff chat, a separate program allowing DPR to communicate only with his employees.

Two undercover agents involved in the Silk Road investigation are of particular import to this appeal: Secret Service Special Agent Shaun Bridges and Drug Enforcement Administration ("DEA") Special Agent Carl Force, both of whom were assigned to the Baltimore investigation. Both Force and Bridges used their undercover access to exploit the site for their own benefit in various ways, and they eventually pleaded guilty to criminal

charges in connection with their work on the Silk Road investigation.⁶

For example, Force and Bridges took over an administrator account belonging to Curtis Green, who worked for Silk Road under the name Flush. According to the criminal complaint against Force and Bridges, in January 2013, Bridges used the Flush username to change other users' passwords, empty their Bitcoin wallets,⁷ and keep \$350,000 in Bitcoins in offshore bank accounts, all while attempting to hide his activity through a series of transactions.⁸ Specifically, the complaint against Force and Bridges alleges that Bridges "act[ed] as an administrator to reset pins and passwords on various Silk Road vendors' accounts," then exchanged the Bitcoins for U.S. dollars

⁶ Both Force and Bridges pleaded guilty to money laundering and obstruction of justice; Force also pleaded guilty to extortion. Force was sentenced to 78 months in prison, and Bridges received a 71-month sentence.

⁷ According to the criminal complaint against Ulbricht, a Bitcoin wallet is a storage method for Bitcoins. The wallet is associated with a Bitcoin address, which is "analogous to the account number for a bank account, while the 'wallet' is analogous to a bank safe where the money in the account is physically stored." App'x 59. Users can transact in Bitcoin by transferring Bitcoins from one "Bitcoin address to the Bitcoin address of another user, over the Internet." *Id.* Ulbricht does not dispute that definition.

⁸ As described below, the government disclosed shortly before trial that Force was under investigation for Silk Road corruption, but said nothing about Bridges. Specifically, the pretrial disclosure noted that Force was under investigation for using the Flush account to steal \$350,000, but the criminal complaint against the agents alleges that Bridges committed that particular theft. According to the government, both Force and Bridges had access to the Flush account, which might explain their initial suspicion that Force stole the funds.

using the Mt. Gox exchanger.⁹ Supp. App'x 180. Shortly after he committed the January 2013 thefts, Bridges asked Force to chat with DPR as Nob, Force's authorized undercover username, to get advice about how to liquidate Bitcoins. He also sought Force's help in convincing Curtis Green (formerly Flush) to help him transfer Bitcoins to other accounts, and he ultimately tried to blame Green for the theft.

With the government's approval, Force also posed as a drug dealer and communicated with DPR as Nob. As part of his official undercover work as Nob, Force agreed to sell fraudulent identification documents to DPR for \$40,000 in Bitcoins. According to the criminal complaint against the agents, Force kept the Bitcoins received by his Nob account in connection with that transaction for his personal use. On another occasion, again as part of his authorized undercover work, Force advised DPR that he had access to information about Silk Road from an invented corrupt government employee. DPR paid Force \$50,000 in Bitcoins for purported inside law enforcement information; Force allegedly purloined that payment as well. Moreover, outside his authorized undercover work, Force operated another account under the name French Maid, through which he again offered to sell DPR information about the government's Silk Road investigation. Acting as French Maid, Force received about \$100,000 in Bitcoins that he kept for his personal use.

Force created yet another unauthorized Silk Road account, under the name DeathFromAbove, which was unknown to law enforcement until the defense identified it during trial. Force used the DeathFromAbove account to

⁹ Mt. Gox was a prominent Bitcoin exchanger owned by Mark Karpeles.

try to extort money from DPR. For example, in one such chat that took place on April 16, 2013, DeathFromAbove told DPR that he knew that DPR's true identity was Anand Athavale. DeathFromAbove demanded a payment of \$250,000 in exchange for which DeathFromAbove would remain silent about DPR's identity.¹⁰ There is no evidence that DPR made the requested payment to DeathFromAbove; indeed, DPR shrugged off the attempted blackmail as "bogus." App'x 710.

As will be explained in more detail below, the district court prevented Ulbricht from introducing evidence at trial related to Force's corruption because doing so would have exposed the ongoing grand jury investigation into Force's conduct. The district court also denied Ulbricht discovery related to the investigation and excluded certain hearsay statements that arguably revealed Force's corruption. Ulbricht contends on appeal that the district court's various rulings concerning evidence related to Force deprived him of a fair trial. Additionally, Ulbricht did not learn of Bridges's corrupt conduct until after trial when the criminal complaint against both agents was unsealed. Thus, in his motion for a new trial, he argued that the belated disclosure violated his due process rights under *Brady v. Maryland*, 373 U.S. 83 (1963). Ulbricht contends on appeal that the district court incorrectly denied that motion.

¹⁰ DeathFromAbove also referred to the \$250,000 payment he demanded as "punitive damages." App'x 875. In the government's view, the "punitive damages" remark referenced the murder of a Silk Road administrator that Ulbricht ordered and paid for (but that was never carried out). That and other killings that DPR commissioned will be described in more detail below.

II. Ulbricht's Arrest

Ulbricht was arrested in a San Francisco public library on October 1, 2013, after the government had amassed significant evidence identifying him as Dread Pirate Roberts. The arrest was successfully orchestrated to catch Ulbricht in the act of administering Silk Road as DPR. Federal agents observed Ulbricht enter the public library, and a few minutes later Dread Pirate Roberts came online in the Silk Road staff chat. Der-Yeghiayan, under the undercover administrator username Cirrus, initiated a chat with DPR, asking him to go to a specific place on the Silk Road site to address some flagged messages from users. Der-Yeghiayan reasoned that this would “force [Ulbricht] to log in under . . . his Dread Pirate Roberts account” in the Silk Road marketplace, as well as in the staff chat software. Tr. 331-32.

Once Der-Yeghiayan knew that DPR had logged onto the flagged message page in the marketplace, he signaled another agent to effect the arrest. Ulbricht was arrested, and incident to that arrest agents seized his laptop. The same chat that Der-Yeghiayan had initiated with Dread Pirate Roberts a few minutes earlier was open on Ulbricht's screen. Ulbricht also visited the flagged post in the marketplace that Der-Yeghiayan (as Cirrus) had asked DPR to look at during their chat. While he was chatting with Cirrus, moreover, Ulbricht had accessed Silk Road by using the “Mastermind” page. That page was available only to Dread Pirate Roberts.

A great deal of the evidence against Ulbricht came from the government's search of his laptop and his home after the arrest. On the day of Ulbricht's arrest, the government obtained a warrant to seize Ulbricht's laptop and search it for a wide variety of information related to Silk Road and information that would identify Ulbricht as

Dread Pirate Roberts. Ulbricht moved to suppress the large quantity of evidence obtained from his laptop, challenging the constitutionality of that search warrant. Ulbricht argues on appeal that the district court erred in denying his motion to suppress. More details concerning the search warrant will be described in context below.

III. The Trial

Ulbricht's trial lasted approximately three weeks, from January 13 through February 4, 2015. Judge Forrest handled the complex and contentious trial with commendable patience and skill. Although Ulbricht does not challenge the sufficiency of the evidence to support the jury's verdict on any of the counts of conviction, we summarize the evidence presented at trial as context for the issues raised on appeal.

A. The Government's Case

The government presented overwhelming evidence that Ulbricht created Silk Road in 2011 and continued to operate the site throughout its lifetime by maintaining its computer infrastructure, interacting with vendors, crafting policies for site users, deciding what products would be available for sale on the site, and managing a small staff of administrators and software engineers. Defense counsel conceded in his opening statement that Ulbricht did in fact create Silk Road.

According to Ulbricht's own words in a 2009 email, Ulbricht originally conceived of Silk Road as "an online storefront that couldn't be traced back to [him] . . . where [his] customers could buy [his] products" and pay for them "anonymously and securely." Tr. 991. From 2009 through 2011, Ulbricht worked to get the site up and running, relying on computer programming assistance from others, including his friend Richard Bates. According to

one of the journal entries discovered on his laptop, in 2010 Ulbricht began to grow hallucinogenic mushrooms to sell on the site “for cheap to get people interested.” Tr. 899. As the site began to garner significant interest in 2011, Ulbricht wrote in his journal that he was “creating a year of prosperity and power beyond what I have ever experienced before. Silk Road is going to become a phenomenon and at least one person will tell me about it, unknowing that I was its creator.” Tr. 899-900.

1. Evidence Linking Ulbricht to Dread Pirate Roberts

Around January 2012, the Silk Road user who represented himself as the lead administrator of the site adopted the username Dread Pirate Roberts.¹¹ The name alludes to the pseudonym of a pirate in the popular novel and film *The Princess Bride* that is periodically passed on from one individual to another.¹² In order to assure users that posts purporting to be authored by DPR were indeed his own, DPR authenticated his posts using an electronic signature known as a PGP key.¹³ Silk Road users had access to a public PGP key, and DPR had a private PGP key that he alone could use to sign his Silk Road posts. When DPR signed a post using his private key, Silk Road users could run the code in the public key, and if the post was signed with the correct private key the user would receive a message that the authentication was successful. The

¹¹ The timing of this change corresponds to a January 15, 2012 Tor chat between a user named “vj” and Ulbricht, in which vj advised Ulbricht to change his username from Admin to Dread Pirate Roberts.

¹² See William Goldman, *The Princess Bride: S. Morgenstern’s Classic Tale of True Love and High Adventure* (1973); *The Princess Bride* (20th Century Fox 1987).

¹³ PGP stands for “Pretty Good Privacy.”

government recovered DPR's private PGP key on Ulbricht's laptop. Importantly, the public PGP key did not change during the site's life span, meaning that DPR used the same private key to sign his posts throughout the time that he administered Silk Road.

Additional evidence supported the conclusion that Ulbricht was Dread Pirate Roberts. For example, the instructions that DPR provided to Cirrus (the account that Der-Yeghiayan later used for undercover work) for how to access the staff chat and contact DPR directly were found in a file on Ulbricht's laptop. The government also discovered the following evidence, covering the entire period during which DPR managed the Silk Road site, on Ulbricht's computer: thousands of pages of chat logs with Silk Road employees; detailed journal entries describing Ulbricht's ownership of the site; a list that tracked Ulbricht's tasks and ideas related to Silk Road; a copy of Silk Road's database; and spreadsheets cataloguing both the servers that hosted Silk Road and expenses and profits associated with the site. The government seized approximately \$18 million worth of Bitcoins from the wallet on Ulbricht's laptop and analyzed their transaction history (through blockchain records) to determine that about 89% of the Bitcoins on Ulbricht's computer came from Silk Road servers located in Iceland.

A search of Ulbricht's home yielded additional evidence linking him with the site. That evidence included two USB hard drives with versions of documents related to Silk Road that were also stored on Ulbricht's laptop. There were also handwritten notes crumpled in Ulbricht's bedroom trash can about ideas for improving Silk Road's vendor rating system—an initiative that Dread Pirate Roberts had just revealed through a post in a discussion forum on the site.

The government also introduced other circumstantial evidence connecting Ulbricht to DPR's activity on Silk Road, such as evidence matching Ulbricht's actual travel history with DPR's online discussion of his travel plans. As one concrete example, the government discovered a Tor Chat log¹⁴ on Ulbricht's laptop memorializing DPR's chat with a user named H7. On October 30, 2011, DPR told H7 that he would be traveling soon. On Ulbricht's Gmail account, which uses an email address that incorporates his full name, the government discovered a travel itinerary from CheapAir that indicated that Ulbricht would be traveling on November 15, 2011.

The government introduced several additional examples of DPR discussing travel plans that matched up with travel disclosed in Ulbricht's email and social media activity. At one point, for example, Ulbricht uploaded photos to his Facebook account in an album entitled "Thailand, February 2012." DPR discussed going to Thailand in a Tor chat on January 27, 2012, indicating that he was in "Thailand now," attracted by the "allure of a warm beach." Tr. 1300. He also mentioned in a January 26 chat with a user named "vj," which stood for Variety Jones, that he was in Thailand to experience the "beaches and jungles." *Id.* at 1298. One of the photos in the Thailand Facebook album depicted Ulbricht "in front of what appears to be jungles and beaches," both of which were referenced in DPR's chats from late January. *Id.* at 1301.

¹⁴ Tor Chat is a program that allows "communication between people on the Tor network." Tr. 889.

2. Murders Commissioned by Dread Pirate Roberts

The government also presented evidence that DPR commissioned the murders of five people to protect Silk Road's anonymity, although there is no evidence that any of the murders actually occurred.¹⁵ In March 2013, a Silk Road vendor whose username was FriendlyChemist threatened to release "thousands of usernames, order [sic] amounts, [and] addresses" of Silk Road customers and vendors if DPR did not ensure that FriendlyChemist received money from another person, Lucydrop. Tr. 1806. Releasing the information would have destroyed the affected users' anonymity, undermining the security of the site. In a later chat with another person, RealLucyDrop, DPR wrote that it would be "terrible" if the personal information were to be released, and thus he needed FriendlyChemist's "real world identity so I can threaten him with violence if he were to release any names." *Id.* at 1811.

¹⁵ Ulbricht was not charged in this case with crimes based on ordering these killings, although evidence relating to the murders was introduced at trial as actions taken in furtherance of the charged conspiracies and criminal enterprise. The killings were referenced again in connection with Ulbricht's sentencing. He faces open attempted murder-for-hire charges in the District of Maryland, however. *United States v. Ulbricht*, No. 13-0222-CCB (D. Md.). That indictment charges Ulbricht with the attempted murder of Curtis Green (Flush). According to the criminal complaint against the corrupt officers, after Bridges, using Flush's account, stole \$350,000 in Bitcoin in January 2013, DPR recruited Nob (Force) to kill Flush as punishment for the theft. DPR paid Nob \$80,000 to carry out the murder, which Force faked to make Ulbricht believe that the task was complete. Presumably because the government removed from its trial evidence anything that the corrupted agent Force may have touched, it did not present evidence of the Flush murder-for-hire agreement, nor did it rely on that murder at sentencing.

The episode escalated from there. DPR connected with Redandwhite, who was FriendlyChemist's supplier, and wrote that "FriendlyChemist is a liability and I wouldn't mind if he was executed." *Id.* at 1822. After negotiating the logistical details of the murder, Ulbricht agreed to pay Redandwhite \$150,000 in Bitcoins to kill FriendlyChemist. DPR paid Redandwhite, who later confirmed that he had received the payment and carried out the murder, and sent what appeared to be a photo of the dead victim to DPR. DPR replied that he had "received the picture and deleted it," and thanked Redandwhite for his "swift action." *Id.* at 1892. Around the same time, Ulbricht recorded in a file on his laptop that he "[g]ot word that the blackmailer was executed." *Id.* at 1887. The government was not able to develop any evidence linking these conversations to an actual murder. A reasonable jury could easily conclude, however, that the evidence demonstrated that Ulbricht ordered and paid for the killing, and that he believed that it had occurred.

Later, DPR ordered four other murders through Redandwhite. Dread Pirate Roberts identified another Silk Road user, Tony76, who knew FriendlyChemist and might compromise the site's anonymity. After some negotiations, DPR agreed to pay Redandwhite \$500,000 in Bitcoins to kill Tony76 and three of his associates. DPR then sent the payment to Redandwhite. On April 6, 2013, Ulbricht wrote in a file on his laptop that he "[g]ave angels go ahead to find tony76." Tr. 1900. Two days later, Ulbricht recorded that he "[s]ent payment to angels for hit on tony76 and his three associates." *Id.* One of the government's expert witnesses was able to link the payments for all five murders to Bitcoin wallets located on Ulbricht's laptop. Again, while the evidence demonstrates that Ulbricht ordered and paid substantial sums for the murders, there is no evidence that the killings actually took place;

the government theorized that Redandwhite had tricked Ulbricht into thinking that he actually committed the murders, but that in fact he had not.

B. The Defense Case

As noted above, Ulbricht conceded at trial that he had created Silk Road, and he was caught red-handed operating the site at the end of the investigation. His principal defense strategy at trial—more of an effort at mitigation than outright denial of his guilt of the conspiracy and other charges in the indictment—was to admit his role at the beginning and end of the site’s operation, but to contend that he sold Silk Road to someone else in 2011 and abandoned his role as its administrator, only to be lured back by the successor DPR near the end of its operation to take the blame for operating the site. The defense attempted on several occasions to implicate as alternative suspects Karpeles and Athavale, both of whom the government had investigated for a possible connection to Silk Road but later abandoned as candidates for DPR’s real-world identity. As part of his alternative-perpetrator defense, Ulbricht theorized that the person or persons who operated as the true Dread Pirate Roberts during the purported interim period planted incriminating evidence on his laptop in order to frame him. For the most part, the defense advanced this theory through cross-examination of government witnesses. Ulbricht did not testify at trial.

One point in the testimony of Richard Bates exemplifies the defense’s approach and the government’s response. Bates, Ulbricht’s friend who assisted with computer programming issues when Ulbricht launched Silk Road, testified for the government. According to Bates, Ulbricht told him in November 2011 that he had sold Silk Road to someone else, a claim that Bates believed at the time to be true. Moreover, in a February 2013 Google chat

between Bates and Ulbricht, Ulbricht wrote that he was “[g]lad” that Silk Road was “not [his] problem anymore.” Tr. 1140-41.¹⁶ Bates understood that to mean that Ulbricht no longer worked on the site.

To mitigate any damage from Bates’s testimony, the government introduced a December 9, 2011 Tor chat between Ulbricht and vj. In that chat, vj asked Ulbricht whether anyone else knew about his involvement in Silk Road. Ulbricht responded: “[U]nfortunately yes. There are two, but they think I sold the site and got out and they are quite convinced of it.” Tr. 1191. He further wrote that those two people thought he sold the site “about a month ago,” *id.*, which roughly corresponds to the November 2011 conversation between Bates and Ulbricht. Significantly, it was shortly after this conversation that vj suggested that Ulbricht change his online identity to DPR. In view of the fictional character it referenced, the government contended that the online moniker DPR was deliberately adopted to support the cover story that the lead administrator of Silk Road changed over time.

Thus, although the government elicited testimony that Ulbricht told Bates that he sold the site in 2011, it also presented evidence that Ulbricht had lied to Bates about that sale and continued to operate the site in secret.

1. Cross-Examination of Government Witnesses

Ulbricht’s defense depended heavily on cross-examination of government witnesses, much of which was designed to support the argument that either Karpeles or

¹⁶ There are two versions of the trial transcript for January 22, 2015 on the district court docket. The page citations here refer to the version of the transcript marked “corrected,” which is listed on the district court docket as Document No. 208 (14-cr-68).

Athavale was the real DPR, or that multiple people operated as Dread Pirate Roberts during Silk Road's life span. The district court limited his cross-examination in two ways that Ulbricht challenges on appeal. First, the district court prevented Ulbricht from exploring several specific topics with Der-Yeghiayan, the government's first witness, through whom it introduced much of its evidence. Those topics included, *inter alia*, Der-Yeghiayan's prior suspicions that Karpeles was DPR. Second, the district court limited Ulbricht's ability to cross examine FBI computer scientist Thomas Kiernan, who testified about evidence that he discovered on Ulbricht's laptop, concerning several specific technical issues related to software on Ulbricht's computer. More details about those attempted cross-examinations will be discussed in context below.

2. Hearsay Statements

Ulbricht also attempted to introduce two hearsay statements in his defense, both of which the district court excluded as inadmissible. Those hearsay statements comprise: (1) chats between DPR and DeathFromAbove (Force) concerning Force's attempt to extort money from DPR in exchange for information about the government's investigation of Silk Road; and (2) the government's letter describing a statement by Andrew Jones, a site administrator, concerning one particular conversation that he had with DPR. The contents of those hearsay statements and other relevant facts will be discussed in more detail below.

3. Defense Expert Witnesses

Long after the trial began on January 13, 2015, and shortly before the government rested on February 2 and the defense rested on February 3, Ulbricht disclosed to the government his intent to call two expert witnesses:

Dr. Steven Bellovin and Andreas Antonopoulos.¹⁷ The Antonopoulos disclosure indicated that he would testify on several subjects relevant to Silk Road, including “the origins of Bitcoin,” “the various purposes and uses of Bitcoin,” “the mechanics of Bitcoin transactions,” “the value of Bitcoin over time since its inception,” and “the concepts of Bitcoin speculating and Bitcoin mining,” among other things. App’x 349. The Bellovin disclosure followed a similar pattern, indicating that he would testify about “[g]eneral principles of internet security and vulnerabilities,” the “import of some lines of PHP code provided to defense counsel in discovery,” and “[g]eneral principles of public-key cryptography,” among other topics. *Id.* at 360. Neither disclosure summarized the opinions that the experts would offer on those subjects, nor did either identify the bases for the experts’ opinions.

On January 29 and 31, the government moved to preclude the testimony of both proffered experts. The government argued that the expert notices were untimely and did not contain the information required by Rule 16 of the Federal Rules of Criminal Procedure, including a summary of the opinions that the experts would offer on the stand.¹⁸ On February 1—three days before the end of the trial—the district court granted the government’s motions and precluded both experts from testifying, concluding that the defendant’s notices were late and that the disclosures were substantively inadequate under Rule 16.

¹⁷ Ulbricht noticed his intent to call Antonopoulos on January 26 and Bellovin on January 30, 2015.

¹⁸ The government also argued generally that some of the topics identified in the disclosures were not relevant to Ulbricht’s case or did not require expert testimony.

Ulbricht claims that the district court erred in precluding his experts from testifying.

In sum, the defense case was limited to cross-examining government witnesses, briefly calling four character witnesses, having a defense investigator authenticate a task list on Ulbricht's computer, and reading a few of DPR's posts into the record. Ulbricht contends, however, that his defense was hamstrung by the rulings described above.

C. The Verdict and Post-Trial Motion

After deliberating for about three and a half hours, the jury returned a guilty verdict on all seven counts in the Indictment. As described in more detail below, Ulbricht then moved for a new trial under Rule 33, Fed. R. Crim. P. The district court denied the motion, and Ulbricht argues here that it erred in doing so.

IV. Sentencing

The United States Probation Office prepared the Pre-Sentence Investigation Report ("PSR") in March 2015. It described the offense conduct in detail and discussed the five murders that Ulbricht allegedly hired Redandwhite to commit.¹⁹ Over Ulbricht's objection, the PSR also discussed six drug-related deaths that the government contended, and the district court found, were connected with Silk Road. Circumstantial evidence linked each of those fatalities with varying degrees of certainty to the decedent's purchase of drugs on Silk Road. For example, one user died from an overdose of heroin combined with other drugs. The deceased individual was found with

¹⁹ The PSR did not refer to the additional murder of "Flush" that DPR allegedly paid Force, under his undercover identity Nob, to commit. *See supra* note 15.

a needle and a bag of heroin, as well as a torn-open delivery package. Open on his computer was a Silk Road chat in which a vendor described the package of heroin that was due to arrive that day, including a tracking number that matched the opened package.

Two other individuals whose deaths the PSR described were Silk Road customers who purchased drugs on the site shortly before their deaths. A fourth person died after ingesting a synthetic drug originally purchased on Silk Road that he obtained through an intermediary dealer, and a fifth died after leaping from a balcony while high on a psychedelic drug that he bought from the site. A sixth person died of pneumonia after placing over thirty orders for heroin and other drugs on Silk Road; the autopsy report theorized that his drug use may have “blunted the deceased’s perception of the severity of his illness,” thus contributing to his premature death. PSR ¶ 83. In arguing that the district court should consider the six deaths, the government explained that they “illustrate the obvious: that drugs can cause serious harm, including death.” App’x 902.

In the first of several sentencing submissions, Ulbricht urged the district court not to consider the six drug-related deaths and to strike them from the PSR. In support of that argument, Ulbricht claimed that Silk Road had harm-reducing effects, meaning that it made drug use less dangerous. Specifically, Ulbricht employed Dr. Fernando Caudevilla (username Doctor X), a physician who provided drug-use advice to the site’s customers. Caudevilla spent up to two or three hours a day on Silk Road discussion fora and sent over 450 messages providing guidance about illegal drug dosage and administration, as well as information about the harms associated with certain drugs. Caudevilla also provided weekly reports to

DPR concerning the advice he gave to the site's users. Ulbricht further claimed that Silk Road allowed for better drug quality control because vendors were subject to a rating system,²⁰ buyers were able to choose from among many different sellers, and the site's anonymity encouraged free dialogue about drug use that helped mitigate the stigma accompanying drug addiction.²¹ According to Caudevilla, when the site received negative feedback about the quality of the drugs sold by a vendor, that vendor was removed from the site. Finally, Ulbricht claimed that the site reduced violence associated with the drug trade by providing a safe, computer-based method of purchasing drugs.

Ulbricht also submitted an expert report from Dr. Mark Taff, which provided an alternative reason for excluding the six deaths from the PSR. In his report, Dr. Taff explained that, based on the information available, it was impossible to know with medical certainty that Silk Road drugs caused the six deaths described in the PSR. There were "gaping holes" in the investigations into each death, and some were missing autopsy reports, toxicology reports, and death certificates. App'x 911. Moreover, Dr. Taff claimed that it was impossible to know the cause of each death because several of the deceased had ingested

²⁰ As the government pointed out in its sentencing submission, fake vendor reviews were commonplace, and vendors sometimes coerced customers into giving them perfect ratings.

²¹ Ulbricht referenced a study by Tim Bingham, who researched Silk Road users between September 2012 and August 2013. Bingham interviewed Silk Road customers and concluded that the site operated as a "novel technological drug subculture, potentially minimiz[ing] drug-related stigma by reinforcing a[] sense of community." App'x 905. Thus, Bingham concluded, and Ulbricht argued, that Silk Road encouraged more "responsible forms of recreational drug use." *Id.* at 906.

multiple drugs prior to their deaths. Ulbricht argued that, absent a clear causal link between the deaths and the offense conduct, the deaths were not relevant to his sentencing at all.

The defense later submitted another sentencing memorandum, which included 97 letters from friends and family describing Ulbricht's good character as well as academic articles about the myriad problems associated with unduly severe sentences for drug crimes. He also urged the district court not to consider the five murders commissioned by DPR, in part because he claimed only to have fantasized about the murders, implying that he did not expect them to be carried out. In its sentencing submission, the government requested that the district court impose a sentence substantially above the twenty-year mandatory minimum.

Ulbricht's sentencing hearing took place on May 29, 2015.²² The district court concluded that Ulbricht's offense level was 43—the highest possible offense level under the Sentencing Guidelines—and that his criminal history category was I.²³ The high offense level largely resulted from the massive quantity of drugs trafficked using Silk Road,

²² At sentencing, the district court vacated Ulbricht's convictions on Counts One and Three because they were lesser included offenses of Counts Two and Four respectively. Ulbricht was therefore sentenced on Counts Two, Four, Five, Six, and Seven. The district court based its Guidelines calculation only on those counts.

²³ The calculated offense level was actually 50, which is higher than the maximum offense level of 43 on the Guidelines sentencing table. The Guidelines provide that "[a]n offense level of more than 43 is to be treated as an offense level of 43." U.S.S.G. ch. 5 pt. A, cmt. n.2.

as well as several enhancements, including one for directing the use of violence, U.S.S.G. § 2D1.1(b)(2).²⁴ Ulbricht does not dispute that calculation. Due to the high offense level, the Guidelines advisory sentence “range” was life in prison, and the U.S. Probation Office recommended that sentence.

At the sentencing hearing, the district court resolved several disputed issues of fact. For example, because Ulbricht contested his responsibility for the five commissioned murders for hire, the district court found by a preponderance of the evidence that Ulbricht did in fact commission the murders, believing that they would be carried out. The district court characterized the evidence of the murders for hire, which included Ulbricht’s journal, chats with other Silk Road users, and the evidence showing that Ulbricht actually paid a total of \$650,000 in Bitcoins for the killings, as “ample and unambiguous.” App’x 1465.

The court then turned to the six drug-related deaths described in the PSR. Over Ulbricht’s objection, the district court found that the deaths were “related conduct relevant to his sentencing” because the “question as to whether this information is properly included in the PSR is whether the Court finds, by a preponderance of the evidence[,] that the deaths, in some way, related to Silk Road.” *Id.* at 1472. It went on to explain that “the relevant offense committed is the unlawful distribution of drugs and the running of a criminal drug enterprise, . . . [and] based on the evidence before the Court, the sale of the drugs through Silk Road caused harm to the decedents.”

²⁴ Because of the grouping rules, U.S.S.G. ch. 3 pt. D, the lower offense levels of the computer hacking and fraudulent identification charges did not contribute to Ulbricht’s offense level.

Id. at 1473. The district court described the facts associated with five of the deaths and specifically found that each was connected to Silk Road, rejecting the defendant’s argument that but-for causation was required in order for the court to consider the deaths as relevant to the offense conduct.²⁵ Parents of two of the decedents also made statements at the proceeding, describing the emotional impact that the losses had on them and their families.

In the course of explaining its reasons for choosing Ulbricht’s sentence, the district court discussed the facts of Ulbricht’s offense, his apparent character, and the purposes of criminal punishment. The court described Doctor X as “enabling,” App’x 1530, rather than reducing the harms associated with drug use, emphasized the social costs attendant to expanding the scope of the drug market, discussed the five murders for hire, and stated that the sentence imposed on Ulbricht could have a powerful general deterrent effect because the case had attracted an unusually large amount of publicity. The court then sentenced Ulbricht principally to life imprisonment.

This appeal followed.

DISCUSSION

On appeal, Ulbricht raises a number of claims of error. For purposes of organizational clarity, we group them into three categories, and present them in the order in

²⁵ The district court did not specifically address one of the six deaths. That decedent was a frequent Silk Road customer who was found dead in his home with a used syringe and other drug paraphernalia. The record does not indicate why the district court did not discuss that case, and neither party makes any argument based on that omission.

which the issues arose in the district court. Accordingly, we discuss first Ulbricht's claims that much of the evidence against him should have been suppressed because it was obtained in violation of his Fourth Amendment rights; second, his arguments that the district court's evidentiary errors denied him a fair trial; and third, his objections to his sentence.

I. Fourth Amendment Issues

Ulbricht claims that the district court erred in denying his motion to suppress evidence obtained in violation of the Fourth Amendment. On appeal from a denial of a suppression motion, "we review a district court's findings of fact for clear error, and its resolution of questions of law and mixed questions of law and fact *de novo*." *United States v. Bohannon*, 824 F.3d 242, 247-48 (2d Cir. 2016). Ulbricht raises two principal arguments. First, he contends that the pen/trap orders that the government used to monitor IP address traffic to and from his home router violated the Fourth Amendment because the government obtained the orders without a warrant. Second, he claims that the warrants authorizing the government to search his laptop as well as his Google and Facebook accounts violated the Fourth Amendment's particularity requirement. We reject those contentions and affirm the denial of Ulbricht's motion to suppress.

A. Pen/Trap Orders

Pursuant to orders issued by United States magistrate judges in the Southern District of New York, the government used five pen registers and trap and trace devices to monitor IP addresses associated with Internet traffic to and from Ulbricht's wireless home router and devices that regularly connected to that router. The government obtained the orders pursuant to the Pen/Trap

Act, which provides that a government attorney “may make [an] application for an order . . . authorizing or approving the installation and use of a pen register or a trap and trace device . . . to a court of competent jurisdiction.” 18 U.S.C. § 3122(a)(1). A “pen register” is defined as a “device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted,” and “shall not include the contents of any communication.” *Id.* § 3127(3). A “trap and trace” device means “a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication.” *Id.* § 3127(4). Like pen registers, trap and trace devices may not capture the “contents of any communication.” *Id.* The statute does not require a search warrant for the use of a pen register or trap and trace device, nor does it demand the kind of showing required to obtain such a warrant. Rather, the statute requires only that the application contain a “certification . . . that the information likely to be obtained is relevant to an ongoing criminal investigation.” *Id.* § 3122(b)(2).

The orders in this case authorized the government to “use a pen register and trap and trace device to identify the source and destination [IP] addresses, along with the dates, times, durations, ports of transmission, and any Transmission Control Protocol (‘TCP’) connection data,”²⁶

²⁶ Data are transmitted on the Internet via discrete packets, rather than in a continuous stream. TCP is a “communications protocol used to process such data packets associated with popular Internet appli-

associated with any electronic communications sent to or from” various devices, including Ulbricht’s home wireless router and his laptop.²⁷ S.A. 93. In each order, the government specified that it did not seek to obtain the contents of any communications. Instead, it sought authorization to collect only “dialing, routing, addressing, and signaling information” that was akin to data captured by “traditional telephonic pen registers and trap and trace devices.” *Id.* at 130. Ulbricht claims that the pen/trap orders violated the Fourth Amendment because he had a reasonable expectation of privacy in the IP address routing information that the orders allowed the government to collect.²⁸

cations,” such as browser and email applications. S.A. 97. Like IP address data, the TCP data that the orders permitted the government to acquire do not include the contents of communications, and Ulbricht has not expressed any independent concern over the government’s collection of TCP connection data.

²⁷ Some of the pen/trap orders phrased the scope of the order slightly differently. For example, one order authorized installing “a trap and trace device to identify the source [IP] address of any Internet communications directed to, and a pen register to determine the destination IP addresses of any Internet communications originating from,” the relevant devices. S.A. 67. In other words, not every order sought TCP connection data as well as IP address information. Neither party has suggested that the differences among the pen/trap orders are material to any issue presented by this appeal.

²⁸ In the district court, Ulbricht made the same arguments concerning his Fourth Amendment privacy interest in the information captured by the pen registers and trap and trace devices. The district court ruled generally that the “type of information sought [in the orders] was entirely appropriate for that type of order.” App’x 208. The court declined to address Ulbricht’s “novel Fourth Amendment arguments” regarding the pen/trap devices because he had “not established the requisite privacy interest . . . to” demonstrate his standing to challenge the orders. *Id.* The government has agreed that Ulbricht has standing to pursue his Fourth Amendment arguments on appeal.

The Fourth Amendment to the United States Constitution provides that: “The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.” 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.” *United States v. Haqq*, 278 F.3d 44, 47 (2d Cir. 2002) (internal quotation marks omitted). 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.” *United States v. Hayes*, 551 F.3d 138, 143 (2d Cir. 2008).

The Supreme Court has long 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. *Smith v. Maryland*, 442 U.S. 735, 743-44 (1979). This is so because 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 business purposes.” *Id.* at 743. Similarly, “e-mail and Internet users . . . rely on third-party equipment in order to engage in communication.” *United States v. Forrester*, 512 F.3d 500, 510 (9th Cir. 2008). Internet users thus “should know that this information is provided to and used by Internet service providers for the specific purpose of directing the routing of information.” *Id.* Moreover, “IP

addresses are not merely passively conveyed through third party equipment, but rather are voluntarily turned over in order to direct the third party's servers." *United States v. Christie*, 624 F.3d 558, 574 (3d Cir. 2010) (internal quotation marks omitted).

Ulbricht notes that questions have been raised about whether some aspects of modern technology, which entrust great quantities of significant personal information to third party vendors, arguably making extensive government surveillance possible, call for a re-evaluation of the third-party disclosure doctrine established by *Smith*. See, e.g., *United States v. Jones*, 565 U.S. 400, 417-18 (2012) (Sotomayor, J., concurring); *American Civil Liberties Union v. Clapper*, 785 F.3d 787, 824 (2d Cir. 2015). We remain bound, however, by that rule until and unless it is overruled by the Supreme Court. See *United States v. Gomez*, 580 F.3d 94, 104 (2d Cir. 2009); see also *United States v. Wheelock*, 772 F.3d 825, 829 (8th Cir. 2014).

Moreover, whatever novel or more intrusive surveillance techniques might present future questions concerning the appropriate scope of the third-party disclosure doctrine, the orders in this case do not present such issues. 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*. That is why the orders here fit comfortably within the language of a statute drafted with the earlier technology in mind. The substitution of electronic methods of communication for telephone calls does not alone create a reasonable expectation of privacy in the identities of devices with whom one communicates. Nor does it 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. Like telephone companies, Internet service providers require that identifying information be disclosed in order to make communication among electronic devices possible. In light of the *Smith* rule, no reasonable person could maintain a privacy interest in that sort of information.

We therefore join the other circuits that have considered this narrow question and hold that collecting IP address information devoid of content is “constitutionally indistinguishable from the use of a pen register.” *Forrester*, 512 F.3d at 510; *see, e.g., Wheelock*, 772 F.3d at 828 (holding that the defendant “cannot claim a reasonable expectation of privacy in [the] government’s acquisition of his subscriber information, including his IP address and name,” because it had been “revealed to a third party” (internal quotation marks omitted)); *Christie*, 624 F.3d at 573 (holding that there is no expectation of privacy in “subscriber information provided to an internet provider,” such as an IP address (internal quotation marks omitted)); *see also Guest v. Leis*, 255 F.3d 325, 336 (6th Cir. 2001) (holding that “computer users do not have a legitimate expectation of privacy in their [bulletin board] subscriber information because they have conveyed it to another person”); *United States v. Graham*, 824 F.3d 421, 432 (4th Cir. 2016) (en banc) (noting that “third-party information relating to the sending and routing of electronic communications does not receive Fourth Amendment protection”); *United States v. Carpenter*, 819 F.3d 880, 887 (6th Cir. 2016) (“[C]ourts have not (yet, at least) extended [Fourth Amendment] protections to the internet analogue to envelope markings, namely the metadata used to route internet communications, like . . . IP addresses.”). Where, as here, the government did not access the contents of any of Ulbricht’s communications, it did

not need to obtain a warrant to collect IP address routing information in which Ulbricht did not have a legitimate privacy interest. We therefore reject Ulbricht's contention that the issuance of such orders violated his Fourth Amendment rights.²⁹

Ulbricht's additional arguments are not persuasive. Ulbricht contends generally that pen/trap orders may monitor a communication's content by tracking metadata, but he does not identify what metadata the government might have collected or explain how the pen/trap orders in this case gave the government information concerning the content of his communications. He also claims that the orders violated the Fourth Amendment by impermissibly monitoring activity within his home, relying on *Kyllo v. United States*, 533 U.S. 27 (2001). In *Kyllo*, the Court held that using thermal-imaging technology from outside the home to discern whether a person was growing marijuana in the home might reveal innocent, non-criminal information in which a resident has a privacy interest. *Id.* at 38.

²⁹ The issue presented in this case is narrowly confined to orders that are limited to the capture of IP addresses, TCP connection data, and similar routing information. Our holding therefore does not address other, more invasive surveillance techniques that capture more information (such as content), which may require a warrant issued on probable cause or an order pursuant to Title III of the Omnibus Crime Control and Safe Streets Act of 1968, codified as amended at 18 U.S.C. §§ 2510-22. *See generally In the Matter of a Warrant for All Content & Other Info. Associated with the Email Account xxxxxxxx@gmail.com Maintained at Premises Controlled by Google, Inc.*, 33 F.Supp.3d 386, 393-96 (S.D.N.Y. 2014), as amended (Aug. 7, 2014) (describing the available caselaw concerning search warrants of email accounts). Similarly, to the extent that some of the out-of-circuit cases cited in the text also address the Fourth Amendment status of other types of evidence, such as historical cell-site location information, we express no views on such issues, which are not presented in this case.

Ulbricht contends that monitoring IP address traffic through his router is similar to the thermal-imaging technology because it might reveal when and how Ulbricht used his computer when he was at home. The same can be said, however, of an ordinary telephone pen register, which can reveal if, when, and how a person uses his or her home phone to make calls. *See Smith*, 442 U.S. at 743. IP address traffic similarly reveals whether an Internet subscriber (or, more precisely, a person who uses the subscriber's Internet connection) is home and using the Internet. Nothing in *Kyllo* suggests that government monitoring of data disclosed to an outside telephone or Internet provider for ordinary business purposes becomes constitutionally suspect when investigators use that information to draw inferences about whether someone is making telephone calls or accessing websites from inside his or her home. We therefore see no constitutional difference between monitoring home phone dialing information and IP address routing data. Thus, we conclude that the pen register and trap and trace orders did not violate the Fourth Amendment.³⁰

³⁰ Ulbricht's alternative argument, that the pen/trap orders violated the Pen/Trap Act and the Stored Communications Act ("SCA") because they sought prospective data, is without merit. Ulbricht claims that the orders were obtained both through the Pen/Trap Act, 18 U.S.C. §§ 3121-27, and the SCA, 18 U.S.C. § 2703(d). To the contrary, each pen/trap order (and the underlying requests for such orders) relied exclusively on the Pen/Trap Act, not the SCA. The fact that one of the government's goals was to monitor IP address traffic to match Ulbricht's Internet activity with DPR's does not undermine the validity of the orders. The orders themselves did not allow the government to track the location of the router and other equipment to which the trap and trace device was attached. Thus, they were not "geo-locating" devices, as Ulbricht suggests, any more than subpoenas for hotel registers, parking tickets, and credit card receipts, or

B. Search Warrants

Ulbricht also contends that the warrants authorizing the search and seizure of his laptop as well as his 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 describ[e] the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV. "It is familiar history that indiscriminate searches and seizures conducted under the authority of 'general warrants' were the immediate evils that motivated the framing and adoption of the Fourth Amendment." *Payton v. New York*, 445 U.S. 573, 583 (1980). Those general warrants "specified only an offense," leaving "to the discretion of the executing officials the decision as to which persons should be arrested and which places should be searched." *Steagald v. United States*, 451 U.S. 204, 220 (1981). The principal defect in such a warrant was that it permitted a "general, exploratory rummaging in a person's belongings," *Andresen v. Maryland*, 427 U.S. 463, 480 (1976) (internal quotation marks omitted), a problem that the Fourth Amendment attempted to resolve by requiring the warrant to "set out with particularity" the "scope of the authorized search," *Kentucky v. King*, 563 U.S. 452, 459 (2011).³¹

any other methods by which the government obtains information that can be used to identify a suspect's location at particular points in time.

³¹ In addition to preventing general searches, the particularity requirement serves two other purposes not relevant to this appeal: "preventing the seizure of objects upon the mistaken assumption that they fall within the magistrate's authorization, and preventing the issuance of warrants without a substantial factual basis." *United States v. Young*, 745 F.2d 733, 759 (2d Cir. 1984).

To be sufficiently particular under the Fourth Amendment, a warrant must satisfy three requirements. First, “a warrant must identify the specific offense for which the police have established probable cause.” *United States v. Galpin*, 720 F.3d 436, 445 (2d Cir. 2013). Second, “a warrant must describe the place to be searched.” *Id.* at 445-46. Finally, the “warrant must specify the items to be seized by their relation to designated crimes.” *Id.* at 446 (internal quotation marks omitted).

“Where, as here, the property to be searched is a computer hard drive, the particularity requirement assumes even greater importance.” *Id.* A general search of electronic data is an especially 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.” *Id.* The “seizure of a computer hard drive, and its subsequent retention by the government, can [therefore] give the government possession of a vast trove of personal information about the person to whom the drive belongs, much of which may be entirely irrelevant to the criminal investigation that led to the seizure.” *United States v. Ganius*, 824 F.3d 199, 217 (2d Cir. 2016) (en banc). Such sensitive records might include “[t]ax records, diaries, personal photographs, electronic books, electronic media, medical data, records of internet searches, [and] banking and shopping information.” *Id.* at 218. Because of the nature of digital storage, it is not always feasible to “extract and segregate responsive data from non-responsive data,” *id.* at 213, creating a “serious risk that every warrant for electronic information will become, in effect, a general warrant,” *Galpin*, 720 F.3d at 447 (internal quotation marks omitted). Thus, we have held that warrants that fail to “link [the evidence sought] to the criminal activity supported by probable cause” do not satisfy the particularity requirement because they

“lack[] meaningful parameters on an otherwise limitless search” of a defendant’s electronic media. *United States v. Rosa*, 626 F.3d 56, 62 (2d Cir. 2010).

The Fourth Amendment does not require a perfect description of the data to be searched and seized, however. Search warrants covering digital data may contain “some ambiguity . . . so long as law enforcement agents have done the best that could reasonably be expected under the circumstances, have acquired all the descriptive facts which a reasonable investigation could be expected to cover, and have insured that all those facts were included in the warrant.” *Galpin*, 720 F.3d at 446 (internal quotation marks omitted).

Moreover, it is important to bear in mind that a search warrant does not necessarily lack particularity simply because it is broad. Since a search of a computer is “akin to [a search of] a residence,” *id.*, searches of computers may sometimes need to be as broad as searches of residences pursuant to warrants. Similarly, traditional searches for paper records, like searches for electronic records, have always entailed the exposure of records that are not the objects of the search to at least superficial examination in order to identify and seize those records that are. And in many cases, the volume of records properly subject to seizure because of their evidentiary value may be vast. None of these consequences necessarily turns a search warrant into a prohibited general warrant.

1. Laptop Search Warrant

The warrant authorizing the search and seizure of Ulbricht’s laptop (the “Laptop Warrant”) explicitly incorporated by reference an affidavit listing the crimes charged, which at the time included narcotics trafficking, computer hacking, money laundering, and murder-for-hire offenses

in violation of 21 U.S.C. § 846, 18 U.S.C. §§ 1030, 1956, and 1958. *See In re 650 Fifth Ave. & Related Properties*, 830 F.3d 66, 101 (2d Cir. 2016) (describing the requirements for a criminal search warrant’s incorporation of an affidavit by reference).³² The affidavit also described the workings of Silk Road and the role of Dread Pirate Roberts in operating the site and included a wealth of information supporting a finding that there was probable cause to believe that Ulbricht and DPR were the same person. Based on that information, the Laptop Warrant alleged that Ulbricht “use[d] [the laptop] in connection with his operation of Silk Road,” and that there was “probable cause to believe that evidence, fruits, and instrumentalities of the [charged offenses]” would be found on the laptop. S.A. 246.³³

Generally speaking, the Laptop Warrant divided the information to be searched for and seized into two categories. The first covered evidence concerning Silk Road that was located on the computer, including, *inter alia*, “data associated with the Silk Road website, such as web content, server code, or database records”; any evidence concerning servers or computer equipment connected with Silk Road; e-mails, private messages, and forum postings or “other communications concerning Silk Road in any way”; evidence concerning “funds used to facilitate or proceeds derived from Silk Road,” including Bitcoin wallet files and transactions with Bitcoin exchangers, or “information concerning any financial accounts . . . where Silk

³² Because the warrant incorporated the affidavit by reference, we refer to the documents together as the Laptop Warrant for the sake of simplicity.

³³ Ulbricht does not challenge the existence of probable cause to believe both that he committed these offenses and that the laptop would contain evidence of them.

Road funds may be stored”; and “any evidence concerning any illegal activity associated with Silk Road.” *Id.* at 246-48.

The second category of information in the Laptop Warrant included “evidence relevant to corroborating the identification of Ulbricht as the Silk Road user ‘Dread Pirate Roberts.’ ” *Id.* at 248. In order to connect Ulbricht with DPR, the Laptop Warrant authorized agents to search for: “any communications or writings by Ulbricht, which may reflect linguistic patterns or idiosyncra[s]ies associated with ‘Dread Pirate Roberts,’ or political/economic views associated with [DPR] . . .”; “any evidence concerning any computer equipment, software, or usernames used by Ulbricht, to allow comparison with” computer equipment used by DPR; “any evidence concerning Ulbricht’s travel or patterns of movement, to allow comparison with patterns of online activity of [DPR]”; “any evidence concerning Ulbricht’s technical expertise concerning Tor, Bitcoins,” and other computer programming issues; any evidence concerning Ulbricht’s attempts to “obtain fake identification documents,” use aliases, or otherwise evade law enforcement; and “any other evidence implicating Ulbricht in the subject offenses.” *Id.* at 248-49 (footnote omitted).

After careful consideration of the warrant, the supporting affidavit, and Ulbricht’s arguments, we conclude that the Laptop Warrant did not violate the Fourth Amendment’s particularity requirement.³⁴ We note, at the

³⁴ The district court ruled that Ulbricht did not have standing to raise his Fourth Amendment challenges because he did not establish that he had a personal expectation of privacy in the laptop or his Facebook and Google accounts. We express no view on that issue, since the district court also reached the merits of the motion to suppress

outset of our review, that the warrant plainly satisfies the basic elements of the particularity requirement as traditionally understood. By incorporating the affidavit by reference, the Laptop Warrant lists the charged crimes, describes the place to be searched, and designates the information to be seized in connection with the specified offenses. Each category of information sought is relevant to Silk Road, DPR's operation thereof, or identifying Ulbricht as DPR. We do not understand Ulbricht's arguments to contest the Laptop Warrant's basic compliance with those requirements.³⁵

Rather, Ulbricht's arguments turn on the special problems associated with searches of computers which, as we have acknowledged in prior cases, *Galpin*, 720 F.3d at 447; *Ganias*, 824 F.3d at 217–18, can be particularly intrusive. These arguments merit careful attention. For example, Ulbricht questions the appropriateness of the protocols that the Laptop Warrant instructed officers to use in executing the search. Those procedures included opening or “cursorily reading the first few” pages of files to “determine their precise contents,” searching for deliberately hidden files, using “key word searches through all electronic storage areas,” and reviewing file “directories” to determine what was relevant. S.A. 253. Ulbricht, supported by *amicus* the National Association of Criminal Defense Lawyers (“NACDL”), argues that the warrant

and the government has agreed that Ulbricht has standing to challenge the warrants and accompanying searches.

³⁵ It is worth noting that Ulbricht does not challenge the validity of the search warrant covering his home, although that warrant is quite similar to the Laptop Warrant and appears to be just as broad. Specifically, the home search warrant allows the government to search for and seize evidence concerning Ulbricht's travel or patterns of movement and any of his communications or writings.

was insufficiently particular because the government and the magistrate judge failed to specify the search terms and protocols *ex ante* in the warrant.

We cannot agree. As illustrated by the facts of this very case, it will often be impossible to identify in advance the words or phrases that will separate relevant files or documents before the search takes place, because officers cannot readily anticipate how a suspect will store information related to the charged crimes. Files and documents can easily be given misleading or coded names, and words that might be expected to occur in pertinent documents can be encrypted; even very simple codes can defeat a pre-planned word search. For example, at least one of the folders on Ulbricht's computer had a name with the misspelling "aliaces." App'x 309. For a more challenging example, Ulbricht also kept records of certain Tor chats in a file on his laptop that was labeled "mbsob-zvkhwx4hmjt." *Id.* at 398.³⁶

The agents reasonably anticipated that they would face such problems in this case. Operating Silk Road involved using sophisticated technology to mask its users' identities. Accordingly, although we acknowledge the NACDL's suggestions in its *amicus* submission for limit-

³⁶ We note that Ulbricht and *amicus* NACDL somewhat exaggerate the novelty of computer searches in this regard. A traditional physical search for paper "drug records" or "tax records" may entail a similar examination of all sorts of files and papers to determine whether such records are hidden in files with innocuous or misleading names or written in coded terms to mask their content. For obvious reasons, search warrants authorizing the seizure of such evidence have not traditionally specified that agents may look only at file folders labeled "drug records" or may seize only papers containing the word "cocaine"—the equivalent of the *ex ante* "search terms" demanded by Ulbricht.

ing the scope of such search terms, the absence of the proposed limitations does not violate the particularity requirement on the facts of this case. We therefore conclude that, in preparing the Laptop Warrant, “law enforcement agents [did] the best that could reasonably be expected under the circumstances, [had] acquired all the descriptive facts which a reasonable investigation could be expected to cover, and [had] insured that all those facts were included in the warrant.” *Galpin*, 720 F.3d at 446 (internal quotation marks omitted).

The fundamental flaw in Ulbricht’s (and the NACDL’s) argument is that it confuses a warrant’s breadth with a lack of particularity. As noted above, breadth and particularity are related but distinct concepts. A warrant may be broad, in that it authorizes the government to search an identified location or object for a wide range of potentially relevant material, without violating the particularity requirement. For example, a warrant may allow the government to search 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, “[w]hen the criminal activity pervades [an] entire business, seizure of all records of the business is appropriate, and broad language used in warrants will not offend the particularity requirements.” *U.S. Postal Serv. v. C.E.C. Servs.*, 869 F.2d 184, 187 (2d Cir. 1989). Ulbricht used his laptop to commit the charged offenses by creating and continuing to operate Silk Road. Thus, a broad warrant allowing the government to search his laptop for potentially extensive evidence of those crimes does not offend the Fourth Amendment, as long as that warrant meets the three particularity criteria outlined above.

It is also true that allowing law enforcement to search his writings for linguistic similarities with DPR authorizes a broad search of written materials on Ulbricht's hard drive. That fact, however, does not mean that the warrants violated the Fourth Amendment. The Laptop Warrant clearly explained that the government planned to compare Ulbricht's writings to DPR's posts to confirm that they were the same person, by identifying both linguistic patterns and distinctive shared political or economic views. Ulbricht and the NACDL similarly claim that searching for all evidence of his travel patterns and movement violates the Fourth Amendment's particularity requirement. Again, the warrant explained that it sought information about Ulbricht's travel "to allow comparison with patterns of online activity of 'Dread Pirate Roberts' and any information known about his location at particular times." S.A. 248. Thus, the Laptop Warrant connects the information sought to the crimes charged and, more specifically, its relevance to identifying Ulbricht as the perpetrator of those crimes.³⁷

³⁷ Evidence revealing a suspect's past movements is often highly relevant to a criminal investigation. Such evidence might be used to establish—or rule out—the suspect's presence at a crime scene or other pertinent location at a particular time. It may also disclose other, unrelated information about the suspect's noncriminal associations, interests, and behavior, and may be drawn from a wide variety of sources. Government efforts to develop such information, including by search warrants authorizing its seizure, are not inherently questionable under the Fourth Amendment. Using piecemeal or laborious investigative techniques, it might take law enforcement officers a great deal of time and effort to compile a comprehensive record of a suspect's travel or other movements. The fact that extensive travel records are stored on a digital device and may be accessed readily via a keystroke or quick search does not immunize those records from

We remain sensitive to the difficulties associated with preserving a criminal defendant's privacy while searching through his electronic data and computer hard drives. In the course of searching for information related to Silk Road and DPR, the government may indeed have come across personal documents that were unrelated to Ulbricht's crimes. Such an invasion of a criminal defendant's privacy is inevitable, however, in almost any warranted search because in "searches for papers, it is certain that some innocuous documents will be examined, at least cursorily, in order to determine whether they are, in fact, among those papers authorized to be seized." *Ganias*, 824 F.3d at 211, quoting *Andresen*, 427 U.S. at 482 n.11. The Fourth Amendment limits such "unwarranted intrusions upon privacy," *id.* (internal quotation marks omitted), by requiring a warrant to describe its scope with particularity. The Laptop Warrant satisfied that requirement. Ulbricht has challenged only the facial validity of the Laptop Warrant and not its execution. Because we have no reason to doubt that the officers faithfully executed the warrant, its execution did not result in an undue invasion of Ulbricht's privacy.

Finally, we note that the crimes charged in this case were somewhat unusual. This case does not involve a more typical situation in which officers searched for evidence of a physician's illegal distribution of pain medications, to use the NACDL's example, which may have electronically-stored data associated with the alleged crimes on a hard drive that largely contains non-criminal information. Here the crimes under investigation were committed largely through computers that there was probable cause

seizure. Indeed, the seizure of a paper journal or calendar in a conventional search will often allow officers to map out a defendant's travel history with similar ease.

to believe included the laptop at issue, and the search warrant application gave ample basis for the issuing magistrate judge to conclude that evidence related to Silk Road and Ulbricht's use of the DPR username likely permeated Ulbricht's computer. Thus, given the nature of Ulbricht's crimes and their symbiotic connection to his digital devices, we decline to rethink the well-settled Fourth Amendment principles that the Laptop Warrant may implicate. 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.

2. The Google and Facebook Warrants

Ulbricht also challenges the warrants that allowed the government to search his Google and Facebook accounts, although he does not present any specific arguments related to those warrants. Both warrants, through affidavits incorporated by reference, set forth the basis for probable cause to search those accounts for evidence of Ulbricht's involvement in Silk Road. The warrants also authorized the government to search his Google and Facebook accounts for "evidence, fruits, and instrumentalities" of the specified offenses, including, *inter alia*: "any communications or writings by Ulbricht"; "any evidence concerning any computer equipment, software, or usernames used by Ulbricht"; "any evidence concerning Ulbricht's travel or patterns of movement"; and any "other evidence of the" crimes charged. S.A. 334-35, 393-94. The scope of the Google and Facebook warrants thus substantially paralleled that of the Laptop Warrant.

The Google and Facebook warrants were constitutional for the same reasons that the Laptop Warrant was valid. They satisfied all three of the particularity requirements because they listed the subject offenses, described

the things to be searched, and identified the information to be seized in relation to the charged crimes. Ulbricht does not advance any additional arguments specific to the Google and Facebook warrants, nor have we identified any independent reason to find them unconstitutionally lacking in specificity.

3. Conclusion

In sum, the issuance of the pen/trap orders and the three search warrants that Ulbricht challenges in this appeal did not violate the Fourth Amendment.³⁸ Thus, we affirm the district court's denial of Ulbricht's suppression motion.

II. The District Court's Trial Rulings and Ulbricht's Rule 33 Motion

Ulbricht contends that he did not receive a fair trial for several reasons: (1) the district court's rulings surrounding corrupt agents Force and Bridges violated his due process rights; (2) the district court erroneously precluded two defense experts from testifying; (3) the district court abused its discretion when it curtailed Ulbricht's cross-examination of two government witnesses; and (4) the district court erred when it ruled that certain hearsay statements were inadmissible. He also contends that, even if each individual error is harmless, the cumulative effect of those errors prejudiced him to the extent that his

³⁸ The government also contends that, even if the warrants were invalid, the good faith exception prevents the application of the exclusionary rule. In general, the "exclusion of evidence is inappropriate when the government acts in objectively reasonable reliance on a search warrant, even when the warrant is subsequently invalidated." *Ganias*, 824 F.3d at 221 (internal quotation marks omitted). Because we conclude that all three of the warrants were valid, we need not address the government's alternative argument.

trial was fundamentally unfair. We detect no error in the district court's rulings on any of those issues and therefore conclude that Ulbricht was not deprived of his right to a fair trial.

A. Corrupt Agents Force and Bridges

Ulbricht's principal fair trial argument is that the district court erred in numerous ways by preventing him from relying on information related to the corruption of two federal agents, Force and Bridges, involved in the investigation of the Silk Road site. Before trial, the district court (1) precluded Ulbricht from referring at trial to the secret grand jury proceeding against Force; (2) denied Ulbricht discovery related to the Force investigation; and (3) denied Ulbricht an adjournment of the trial until the Force investigation was complete. During trial, the district court excluded as hearsay certain chats that related to Force's illicit use of Silk Road. Finally, Ulbricht learned after trial that the government was investigating a second corrupt agent, Bridges. Ulbricht contends that the failure to disclose Bridges's corruption until after the trial violated *Brady v. Maryland*, 373 U.S. 83 (1963), and that the district court erroneously denied his motion for a new trial on that ground.

Without question, the shocking personal corruption of these two government agents disgraced the agencies for which they worked and embarrassed the many honorable men and women working in those agencies to investigate serious criminal wrongdoing. Even more importantly, when law enforcement officers abuse their offices for personal gain, commit other criminal acts, violate the rights of citizens, or lie under oath, they undermine the public's vital trust in the integrity of law enforcement. They may also compromise the investigations and prosecutions on which they work.

At the same time, the venality of individual agents does not necessarily affect the reliability of the government's evidence in a particular case or become relevant to the adjudication of every case in which the agents participated. Courts are obligated to ensure that probative evidence is disclosed to the defense, carefully evaluated by the court for its materiality to the case, and submitted for the jury's consideration where admissible. But courts must also take care that wrongdoing by investigators that has no bearing on the matter before the court not be used as a diversion from fairly assessing the prosecution's case. Like any other potential evidence, information about police corruption must be evaluated by reference to the ordinary rules of criminal procedure and evidence, a task to which we now turn.

1. Background: Pretrial Disclosure of the Force Investigation

The government disclosed its investigation into Force's corruption to the defense about six weeks before trial. Initially, on November 21, 2014, the government wrote a sealed *ex parte* letter to the district court seeking permission to disclose to the defense information about the Force grand jury investigation subject to a protective order.³⁹ The district court granted the application. On December 1, the government provided a copy of the November 21 letter, which otherwise remained sealed, to defense counsel. According to the letter, Force leaked information to DPR in exchange for payment and "corruptly ob-

³⁹ The government required such an order because grand jury proceedings are secret and a government attorney "must not disclose a matter occurring before the grand jury," Rule 6(e)(2)(B)(vi), Fed. R. Crim. P., without a court order, Rule 6(e)(3)(E), subject to limited exceptions not relevant here.

tain[ed] proceeds from the Silk Road website and convert[ed] them to his personal use.” App’x 649. The government then undertook to purge its trial evidence of anything arguably traceable to Force.

Ulbricht moved to unseal the entire November 21 letter so that he could rely on the information in the letter that related to Force’s corruption at trial, arguing that the letter included *Brady* information and that he therefore had a particularized need to disclose the information that outweighed the presumption of grand jury secrecy. He also requested discovery and subpoenas under Rules 16 and 17, Fed. R. Crim. P., to learn more about the scope of Force’s corruption. In the alternative, Ulbricht sought an adjournment of the trial until the Force investigation concluded and information about his corruption might become public through the filing of charges against him. On December 15, the district court held a sealed hearing on that issue and invited further written submissions, including a particularized list of Ulbricht’s discovery requests. One week later, the district court issued a sealed and partially redacted opinion⁴⁰ denying all of Ulbricht’s requests. The court did indicate, however, that throughout the trial it would “entertain specific requests to use information from the November 21, 2014 Letter on cross-examination.” App’x 700. Moreover, the court explained that it would “entertain a renewed application” for a “particularized disclosure” of facts relevant to Force’s corruption if

⁴⁰ Portions of the district court opinion were redacted because they referenced the defendant’s *ex parte* submissions explaining how he would use information related to the Force investigation at trial. This Court has reviewed an unredacted version of the district court opinion in connection with this appeal, but not the *ex parte* letters that the opinion references.

the government's trial tactics or evidence "open[ed] the door" to such facts. *Id.*

2. Preclusion of Force Investigation Evidence:
Rule 6(e)

On appeal, Ulbricht claims that the district court erred in denying his motion to unseal the November 21 letter because he demonstrated a particularized need that rebutted the presumption of secrecy that attaches to grand jury investigations. We disagree.

"[T]he proper functioning of our grand jury system depends upon the secrecy of grand jury proceedings." *Douglas Oil Co. of California v. Petrol Stops Nw.*, 441 U.S. 211, 218 (1979). We have described five rationales for such secrecy:

(1) To prevent the escape of those whose indictment may be contemplated; (2) to insure the utmost freedom to the grand jury in its deliberations, and to prevent persons subject to indictment or their friends from importuning the grand jurors; (3) to prevent subornation of perjury or tampering with the witnesses who may testify before the grand jury and later appear at the trial of those indicted by it; (4) to encourage free and untrammelled disclosures by persons who have information with respect to the commission of crimes; (5) to protect the innocent accused who is exonerated from disclosure of the fact that he has been under investigation, and from the expense of standing trial where there was no probability of guilt.

In re Grand Jury Subpoena, 103 F.3d 234, 237 (2d Cir. 1996). Rule 6(e)(6) of the Federal Rules of Criminal Procedure implements this policy of secrecy by requiring that “all records, orders, and subpoenas *relating to* grand jury proceedings [must] be sealed.” *In re Grand Jury Subpoena*, 103 F.3d at 237 (emphasis in original).

Information falling within Rule 6(e)’s protections is entitled to a “presumption of secrecy and closure.” *Id.* at 239. To rebut the presumption of secrecy, the party “seeking disclosure [must] show a particularized need that outweighs the need for secrecy.” *Id.* (internal quotation marks omitted). To prove a particularized need, parties seeking disclosure must show that the “material they seek is needed to avoid a possible injustice in another judicial proceeding, that the need for disclosure is greater than the need for continued secrecy, and that their request is structured to cover only material so needed.” *Id.* (internal quotation marks omitted). “A district court’s decision as to whether the burden of showing a particularized interest has been met will be overturned only if the court has abused its discretion.” *Id.*

We cannot say that the district court abused its discretion when it denied Ulbricht’s request to unseal the November 21 letter discussing the Force grand jury investigation. It is undisputed that the letter contained information related to a grand jury proceeding that, if made public, would disclose matters occurring before the grand jury. Ulbricht did not demonstrate a particularized need for disclosure because he did not show that the need for disclosure was greater than the need for continued secrecy or that a possible injustice would result if the grand jury investigation was not disclosed. Specifically, the district court did not err in concluding that revealing the entire letter could have compromised the Force grand jury

investigation in a number of ways. For example, potential co-conspirators might have learned of the investigation and attempted to intimidate witnesses or destroy evidence. The investigation was also likely to garner significant media attention, a fact that might influence witnesses or grand jurors. And, although Force knew of the investigation, revealing its existence to the public might have harmed him if the allegations had ultimately proved untrue. Finally, Ulbricht's request was not structured to cover only the information needed to avoid any possible injustice; instead, he sought to unseal the entire November 21 letter and did not propose a more narrowly tailored disclosure.

In redacted portions of its opinion, the district court also considered *ex parte* arguments concerning how the Force investigation might be relevant to Ulbricht's defense. In general terms, Ulbricht argued that the agents' corruption was critical to his defense because it would reveal the agents' ability to falsify evidence against him and demonstrate their motive to do so. According to the district court's characterization of his *ex parte* letters, Ulbricht speculated that Force may have used Curtis Green's (Flush) administrative capabilities to impersonate DPR; Force's corrupt conduct might have demonstrated technical vulnerabilities in the site that would render it susceptible to hacking; and learning that Force had good information about the Silk Road investigation might have caused the true DPR to recruit Ulbricht as his successor.⁴¹

⁴¹ As noted above, *see* note 5, we have carefully considered to what extent it is appropriate to refer to portions of the record that remain under seal. We have been especially careful in describing the portions of the district court's opinion that remain redacted and therefore are

The district court reasoned that much of the information that might have arguably supported any of those theories was made available to the defense in discovery. The only new information in the November 21 letter concerned the investigation of Force's corruption; the fact of that investigation and its scope does not bolster any of the defense theories that Ulbricht described before the district court or on appeal. That Force was personally corrupt and used his undercover identity to steal money from Silk Road and DPR does not suggest either a motive or an ability on his part to frame Ulbricht as DPR. Absent any explanation of how Force could have orchestrated a massive plant of incriminating information on Ulbricht's personal laptop, his larcenous behavior does not advance the claim that such a frame-up was possible beyond mere

still not available to the government or to the public. We appreciate that charges against Ulbricht remain pending in Maryland and that the redacted information describes what would have been his trial strategy had he been able to reference Force's corruption. We have thus described the defense's redacted arguments at a fairly high level of generality. We are confident that any experienced prosecutor could anticipate those arguments, and that in any event the information is largely stated or implied in Ulbricht's own publicly filed briefs on appeal. Particularly given that our description relates to how the Force information might have been used at a trial that is now completed, and that we now hold that Ulbricht is not entitled to a new trial, we conclude that the public's need to understand and evaluate Ulbricht's arguments that he was unfairly prejudiced by the district court's rulings, as well as our reasons for rejecting those arguments, outweighs any minimal interest that Ulbricht might have in withholding his contentions from the government.

speculation. Thus, Ulbricht was equally capable of presenting his various defense theories to the jury with or without the November 21 letter.⁴²

The government's commitment to eliminating all evidence that came from Force's work on the Silk Road investigation⁴³ further undermines Ulbricht's claim that he needed the information to avoid a possible injustice. Had Force been called as a government witness, or had any of the government's evidence relied on his credibility, his character for truthfulness would have been at issue during the trial, and information that impeached his credibility would have become highly relevant. Ulbricht's reliance on the general fact of cooperation among different government agencies and different U.S. Attorney's Offices does not undermine the government's explicit representations that none of the evidence presented at trial derived from Force, and nothing in the record suggests that those representations were false. Ulbricht had no need to rely on the grand jury investigation of Force to attack the credibility of the actual government witnesses or the integrity of its other evidence.

In sum, Ulbricht has not shown that the district court abused its discretion in maintaining the secrecy of the Force grand jury investigation. He did not demonstrate

⁴² Even on appeal, moreover, after the disclosure of additional information in the prosecutions of Bridges and Force, Ulbricht does not provide any concrete explanation of how the techniques used by the corrupt agents to steal money from Silk Road could have been used, by them or by others, to plant the massive amounts of incriminating information found on Ulbricht's laptop and in his house.

⁴³ For example, the government declined to present evidence of DPR's attempt to commission an additional murder because that conduct involved Force acting as Nob.

to the district court, and has not demonstrated on appeal, that keeping the November 21 letter under seal resulted in any injustice, or that his need for disclosing the investigation was greater than the need for continued secrecy.⁴⁴

3. Denial of Discovery Related to Force

Ulbricht claims that the district court erred in denying him discovery, including requested subpoenas, related to the Force investigation. Rule 16(a)(1)(E), Fed. R. Crim. P., requires the government to disclose information within its control if the information is “material to preparing the defense” or will be a part of the government’s case-in-chief. Evidence is material if it “could be used to counter the government’s case or to bolster a defense.” *United States v. Stevens*, 985 F.2d 1175, 1180 (2d Cir. 1993). “An appellate court, in assessing the materiality of withheld information, considers not only the logical relationship between the information and the issues in the case, but also the importance of the information in light of the evidence as a whole.” *Id.* To justify a new trial, there “must be some indication that the pretrial disclosure of the disputed evidence would have enabled the defendant significantly to alter the quantum of proof in his favor.” *Id.* (internal quotation marks omitted).

Rule 17(c), Fed. R. Crim. P., allows parties to subpoena documents and objects to be introduced at criminal

⁴⁴ Moreover, the district court specifically ruled that it would entertain Ulbricht’s applications to rely on specific parts of the letter at trial if doing so would be necessary for effective cross-examination. Thus, Ulbricht was given the opportunity to show particularized need in the context of specific trial evidence. Ulbricht has not identified any point in the trial where he attempted to show that Force’s behavior had become relevant to challenging the credibility of particular aspects of the prosecution’s case.

trials. A subpoena must meet three criteria: “(1) relevancy; (2) admissibility; [and] (3) specificity.” *United States v. Nixon*, 418 U.S. 683, 700 (1974). The party requesting the subpoena must also show that the information sought is “not otherwise procurable reasonably in advance of trial by exercise of due diligence,” that “the party cannot properly prepare for trial without such production,” and that “the application is made in good faith and is not intended as a general ‘fishing expedition.’” *Id.* at 699-700. We review the district court’s discovery rulings for abuse of discretion. *United States v. Rigas*, 583 F.3d 108, 125 (2d Cir. 2009).

The district court did not abuse its discretion when it denied Ulbricht’s discovery requests related to the Force investigation. Ulbricht submitted 28 individual discovery requests in connection with the Force disclosure. Those ranged from the reasonably specific, such as “records from any and all Bitcoin accounts” used by Force, to the very broad, such as “any spending, net worth, or other financial analysis conducted with respect to former SA Force,” “any and all phone records relating to former SA Force,” and “bank account records from any and all bank accounts maintained by former SA Force or his spouse.” App’x 669-70. The district court concluded that those requests were too broad and unfocused, and that the information requested was not material in the Rule 16 sense because the defense “has not articulated a coherent and particular reason why” the Force investigation could “counter the government’s case or bolster a defense.” *Id.* at 697. Next, the district court concluded that the Rule 17 subpoenas were part of the same overall fishing expedition and that the issuance of such subpoenas could compromise the Force grand jury investigation.

There was no abuse of discretion in those rulings. Ulbricht has not shown that, had the government produced every piece of requested information, he would have been able to alter the quantum of proof in his favor at trial. That is so because there is no indication, beyond Ulbricht's speculation, that Force manufactured any of the evidence on which the government relied at trial, let alone the most damning evidence discovered on the hard drive on Ulbricht's laptop and at his apartment. Because Force did not testify at trial, information related to his corruption would not have been relevant to attack the credibility of any testimony he would have given. Moreover, Ulbricht has not identified any specific aspect of the trial evidence that he could have undermined using the requested information. Thus, even if the district court erred in not granting at least some of Ulbricht's discovery requests, any such error does not justify a new trial.

4. Ulbricht's Motion to Adjourn the Trial

Ulbricht contends that the district court erred in denying his request to adjourn the trial until the Force investigation was complete. "[A] district court has a great deal of latitude in scheduling trials." *United States v. Griffiths*, 750 F.3d 237, 241 (2d Cir. 2014) (internal quotation marks omitted). Thus, "trial courts enjoy very broad discretion in granting or denying trial continuances." *United States v. Stringer*, 730 F.3d 120, 127 (2d Cir. 2013). A decision to grant or deny a request for an adjournment is reviewed for abuse of discretion, and we "will find no such abuse unless the denial was an arbitrary action that substantially impaired the defense." *Id.* (internal quotation marks omitted). Thus, the party seeking a continuance has the burden of showing "both arbitrariness and prejudice in order to obtain reversal" based on a denial of an

adjournment. *Id.* at 128 (internal quotation marks omitted).

The district court did not abuse its discretion in denying Ulbricht's request for an adjournment of the trial. In a sealed portion of the proceedings on the first day of trial, the district court explained its reasons for denying the adjournment. The court ruled that because none of the evidence revealed by the government concerning Force's corruption was exculpatory, there was no reason to believe that delaying the trial would assist Ulbricht's defense. That analysis was not irrational or arbitrary. Moreover, as explained in more detail both above and below, Ulbricht has not shown how information related to Force's corruption was either exculpatory or material to his defense. Thus, he has not shown that the district court's refusal to adjourn the trial was prejudicial, let alone substantially so.

5. Preclusion of the DeathFromAbove Chats

As already described, Force used DeathFromAbove as an unauthorized Silk Road username through which he attempted to extort money from DPR. The government only learned of Force's activity as DeathFromAbove during trial, when the defense attempted to introduce a redacted chat between DPR and DeathFromAbove. In the chat at issue, DeathFromAbove implied that he knew that DPR's real identity was Anand Athavale. DeathFromAbove then attempted to blackmail DPR by saying that, if DPR gave him \$250,000, he would not "give you [*sic*] identity to law enforcement." App'x 712.

The government objected to admitting the chat on three grounds: (1) it was hearsay; (2) its probative value was substantially outweighed by unfair prejudice under

Rule 403, Fed. R. Evid.; and (3) it was a “back-door attempt to re-inject” Force’s corruption into the defense’s trial evidence. App’x 707. The district court excluded the chat as hearsay. At trial, Ulbricht claimed that the chat was not being offered for its truth, but instead to show its effect on DPR; that is, if DPR was actually Athavale, one would expect DPR to take certain steps to protect his identity. The district court disagreed and ruled that the DeathFromAbove chat was hearsay because it was offered for the truth of the matter asserted therein—that government agents at one time thought that Athavale was DPR—and it did not fall into any hearsay exceptions. In the alternative, the district court found that the Athavale-as-DPR theory lacked sufficient support, was speculative, and risked jury confusion.

In general, hearsay is not admissible unless an exception applies. *See* Fed. R. Evid. 802. “The Federal Rules of Evidence define hearsay as a declarant’s out-of-court statement offered in evidence to prove the truth of the matter asserted in the statement.” *United States v. Dupree*, 706 F.3d 131, 136 (2d Cir. 2013) (internal quotation marks and alterations omitted). If “the significance of an offered statement lies solely in the fact that it was made, no issue is raised as to the truth of anything asserted, and the statement is not hearsay.” *Id.* (internal quotation marks omitted). “The trial court’s ultimate decisions as to the admission or exclusion of evidence are reviewed for abuse of discretion.” *Davis v. Velez*, 797 F.3d 192, 201 (2d Cir. 2015).

The district court concluded that the Death-FromAbove chat was hearsay because it was an out-of-court statement being offered for the truth of the matter asserted therein. That ruling was not an abuse of discretion. Contrary to Ulbricht’s assertions on appeal,

the district court did not rest its decision on the need for grand jury secrecy to protect the Force investigation. Instead, the decision was a straightforward application of the rule against hearsay.

Ulbricht does not provide any detailed arguments to the contrary that are specific to the DeathFromAbove chat; instead, he discusses the district court's preclusion of all of the evidence related to the Force investigation collectively. At trial, however, he claimed that the statement was offered only to demonstrate "the fact that it was communicated to DPR . . . in that this particular piece of evidence communicates to DPR the name and profile of the person [D]eath[F]rom[A]bove believes is DPR." Tr. 1866. Ulbricht claimed that the statement was "offered for the fact that DPR was getting information about people who were supposed to be DPR," and "one of these people is [Athavale]." *Id.* at 1867. Once the district court expressed skepticism about his argument, Ulbricht claimed that he sought to admit the chat to demonstrate its effect on DPR: "if you're DPR and you get a name . . . this Anand Athavale and a profile and details . . . and you're put on notice that it's you, you're going to take steps." *Id.* at 1867-68. In other words, Ulbricht claimed that he did not offer it for the truth of the matter asserted in the chat: that agents in the Baltimore investigation, including Force, believed that Athavale was the real Dread Pirate Roberts, or that Athavale was in fact the real DPR.

Ulbricht's proposed non-hearsay use of the chat—to show its effect on DPR—is not sufficiently probative that the evidence's exclusion prejudiced him. The statement does not appear to have had an effect on DPR that would bolster Ulbricht's defense. DPR did not alter his behavior in response to the extortion attempt. Indeed, he referred to it as "bogus" in one of the journal entries discovered on

Ulbricht's laptop. App'x 710. If Athavale had been the real Dread Pirate Roberts, he likely would have had a different reaction to the threatened exposure of his identity. DPR's reactions to other attempts to destroy the site's anonymity were dramatic, and included hiring people to kill the users who threatened to compromise Silk Road. Therefore, even if Ulbricht did not offer the chat for its truth, any relevance of the arguably non-hearsay use of the statement was entirely too remote to outweigh the possible jury confusion that would result from the injection of Force into the trial or the likelihood that the jury would confuse the hearsay and non-hearsay significance of the evidence.

6. Ulbricht's Rule 33 Motion: *Brady v. Maryland*

Ulbricht moved for a new trial under Rule 33, Fed. R. Crim. P., raising several issues concerning the unfairness of the assertedly belated disclosures of the investigations into Force and Bridges.⁴⁵ The only argument that he pursues in this appeal is that the belated disclosures violated his due process rights under *Brady* because the information was both material and exculpatory.

Rule 33(a) provides that, on “the defendant’s motion, the court may vacate any judgment and grant a new trial if the interest of justice so requires.” We have advised district courts to “exercise Rule 33 authority sparingly and in the most extraordinary circumstances.” *United States v. Côté*, 544 F.3d 88, 101 (2d Cir. 2008) (internal quotation marks omitted). “Where a defendant’s *Brady* claim was

⁴⁵ Ulbricht filed his Rule 33 motion on March 6, 2015. The criminal complaint against Force and Bridges was unsealed on March 30, which is the first time that Ulbricht learned that Bridges was corrupt and was involved in the case.

raised in a motion for a new trial pursuant to Rule 33[,] . . . we review the denial of the motion for abuse of discretion.” *United States v. Douglas*, 525 F.3d 225, 245 (2d Cir. 2008) (internal quotation marks omitted). In the context of denying a Rule 33 motion, a “district court abuses . . . the discretion accorded to it when (1) its decision rests on an error of law . . . or a clearly erroneous factual finding, or (2) its decision—though not necessarily the product of a legal error or a clearly erroneous factual finding—cannot be located within the range of permissible decisions.” *United States v. Forbes*, 790 F.3d 403, 406 (2d Cir. 2015) (internal quotation marks omitted).

There are three components of a *Brady* violation: “(1) The evidence at issue must be favorable to the accused, either because it is exculpatory or because it is impeaching; (2) that evidence must have been suppressed by the [government], either willfully or inadvertently; and (3) prejudice must have ensued.” *United States v. Certified Env'tl. Servs., Inc.*, 753 F.3d 72, 91 (2d Cir. 2014) (internal quotation marks omitted). Information is exculpatory if it relates to the defendant’s guilt or innocence. *United States v. Avellino*, 136 F.3d 249, 255 (2d Cir. 1998). In order to show that he has been prejudiced, a defendant must demonstrate “a reasonable probability that, had the evidence been disclosed, the result of the proceeding would have been different, such that the failure to disclose undermines confidence in the verdict.” *Certified Env'tl. Servs., Inc.*, 753 F.3d at 91 (internal quotation marks and alterations omitted). Thus, the prosecution “must disclose . . . exculpatory and impeachment information no later than the point at which a reasonable probability will exist that the outcome would have been different if an earlier disclosure had been made.” *Id.* at 92 (internal quotation marks omitted). In general, a “prudent prosecutor will err on the side of transparency, resolving doubtful questions

in favor of disclosure.” *Cone v. Bell*, 556 U.S. 449, 470 n.15 (2009).

Although the agents’ illegal behavior in connection with the Silk Road investigation is deeply troubling, the government’s December 2014 disclosure of the Force investigation and the post-trial disclosure of Bridges’s corruption did not violate Ulbricht’s due process rights. Evidence concerning the agents’ corruption is not *Brady* information because it is not exculpatory or impeaching of the government’s trial evidence. For this reason, the government’s failure to reveal the full extent of the investigations until after Ulbricht’s trial did not prejudice him. As already explained, the fact that Force purloined Bitcoins from Silk Road and attempted to blackmail DPR does not relate to Ulbricht’s guilt or innocence; the same logic applies to Bridges’s similar behavior. The agents’ corruption has nothing to do with whether Ulbricht operated the site as Dread Pirate Roberts. Ulbricht has not raised any credible doubts about the reliability of the evidence that the government presented at trial, nor has he explained why the agents’ illegal actions relate to *his* guilt at all. Indeed, the government removed from its exhibit list the items relevant to Force, including communications between Nob (his authorized undercover username) and DPR. Those communications included an instance in which DPR hired Nob to kill Curtis Green (Flush) as punishment for using his administrator status to steal Bitcoins from Silk Road users. Ulbricht does not identify any particular evidence introduced by the government at trial that is traceable to either Force or Bridges, or the admissibility of which depends on either agent’s integrity.

Ulbricht’s arguments to the contrary largely rest on speculation. First, Ulbricht contends that the Silk Road

investigations occurring in Baltimore and New York were “[c]oordinated and [c]ombined,” suggesting that Force’s corruption may have somehow infected the evidence that the New York office used in its prosecution. Appellant Br. 40. Ulbricht explains that the offices communicated frequently and shared information through emails and reports. Assuming that Ulbricht is correct, the fact that the Silk Road investigation took place in several offices, one of which employed two corrupt agents, does not alter our analysis. Ulbricht still has not shown how the agents’ corrupt behavior is exculpatory as to him, even if Force and Bridges at times shared their work product with New York and that work product influenced the larger investigation. The relevant question, on which none of Ulbricht’s arguments casts any light or raises any doubt, is whether any particular item of evidence was tainted in some way by the misconduct of Bridges or Force.

Next, Ulbricht surmises that the agents may have fabricated evidence suggesting that Ulbricht was DPR. In so arguing, Ulbricht implies that Force and Bridges may have had sufficiently high-level administrator access to Silk Road to manipulate the “financial, transactional, and communications infrastructure of the Silk Road site.” Reply Br. 14. Nothing in the government’s disclosures, and nothing that Ulbricht identifies in the record or has produced from any independent source, suggests that either Bridges or Force had such capacity. Absent further detail or evidence that Force and Bridges were able to infiltrate DPR’s communications or transactions, Ulbricht’s argument is simply too speculative to warrant a new trial. Ulbricht further claims that Bridges used sophisticated techniques to try to place blame on others for his corrupt conduct, reflecting a pattern of framing others for his own crimes. That fact alone does not suggest that Bridges fabricated any evidence against Ulbricht or attempted to

frame him. That Bridges undertook to deflect blame for things *he* had done does not suggest any reason why Bridges would be motivated to frame Ulbricht for things that DPR had done. Nor does Ulbricht explain how Bridges's actions should undermine our confidence in any of the specific evidence on which the government relied at trial.⁴⁶

Finally, Ulbricht submitted a supplemental appendix that included a newly-discovered, unredacted report from the Joint Automated Booking System ("JABS").⁴⁷ In that report, under the heading "Arrested or Received Information," Force is listed as the officer on the case, and the Baltimore DEA is listed as the relevant agency. Ulbricht apparently means to suggest that this report shows that Force played a more pervasive role in the investigation than the government has acknowledged. In response, the government argues that Force was simply the most recent person to make changes to the JABS report by updating it to include information about Ulbricht's family members and the pending charges in Maryland. In any event, the JABS report bearing Force's name does not show how information related to Force's corruption excul-

⁴⁶ In a footnote, Ulbricht claims that failing to disclose the full extent of the agents' corruption deprived him of an opportunity to "attack[] the investigation as shoddy." *Kyles v. Whitley*, 514 U.S. 419, 442 n.13 (1995). Now that he has all of the relevant information, he still does not explain how he might have demonstrated deficiencies in the government's investigation of his or one of the other initial suspects' conduct that would undermine our confidence in the verdict.

⁴⁷ As the government explains, and Ulbricht does not dispute, JABS is a database maintained by the United States Marshals Service that catalogues information regarding alleged offenders who have been arrested and booked by federal, state, or local law enforcement agencies.

pates Ulbricht. It merely confirms that Force was a participant in the Baltimore Silk Road investigation and that he continued to be involved in the case after Ulbricht was arrested. In the face of the entire record of the trial, in which the provenance of the government’s evidence was exhaustively displayed without indication that Force was responsible for any of it, this single report has little or no probative value.

In sum, we conclude that the Force and Bridges complaint did not contain *Brady* information because the agents’ corruption does not bear on Ulbricht’s guilt or innocence. Thus, any delay in the government’s disclosure of their corruption did not violate Ulbricht’s due process rights.

B. Preclusion of Defense Experts

The district court precluded both of Ulbricht’s proposed expert witnesses from testifying because he did not timely or adequately disclose his intent to call them under Rule 16, Fed. R. Crim. P. In general, the “defendant must, at the government’s request, give to the government a written summary of any [expert] testimony that a defendant intends to use. . . . This summary must describe the witness’s opinions, the bases and reasons for those opinions, and the witness’s qualifications.”⁴⁸ Fed. R. Crim. P. 16(b)(1)(C). The purpose of the expert disclosure requirement is to “minimize surprise that often results from unexpected expert testimony, reduce the need for continuances, and to provide the opponent with a fair opportunity to test the merit of the expert’s testimony through focused cross-examination.” Fed. R. Crim. P. 16, advisory committee’s note to 1993 amendment. Indeed, “[w]ith increased

⁴⁸ It is undisputed that the government requested such disclosure on December 29, 2014, two weeks before trial began.

use of both scientific and nonscientific expert testimony, one of counsel's most basic discovery needs is to learn that an expert is expected to testify." *Id.*

If a party fails to comply with Rule 16, the district court has "broad discretion in fashioning a remedy," which may include granting a continuance or "ordering the exclusion of evidence." *United States v. Lee*, 834 F.3d 145, 158 (2d Cir. 2016) (internal quotation marks omitted); see Fed. R. Crim. P. 16(d)(2)(A)-(D) (a district court may order "any other [remedy] that is just under the circumstances"). We thus review the district court's choice of remedy for abuse of discretion. "In considering whether the district court abused its discretion, we look to the reasons why disclosure was not made, the extent of the prejudice, if any, to the opposing party, the feasibility of rectifying that prejudice by a continuance, and any other relevant circumstances." *Lee*, 834 F.3d at 159 (internal quotation marks omitted).

The district court did not abuse its discretion in precluding the defense from calling its proposed experts. Not only were the disclosures late, more importantly, they were plainly inadequate. Both disclosures merely listed general and in some cases extremely broad topics on which the experts might opine. For example, the disclosures indicated that the experts would testify on general topics, including: "the origins of Bitcoin," "the various purposes and uses of Bitcoin," "the mechanics of Bitcoin transactions," "the value of Bitcoin over time since its inception," "the concepts of Bitcoin speculating and Bitcoin mining," "[g]eneral principles of internet security and vulnerabilities," the "import of some lines of PHP code provided to defense counsel in discovery," and "[g]eneral principles of public-key cryptography," among others.

App'x 349, 360. They did not summarize the experts' opinions about those topics, let alone describe the bases for the experts' opinions.

Indeed, although the listed topics certainly pertained generally to Silk Road, the disclosures were so vague that it is difficult to discern whether the proffered expert testimony would have been at all relevant under Rules 401 and 702(a), Fed. R. Evid.⁴⁹ In his opposition to the government's motion to preclude Antonopoulos, Ulbricht described the expert's proposed testimony in more detail, but he still did not disclose the opinions that the expert intended to offer. For example, that supplemental disclosure indicated that an "[i]ndependent defense investigation has uncovered that" the government's claim that over 700,000 Bitcoins were transferred to Ulbricht's Bitcoin wallet "is implausible," and the expert would "dispute this finding." App'x 382. Although that is more specific, it is not a summary of Antonopoulos's opinion, nor does it identify the basis for that opinion. Thus, to this day Ulbricht has not described what opinions the experts would offer or explained the methods they used to arrive at any of those conclusions.

⁴⁹ In particular, Ulbricht's disclosures did not discuss, and he has not described on appeal, how one expert's proposed testimony on "[g]eneral principles of internet security and vulnerabilities" would have linked to the defense claim that the damning documentary evidence of Ulbricht's guilt found on his laptop was or could have been fabricated or planted. The jury was aware from other evidence, and indeed it is within ordinary lay experience, that various forms of hacking are possible. What was lacking, what the defense expert disclosures did not purport to address, and what Ulbricht still has not provided on appeal, is any explanation, let alone a credible explanation, of how the breadth and variety of information, from the laptop and other sources, could have been planted.

The district court also did not abuse its discretion in finding that the government would be prejudiced by the belated and inadequate disclosures, in part because the government was due to rest the following day, providing it with no time to prepare to respond to the experts. Moreover, the district court considered intermediate sanctions short of preclusion but found them to be inadequate. In rejecting a continuance as a possible remedy, the district court emphasized the “known issues with a continuance,” especially in a lengthy trial. *Id.* at 369. Two of the jurors had time constraints, and a continuance might have caused the court to lose one or both of those jurors, especially if the continuance was lengthy. If it were to grant a continuance, the court would also need to perform its function as a gatekeeper of expert testimony under *Daubert v. Merrell Dow Pharm., Inc.*, 509 U.S. 579, 592-93 (1993), which requires the district court to make a “preliminary assessment of whether the reasoning or methodology underlying the [expert] testimony is scientifically valid” and “can be applied to the facts in issue.”⁵⁰ The district court cannot perform that complex evaluation of an expert’s proposed methodology without a clear articula-

⁵⁰ We have explained that a *Daubert* reliability assessment requires a district court to consider the “extent to which [the expert’s theory] has been subjected to peer review and publication,” whether the technique is “subject to standards controlling the technique’s operation,” the “known or potential rate of error,” and the “degree of acceptance within the relevant scientific community.” *United States v. Romano*, 794 F.3d 317, 330 (2d Cir. 2015) (internal quotation marks omitted). That inquiry is a “flexible one,” however, and *Daubert* is not a “definitive checklist or test” for the reliability of expert testimony. *Id.* (internal quotation marks omitted). Thus, “[w]hether *Daubert*’s specific factors are, or are not, reasonable measures of reliability in a particular case is a matter that the law grants the trial judge broad latitude to determine.” *Id.* at 331 (internal quotation marks omitted).

tion of what the expert's opinions are and, even more importantly, of the bases for those opinions. In light of the risk of losing jurors and the lack of a sufficiently compelling reason for the defense's clear violation of Rule 16, the district court was within its discretion when it determined that a continuance was not practical and that the appropriate remedy was to preclude the witnesses altogether.

Ulbricht's arguments to the contrary are not persuasive. First, Ulbricht argues that the two experts were necessary to rebut portions of the government's case that he was precluded from addressing during cross-examination, as well as the testimony of Ilhwan Yum, a government witness who analyzed transactions associated with Bitcoin wallets found on Ulbricht's laptop. Ulbricht now contends that portions of Yum's testimony were incorrect, including his description of what a "hot" Bitcoin wallet is.⁵¹ Ulbricht does not, however, explain *how* Yum's testimony was incorrect, what contrary evidence his experts would have provided had they been allowed to testify, or how any purported correction of Yum's testimony would have affected the case against Ulbricht. Nor has he produced any summaries of his proposed expert testimony or described how that testimony would have been material to Ulbricht's guilt or innocence. In other words, Ulbricht has not shown that precluding Bellovin and Antonopoulos

⁵¹ "The terms hot wallet and cold wallet derive from the more general terms hot storage, meaning online storage, and cold storage, meaning offline storage. A hot wallet is a Bitcoin wallet for which the private keys are stored on a network-connected machine (*i.e.*, in hot storage). By contrast, for a cold wallet the private keys are stored offline." Steven Goldfeder *et al.*, *Securing Bitcoin Wallets via a New DSA/ECDSA Threshold Signature Scheme*, Princeton University 10, available at http://www.cs.princeton.edu/~stevenag/threshold_sigs.pdf.

from testifying prejudiced him. Ulbricht's alternative argument that the disclosures were in fact adequate is incorrect for the reasons already explained.

Ulbricht next argues that preclusion was an unduly harsh remedy under the circumstances. Along those lines, he claims that certain exhibits, such as the summary chart on which Yum relied, were not produced until mid-trial. Thus, according to Ulbricht, he could not have known about his need for expert witnesses to counter specific trial exhibits until it was already too late to comply with Rule 16. In his view, the district court should not have held him so strictly to Rule 16's requirements because he could not have known until Yum testified that he would need to call an expert.

While Ulbricht is correct that excluding his experts was a harsh sanction and was not to be imposed lightly, the district court considered the possibility of granting a continuance or a more limited sanction and found those remedies to be inappropriate under the circumstances. Such careful consideration of a range of possible sanctions short of preclusion is especially important in the atypical case where a criminal defendant, rather than the government, is precluded from putting on his case because of a Rule 16 violation. Limiting the defense's presentation of his case implicates the fundamental right of "an accused to present witnesses in his own defense." *Chambers v. Mississippi*, 410 U.S. 284, 302 (1973). However, the defendant must still "comply with established rules of procedure and evidence designed to assure both fairness and reliability in the ascertainment of guilt and innocence." *Id.* Here, Ulbricht did not comply with the procedural requirements associated with expert disclosures. The dis-

strict court gave the issue due consideration and appropriately exercised its discretion in remedying the defense's Rule 16 violation.

Finally, Ulbricht cannot credibly argue that Yum's testimony was the first notice he had about the possible need for an expert witness to testify as part of his affirmative case. The Silk Road prosecution was uniquely laden with issues related to technology, computer servers, forensics, cyber security, digital currency, and myriad other issues that are indisputably "beyond the ken of the average juror." *United States v. Mejia*, 545 F.3d 179, 191 (2d Cir. 2008) (internal quotation marks omitted). Ulbricht surely knew from the outset that, in order to mount a meaningful attack on the government's voluminous and technically complex evidence, he would need to call his own expert. Indeed, in his opening statement, Ulbricht's counsel claimed that he would show that the Bitcoins in Ulbricht's wallet were from innocent transactions associated with Bitcoin speculation, rather than, as the government contended, related to Silk Road.⁵² Ulbricht's opening statement also implied that BitTorrent's⁵³ security deficiencies could have allowed the true DPR to plant incriminating evidence on his laptop. It is difficult to fathom

⁵² No evidence about the source of those Bitcoins was in fact presented by Ulbricht, and neither the expert disclosures presented to the district court nor Ulbricht's arguments on appeal suggest that either Bellovin or Antonopoulos would have provided an analysis or explanation of Ulbricht's Bitcoin transactions that would have revealed a non-Silk Road source for Ulbricht's Bitcoins.

⁵³ BitTorrent is a peer-to-peer file sharing service that is used to transfer large files without disrupting Internet servers. It has both legitimate and illicit purposes. *See Next Phase Distribution, Inc. v. John Does 1-27*, 284 F.R.D. 165, 167 (S.D.N.Y. 2012).

how he planned to advance those theories without relying on expert testimony.

In short, Ulbricht argues that the district court's preclusion of his proffered expert witnesses denied him a fair opportunity to present his defense. But the same failings that render Ulbricht's expert disclosures inadequate under Rule 16 preclude us from finding the kind of prejudice he asserts. Ulbricht did not disclose to the district court, and has not presented on appeal, any explanation of what the proposed experts would have said that would have supported a non-speculative basis for doubting the probative value of evidence from a variety of electronic and other sources identifying Ulbricht as DPR throughout the life of Silk Road. Thus, we cannot conclude that he was prejudiced by the experts' exclusion.

C. Curtailing Cross-Examination

Ulbricht contends that the district court erred in limiting his ability to cross-examine two government witnesses: Der-Yeghiayan and Kiernan. "We review a trial court's decision to limit the scope of cross-examination for abuse of discretion." *United States v. Cedeno*, 644 F.3d 79, 81 (2d Cir. 2011). "A district court is accorded broad discretion in controlling the scope and extent of cross-examination." *United States v. James*, 712 F.3d 79, 103 (2d Cir. 2013) (internal quotation marks omitted); see Fed. R. Evid. 611(a). Thus, "a district court may impose reasonable limits on cross-examination to protect against, *e.g.*, harassment, prejudice, confusion, and waste." *James*, 712 F.3d at 103 (internal quotation marks omitted). In general, however, a "district court should afford wide latitude to a defendant in a criminal case to cross-examine government witnesses." *Id.* (internal quotation marks omitted). That is so because the Confrontation Clause gives "a de-

fendant the right not only to cross-examination, but to effective cross-examination.” *Id.* “[I]t does not follow, of course, that the Confrontation Clause prevents a trial judge from imposing *any* limits” on defense counsel’s cross-examination of government witnesses. *Id.* (emphasis in original).

1. Agent Der-Yeghiayan

Ulbricht argues that the district court erred when it struck portions of Der-Yeghiayan’s testimony that referenced his prior belief that Karpeles might be Dread Pirate Roberts. Ulbricht also challenges the striking of a similar but analytically distinct piece of testimony: Der-Yeghiayan’s statement that Karpeles’s attorney had offered information about Silk Road in exchange for Karpeles receiving immunity from prosecution. Ulbricht wanted the jury to infer that Karpeles had some criminal involvement in Silk Road that motivated him to pursue a cooperation agreement with the government.

Der-Yeghiayan answered the defendant’s initial questions about those topics, and the government did not object to them until a later side bar. During the side bar, the district court expressed its initial view that the questions were proper, but requested written briefing on the subject. After reviewing the parties’ submissions, the district court agreed with the government that neither Der-Yeghiayan’s prior opinions about whether Karpeles was DPR nor Karpeles’s offer of information about Silk Road was relevant to Ulbricht’s case. The court thus directed the government to identify portions of Der-Yeghiayan’s testimony to strike. After the government identified the improper testimony, the district court gave a general limiting instruction to the jury:

You heard testimony while Mr. Der-Yeghiayan was on the stand regarding personal beliefs or suspicions he may have had about particular individuals at various points during his investigation. And I instruct you that what the agent suspected about others isn't evidence and should be disregarded. Now, consistent with all of the instructions I'm going to give you at the end of the case, there was other testimony that Mr. Der-Yeghiayan provided which you may consider during your deliberations and give it the weight that you deem that it deserves. So it's the suspicions, all right?

Tr. 974. Ulbricht contends on appeal that the district court erred in striking the testimony.

We disagree. The district court did not err in concluding that Der-Yeghiayan's prior beliefs about Karpeles as a possible DPR suspect were not relevant to the charges against Ulbricht. In order to elicit testimony implicating an alternative perpetrator, a defendant "must show that his proffered evidence on the alleged alternative perpetrator is sufficient, on its own or in combination with other evidence in the record, to show a nexus between the crime charged and the asserted alternative perpetrator." *Wade v. Mantello*, 333 F.3d 51, 61-62 (2d Cir. 2003) (internal quotation marks omitted). Thus, to avoid a "grave risk of jury confusion," a defendant must offer more than "unsupported speculation that another person may have done the crime." *Id.* at 62 (internal quotation marks omitted). An "agent's state of mind as the investigation progressed is ordinarily of little or no relevance to the question of the defendant[s] guilt." *United States v. Johnson*, 529 F.3d 493, 501 (2d Cir. 2008). Thus, striking Der-Yeghiayan's

testimony and instructing the jury to disregard his earlier opinions about Karpeles's possible guilt was not error.⁵⁴

Further, any arguable error that occurred was harmless. Defense counsel continued to cross-examine Der-Yeghiayan and elicited admissible testimony about the earlier investigation into Karpeles; indeed, the district court took over cross-examination at several points to assist the defense in asking proper questions. *Cf. Cotto v. Herbert*, 331 F.3d 217, 254 (2d Cir. 2003) (in considering whether a Confrontation Clause violation is harmless, we consider, *inter alia*, “the extent of cross-examination otherwise permitted”). Moreover, Ulbricht discussed the investigation of Karpeles in his summation without objection. What was relevant at trial was any actual evidence pointing to Karpeles as the true Dread Pirate Roberts. The district court did not limit Ulbricht's cross-examination of Der-Yeghiayan as to his knowledge of such evidence. The district court directed the jury to disregard only testimony as to the agent's “suspicions,” Tr. 974, a subject of “little or no relevance to . . . the defendant[s] guilt,” *Johnson*, 529 F.3d at 501.

We similarly reject Ulbricht's contention that striking Der-Yeghiayan's testimony concerning Karpeles's offer to provide information about Silk Road in exchange for

⁵⁴ Ulbricht also contends on appeal that the government's objection to the testimony, which occurred at a later sidebar, was untimely. He cites no law in support of that argument. In general, an “objection should be made after the question has been asked but before an answer has been given.” *Hutchinson v. Groskin*, 927 F.2d 722, 725 (2d Cir. 1991). That “rule is not inflexible,” *id.*, however, and we do not “necessarily find [a]n objection affirmatively waived because it might have been interposed a few questions earlier,” *United States v. Pujana-Mena*, 949 F.2d 24, 33 (2d Cir. 1991). Thus, although a contemporaneous objection is preferable, the district court was within its discretion to sustain the later objection and strike the testimony.

immunity was an abuse of discretion. Absent other evidence in the record regarding Karpeles, it was proper to exclude wholly speculative suggestions of an alternative perpetrator defense based on Karpeles's attorney's offer of information in exchange for his client's immunity. And even assuming, *arguendo*, that the district court erred in striking the testimony, any error was harmless. To the extent this testimony was stricken from the trial record, that ruling occurred outside the presence of the jury. All the jury was told was to disregard testimony about "what the agent suspected about others," Tr. 974, a category that hardly would be understood by the jury to encompass testimony about the actions of Karpeles's attorney. As explained in detail above, moreover, the evidence identifying Ulbricht as Dread Pirate Roberts was overwhelming and largely unchallenged. That Karpeles may have had information about Silk Road does not imply that he was DPR, only that he had some knowledge of or involvement with the site. Particularly given that Karpeles likely had some knowledge about Silk Road simply because of his operation of Mt. Gox, a prominent Bitcoin exchanger, any marginal probative value in the fact that he claimed to have such knowledge, and offered to provide it to the government, could not have meaningfully affected the balance of evidence available to the jury regarding the identity of DPR.

2. Agent Kiernan

Defense counsel cross-examined Kiernan extensively, and Ulbricht contends on appeal that the district court erred in preventing him from exploring certain topics during that cross-examination. Those excluded topics include:

the meaning of various acronyms, the significance of a certain line of PHP code,⁵⁵ whether the FBI allowed Kiernan to run BitTorrent on his work computer despite its lack of security, and whether the Linux kernel⁵⁶ that Kiernan used on his work computer was the same as the one that Ulbricht installed on his laptop. Ulbricht explains that he was attempting to show that Kiernan's conclusions about Ulbricht's laptop were inaccurate because they were based on unreliable information.

The district court sustained objections to those questions because, in its view, they were outside the scope of Kiernan's direct testimony. *See* Fed. R. Evid. 611(b) ("Cross-examination should not go beyond the subject matter of the direct examination and matters affecting the witness's credibility."); *Baker v. Goldman Sachs & Co.*, 669 F.3d 105, 110 (2d Cir. 2012) ("Once any direct examination is concluded, cross-examination within the scope of the direct follows.").

On appeal, Ulbricht claims that, because Kiernan testified about the operation of Tor Chat and other forensic computer issues during his direct testimony, the precluded questions were within that testimony's scope and should have been allowed. Even assuming that Ulbricht is correct, any error is harmless. Ulbricht was permitted to question Kiernan about whether Linux was customizable, and Kiernan admitted during cross that he did not know whether he used the same version of Tor Chat that Ulbricht had installed on his laptop. Ulbricht's counsel also asked several questions about the security vulnerabilities

⁵⁵ PHP is a common computer programming language that is used primarily in website development

⁵⁶ A kernel is an operating system's core, and it "is an essential part of the Linux operating system." Tr. 1070.

of BitTorrent, conveying to the jury that using BitTorrent might have rendered Ulbricht's computer susceptible to hacking. Thus, Ulbricht was able to elicit testimony supporting his proposed inference that Kiernan's conclusions based on the Tor Chat evidence were flawed. Ulbricht does not explain how he was prejudiced when the district court prohibited him from asking Kiernan certain other questions. We therefore identify no reversible error in the district court's limitations on Kiernan's cross examination.

D. Andrew Jones Hearsay Statement

The district court excluded a statement allegedly made by Andrew Jones, who was a Silk Road administrator under the username Inigo. Jones cooperated with the government and was on the government's witness list until the middle of trial, when the government decided not to call him. Defense counsel explored the possibility of calling Jones as a witness, but Jones's attorney advised Ulbricht that Jones would invoke the Fifth Amendment and refuse to testify if compelled to appear. In light of Jones's unavailability, Ulbricht sought to admit a December 29, 2014 letter from the government to defense counsel that described a statement that Jones made during one of his interviews.⁵⁷ The relevant portion of the government's letter is as follows:

At some point in or about August or September 2013, Jones tried to authenticate that the Silk Road user "Dread Pirate Roberts" whom he was talking to at the time . . . was the same person with whom he had been communicating in the past with this

⁵⁷ The government did not concede that the statement was *Brady* information, but disclosed it "in an abundance of caution." App'x 398.

username. Previously, . . . Jones and “Dread Pirate Roberts” had agreed upon a “handshake” to use for authentication, in which Jones would provide a certain prompt and “Dread Pirate Roberts” would provide a certain response. When, during the 2013 chat in question, Jones provided what he believed to be the designated prompt, “Dread Pirate Roberts” was unable to provide the response Jones thought they had agreed on. However, later in the chat, Jones asked “Dread Pirate Roberts” to validate himself by specifying the first job that “Dread Pirate Roberts” assigned to him (running the “DPR Book Club”), which “Dread Pirate Roberts” was able to do.

App’x 398. Ulbricht argues that the Jones statement⁵⁸ supports his theory that more than one person acted as Dread Pirate Roberts, because at one point DPR could authenticate his identity to Jones, but at another time he could not.

When it became clear that Jones was unavailable to testify, Ulbricht asked the government to stipulate that the Jones statement could be read to the jury. The government initially agreed, but then changed its mind and opposed admitting the Jones statement. The defense acknowledged that the statement was hearsay, but claimed that it was admissible under two hearsay exceptions: under Rule 804(b)(3), Fed. R. Evid., as a statement

⁵⁸ What Ulbricht sought to introduce was the government’s letter paraphrasing a statement made by Jones during an interview, not a verbatim transcript of what Jones had said. We refer to it as the “Jones statement” for the sake of simplicity.

against interest, and under Rule 807's residual exception. The district court ruled that the statement was inadmissible, specifically addressing only Rule 804(b)(3). On appeal, Ulbricht continues to argue that the statement was admissible under either exception. Neither of his theories is persuasive.⁵⁹

A district court's "ultimate decisions as to the admission or exclusion of evidence are reviewed for abuse of discretion, and will not be disturbed unless they are manifestly erroneous." *Davis*, 797 F.3d at 201 (internal quotation marks and citations omitted). To invoke the 804(b)(3) exception for a statement against interest, the proponent of the statement "must show (1) that the declarant is unavailable as a witness, (2) that the statement is sufficiently reliable to warrant an inference that a reasonable man in [the declarant's] position would not have made the statement unless he believed it to be true, and (3) that corroborating circumstances clearly indicate the trustworthiness of the statement." *United States v. Wexler*, 522 F.3d 194, 202 (2d Cir. 2008) (internal quotation marks omitted). The exception applies "only if the district court determines that a reasonable person in the declarant's shoes would perceive the statement as detrimental to his or her own penal interest." *United States v. Saget*, 377 F.3d 223, 231 (2d Cir. 2004). The key to this inquiry is whether the

⁵⁹ We note that the Jones statement is double hearsay, in that the defense sought to admit the government's subsequent characterization of Jones's interview, and both the government's letter and Jones's statement to the agents were out of court statements offered for their truth. When confronted with "hearsay within hearsay, or double hearsay," courts must determine that "each part of the combined statement[]" is independently admissible. *United States v. Williams*, 927 F.2d 95, 100 (2d Cir. 1991). Because we conclude that no hearsay exception applied to the Jones statement at all, we need not address the double hearsay issue.

statement is sufficiently “self-inculpatory,” which the district court must evaluate on a “case-by-case basis.” *United States v. Williams*, 506 F.3d 151, 155 (2d Cir. 2007).

The district court did not err in concluding that the Jones statement did not fall within Rule 804(b)(3)’s hearsay exception. There is no dispute that Jones was unavailable to testify because he planned to invoke his Fifth Amendment privilege. The court ruled that the Rule 804(b)(3) exception did not apply because Jones was under a cooperation agreement at the time that he made the relevant statement to the government and the chat did not have any particular impact on Jones’s penal interests. On appeal, Ulbricht claims that the extent of Jones’s criminal liability was unknown when he made the statement because he could still be vulnerable to prosecution in other jurisdictions, and he had not yet been sentenced when he made the statement to the government. *See Mitchell v. United States*, 526 U.S. 314, 326 (1999) (in the Fifth Amendment context, there can be a “legitimate fear of adverse consequences from further testimony” where a sentence has not yet been imposed).

We are not persuaded that Jones’s statement was against his penal interests. Given the cooperation agreement, the government’s role at Jones’s future sentencing, and the penalties for lying to the government, it is far from clear that it was against Jones’s interest to disclose details of his criminal activities at the time the statement in question was made. Moreover, even to the extent that Jones’s disclosures taken as a whole constituted inculpatory admissions, the particular statement in question had little adverse effect on Jones. Jones’s inculpatory admissions to the government concern whether he committed crimes connected to Silk Road. His description of his

“handshake” with DPR presupposes that he had already discussed his own crimes with the government. Whether DPR did or did not recognize Jones’s identifying prompt does not bear on Jones’s guilt of any crime associated with the site, since he had already confirmed his role working for DPR. The details of this conversation with DPR thus do not inculcate *Jones*; instead, they either help or hurt Ulbricht. Accordingly, the district court did not abuse its discretion in holding that Rule 804(b)(3) does not apply.

Rule 807 provides for a limited, residual exception to the rule against hearsay where no other exception applies. A hearsay statement may be admissible under Rule 807 if: “(i) it is particularly trustworthy; (ii) it bears on a material fact; (iii) it is the most probative evidence addressing that fact; (iv) its admission is consistent with the rules of evidence and advances the interests of justice; and (v) its proffer follows adequate notice to the adverse party.” *United States v. Morgan*, 385 F.3d 196, 208 (2d Cir. 2004) (internal quotation marks omitted). The “residual hearsay exception[] will be used very rarely, and only in exceptional circumstances.” *Parsons v. Honeywell, Inc.*, 929 F.2d 901, 907 (2d Cir. 1991) (internal quotation marks omitted).

The district court did not specifically address Ulbricht’s request to admit the statement under Rule 807, but we conclude that the limited residual exception does not assist Ulbricht. We are loath to assume that a statement made by a criminal in debriefings to the government pursuant to a cooperation agreement is categorically “particularly trustworthy,” as Rule 807 requires. But even if Jones’s statement meets that criterion, and was offered “as evidence of a material fact,” we cannot say that it is “more probative on the point for which it is offered than any other evidence that the proponent can obtain through

reasonable efforts.” Fed. R. Evid. 807(a)(2)-(3). Ulbricht has not attempted to explain how the Jones statement satisfies this requirement.

Finally, even if the district court erred in excluding the statement under either hearsay exception, any error was certainly harmless. The conversation between Jones and DPR in its totality was not actually helpful to Ulbricht. As explained, during the chat in question, DPR was at one point unable to provide the designated response, but later he identified himself to Jones’s satisfaction. The statement thus contains the seeds of its own refutation. Since DPR’s alleged failure to verify his identity and his subsequent remedy of that failure occurred during the same online chat, the interaction provides little or no support for the defense theory that different individuals acted as DPR at different times.

E. Cumulative Error

Ulbricht argues that the cumulative effect of the district court’s evidentiary rulings deprived him of a fair trial. *See United States v. Al-Moayad*, 545 F.3d 139, 178 (2d Cir. 2008). We have exhaustively reviewed his contentions of trial error and have concluded that none of those contentions has merit. The challenged trial rulings were well within the district court’s discretion, and the various exclusions did not prevent the defense from offering evidence probative of innocence. At the trial in this case, the government presented overwhelming evidence that Ulbricht was indeed Dread Pirate Roberts. The evidence that the defense was precluded from offering to refute that proof was excluded because it was speculative, unreliable, offered in contravention of the Federal Rules of Evidence or of Criminal Procedure, or otherwise inadmissible. The few instances in which the district court’s rulings may be questioned, where we noted the relevance of the

harmless error rule, involved minor and marginal points. Accordingly, whether considered separately or cumulatively, none of Ulbricht’s evidentiary arguments lead us to doubt that he was found guilty after a fair trial.

III. Sentencing

“[A] district court has broad latitude to impose either a Guidelines sentence or a non-Guidelines sentence.” *Rigas*, 583 F.3d at 114 (internal quotation marks omitted). “Accordingly, the role of the Court of Appeals is limited to examining a sentence for reasonableness, which is akin to review under an ‘abuse-of-discretion’ standard.” *Id.* “This standard applies both to the [substantive reasonableness of the] sentence itself and to the procedures employed in arriving at the sentence.” *Id.* (internal quotation marks omitted). Ulbricht and *amici*⁶⁰ challenge his life sentence as both procedurally and substantively unreasonable.

A. Procedural Reasonableness

“A sentence is procedurally unreasonable if the district court fails to calculate (or improperly calculates) the Sentencing Guidelines range, treats the Sentencing Guidelines as mandatory, fails to consider the § 3553(a) factors, selects a sentence based on clearly erroneous facts, or fails adequately to explain the chosen sentence.” *United States v. Jesurum*, 819 F.3d 667, 670 (2d Cir. 2016) (internal quotation marks and emphasis omitted). To “hold that a factual finding is ‘clearly erroneous,’ we must be left with the definite and firm conviction that a mistake has been committed.” *United States v. DeSilva*, 613 F.3d

⁶⁰ The *amici* who join Ulbricht’s challenge to his life sentence include: the Drug Policy Alliance, Law Enforcement Against Prohibition, JustLeadershipUSA, and retired District Judge Nancy Gertner.

352, 356 (2d Cir. 2010). Where “there are two permissible views of the evidence, the factfinder’s choice between them cannot be clearly erroneous.” *United States v. Norman*, 776 F.3d 67, 76 (2d Cir. 2015) (internal quotation marks omitted). In general, a “sentencing court has discretion to consider a wide range of information in arriving at an appropriate sentence.” *United States v. Prescott*, 920 F.2d 139, 143 (2d Cir. 1990). “The district court’s factual findings at sentencing need be supported only by a preponderance of the evidence.” *Norman*, 776 F.3d at 76. “Where we identify procedural error in a sentence, but the record indicates clearly that the district court would have imposed the same sentence in any event, the error may be deemed harmless, avoiding the need to vacate the sentence and to remand the case for resentencing.” *United States v. Jass*, 569 F.3d 47, 68 (2d Cir. 2009) (internal quotation marks omitted); *see also United States v. Cavera*, 550 F.3d 180, 197 (2d Cir. 2008) (en banc) (declining to reach claim that district court erred in relying on vague concern about gun violence because it was clear that the “district court would have imposed the same sentence had it relied solely on” the permissible concern about deterrence).

Ulbricht’s only claim of procedural error is that it was improper for the district court to consider six drug-related deaths as relevant to his sentence because there was insufficient information connecting them with drugs purchased on Silk Road. In terms of our sentencing jurisprudence, Ulbricht claims that the district court relied on clearly erroneous facts in imposing sentence. We are not persuaded.

Ulbricht submitted an expert report in which Dr. Mark Taff wrote that the records associated with the six deaths were substantially incomplete. For example, many

did not include full autopsies, rendering it difficult to discern the precise cause of death to a reasonable degree of medical certainty in five of the cases.⁶¹ Equally importantly, Dr. Taff wrote that he could not conclusively connect the specific drugs that the decedents consumed with Silk Road, because it is impossible to “correlate the time of purchase/acquisition from an alleged Silk Road vendor” and the “time of usage of the alleged Silk road purchase” with the deaths.⁶² S.A. 446. We assume for purposes of this opinion that Dr. Taff’s conclusions are sufficiently sound to raise a genuine question about whether the deaths described in the PSR were caused by drugs purchased on Silk Road. As explained above, however, Ulbricht was not being prosecuted or punished for homicide on a theory that he personally caused those deaths. Nor did the fact of the deaths increase his offense level under the Guidelines. The question before the district court was whether the sale of large quantities of drugs on Silk Road created a sufficient risk of death to permit the district

⁶¹ In the sixth case, Dr. Taff concluded that the cause of death was ingesting multiple drugs coupled with a pre-existing heart condition. The original forensic reports concerning that death did not factor in the presence of drugs other than synthetic marijuana (obtained via Silk Road) and did not include the heart condition as a contributing cause.

⁶² Sentencing *amici* make a similar argument, claiming that a complex array of causes are responsible for drug-related deaths, including societal failures. Assuming that is correct, the increased availability of drugs is certainly one of the causes of overdose and other drug-related accidental deaths. Thus, the district court did not err in concluding that Silk Road, which was by all accounts a market-expanding drug enterprise, contributed to the general social costs of drug trafficking. Those harms are numerous and include the risk of death.

court to take the deaths into account in assessing the seriousness of Ulbricht's crimes when it considered the factors listed in 18 U.S.C. § 3553(a).

As with other facts relevant to sentencing, that question is for the district court to answer, based on the preponderance of the evidence. *Norman*, 776 F.3d at 76. Contrary to Ulbricht's claims, the district court did not summarily reject Dr. Taff's conclusions. Rather, it addressed his report carefully and acknowledged the evidentiary challenges of connecting the deaths to Silk Road. The court concluded that Dr. Taff's proposed "reasonable degree of medical certainty" standard was simply too high an evidentiary standard for purposes of including the deaths in the PSR. The court reasoned that it was "not asking whether the but for cause of death is drugs purchased on Silk Road," but rather "whether there is a connection between the purchase of drugs on Silk Road and [the] death" in the sense that the sale of those drugs created a risk of death. App'x 1476.

For those limited purposes and judged by that standard, the circumstantial evidence connecting the drug-related deaths to Silk Road was sufficient to consider them at Ulbricht's sentencing. To take the strongest example, one decedent was found in his apartment with a package torn open. His computer had the Silk Road site open, with chat messages from the vendor describing the heroin and prescription drug purchase as well as the package tracking information. The tracking number matched the information on the torn package in the apartment. A toxicology report determined that he died of an overdose of heroin combined with other prescription drugs. The facts connecting the other five deaths to Silk Road varied in strength. The available evidence was sufficient, however, to allow the district court find by a preponderance of the

evidence that the deaths were connected to Silk Road; therefore, the court could consider the risk of death that the site created. Nothing in the sentencing transcript suggests that the court considered the information for any other purpose.

We are sensitive to the possibility that the evidence of the six deaths was emotionally inflammatory and risked implicitly escalating Ulbricht's responsibility from facilitating the sale of drugs to causing the deaths of several drug users.⁶³ But there is no indication that the deaths in question played such a role in the district court's sentencing determination. In urging the court to consider evidence of the deaths, the government explained that the deaths "illustrate the obvious: that drugs can cause serious harm, including death." App'x 902. *See United States v. Pacheco*, 489 F.3d 40, 48 n.5 (1st Cir. 2007) (observing that a defendant who "engaged in the commercial trade of potent substances . . . must have known [that such trade] could have dire consequences").

Of course, to the extent that the harms of the drug trade were obvious, there was no need to introduce evidence of these particular incidents, let alone to hammer the point home with unavoidably emotional victim impact statements by parents of two of the decedents.⁶⁴ No federal judge needs to be reminded of the tragic consequences of the traffic in dangerous substances on the lives

⁶³ Ulbricht does not argue that the evidence related to the accidental overdose deaths should have been excluded due to its emotional nature; his argument is based solely on the claim that the evidence was irrelevant because the deaths were not sufficiently linked to Silk Road.

⁶⁴ Ulbricht does not challenge the propriety of those statements apart from his general argument that it was procedurally unreasonable to consider the six deaths as relevant to his sentence.

of users and addicts, or of the risks of overdose and other ramifications of the most dangerous of illegal drugs. Those consequences are among the reasons why illegal drugs are prohibited and constitute a principal justification advanced for the extremely lengthy sentences provided by federal statutes and sentencing guidelines for trafficking in illicit substances. Absent reason to believe that a drug dealer's methods were unusually reckless, in that they enhanced the risk of death from drugs he sold beyond those already inherent in the trade, we do not think that the fact that the ever-present risk of tragedy came to fruition in a particular instance should enhance those sentences, or that the inability of the government to link a particular dealer's product to a specific death should mitigate them. The government's insistence on proceeding with this evidence generated an appellate issue that has taken on a disproportionate focus in relation to the reasons actually advanced by the district court in its lengthy and careful statement of the reasons for the sentence it imposed. App'x 1509-41.

We are not persuaded, however, that the introduction of the evidence in this case was error, although it may have been incautious for the government to insist on presenting it to the district court. As already explained, it was certainly appropriate for the district court to consider the risk of death from use of drugs in assessing the seriousness of the offense conduct, one of the factors that a judge must consider in imposing sentence. *See* 18 U.S.C. § 3553(a)(2)(A). That appears to be the only way the judge in this case used the evidence of the drug-related deaths. Emotionally wrenching as the statements of the decedents' parents were, we cannot and do not assume that federal judges are unable to put their sympathies for particular victims to one side and assess the evidence for its rational relationship to the sentencing decision. And here,

the record makes clear that the district court did not use the evidence of the drug-related deaths to enhance Ulbricht's sentence, either as a formal matter under the Guidelines or otherwise. For all the extensive litigation of the propriety of including this information in the PSR, in imposing sentence the district court did not refer to the drug-related deaths as an aggravating factor. Indeed, the only mention of that evidence at all was a passing reference to "facts brought out in connection with [those] death[s]" that "provide evidence of first-time and expanded [drug] usage." App'x 1521-22. This reference occurred in the entirely appropriate context of a lengthy discussion of the general social harms of Ulbricht's massive drug-trading marketplace. *Id.* at 1522-28.

That discussion was particularly germane to this case for several reasons. First, Ulbricht claimed that Silk Road reduced the harms associated with the drug trade in several ways. For example, he argued that trafficking in drugs over the Internet reduced violence associated with hand-to-hand transactions and the societal stigma of drug use, and Silk Road's vendor rating system ensured that customers had access to better quality drugs and more information about the drugs that they were purchasing. Those arguments prompted the district court to reflect broadly on the costs of the drug trade and discuss Silk Road's participation in those harms. Reasonable people may and do disagree about the social utility of harsh sentences for the distribution of controlled substances, or even of criminal prohibition of their sale and use at all. It is very possible that, at some future point, we will come to regard these policies as tragic mistakes and adopt less punitive and more effective methods of reducing the incidence and costs of drug use.

At this point in our history, however, the democratically-elected representatives of the people have opted for a policy of prohibition, backed by severe punishment. That policy results in the routine incarceration of many traffickers for extended periods of time. This case involves a defendant who stood at one remove from the trade, who did not for the most part dirty his hands with the actual possession and sale of drugs and other contraband that his site offered. But he did take a cut of the proceeds, in exchange for making it easier for such drugs to be purchased and sold, in a way that may well have expanded the market by allowing more people access to drugs in greater quantities than might otherwise have been available to them. In the routine instances of sentencing drug sellers, the dangerous aspects of the trade are close to the surface and require little emphasis. In this case, a reminder of the consequences of facilitating such transactions was perhaps more necessary, particularly because Ulbricht claimed that his site actually made the drug trade safer, and he appeared to contest the legitimacy of the laws he violated.⁶⁵

⁶⁵ In a footnote in his reply brief, Ulbricht raises for the first time an additional argument: that the district court improperly gave him a life sentence because of the political and philosophical beliefs that led him to start Silk Road in the first instance. Ulbricht argues that reliance on political beliefs at sentencing is prohibited by the Guidelines, U.S.S.G. § 5H1.10, and the First Amendment. The district court reflected on Ulbricht's philosophy, however, only in the course of discussing his character and his reasons for committing the offense. *See* 18 U.S.C. § 3553(a)(1). That discussion was relevant to sentencing. Ulbricht, as the district court concluded, "viewed Silk Road both as above the law and the laws didn't apply." App'x 1515. He appeared to believe that his personal views about the propriety of the drug laws and the paramount role of individual liberty entitled him to violate democratically-enacted criminal prohibitions. For example, some of

Finally, we need look no further than the district court's express reasons for imposing sentence to conclude that drug-related deaths played little part in dictating the sentence imposed. As tragic as they are, and as foreseeable in light of the volume of dangerous drugs trafficked through Silk Road, those deaths were accidents. In light of the overwhelming evidence, discussed below, that Ulbricht was prepared, like other drug kingpins, to protect his profits by paying large sums of money to have individuals who threatened his enterprise murdered, it would be plainly wrong to conclude that he was sentenced for accidental deaths that the district court discussed only in passing in imposing sentence. Even were we to conclude that the evidence of the Silk Road-related deaths should not have been received, any error would be harmless, because the record is absolutely clear that the district court, after finding that Ulbricht commissioned five murders, would have imposed the same sentence if the evidence of the drug-related deaths had been excluded.

his Silk Road posts “discuss the laws as the oppressor” and proclaim that “each transaction is a victory over the oppressor.” *Id.* at 1516. That Ulbricht believes that drug use should be legalized is not relevant to sentencing; that he believes he is entitled to break the laws that prohibit certain substances is relevant to his likelihood of recidivism, a mandated sentencing consideration. 18 U.S.C. § 3553(a)(2)(C). The district court therefore did not sentence Ulbricht based on any prohibited characteristic, nor did the court place more weight on that factor than the facts warranted. *Cf. United States v. Jenkins*, –F.3d.–, 2017 WL 1371399 (2d Cir. Apr. 17, 2017) (vacating a sentence as substantively unreasonable where the district court relied exclusively on the defendant's “disdain for the law” in “dramatically increasing” a defendant's sentence for child pornography offenses). Ulbricht's disrespect for the law was simply one factor that the district court considered in imposing sentence, along with many others, and was not accorded undue weight in determining the sentence.

The sentencing *amici* advance one additional argument: that the district court’s consideration of the drug-related deaths violated the Fifth and Sixth Amendments because the fact of those deaths was not charged in the Indictment and proven to the jury. “While we are not required to address arguments raised only by an *amicus*,” *Am. Atheists, Inc. v. Port Auth. of N.Y. & New Jersey*, 760 F.3d 227, 237 n.11 (2d Cir. 2014), we do so here in an excess of caution. The argument is without merit under *Apprendi v. New Jersey*, 530 U.S. 466 (2000), and its progeny.

A district court may consider as part of its sentencing determination uncharged conduct proven by a preponderance of the evidence as long as that conduct does not increase either the statutory minimum or maximum available punishment. See *United States v. Stevenson*, 834 F.3d 80, 85 (2d Cir. 2016); *United States v. Ryan*, 806 F.3d 691, 693-94 (2d Cir. 2015). The Supreme Court has “long recognized that broad sentencing discretion, informed by judicial factfinding, does not violate the Sixth Amendment.” *Alleyne v. United States*, 133 S. Ct. 2151, 2163 (2013). Here, the six drug-related deaths (and more importantly, Ulbricht’s attempted murders for hire) were uncharged facts that did not increase either the statutory twenty-year minimum or the maximum life sentence applicable to the crimes of which he was found guilty, beyond a reasonable doubt, by the jury. Thus, the district court did not violate the Constitution when it found by a preponderance of the evidence that the six deaths were connected to Silk Road and that they were relevant to Ulbricht’s sentence because they were part of the harm that the site caused.

In sum, we might not, in the prosecutors' shoes, have chosen to offer this evidence at sentencing, or have admitted it as district judges. We conclude, however, (1) that the district court did not clearly err when it found by a preponderance of the evidence that the six deaths were connected to Silk Road; (2) that it did not abuse its discretion in determining that it was appropriate to consider those acts as bearing on the seriousness of the narcotics offenses of which Ulbricht was convicted, one of many factors the district court was required to consider in exercising its discretion under § 3553(a); and (3) that the evidence in question in fact played a minimal role, if any, in the actual sentencing, and that in light of the reasons given by the district court for its sentencing decision, we can be absolutely certain that the same sentence would have been imposed if the evidence had not been received. Ulbricht's sentence was therefore not procedurally unreasonable.

B. Substantive Unreasonableness

"We will . . . set aside a district court's substantive [sentencing] determination only in exceptional cases where the trial court's decision cannot be located within the range of permissible decisions." *Cavera*, 550 F.3d at 189 (emphasis and internal quotation marks omitted). Our review is "deferential," and this Court does "not consider what weight we would ourselves have given a particular factor." *Rigas*, 583 F.3d at 122. "Rather, we consider whether the factor, as explained by the district court, can bear the weight assigned it under the totality of the circumstances in the case." *Id.* Our role in "patrolling the boundaries of reasonableness" is modest. *United States v. Broxmeyer*, 699 F.3d 265, 289 (2d Cir. 2012) (alterations and internal quotation marks omitted). Accordingly, we

“will set aside only those outlier sentences that reflect actual abuse of a district court’s considerable sentencing discretion.” *United States v. Messina*, 806 F.3d 55, 66 (2d Cir. 2015).

In light of the deferential standard of review, we cannot say that Ulbricht’s life sentence was substantively unreasonable. The district court identified numerous facts that made Ulbricht’s case extraordinary, in its view rendering a life sentence “sufficient, but not greater than necessary, to comply with the purposes” of sentencing. 18 U.S.C. § 3553(a). The court described the crime as a “planned, comprehensive, and deliberate scheme . . . which posed serious danger to public health and to our communities.” App’x 1511-12. Silk Road was a “worldwide criminal drug enterprise with a massive geographic scope.” *Id.* at 1512. The fact that Ulbricht operated the site from behind a computer, rather than in person like a more prototypical drug kingpin, does not make his crime less serious or less dangerous. Moreover, Silk Road uniquely expanded the drug market by providing an easy avenue for people to become first-time drug users and dealers. Because drugs were shipped to customers in the mail, Silk Road brought “drugs to communities that previously may have had no access to such drugs . . . in such quantities.” *Id.* at 1522.

The quantity and nature of the drugs sold on Silk Road are staggering. According to the PSR, from 2011 through 2013, Silk Road customers transacted in approximately \$183 million worth of illegal drugs. At the time the government shut down Silk Road on October 2, 2013, there were approximately 13,802 listings for controlled substances on the website. Of those listings, there were 643 listings for cocaine-based products, 305 for LSD products, and 261 for methamphetamine products. The drugs were

sold mostly for individual, personal use, but some drugs such as heroin and cocaine were also available in “multi-kilogram quantities.” PSR ¶ 26. The available drugs were not limited to heroin, narcotics, synthetic marijuana, and other dangerous but recreational substances. For example, after being told that cyanide was “the most well known assassination suicide [*sic*] poison out there,” Ulbricht allowed vendors to sell it on Silk Road despite its singular, deadly purpose. App’x 1519. As the district court noted, despite earlier protestations that Silk Road would not allow the sale of products that could be used to inflict deliberate harm on others, it took Ulbricht all of six minutes to decide “that it is okay to sell cyanide,” *id.*, in exchange for the customary cut of the proceeds.

The drug offenses alone—ignoring all other illicit materials sold on the site⁶⁶—yielded a calculated offense level

⁶⁶ As explained, Silk Road also trafficked in illegal goods such as counterfeit identification documents and computer hacking tools and services. When the government shut down Silk Road, there were 156 listings for forged identity documents on the site. The specific computer hacking tools available included software for compromising usernames and passwords of electronic accounts, including email and Facebook; Remote Access Tools (“RATs”) that allow hackers to obtain remote access to a victim’s computer, including turning on and using the computer’s webcam; keyloggers, which allow a user to monitor keystrokes inputted by a victim to discern their passwords and other sensitive information; and Distributed Denial of Service (“DDoS”) tools, which allow hackers to disable websites by flooding networks with malicious Internet traffic. Silk Road also offered money laundering services through vendors who sold U.S. currency and anonymous debit cards. Because the adjusted offense levels for those groups of offenses were substantially lower than the offense level for the drug group, they did not contribute to Ulbricht’s overall offense level. In assessing the substantive reasonableness of the sentence imposed, however, it is well to remember that the sentence encompassed Ulbricht’s role not only in the distribution of controlled substances, but in a wide variety of other criminal offenses as well.

of 50. Of that calculation, only two levels are attributable to Ulbricht’s “credible threats of directed violence” associated with the murders for hire. PSR ¶ 94. Thus, even without considering that enhancement, the drug convictions yielded an offense level of 48, which is higher than the maximum offense level recognized by the Guidelines, for which a sentence of life imprisonment is recommended even for someone who, like Ulbricht, has no prior criminal convictions. Ulbricht does not challenge the accuracy of the Guidelines calculation or of the fact-findings on which it is based.

That the sentence imposed accorded with the Guidelines recommendation does not automatically render it reasonable. *See United States v. Dorvee*, 616 F.3d 174, 182 (2d Cir. 2010). The Guidelines are, however, themselves a factor that Congress has directed district courts to consider. 18 U.S.C. § 3553(a)(4)(A). Moreover, as the considered judgment of the United States Sentencing Commission, they bear on the other factors that Congress has required courts to evaluate, including the need to reflect the seriousness of the offense, *id.* § 3553(a)(2)(A), to provide adequate deterrence, *id.* § 3553(a)(2)(B), and, because they are considered by all judges throughout the federal system, the need to “avoid unwarranted sentence disparities among defendants with similar records who have been found guilty of similar conduct,” *id.* § 3553(a)(6).

Accordingly, while a life sentence for selling drugs alone would give pause, we would be hard put to find such a sentence beyond the bounds of reason for drug crimes of this magnitude.⁶⁷ But the facts of this case involve much

⁶⁷ Note that such a sentence is *mandatory* under federal law for selling just five kilograms of cocaine after two prior convictions for

more than simply facilitating the sale of narcotics. The district court found by a preponderance of the evidence that Ulbricht commissioned at least five murders in the course of protecting Silk Road’s anonymity, a finding that Ulbricht does not challenge in this appeal.⁶⁸ Ulbricht discussed those anticipated murders callously and casually in his journal and in his communications with the purported assassin Redandwhite. For example, in connection with the first hit, he wrote to Redandwhite that “Friendly-Chemist is a liability and I wouldn’t mind if he was executed.” Tr. 1822. In the course of negotiating the price for the killing, DPR claimed that “[n]ot long ago, I had a clean hit done for \$80k,” *id.* at 1883, but that he had “only ever commissioned the one other hit, so I’m still learning this market,” *id.* at 1884. He then paid \$150,000 in Bitcoins for the murder, and he received what purported to be photographic documentation of its completion. Ulbricht then wrote in his journal that he “[g]ot word that the black-mailer was executed,” *id.* at 1887, before returning quickly to other tasks associated with running the site.

any felony narcotics offense, *see* 21 U.S.C. § 841(b)(1)(A), and the Supreme Court has upheld against constitutional challenge a mandatory sentence of life imprisonment for selling 650 grams of cocaine, *Harmelin v. Michigan*, 501 U.S. 957 (1991).

⁶⁸ Ulbricht does not mention his orders for the commission of those murders until his reply brief. Even there, he does not argue that the district court erred in concluding that he deliberately commissioned those murders; rather, he claims instead only that the murders did not support a life sentence because they did not actually take place. But in evaluating Ulbricht’s character and dangerousness, the most relevant points are that he wanted the murders to be committed, he paid for them, and he believed that they had been carried out. The fact that his hired assassin may have defrauded him does not reflect positively on Ulbricht’s character. Commissioning the murders significantly justified the life sentence.

In negotiating the other four killings, Ulbricht initially resisted multiple murders. He instructed Redandwhite to “just hit Andrew [usernames Tony76 and nipplesuckcannuck] and leave it at that.” *Id.* at 1897. Redandwhite said he could do it for “150 just like last time,” but that he would not be able to recover any of DPR’s money if he killed only one person because he would have to commit the murder outside of the victim’s home or office where he stored his funds. *Id.* If Ulbricht wanted him to recover money, the self-professed assassin claimed, he would have to kill not only Tony76, but also his three associates. DPR responded that he would “defer to [Redandwhite’s] better judgment and hope[d] [to] recover some assets” from the hit. *Id.* at 1899. He then sent \$500,000 in Bitcoins, the agreed-upon price for four killings, to Redandwhite. As the district court stated in discussing Ulbricht’s journal entries concerning these projected murders, his words are “the words of a man who is callous as to the consequences or the harm and suffering that [his actions] may cause others.” App’x 1521.

The record was more than sufficient to support the district court’s reliance on those attempted murders in sentencing Ulbricht to life in prison. The attempted murders for hire separate this case from that of an ordinary drug dealer, regardless of the quantity of drugs involved in the offense, and lend further support to the district court’s finding that Ulbricht’s conduct and character were exceptionally destructive. That he was able to distance himself from the actual violence he paid for by using a computer to order the killings is not mitigating. Indeed, the cruelty that he displayed in his casual and confident negotiations for the hits is unnerving. We thus cannot say that a life sentence was outside the “range of permissible decisions” under the circumstances. *Cavera*, 550 F.3d at 189.

Ulbricht's arguments on appeal have rhetorical power because of the sheer magnitude of his sentence, but they do not provide a legal basis for vacating that sentence as substantively unreasonable. He contends that the district court ignored the letters submitted on his behalf, thus failing to consider his positive contributions to his family and society as well as his potential productivity should he be released from prison. To the contrary, however, the district court "read each and every one of [the letters] with care," some "more than once." App'x 1534. Recognizing that the letters were "beautiful" and "profoundly moving," the district court observed that they reveal Ulbricht's human complexity. *Id.* at 1534-35. Nothing in the record supports the claim that the district court failed to recognize the importance of the letters, incorrectly discounted Ulbricht's more favorable characteristics, or otherwise inappropriately dismissed their role in its sentencing determination.

Similarly, Ulbricht's argument that the district court ignored his contention that Silk Road reduced the harmful effects of drug crimes must be rejected. The district court thoroughly discussed Doctor X's role at Silk Road and Ulbricht's claims that the site reduced violence, overdoses, and other harms associated with drug trafficking, and concluded that they were unpersuasive. We see no error in its analysis, and Ulbricht's arguments concerning harm reduction do not render his sentence substantively unreasonable.

Ulbricht also claims that there is an unwarranted disparity between his sentence and the approximately 17-month sentence that Peter Nash, a Silk Road administrator, received. Again, however, the district court considered the arguments concerning Nash's sentence and found them to be irrelevant to Ulbricht's crime because

Nash was a low-level site administrator who pleaded guilty and cooperated with the government. Along those same lines, Ulbricht notes that Silk Road drug dealers received lower sentences than he did. For example, one such drug dealer received a ten-year sentence. The fact that different people involved with the site received dramatically lower sentences does not mean that Ulbricht's own sentence was substantively unreasonable on the individual facts of his case.⁶⁹ Ulbricht was the creator and head administrator of the site. That fact alone distinguishes his case from that of any individual seller or employee who used or worked for the site. Ulbricht profited from every sale on Silk Road, and he facilitated the acts of each drug dealer and drug organization that used it. Moreover, he attempted to commission at least five murders to protect his criminal enterprise. Those facts render his case distinguishable from those who committed other crimes using Silk Road or otherwise facilitated its operation.

Ulbricht next reiterates his argument that he was more like someone running a crack house than like a drug kingpin because he created the online platform that *others* used to sell drugs and was not himself a drug dealer.⁷⁰ That argument also understates the vast extent of Silk Road's drug market, which had thousands of customers and trafficked in about \$183 million in illegal drugs. People may differ about whether "respectable" people who,

⁶⁹ In his reply, Ulbricht references other instances in which people involved with Silk Road (and its apparent reincarnation, Silk Road 2.0) received significantly lower sentences. Ulbricht does not provide sufficient detail about those individuals' conduct, however, to permit meaningful comparisons with his case.

⁷⁰ Ulbricht did sell drugs on Silk Road for at least some brief period of time, when he grew and sold hallucinogenic mushrooms to drum up interest in the site.

acting as property owners, money launderers, or other facilitators of crime for personal gain are less guilty than those who personally handle the narcotics. We cannot fault the district court for rejecting the argument that Ulbricht's contribution to the narcotics trade was inherently less culpable than that of the dealers who paid him to use Silk Road to complete their transactions.

Both the sentencing *amici* and Ulbricht further contend that the district court placed too much weight on the notion of general deterrence in meting out the life sentence. Specifically, Ulbricht fears that resorting to "general deterrence without any confining principles . . . guarantees that [the sentence] will create disparity." Appellant Br. 139. *Amici* also observe that academic studies counsel against placing too much emphasis on general deterrence in sentencing because severe criminal punishments do not actually decrease either supply or demand for illegal drugs. Further, according to *amici*, the threat of a long sentence does not deter criminal conduct more effectively than the threat of a shorter sentence. In his reply, Ulbricht identifies several lucrative dark markets that have emerged since Silk Road's demise in 2013. In his view, the existence of multiple copycat Tor-based illegal marketplaces proves that general deterrence is illusory and that the district court placed too much weight on that factor.

Although those arguments have some support among scholars and researchers, the ability of a sentence to "afford adequate deterrence to criminal conduct" is a factor that district courts are *required* by Congress to consider in arriving at the appropriate sentence. 18 U.S.C. § 3553(a)(2)(B); *see United States v. Tran*, 519 F.3d 98, 107 (2d Cir. 2008). Congress, moreover, has not concluded that the persistence of narcotics crimes is a reason to

abandon the efforts to deter them by lengthy sentences. The district court observed that “general deterrence plays a particularly important role” in Ulbricht’s case because Silk Road is “without serious precedent” and generated an unusually large amount of public interest. App’x 1532-33. The court thus carefully analyzed the role that general deterrence played in Ulbricht’s individual case. At the same time, it is evident from the sentencing transcript that general deterrence was “just one element in the [district court’s] analysis,” *id.* at 1533, and the district court considered many other factors before sentencing Ulbricht to life in prison. Thus, the factor of general deterrence, “as explained by the district court, can bear the weight assigned it under the totality of circumstances in this case.” *Rigas*, 583 F.3d at 122.

Finally, Ulbricht and *amici* point out that life sentences are rare in the federal system, typically reserved for egregious violent crimes, thus rendering Ulbricht’s sentence substantively unreasonable.⁷¹ Moreover, according to *amici*, life sentences are normally imposed in cases where that is the district judge’s only sentencing option. Thus, they claim that Ulbricht’s life sentence is substantively unreasonable in the context of the federal system, where life sentences are particularly rare for those with no criminal history who are convicted of drug crimes.⁷²

⁷¹ *Amici* also claim that Ulbricht’s life sentence violates the Eighth Amendment’s ban on cruel and unusual punishment. That argument is plainly incorrect in light of binding Supreme Court precedent to the contrary. See *Harmelin*, 501 U.S. 957.

⁷² In his reply, Ulbricht raises a distinct but related argument for the first time. He argues that “concurrences from Supreme Court opinions and dissents from denials of certiorari suggest[] that judicial factfinding violates a defendant’s constitutional right to a jury trial

We agree with Ulbricht that life sentences are extraordinary and infrequent, which is as it should be. But the rarity of life sentences does not mean that the imposition of such a sentence in this case is substantively unreasonable under our law. Each case must be considered on its own facts and in light of all of the circumstances of a particular offense as well as other relevant conduct, which, in this case, includes five attempted murders for hire. As we have described, the district court carefully considered Ulbricht's offense, his personal characteristics, and the context for his crimes, recognizing that only exceptional cases justify such a severe sentence. Although we might not have imposed the same sentence ourselves in the first instance, on the facts of this case a life sentence was "within the range of permissible decisions" that the district court could have reached. *Rigas*, 583 F.3d at 122.

We do not reach our conclusion lightly.⁷³ A life sentence is the second most severe penalty that may be imposed in the federal criminal justice system. "The size of

where the factfinding renders reasonable an otherwise substantively unreasonable sentence." Reply Br. 60. For that proposition, he cites *United States v. Hebert*, 813 F.3d 551, 563 (5th Cir. 2015), *cert. denied*, 137 S. Ct. 37 (2016), *Jones v. United States*, 135 S. Ct. 8 (2014) (Scalia, J., dissenting from denial of certiorari), and *United States v. White*, 551 F.3d 381, 386 (6th Cir. 2008) (Merritt, J., dissenting). His argument, however, has no support in existing law.

⁷³ The life sentence is particularly severe because, as in all federal cases, Ulbricht will never be eligible for parole. Unlike state sentences in jurisdictions permitting a sentence of, for example, "25 years to life," there is no automatic reconsideration of this sentence, or of whether an offender has reformed, after any lengthy period of incarceration. We note that, particularly in the case of a young offender, the prisoner will all but certainly change (for better or worse) after many years of incarceration. In a system without parole, how-

[Ulbricht’s] sentence alone [therefore] counsels our careful, searching review of it.” *United States v. Brown*, 843 F.3d 74, 85 (2d Cir. 2016) (Sack., J., concurring). Courts have the power to condemn a young man to die in prison, and judges must exercise that power only in a small number of cases after the deepest thought and reflection. Of course, any “sentencing proceeding is a solemn occasion at which the judge has the weighty duty of determining the fate of another human being.” *United States v. Alcantara*, 396 F.3d 189, 199 (2d Cir. 2005). We must be especially sensitive to that duty where the most severe sentences are in question. The district court gave Ulbricht’s sentence the thorough consideration that it required, reviewing the voluminous sentencing submissions, analyzing the factors required by law, and carefully weighing Ulbricht’s mitigating arguments. The extraordinarily detailed sentencing transcript shows that the district court appreciated its important responsibility in considering a sentence of such magnitude and carried out that responsibility with care and prudence. Under the law, we cannot say that its decision was substantively unreasonable.

CONCLUSION

For the foregoing reasons, we **AFFIRM** the judgment of the district court in all respects.

ever, a sentencing court is forced to exercise its best judgment to predict whether a sentence of life imprisonment or one of 25, 30, or 50 years is required to serve the purposes of sentencing, without the option of deferring that judgment to a point at which the effects of incarceration, and the passage of time, will be more apparent.

APPENDIX C

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

No. 14-cr-68 (KBF)

October 10, 2014

UNITED STATES OF AMERICA,

v.

ROSS WILLIAM ULBRICHT
a/k/a “Dread Pirate Roberts,”
a/k/a “DPR,”
a/k/a “Silk Road,”

Defendant,

OPINION & ORDER

KATHERINE B. FORREST, District Judge.

On February 4, 2014, Ross Ulbricht (“defendant” or “Ulbricht”) was indicted on four counts. (ECF No. 12.) On September 5, 2014, he was arraigned on superseding indictment S114 Cr. 68 (KBF) (the “Indictment”). The Indictment charges Ulbricht with the following crimes: Narcotics Trafficking (Count One), Distribution of Narcotics

by Means of the Internet (Count Two), Narcotics Trafficking Conspiracy (Count Three), Continuing Criminal Enterprise (“CCE”) (Count Four), Conspiracy to Commit and Aid and Abet Computer Hacking (Count Five), Conspiracy to Traffic in Fraudulent Identification Documents (Count Six), and Money Laundering Conspiracy (Count Seven). (ECF No. 52 (“Ind.”).) Ulbricht’s trial is scheduled to commence on November 10, 2014.

Before this Court is defendant’s motion to suppress virtually all evidence in the case, for a bill of particulars, and to strike surplusage. (ECF No. 46.) For the reasons set forth below, the motion is **DENIED**.

I. BACKGROUND

A. Allegations against Ulbricht

Ulbricht is charged with seven separate crimes—all involving the creation, design, administration and operations of an online marketplace known as “Silk Road.” The Government alleges that Ulbricht created Silk Road (Ind.¶ 1) and that he has been in control of all aspects of its administration and operations (Ind.¶ 3). The Government’s charges against Ulbricht are premised upon a claim that through Silk Road, defendant enabled and facilitated anonymous transactions in a variety of illicit goods and services including, *inter alia*, narcotics, fake identification documents, and materials used to hack computers, and that he conspired, participated directly in, or aided and abetted others in substantive crimes.

Silk Road is alleged to have operated on the Tor network (“Tor”). (Declaration of Christopher Tarbell ¶¶ 4-5, ECF No. 57 (“Tarbell Decl.”).) The Tor network is designed to conceal the Internet Protocol (“IP”) addresses

of the computers operating on it, “including servers hosting websites on Tor, such as Silk Road.” (Tarbell Decl. ¶ 4.) The Government alleges that Silk Road also supported anonymity through its reliance on “Bitcoin” as a method of payment.¹ (Ind.¶ 28.) The use of Bitcoins concealed the identities and locations of users transmitting and receiving funds. (Ind.¶ 28.) The Government alleges that over the period of time it was up and running, Silk Road was used by several thousand drug dealers and well over one hundred thousand buyers worldwide to purchase illegal narcotics and illicit goods, and that it was also used to launder hundreds of millions of dollars derived from these transactions. (Ind.¶ 2.) Ulbricht himself is alleged to have made commissions worth tens of millions of dollars from these sales. (Ind.¶ 3.)

B. The Investigation of Ulbricht

The instant motion is primarily concerned with whether the Government’s methods for investigating Ulbricht violated his Fourth Amendment right to be free from unreasonable searches and seizures. Importantly, while the Government alleges that Ulbricht and Silk Road are one and the same, Ulbricht has not conceded that he created Silk Road, or that he administered or oversaw its operations, or even that he used or accessed it at all. Ulbricht has not submitted a declaration or affidavit attesting to any personal privacy interest that he may have in any of the items searched and/or seized and as to which

¹ Bitcoin is the name of an encrypted online currency. It is managed through a private network and not through any Government, central bank or formal financial institution. The Government does not allege that the use of Bitcoin itself is illegal.

his motion is directed. Ulbricht’s lawyer has, however, argued that his “expectation of privacy in his laptop, Google or Facebook accounts” is “manifest” (ECF No. 83 at 2 n. 2), and the Government has stipulated to his “expectation of privacy” in those (ECF No. 85).²

The Government’s investigation involved, inter alia, the imaging and subsequent search of a server located in Iceland (the “Icelandic server”) in July 2013. Based in large part on the results of information learned from the Icelandic server, the Government then obtained various court orders for pen-registers and trap and trace devices (the “Pen-Trap Orders”), and warrants to seize and then search a number of other servers located within the United States, as well as a laptop associated with Ulbricht and his Facebook and Gmail accounts. In total, the Government obtained 14 warrants and court orders over the course of its investigation. (Declaration of Joshau L. Dratel ¶ 3(a)-(n), ECF No. 47 (“Dratel Decl.”).) Those warrants and orders are as follows:

Warrant No. 1: Windstream “JTan” server
1 (Pennsylvania) (9/9/13);

Warrant No. 2: Windstream “JTan” server
2 (Pennsylvania) (9/9/13);

Warrant No. 3: Voxility server (California)
(9/19/13);

² On October 7, 2014, the Court issued an order in which it provided the defendant a “final opportunity” to submit a declaration or affidavit establishing some privacy interest in the items searched and/or seized. (ECF Nos. 76-77.) By letter dated October 7, 2014, his lawyer responded that “Mr. Ulbricht rests on his papers already submitted.” (ECF No. 83.)

Warrant No. 4: Windstream servers assigned host numbers 418, 420 and 421 (Pennsylvania) (10/1/13);

Warrant No. 5: Voxility server with IP addresses 109.163.234 .40 and 109.163.234.37 (California) (10/1/13);

Warrant No. 6: Samsung laptop with MAC address 88-53-2E-9C-81-96 (California) (10/1/13);

Warrant No. 7: Premises at 235 Monterey Boulevard (California) (10/1/13);

Warrant No. 8: The Facebook account associated with username “rossulbricht” (California) (10/8/13);

Warrant No. 9: The Gmail account rossulbricht@gmail.com (10/8/13);

Pen-Trap Order No. 1: To Comcast re IP address 67.170.232.207 (9/16/13);

Pen-Trap Order No. 2: To Comcast re IP address 67.169.90.28 (9/19/2013);

Pen-Trap Order No. 3: Re the wireless router with IP address 67.169.90.28 located at 235 Monterey Boulevard (California) (9/20/13);

Pen-Trap Order No. 4: Re certain computer devices associated with MAC addresses including 88-53-2E-9C-81-96, (9/20/13); and

Pen-Trap Order No. 5: Re the wireless router with IP address 67.169.90.28 located

at 235 Monterey Boulevard (California)
(9/19/13).

According to defendant, virtually all of the Government's evidence stems from the initial search of the Icelandic server in July 2013, which occurred before any of the above warrants issued.³ The vast bulk of defendant's submission is concerned with raising questions regarding how the Government obtained the information that led it to the Icelandic server. One of defendant's lawyers, Joshua Horowitz, has some technical training, and he asserts that the Government's explanation of the methods it used is implausible. (*See* Declaration of Joshua J. Horowitz ¶¶ 4-8, 17-51, ECF No. 70 ("Horowitz Decl.")) Defendant insists that this Court must therefore hold an evidentiary hearing to determine whether the methods the Government asserted it used and that led it to the Icelandic server were in fact its actual methods or not. (*See* Memorandum of Law in Support of Defendant Ross Ulbricht's Pre-Trial Motions to Suppress Evidence, Order Production of Discovery, for a Bill of Particulars, and to Strike Surplusage at 28-34, ECF No. 48 ("Def.'s Br."); Reply Memorandum of Law in Support of Defendant Ross Ulbricht's Pre-Trial Motions to Suppress Evidence, Order Production of Discovery, for a Bill of Particulars, and to Strike Surplusage at 4-8, ECF No. 69 ("Def.'s Reply Br.")) Defendant argues that if that search of the Icelandic server was only possible because of a preceding

³ U.S. law enforcement began working with law enforcement in Iceland on this investigation as early as February 2013. A server—later determined to no longer be in primary use—was imaged in the spring or early summer of 2013 ("Icelandic Server # 1"). Ulbricht asserts that the process leading to the imaging of the server may also have been constitutionally infirm. But Icelandic Server # 1 is in all events irrelevant, as the Government has represented that it does not intend to use any evidence obtained from that server.

constitutionally infirm investigation, then all subsequent warrants and court orders based on that search constitute fruits of the poisonous tree and must be suppressed.

In addition, defendant also asserts that the warrants relating specifically to the servers located in Pennsylvania (nos. 1, 2 and 4) as well as the warrants relating to Ulbricht's laptop, Facebook and Gmail accounts (nos. 6, 8 and 9) are unconstitutional general warrants; and finally that the Pen-Trap Orders were unlawful because a warrant was required and they failed to include appropriate minimization procedures. Defendant has retained experienced counsel who certainly understand Fourth Amendment jurisprudence. It has long been established—indeed, it is a point as to which there can be no dispute—that (1) the Fourth Amendment protects the constitutional right of an individual to be free from unreasonable searches and seizures; (2) the rights conferred by the Fourth Amendment may not be vicariously asserted; and (3) the Fourth Amendment does not confer any general right available to anyone impacted by an investigation to pursue potentially or actually unlawful law enforcement techniques. The only exception to that is extremely narrow: when law enforcement techniques are so egregious (defined as actions such as torture, not simply unlawful conduct) as to violate the Fifth Amendment, a court may suppress the evidence.

Defendant has not asserted a violation of the Fifth Amendment—nor could he. Defendant has, however, brought what he must certainly understand is a fatally deficient motion to suppress. He has failed to take the one step he needed to take to allow the Court to consider his substantive claims regarding the investigation: he has failed to submit anything establishing that he has a personal privacy interest in the Icelandic server or any of the

other items imaged and/or searched and/or seized. Without this, he is in no different position than any third party would be vis-à-vis those items, and vis-à-vis the investigation that led U.S. law enforcement officers to Iceland in the first place.

There is no doubt that since defendant was indicted and charged with seven serious crimes resulting from that initial investigation and the searches that followed it, he has a “personal interest” in the Icelandic server in a colloquial sense. But longstanding Supreme Court precedent draws a stark difference between that sort of interest and what the law recognizes as necessary to establish a personal Fourth Amendment right in an object or place. To establish the latter, defendant must show that he has a personal privacy interest in the object (*e.g.*, a server) or premises searched, not just that the search of the specific object or premises led to his arrest. Were this or any other court to ignore this requirement in the course of suppressing evidence, the court would undoubtedly have committed clear error.

Further, defendant could have established such a personal privacy interest by submitting a sworn statement that could not be offered against him at trial as evidence of his guilt (though it could be used to impeach him should he take the witness stand). Yet he has chosen not to do so.

In short, despite defendant’s assertions and the potential issues he and his counsel raise regarding the investigation that led to the Icelandic server, he has not provided the Court with the minimal legal basis necessary to pursue these assertions. Thus, the declaration submitted by Joshua J. Horowitz, Esq. (ECF No. 70) along with all the arguments regarding the investigation and the warrants based on it are not properly before this Court. The only arguments that this Court must consider as a substantive

matter are those concerning property and accounts as to which defendant has an arguable and cognizable (though itself not legally established) personal privacy interest: the laptop, the Gmail account, and the Facebook account.⁴

II. SEARCHES AND SEIZURES

A. The Fourth Amendment

Ulbricht’s motion to suppress evidence is premised upon an assertion that the Government has, or may have, engaged in one or more unreasonable searches and seizures in violation of the Fourth Amendment of the U.S. Constitution. The Fourth Amendment protects the people against unreasonable searches and seizures. U.S. Const. amend. IV. “Ever since its inception, the rule excluding evidence seized in violation of the Fourth Amendment has been recognized as a principal mode of discouraging lawless police conduct.” *Terry v. Ohio*. 392 U.S. 1, 12 (1968). In the absence of a warrant or the applicability of an exception, law enforcement does not have a general right to enter one’s home, rifle through drawers, and take what might be found therein. *See, e.g., United States v. Jenkins*, 876 F.2d 1085, 1088 (2d Cir.1989).

Evidence seized in violation of the Fourth Amendment is subject to exclusion at trial—hence, references to “the exclusionary rule” in Fourth Amendment jurisprudence. *See, e.g., Terry*, 392 U.S. at 13. Exclusion ensures judicial integrity and protects courts from being made a party to “lawless invasions of the constitutional rights of citizens by permitting unhindered governmental use of the fruits

⁴ For reasons the Court does not understand, Ulbricht chose not to submit a declaration claiming any personal privacy interest and expectation of privacy in the search of 235 Monterey Boulevard or the wireless router located at those premises.

of such invasion.” *Id.* Direct and indirect evidence may be subject to preclusion: all evidence that flows directly or indirectly from unlawfully seized evidence is considered “fruit of the poisonous tree.” *Wong Sun v. United States*, 371 U.S. 471, 484–85 (1963) (the exclusionary rule of the Fourth Amendment extends to indirect evidence as well as direct evidence).

“[T]he Fourth Amendment protects people, not places.” *Katz v. United States*, 389 U.S. 347, 351 (1967). In *Katz*, petitioner sought to suppress evidence of his end of a telephone call, obtained by the FBI after it placed a listening device on a public telephone booth. *Id.* at 348-50. The Supreme Court defined the issue not as one regarding whether a particular physical space was a constitutionally protected area, or whether physical penetration of a protected area was required for a Fourth Amendment violation. *Id.* at 350-51. This is important for this Court’s consideration here of Ulbright’s claims. The Supreme Court in *Katz* then stated that the Fourth Amendment cannot be translated into a general constitutional “right to privacy,” nor does it cover some nebulous group of “constitutionally protected area[s].” *Id.* A person’s general right to privacy—his right to be let alone by other people—is, like the protection of his property and his very life, left largely to the law of the individual states. *Id.* Thus, “[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection.” *Id.*

1. *Foreign searches and seizures.*

The law has long been clear that the protections of the Fourth Amendment do not extend to searches conducted outside the United States by foreign law enforcement authorities. *See, e.g., United States v. Lee*, 723 F.3d 134, 139 (2d Cir.2013) (“[T]he Fourth Amendment’s exclusionary

rule, which requires that evidence seized in violation of the Fourth Amendment must be suppressed, generally does not apply to evidence obtained by searches abroad conducted by foreign officials.”); *United States v. Busic*, 592 F.2d 13, 23 (2d Cir.1978) (“[T]he Fourth Amendment and its exclusionary rule do not apply to the law enforcement activities of foreign authorities acting in their own country.”); accord *United States v. Peterson*, 812 F.2d 486, 490 (9th Cir.1987).

An exception to this rule is when foreign law enforcement authorities become agents of U.S. law enforcement officials. See *Lee*, 723 F.3d at 140 (constitutional requirements may attach “where the conduct of foreign law enforcement officials rendered them agents, or virtual agents, of United States law enforcement officials” (quoting *United States v. Maturo*, 982 F.2d 57, 61 (2d Cir.1992))). If, for instance, U.S. law enforcement was able to and did command and control the efforts of foreign law enforcement, an agency relationship might be found. *United States v. Getto*, 729 F.3d 221, 224 (2d Cir.2013) (holding that “ongoing collaboration between an American law enforcement agency and its foreign counterpart in the course of parallel investigations does not—without American control, direction, or an intent to evade the Constitution—give rise to a relationship sufficient to apply the exclusionary rule to evidence obtained abroad by foreign law enforcement”). The foreign searches must, however, be “reasonable.” *In re Terrorist Bombings of U.S. Embassies in E. Africa*, 552 F.3d 157, 167 (2d Cir.2008) (holding that “foreign searches of U.S. citizens conducted by U.S. agents are subject only to the Fourth Amendment’s

requirement of reasonableness”).⁵ As the Supreme Court has explained:

The test of reasonableness under the Fourth Amendment is not capable of precise definition or mechanical application. In each case it requires a balancing of the need for the particular search against the invasion of personal rights that the search entails. Courts must consider the scope of the particular intrusion, the manner in which it is conducted, the justification for initiating it, and the place in which it is conducted.

Bell v. Wolfish, 441 U.S. 520, 559 (1979).

2. Personal privacy interest.

Supreme Court precedent, binding on this and all courts in this land, establishes that the “capacity to claim the protection of the Fourth Amendment depends . . . upon whether the person who claims the protection of the [Fourth] Amendment has a legitimate expectation of privacy in the invaded place.” *Rakas v. Illinois*, 439 U.S. 128, 143 (1978); *see also United States v. Watson*, 404 F.3d 163, 166 (2d Cir. 2005) (affirming denial of a suppression motion on the basis that the defendant had failed to show an expectation of privacy). This principle derives from the Supreme Court’s holding in *Katz v. United States*, in which the Court found that while common law trespass had long governed Fourth Amendment analysis, the capacity to claim the protection of the Fourth Amendment

⁵ It is unclear whether foreign searches of objects or premises in which only non-citizens have a privacy interest are subject to the Fourth Amendment’s reasonableness requirement. *See United States v. Bin Laden*, 126 F. Supp. 2d 264, 276 (S.D.N.Y.2000) (collecting cases).

depended first and foremost on a personal expectation of privacy in the invaded place. 389 U.S. at 352-53. The Court found that even though petitioner was located in a public telephone booth when the search occurred, “the Government’s activities in electronically listening to and recording the petitioner’s words violated the privacy upon which he justifiably relied . . . and thus constituted a ‘search and seizure’ within the meaning of the Fourth Amendment.” *Id.* at 353.

The law therefore leaves no doubt that Fourth Amendment rights are based on a personal, subjective expectation of privacy; they are rights of a person, not rights of a “thing”—whether that thing be a server, a car, or a building. If a person—a human—cannot establish a cognizable personal expectation of privacy in the place or thing searched, there is no Fourth Amendment issue and no reason to undertake a Fourth Amendment analysis.

How, then, is one’s interest in a place or thing established? It must be established by a declaration or other affirmative statement of the person seeking to vindicate his or her personal Fourth Amendment interest in the thing or place searched. *See, e.g., United States v. Smith*, 621 F.2d 483, 487 (2d Cir.1980) (defendants had no legitimate expectation of privacy in trunk of car where they did not assert ownership of car, knowledge of trunk’s contents, or access to trunk); *United States v. Montoya-Echevarria*, 892 F. Supp. 104, 106 (1995) (“The law is clear that the burden on the defendant to establish [Fourth Amendment] standing is met only by sworn evidence, in the form of affidavit or testimony, from the defendant or someone with personal knowledge.”); *United States v. Ruggiero*, 824 F. Supp. 379 (S.D.N.Y.1993) (“It is well established that in order to challenge a search, a defendant must submit an affidavit from someone with personal

knowledge demonstrating sufficient facts to show that he had a legally cognizable privacy interest in the searched premises at the time of the search.”). The Supreme Court has also established that the defendant—not the Government—bears the burden of proving that he has a legitimate expectation of privacy. *Rawlings v. Kentucky*, 448 U.S. 98, 104 (1980); *see also Watson*, 404 F.3d at 166.

The requirement that one must have a personal expectation of privacy at the time of the search in the thing or place searched is not novel and has been repeatedly litigated. One can easily see why: even if one did not have an expectation of privacy at the time of the search, the search might lead to inculpatory evidence. At that point, the now-defendant might certainly desire that the thing or place searched had been left alone.

In *Rakas*, the Supreme Court reviewed the question of whether passengers in a vehicle that was searched could move to suppress the evidence obtained thereby. 439 U.S. at 130-32. In that case, the police received a report of a robbery and the description of a getaway car. *Id.* at 130. Shortly thereafter, an officer stopped and searched a vehicle matching that description. *Id.* The search revealed ammunition and a firearm. *Id.* Petitioners had been passengers in the vehicle and were arrested following the search. *Id.* Neither the car nor the evidence seized belonged to them. *Id.* at 131. They moved to suppress the evidence on the basis that the search violated their rights under the Fourth Amendment. *Id.* at 130-31.

The question before the Court was presented as whether petitioners had “standing” to bring the suppression motion. *Id.* at 131-32. Petitioners urged the Court to relax or broaden the rule of standing so that any criminal defendant at whom a search was “directed” would have standing to challenge the legality of the search. *Id.* at 132.

The Court recognized that prior case law (including *Jones v. United States*, 362 U.S. 257 (1960)) had discussed the concept of standing as whether the individual challenging the search had been the “victim” of the search. Petitioners in *Rakas* urged the Court to broaden the “victim” concept to a “target theory” of standing for Fourth Amendment purposes. *Id.* at 132-33. The Supreme Court declined to do so, reiterating that the law has long been clear that Fourth Amendment rights were personal rights which may not be vicariously asserted. *Id.* at 133-34. The Court recited numerous instances over time in which courts had rejected defendants’ assertions that they were aggrieved by unconstitutional searches of third parties’ premises or objects. *Id.* at 134 (collecting cases). “A person who has been aggrieved by an illegal search and seizure only through the introduction of damaging evidence secured by a search of a third person’s premises or property has not had any of his Fourth Amendment rights infringed.” *Id.* “[I]t is proper to permit only defendants whose Fourth Amendment rights have been violated to benefit from the rule’s protections.” *Id.* The Court stated, “[c]onferring standing to raise vicarious Fourth Amendment claims would necessarily mean a more widespread invocation of the exclusionary rule during criminal trials.” *Id.* at 137. The Court further reasoned that “[e]ach time the exclusionary rule is applied it exacts a substantial social cost for the vindication of Fourth Amendment rights,” in that “[r]elevant and reliable evidence is kept from the trier of fact and the search for truth at trial is deflected.” *Id.*

The Court also concluded that whether a defendant has the right to challenge a search and seizure is best analyzed under “substantive Fourth Amendment doctrine,” and not standing, though the inquiry ought to be the same under either. *Id.* at 139.

Rakas and the case law on which it is based and which has followed it thus require this Court to ask whether a defendant who is challenging a search or seizure has established a sufficient personal privacy interest in the premises or property at issue. A defendant may make such a showing by asserting that he owned or leased the premises (for example, the leasing of a server would count) or had dominion or control over them. *Watson*, 404 F.3d at 166; *United States v. Villegas*, 899 F.2d 1324, 1333 (2d Cir.1990). Indeed, to a limited extent, yet to be defined by the courts, an authorized user of a premises might have a sufficient expectation of privacy. *See Rakas*, 439 U.S. at 142-43 (“[A] person can have a legally sufficient interest in a place other than his own home so that the Fourth Amendment protects him from unreasonable governmental intrusion into that place.”). Factual claims made in an affirmation by defendant’s counsel may be an insufficient basis upon which to challenge a search if they are made without personal knowledge or are otherwise insufficiently probative. *See Watson*, 404 F.3d at 166-67.

There are limited situations—“extreme case[s],” *United States v. Rahman*, 189 F.3d 88, 131 (2d Cir.1999) (per curiam)—in which a government practice might be “so outrageous that due process principles would absolutely bar the [G]overnment from invoking judicial processes to obtain a conviction” *United States v. Russell*, 411 U.S. 423, 431-32 (1973); *see also United States v. Christie*, 624 F.3d 558 (3d Cir.2010) (“The pertinent question is whether the government’s conduct was so outrageous or shocking that it amounted to a due process violation.”); *Czernicki v. United States*, 270 F. Supp. 2d 391, 394-95 (S.D.N.Y. 2003). However, only conduct that “shocks the conscience” amounts to a due process violation in this context. *Rahman*, 189 F.3d at 131 (quoting *Rochin v. California*, 342 U.S. 165, 172(1952)).

Defendant cites *U.S. v. Gelbard*, 408 U.S. 41 (1972), and *United States v. Ghailani*, 743 F. Supp. 2d 261 (S.D.N.Y.2010), for the proposition that “a defendant is entitled to know whether a Government’s investigation was predicated on illegal government conduct, and [obtain] relief therefrom.” (Def.’s Reply Br. at 7.) That is only so to the extent that the issues concern a defendant’s personal Fourth Amendment rights, or if “extreme conduct” is involved. Unlawful conduct alone is not enough. *See, e.g., United States v. Payner*, 447 U.S. 727, 729-31 (1980). In *Ghailani*, the issue concerned whether the court would allow testimony from a cooperating witness who had been tortured. 743 F.Supp.2d at 267. The court ruled that it would not, *id.* at 287-88, but importantly, *Ghailani* was “not a Fourth Amendment search and seizure case,” *id.* at 285.

A defendant seeking both to establish an interest in items seized, and to put the Government to its proof of establishing a connection, is protected to the extent that any declaration or affidavit he submits may not be offered against him at trial. *Simmons v. United States*. 390 U.S. 377, 393-94 (1968) (“[W]hen a defendant testifies in support of a motion to suppress evidence on Fourth Amendment grounds, his testimony may not thereafter be admitted against him at trial on the issue of guilt unless he makes no objection.”). This does not insulate the defendant from all risk, however. His statement may nonetheless be used to impeach him should he take the witness stand in his own defense and, at that time, open the door to the statement. *United States v. Jaswal*, 47 F.3d 539, 543 (2d Cir. 1995); *United States v. Beltran-Gutierrez*, 19 F.3d 1287, 1291 (9th Cir.1994). (Of course, perjury in a declaration or on the stand is never permitted; so there are reasons to expect consistency.) It is certainly true, therefore, that the requirement of a statement of a personal privacy

interest in an item seized requires a defendant to make choices.⁶

Simply asserting a personal privacy interest in a premises or an object does not-even when a warrantless search has occurred-require a finding of a Fourth Amendment violation. A court asks a second question: whether society is willing to recognize that this expectation is, in turn, reasonable. *California v. Ciraolo*, 476 U.S. 207, 211 (1986); *Katz*, 389 U.S. at 360. For instance, that an individual has taken measures to restrict third-party viewing of his activities in a space that he owns or leases does not necessarily mean that that privacy interest is one society is prepared to recognize as reasonable. *See Ciraolo*, 476 U.S. at 209-10, 215 (finding no Fourth Amendment violation when aerial photographs had been taken above a property whose owner had taken fairly extensive measures to shield from view); *see also Oliver v. United States*, 466 U.S. 170, 182-84 (1984) (placement of “No Trespassing” signs on secluded property does not create legitimate privacy interest in marijuana fields).

⁶ The order of proof at trial is known in advance: the Government bears the burden of proof, which means the Government goes first. If, after the Government rests, it has failed to present sufficient evidence, the defendant can move pursuant to Rule 29 of the Federal Rules of Criminal Procedure for a judgment of acquittal. Ulbricht would not take the witness stand (if at all) until those prior steps had occurred, and so the impeachment, if any, of Ulbricht with a statement setting forth a privacy interest in the Icelandic server would not occur until that point. (The Court recognizes that trial strategy is often cemented during open statements.)

Assuming a cognizable privacy interest, the court can then turn to whether the search was lawful.⁷

3. *Warrants.*

Searches not incident to arrest or exigent circumstances are generally based on a warrant. *Kentucky v. King*, 131 S. Ct. 1849, 1856 (2011). The Warrant Clause of the Fourth Amendment provides that “no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.” U.S. Const. amend. IV. An application for a warrant must state under penalty of perjury facts supporting probable cause. *See* U.S. Const. amend. IV (warrant may not issue unless supported by probable cause, supported by “oath or affirmation”). A magistrate judge then reviews the warrant, determines whether the showing of probable cause and particularity is sufficient, and if so, signs it. *See United States v. George*, 975 F.2d 72, 76 (2d Cir.1992) (“The particularity requirement prevents this sort of privacy invasion and reduces the breadth of the search to that which a detached and neutral magistrate has determined is supported by probable cause.”). A magistrate judge’s review is based on the totality of the circumstances. *Illinois v. Gates*, 462 U.S. 213, 238-39 (1983). In later reviewing such

⁷ In the absence of a cognizable privacy interest, the Court has no basis to proceed with a suppression motion, and therefore no basis on which to hold an evidentiary hearing. Evidentiary hearings are only necessary when a defendant makes a sufficient offer of proof with respect to his allegation that a false statement was made knowingly and intentionally, or with reckless disregard for the truth, by an affiant in a warrant affidavit, and if, when material that is the subject of the alleged falsity or reckless disregard is set to one side, there remains sufficient content in the warrant affidavit to support a finding of probable cause, no evidentiary hearing is required. *Franks v. Delaware*, 438 U.S. 154, 171 (1978)

determination on a motion to suppress, the reviewing court is to give the magistrate judge's review a high degree of deference. *See id.* at 236 ("A magistrate's 'determination of probable cause should be paid great deference by reviewing courts.'" (quoting *Spinelli v. United States*, 393 U.S. 410, 419 (1969). *abrogated on other grounds by Gates*, 462 U.S. 213))).

In addition to its probable cause requirement, the Warrant Clause contains a prohibition against "general warrants." *Andresen v. Maryland*, 427 U.S. 463, 480 (1976). "The problem (posed by a general warrant) is not that of intrusion *Per se*, but of a general, exploratory rummaging in a person's belongings . . . (the Fourth Amendment addresses the problem) by requiring a 'particular description' of the things to be seized." *Id.* at 480 (quoting *Coolidge v. New Hampshire*, 403 U.S. 443, 467 (1971)). General warrants are therefore prohibited; the particularity requirement is to ensure that nothing is left to the discretion of the officer when a warrant is being executed—if the item is described as among those to be seized, it may be seized. *See Andresen*, at 480; *see also Stanford v. Texas*, 379 U.S. 476, 485 (1965).

B. The Riley, Jones, and Kyllo Cases

Defendant refers to the decisions in *Riley v. California*, 134 S. Ct. 2473 (2014), *United States v. Jones*, 132 S. Ct. 945 (2012), and *Kyllo v. United States*, 533 U.S. 27 (2001), as supportive of his motions to suppress and as responding to the "essential privacy imperatives of the digital age." (Def.'s Reply Br. at 1, 13, 19, 21-28; *see also* Def.'s Br. at 3, 13-15, 17-19, 22-28, 42, 45-49, 59.) These cases do not help defendant on this motion. They are consistent, not inconsistent, with the above longstanding Fourth Amendment principles.

Riley concerned the search of data on a seized cell phone. The lawfulness of the seizure of the object itself—the cell phone—was not contested. The subsequent search of the data on the cell phone was. In *Riley*, the defendant was stopped for a traffic violation which resulted in his arrest on weapons charges. 134 S. Ct. at 2480. A cell phone was seized as a result of a lawful search of Riley’s person incident to his arrest. *Id.* The arresting officer reviewed the contents of the cell phone without a warrant, and another officer conducted a subsequent and further review of those contents. *Id.* at 2480-81. The Supreme Court articulated the issue before it as how the requirement of “the reasonableness of a warrantless search incident to a lawful arrest” applies to “modern cell phones.” *Id.* at 2482, 2484. The Court acknowledged that the rationale of prior cases dealing with searches incident to arrest involving physical objects (such as those typically found on an arrestee’s person) did not have as much force in the digital context. A “search of the information on a cell phone bears little resemblance to the type of brief, physical search considered in [*United States v. Robinson*, 414 U.S. 218 (1973)].” *Id.* at 2485. Because the data on a cell phone are generally far more extensive than the contents of physical objects and do not present the same type of safety issues, the Court determined that warrants are generally required to search the contents of cell phones. *Id.* at 2485-86. The Court based its decision both on the potential breadth of the information a cell phone might contain, as well as on the fact that digital data generally cannot be used as a weapon or to cause immediate physical danger. *Id.* Nothing in the Court’s opinion in *Riley* suggests any departure from any of the principles regarding the need to establish a personal privacy interest, as discussed above, and as is obvious, the opinion says nothing concerning searches by

foreign law enforcement officers outside the United States.

Jones concerned the warrantless attachment of a Global-Positioning-System (“GPS”) tracking device to a Jeep vehicle and the subsequent monitoring of the movements of that vehicle. 132 S. Ct. at 948. The Supreme Court examined the question of whether the physical placement of the GPS device constituted a search within the meaning of the Fourth Amendment and found that it did. There, the Supreme Court returned to age-old concepts of physical trespass and the Fourth Amendment. See *id.* at 949-54. In this context, the physical attachment of the device was found to unreasonably intrude on the defendant’s reasonable expectation of privacy and, “[b]y attaching to the device to the Jeep, officers encroached on a protected area.” *Id.* at 952. The Court acknowledged that more nuanced cases—such as situations involving the transmission of electronic signals without trespass—were different from the case then at hand and would be subject to analysis under the factors set forth in *Katz*. *Id.* at 953. *Jones* neither alters nor extends Fourth Amendment law in light of the digital era. Indeed, the majority opinion looks more to the past than it does to the future.

In *Kyllo*, the Supreme Court did find that relatively new technology—thermal imaging used on the exterior of a private residence, and which provided information as to what was occurring in that private residence—constituted a search for purposes of the Fourth Amendment. *Kyllo*, 533 U.S. at 40. The thermal imaging was performed from the exterior of the house and occurred over a span of just a few minutes. *Id.* at 29-30. Based upon the information obtained, the investigating agent drew the conclusion that the residence functioned in part as a grow-house for ma-

rijuana. *Id.* at 30. There, too, the Court applied longstanding principles of law to find that the defendant had a reasonable expectation of privacy in his residence—the sanctity of which has long been the concern of Fourth Amendment jurisprudence. *Id.* at 34-40. The Court held that “[w]here, as here, the Government uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a ‘search’ and is presumptively unreasonable without a warrant.” *Id.* at 40.

C. Discussion

Here, the Government obtained nine warrants and five pen-trap orders. Ulbricht argues that all of the warrants and orders suffer from one overarching infirmity: they are based on the cursory recitation of an “investigation” that was only possible as the result of the search that led to the authorities to Iceland. Ulbricht argues that how that search was conducted is unknown, and that if it was conducted in an unlawful manner, then all of the warrants are constitutionally defective.⁸

⁸ Ulbricht also argues that the magistrate judges who received the warrant applications failed appropriately to inquire into how the preliminary investigation was conducted. (Def.’s Br. at 36–37.) For all of the reasons discussed throughout this opinion, he has not established a personal privacy interest that would allow him to pursue this argument. Nevertheless, even if this Court were to perform a substantive review of the merits it would find that there is no deficiency. This Court is to give a receiving magistrate’s determination of probable cause a high degree of deference. *See Gates*, 462 U.S. at 236. It is apparent from the face of the affidavit in support of Warrant No. 1—which contains a handwritten addition by the affiant and the initials of the reviewing magistrate—that the application was carefully reviewed and probable cause established.

Ulbricht's motion is largely, therefore, directed at an investigation and search of objects (servers) and premises in which he has carefully avoided establishing a personal privacy interest. As the above principles make clear, just because the investigation eventually led to his arrest on criminal charges does not ipso facto give him a privacy interest in any Silk Road servers. *Katz*, 389 U.S. at 351 (“[T]he Fourth Amendment protects people, not places.”).

As the Court has set forth above, Ulbricht was provided ample opportunity to establish such an interest—including an additional and specific request by this Court on October 7, 2014. (ECF Nos. 76-77.) He elected to “rest[] on his papers.” (ECF No. 83.) This is either because he in fact has no personal privacy interest in the Icelandic server, or because he has made a tactical decision not to reveal that he does.

The requirement to establish a personal privacy interest might appear to place Ulbricht in a catch-22: if the Government must prove any connection between himself and Silk Road, requiring him to concede such a connection to establish his standing the searches and seizures at issue could be perceived as unfair. But as Ulbricht surely knows, this is not the first court, nor is he the first defendant, to raise such an issue. *See, e.g., Payner*, 447 U.S. 727. In *Payner*, the Government obtained evidence against a defendant based on a “flagrantly illegal search of a [third party’s] briefcase.” *Id.* at 729. The Supreme Court referenced having decided *Rakas* the prior term, reaffirming the “established rule that a court may not exclude evidence under the Fourth Amendment unless it finds that an unlawful seizure violated the defendant’s own constitutional rights.” *Id.* at 731 (collecting cases). “And the defendant’s Fourth Amendment rights are violated only

when the challenged conduct invaded his legitimate expectation of privacy rather than that of a third party.” *Id.* (emphasis in original) (citing, *inter alia*, *Rakas*, 439 U.S. at 143.)

While the district court and the circuit court in *Payner* recognized this rule, they directly stated that a federal court should use its supervisory power to suppress evidence tainted by gross illegalities that did not infringe the defendant’s constitutional rights. *Id.* at 733. The Supreme Court disagreed—and found that the extension of the supervisory power would “enable federal courts to exercise a standardless discretion in their application of the exclusionary rule to enforce the Fourth Amendment.” *Id.* at 733. The Supreme Court reiterated that it did not condone lawless behavior—but nor did lawless behavior command “the exclusion of evidence in every case of illegality.” *Id.* at 734. “Our cases have consistently recognized that unbending application of the exclusionary sanction to enforce ideals of government rectitude would impede unacceptably the truth-finding functions of the judge and jury.” *Id.* The Court concluded that “the supervisory power does not authorize a federal court to suppress otherwise admissible evidence on the ground that it was seized unlawfully from a third party not before the court.” *Id.* at 735.

Ulbricht and other defendants seeking to both establish an interest in items seized, and put the Government to its proof of establishing a connection, are protected to the extent that any declaration or affidavit may not be offered against the defendant at trial. *See Simmons*, 390 U.S. at 393-94 (a defendant’s sworn statements offered in support of a motion to suppress may not thereafter be admitted against him at trial on the issue of guilt unless de-

fendant does not object). This does not insulate the defendant from all risk, however. His statement may nonetheless be used to impeach the defendant should he take the witness stand in his own defense and, at that time, open the door to the statement on direct. *United States v. Jaswal*, 47 F.3d 539, 543 (2d Cir. 1995); *United States v. Beltran-Gutierrez*, 19 F.3d 1287, 1291 (9th Cir. 1994). It is certainly true, therefore, that the requirement of a statement of a personal privacy interest in an item seized requires a defendant to make hard choices. One choice is to establish an interest if such exists to enable a court to take up important issues. That could not or was not done here.

Here, the Court does not know whether Ulbricht made a tactical choice because he is—as they say—between a rock and a hard place, or because he truly has no personal privacy interest in the servers at issue.

It is clear, however, that this Court may not proceed with a Fourth Amendment analysis in the absence of the requisite interest. If a third party leased a server on which the Government unlawfully intruded in the investigation that led to the Icelandic server, under *Katz*, *Rakas*, *Pavner*, and a host of other case law, that is no basis for an assertion by Ulbricht that *his* Fourth Amendment rights were violated. Thus, whatever methods used—lawful or unlawful—are beyond this Court’s purview. *Payner*, 447 U.S. at 735. Ulbricht therefore has no basis to challenge as violations of his Fourth Amendment rights: (1) the investigation that preceded and led to the Icelandic server, (2) the imaging and search of the Icelandic server, and (3) Warrant Nos. 1, 2, 3, 4, 5, and 7.⁹

⁹ Ulbricht has also argued that Warrant Nos. 1, 2, 3, 4, 5, and 7 are unlawful “general warrants.” (See Def.’s Reply Br. at 3.) For the same

Ulbricht has not proffered a statement that he had a personal expectation of privacy in the laptop (Warrant No. 6), Facebook (Warrant No. 8) or Gmail accounts (Warrant No. 9). While his lawyer stated that his privacy interest in the accounts and his laptop is “manifest” (ECF No. 83 at 2 n. 2), the law has long held that statements submitted by attorneys that are merely conclusory or that do not allege personal knowledge on the part of the attorney are insufficient to create an issue of fact. *See United States v. Motley*, 130 Fed. App’x 508, 510 (2d Cir. 2005) (summary order) (citing *Lipton v. Nature Co.*, 71 F.3d 464, 469 (2d Cir. 1995); *United States v. Gillette*, 383 F.2d 843, 848-49 (2d Cir. 1967). While the Court may assume based on his attorney’s statement and the Government’s stated intention not to contest that position that these accounts and the laptop belong to Ulbricht, that does not necessarily mean that he has a reasonable expectation of privacy as to their respective contents. There are, of course, many ways in which users may set up the privacy settings or password protection for their Facebook and Gmail accounts, as well as access to their laptops—and these settings and protections are relevant to a *Katz* analysis. *See United States v. Meregildo*, 883 F. Supp. 2d 523, 525 (S.D.N.Y. 2012) (“When a social media user disseminates his postings and information to the public, they are not protected by the Fourth Amendment. However, postings using more secure privacy settings reflect the user’s intent to preserve information as private and may be constitutionally protected.” (citations omitted)). It is also pos-

reasons that he lacks a sufficient Fourth Amendment interest to challenge the investigatory technique that underlies the probable cause recited in the warrants, so too he lacks a sufficient interest as to this argument.

sible for more than one individual to have access to a single shared Facebook or Gmail account. It also seems likely that many of Ulbricht's emails were to individuals other than himself, which could defeat an expectation of privacy in them. *See United States v. Lifshitz*, 369 F.3d 173, 190 (2d Cir. 2004) (explaining that emailers generally lose a legitimate expectation of privacy in an email that has already reached its recipient (citing *Guest v. Leis*, 255 F.3d 325, 333 (6th Cir. 2001))).¹⁰ The Court has no idea whether Ulbricht had a reasonable subjective expectation that all aspects of his Facebook and Gmail accounts would be private, or none. The Court has no idea whether his laptop was password protected or not. And that makes a difference. The Court cannot just assume a subjective expectation of privacy.¹¹

¹⁰ The Court does not here decide that Ulbricht could never have an expectation of privacy in an email he sent to a third party.

¹¹ It is particularly inappropriate to do so in light of published user terms for both Gmail accounts and Facebook which indicate that under certain circumstances the accounts may be turned over, without notice, to law enforcement. *See Privacy Policy*, Google, <http://www.google.com/policies/privacy/> (last modified Mar. 31, 2014) ("Your domain administrator may be able to . . . receive your account information in order to satisfy applicable law, regulation, legal process or enforceable government request. . . . We will share personal information with companies, organizations or individuals outside of Google if we have a good-faith belief that . . . the information is reasonably necessary to: meet any applicable law, regulation, legal process, or enforceable governmental request."); *Information for Law Enforcement Authorities*, Facebook, <https://www.facebook.com/safety/groups/law/guidelines/> (last visited October 9, 2014) (explaining that under certain circumstances Facebook may provide a user's information to law enforcement authorities without notice to the user).

In any event, the warrants relating to these three items were lawful. As the Court has set forth above, Ulbricht cannot challenge the initial investigation that led to the Icelandic server. Information obtained from the search of that server led law enforcement to other servers within the United States (as to which Ulbricht similarly has no demonstrated privacy interest), and the information gathered as a result of those searches undoubtedly found its way into the probable cause analysis for Warrant Nos. 6, 8 and 9. That probable cause supported Warrants 6, 8 and 9 was well and solidly established—even without the deference this Court must give to the reviewing magistrate judge. *See Gates*, 462 U.S. at 236; *United States v. Martin*, 426 F.3d 68, 73 (2d Cir. 2005) (courts must afford a presumption of validity to the affidavits supporting a search warrant); *United States v. Carpenter*, 341 F.3d 666, 670 (8th Cir. 2003) (“[S]uppression remains an appropriate remedy where ‘the issuing magistrate wholly abandoned his judicial role.’” (quoting *United States v. Leon*, 468 U.S. 897, 923 (1984))). Thus, the warrants do not suffer from any probable cause deficiency.

Nor are these general warrants. A general warrant is one that lacks particularity as to the item to be seized or as to what should be searched. *George*, 975 F.2d at 75. Here, they were specific as to both. The warrants identified the laptop and the accounts by name. There was no lack of specificity as to the items to be seized. Thus, the entirety of the laptop and data on the hard drive of that laptop was seized, along with the entirety of the accounts.

The warrants were also specific, however, as to what type of evidence should be searched for. Each of the warrants listed specific categories of items, including evidence of aliases, evidence concerning attempts to obtain fake identification, writings which can be used as stylistic

comparisons for other “anonymous” writings, evidence concerning Ulbricht’s travel patterns or movement, communications with co-conspirators regarding specified offenses, evidence concerning Bitcoin in connection with the specified offenses, and other evidence relating to the specified offenses. (See Dratel Decl. exs. 11, 13, 14.)

It is certainly true that in order to search for the specified items, the Warrants sought to seize the entirety of the laptop, the Facebook account, and the Gmail account. But this does not transform the warrants into general warrants. Indeed, it is important not to confuse the separate concepts of the seizure of an item—which were quite specifically identified but which were seized in their entirety—with the search itself. The search is plainly related to the specific evidence sought. It has long been perfectly appropriate to search the entirety of a premises or object as to which a warrant has issued based on probable cause, for specific evidence as enumerated in the warrant, which is then to be seized. For instance, warrants have long allowed searching a house high and low for narcotics—indeed, it is rare that drug dealers point out the hidden trap in the basemen—or reviewing an entire file cabinet to find files that serve as evidence of money laundering activity, which might be intermingled with files documenting lawful and irrelevant activity. This case simply involves the digital equivalent of seizing the entirety of a car to search for weapons located within it, where the probable cause for the search is based on a possible weapons offense.

In *In the Matter of a Warrant for All Content and Other Information Associated with the Email Account at xxxxx@Gmail.com Maintained at the Premises Controlled by Google, Inc.*, No. 14 Mag. 309, 2014 WL 3583529 (S.D.N.Y. Aug. 7, 2014) (“*Gmail*”), Magistrate Judge Gorenstein comprehensively reviewed the current state of

the law in this area. In that case, the Government sought a warrant in connection with an investigation to allow it to search the entirety of a Gmail account for specified evidence of a crime, as to which sufficient probable cause had been demonstrated. *Id.* at *1. The warrant did not contain a particular search protocol and did not limit the amount of time the Government could take to review the information Google would provide in response to the warrant. *Id.* The warrant also did not provide for later destruction of the material. *Id.* The court reviewed Fourth Amendment principles with a particular focus on the requirement that courts assess the “reasonableness” of a search. *Id.* at *2. The court noted that courts in Washington, D.C. and Kansas had denied applications seeking warrants for entire email accounts, at least without protocols in place. *Id.* at *3. The court found that under long established precedent, when officers executing warrants went, for instance, to a home or office, and were authorized to seize particular types of documents, they generally were required to look into the places where any and all documents were stored; there was no practice and certainly no requirement that people universally applied to the organization of their documents to assist in quick and direct location of responsive documents should they ever be the subject of a warrant. That was not real life. Some latitude for searches had to be allowed; this was particularly true with regard to electronic evidence would could be even more voluminous and undifferentiated than paper documents. *See id.* at *5.

Judge Gorenstein applied these principles to the warrant before him and determined that because it specified the particular crimes as to which evidence was sought—and as to which probable cause had been established—it was not overbroad. *Id.* at *7. He noted that the Federal Rules of Criminal Procedure had been amended in 2009

to provide for a procedure in which a warrant could authorize the seizure of electronic storage media or the seizure or copying of electronically stored information—and that unless the warrant otherwise requires it, a later review of the media or information is allowed. *Id.* at *6 (citing Fed. R. Crim. P. 41(e)(2)(B)). The decision also noted the Second Circuit’s ruling in *United States v. Ganas*, 755 F.3d 125 (2d Cir. 2014), in which the Second Circuit held that while wholesale removal of all tangible papers from a premises was not generally acceptable, electronic media posed a different set of issues. *Gmail*, 2014 WL 3583529, at *6. In *Ganas*, the Court stated that “[i]n light of the significant burdens on-site review would place on both the individual and the Government, the creation of mirror images for offsite review is constitutionally permissible. . . .” 755 F.3d at 135.

This Court agrees entirely with Judge Gorenstein’s rationale. Warrants 6, 8 and 9 are substantially similar to the warrant before Judge Gorenstein, and similarly have the necessary particularity.¹²

¹² Even if this Court were to find that the magistrate judges who issued the warrants erred by approving the clauses to which Ulbricht objects as overly broad, the application of the exclusionary rule here would still be inappropriate, as the law enforcement agents who executed the searches and seizures at issue were entitled to rely in good faith upon the magistrate judges’ probable cause determinations, and the warrant applications here were not so “lacking in indicia of probable cause” nor so “facially deficient” that reliance upon the warrant was “entirely unreasonable.” *Id.* at 921-23 (quotation omitted).

The Court further notes that while it is certainly true that there are circumstances under which a warrant that authorizes a seizure of “any communications or writings” in the email account of a defendant would be overbroad, it is also true that a magistrate judge’s review of

III. PEN-TRAP ORDERS

Defendant argues that the Pen-Trap Orders were deficient for two reasons: (1) the information obtained through the Pen-Trap Orders should have been the subject of a warrant application, and (2) the orders failed to include appropriate minimization procedures. Both arguments are meritless.

The law is clear—and there is truly no room for debate—that the type of information sought in Pen-Trap orders 1, 2, 3, 4, and 5 was entirely appropriate for that type of order.¹³ See 18 U.S.C. §§ 3121 *et seq.* In *Smith v. Maryland*, 442 U.S. 735 (1979), the Supreme Court found that the use of a pen-register did not constitute a search for Fourth Amendment purposes, *id.* at 745-46. To the extent

a warrant application must be based on the totality of the circumstances. *Gates*, 462 U.S. at 238-39. Here, these circumstances included many steps taken by members of the alleged conspiracy to maintain their anonymity while creating, designing, administering, operating, and using the Silk Road website, and they included the use of idiosyncratic linguistic patterns by the website's administrator. Given the high degree of deference that this Court must afford the review of the magistrate judge, *see id.* at 236, it is not this Court's place to second-guess their decision that the warrants were not overly broad in the context of a case where anonymity and the usage of idiosyncratic linguistic patterns are key issues.

¹³ The information related to the IP addresses of individual packets of data sent to and from a particular IP address. The content of the communications was not requested. Pen-trap devices have frequently been used to obtain precisely that which was sought here. Before the Internet became widely used, pen-trap devices were used to obtain information regarding the telephone numbers associated with incoming and outgoing telephone calls. *Smith v. Maryland*, 442 U.S. 735 (1979).

Ulbricht wants to make novel Fourth Amendment arguments with regard to the Pen-Trap Orders,¹⁴ he has not established the requisite privacy interest (as discussed at length above) to do so. The Court will therefore not consider those arguments.

Ulbricht’s minimization argument is similarly off-base. Minimization refers to protocols and is used in the wiretap context to prevent investigators from listening to conversations irrelevant to their investigation. *See* 28 U.S.C. § 2518 (wiretaps must be conducted “in such a way as to minimize the interception of communications not otherwise subject to interception”). Minimization is directed at *content*. *See United States v. Rizzo*, 491 F.2d 215, 216 n. 3 (2d Cir. 1974) (federal minimization laws do not apply “to mere interception of what telephone numbers are called, as opposed to the interception of the contents of the conversations”). The Pen-Trap Orders do not seek the content of internet communications in any directly relevant sense.

IV. BILL OF PARTICULARS

Defendant moves for an order requiring the Government to provide a bill of particulars. (Def.’s Br. at 65–79.) Defendant argues that in the absence of additional factual detail not contained in the Indictment, he will be unable to prepare his defense and will have an insufficient basis to

¹⁴ Defendant argues that the scope of information that can be gleaned from Internet routing information “allows for a profile of an individual’s activity far more concrete and comprehensive” than what the telephone numbers associated with a telephone call would reveal. (Def.’s Reply Br. at 25.) He urges that as a result, *Smith v. Maryland*—which occurred in the context of landline telephones—is inapposite. This Court cannot consider that argument in light of the lack of a demonstrated privacy interest.

make double jeopardy challenges to potential future charges. (*Id.* at 65.) Defendant argues that the volume of discovery weighs in favor of a bill of particulars. (*Id.* at 65-66.)

Rule 7(f) of the Federal Rules of Criminal Procedure provides that a court may direct the Government to file a bill of particulars. Fed. R. Crim. P. 7(f). However, a bill of particulars is required “only where the charges of the indictment are so general that they do not advise the defendant of the specific acts of which he is accused.” *United States v. Walsh*, 194 F.3d 37, 47 (2d Cir.1999) (quoting *United States v. Torres*, 901 F.2d 205, 234 (2d Cir.1990)).

A bill of particulars is also unnecessary when the Government has produced materials in discovery concerning the witnesses and other evidence. See *id.* (“[A] bill of particulars is not necessary where the government has made sufficient disclosures concerning its evidence and witnesses by other means.”) In *Torres*, the Second Circuit affirmed the district court’s denial of a bill of particulars in part because the defendants were provided with considerable evidentiary detail outside of the indictment. 901 F.2d at 233-34; see also *United States v. Panza*, 750 F.2d 1141, 1148 (2d Cir. 1984). Thus, in determining whether to order a bill of particulars, a court must examine the totality of the information available to defendant, both through the indictment and through pre-trial discovery. *United States v. Bin Laden*, 92 F. Supp. 2d 225, 233 (S.D.N.Y. 2000). The purpose of the bill of particulars is to avoid prejudicial surprise at trial and give defendant sufficient information to meet the charges against him. *Id.* (citing *Torres*, 901 F.2d at 234).

In *Bin Laden*, the court granted the defendants’ motion for a bill of particulars. *Id.* at 227. There, however, the

indictment charged 15 named defendants with 267 discrete criminal offenses, it charged certain defendants with 229 counts of murder, it covered a period of nearly ten years, and it alleged 144 overt acts in various countries. *Id.* at 227-28. The court noted that the “geographical scope of the conspiracies charged in the indictment is unusually vast.” *Id.*

There is no provision in the Federal Rules of Criminal Procedure for the type of broad, sweeping discovery Ulbricht seeks here. Neither the nature of this indictment or the produced discovery calls for a departure from these general rules. That this case has a high profile does not mean that it requires special treatment. Moreover, there can be no doubt that the Indictment here is specific enough to advise Ulbricht of the acts of which he is accused, namely creating, designing, administering and operating the Silk Road website, which allegedly served as an online one-stop-shop for narcotics, fake identification documents, and materials used to hack computers, and which was specifically designed to rely on Bitcoin, a method of payment designed to conceal the identities and locations of users transmitting and receiving funds. This case is unlike *Bin Laden*, which concerned hundreds of offenses associated with over one hundred alleged actions committed in far corners of the globe—it concerns a single defendant who is alleged to have run a single and clearly identified website. Further, the Court has gone to considerable lengths to ensure that Ulbricht has access to evidentiary detail outside of the Indictment, including ensuring that a laptop preloaded with certain discovery materials was provided to Ulbricht for use at the Metropolitan Detention Center (“MDC”) and particular accommodations regarding the length of time he can routinely access the information. (ECF No. 40.) A bill of particulars is

wholly unnecessary to avoid prejudicially surprising Ulbricht at trial.

V. SURPLUSAGE

Rule 7(d) of the Federal Rules of Criminal Procedure provides that, upon a motion by defendant, a court may strike extraneous matter or surplusage from an indictment. Fed.R.Crim.P. 7(d). However, “[m]otions to strike surplusage from an indictment will be granted only where the challenged allegations are not relevant to the crime charged and are inflammatory or prejudicial.” *United States v. Mulder*, 273 F.3d 91, 99 (2d Cir. 2001) (quoting *United States v. Scarpa*, 913 F.2d 993, 1013 (2d Cir. 1990)).

Courts have held that statements providing background are relevant and need not be struck. *Id.* at 99-100 (in action charging extortion relating to labor coalitions, upholding district court’s decision not to strike background on tactics and purposes of labor coalitions).

The surplusage issues defendant has raised relating largely to the murder for hire assertions need not be fully addressed at this time. Courts in this district routinely await the presentation of the Government’s evidence at trial before ruling on a motion to strike surplusage. *See, e.g., Scarpa*, 913 F.2d at 1012; *United States v. Persico*, 621 F. Supp. 842, 861 (S.D.N.Y. 1985); *United States v. Ahmed*, No. 10 Cr. 131 (PKC), 2011 WL 5041456, at *3 (S.D.N.Y. Oct. 21, 2011).

In *Ahmed*, the defendant’s motion to strike surplusage related to background information regarding civil and sectarian violence in Somalia and the anti-American animus of Al Shabaab, which was designated by the Secretary of State as a “foreign terrorist organization.” *Ahmed*, 2011 WL 5041456, at *1-2. The court held that it would

await presentation of the Government's evidence at trial, and stated further that the Government would have some latitude to "demonstrat[e] the nexus between defendant's conduct and American interests, as well as the background of others who are members of the charged conspiracies." *Id.* at *3. The Court noted that denial of the motion without prejudice to renew might also allow the parties to reach a pre-trial stipulation, as had occurred in *United States v. Yousef*, No. S3 08 Cr. 1213 (JFK), 2011 WL 2899244 (S.D.N.Y. June 30, 2011). *Ahmed*, 2011 WL 5041456, at *3. Here, as in *Ahmed*, the Court will await the Government's presentation at trial.

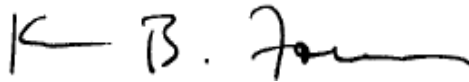
VI. CONCLUSION

For the reasons set forth above, defendant's motion to suppress, for a bill of particulars and to strike surplusage is **DENIED**.

The Clerk of Court is directed to close the motion at ECF No. 46.

SO ORDERED.

Dated: New York, New York
October 10, 2014

A handwritten signature in black ink, appearing to read "K B. Forrest", is written over a horizontal line.

KATHERINE B. FORREST
United States District Judge