No. 17-950

IN THE

Morris Tyler Moot Court of Appeals at Yale

ROSS WILLIAM ULBRICHT,
Petitioner,

v.

UNITED STATES,
Respondent.

On Writ of Certiorari to the United States Court of Appeals for the Second Circuit

BRIEF FOR PETITIONER

ERIC BROOKS
MEGHA RAM

Yale Law School
127 Wall Street
New Haven, CT 06511
(203) 432-4992

Counsel for Petitioner

QUESTIONS PRESENTED[*]

1. Whether the warrantless collection of Petitioner's internet browsing history violated the Fourth Amendment.
2. Whether the Sixth Amendment permits judges to find the facts necessary to support an otherwise unreasonable sentence.

[*] All parties are named in the caption of the case.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

U.S. Constitution

United States Code

State Statutes

Other

OPINIONS BELOW

The opinion of the court of appeals is reported at 858 F.3d 71. The opinions of the district court denying Petitioner's motion for a new trial and denying Petitioner's motion to suppress are unpublished, but are available at 2015 WL 413318 and 2014 WL 5090039.

STATEMENT OF JURISDICTION

The court of appeals entered its judgment on May 31, 2017. The petition for a writ of certiorari was filed on December 22, 2017. This Court has jurisdiction under 28 U.S.C. § 1254(1).

CONSTITUTIONAL PROVISIONS INVOLVED

The Fourth Amendment to the United States Constitution provides:

> 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 Sixth Amendment to the United States Constitution provides:

> In all criminal prosecutions, the accused shall enjoy the right to a speedy and public trial, by an impartial jury of the State and district wherein the crime shall have been committed, which district shall have been previously ascertained by law, and to be informed of the nature and cause of the accusation; to be confronted with the witnesses against him; to have compulsory process for obtaining witnesses in his favor, and to have the Assistance of Counsel for his defense.

Selected portions of the Electronic Communications Privacy Act and the Sentencing Table of the Federal Sentencing Guidelines are printed in an appendix to this brief. See Pet. App., *infra*, 1a-6a.

STATEMENT

A. The government's investigation

1. The government brought this case as part of its investigation into Silk Road, an online criminal marketplace. JA 6. Central to the investigation was the warrantless use of "pen registers" and "trap and trace devices." JA 29. These devices (collectively, "pen registers") record "dialing, routing, addressing, or signaling information" transmitted to or emitted from a telecommunications device. 18 U.S.C. § 3127(3)-(4).

An example of that information is a computer's Internet Protocol (IP) address. "[IP] addresses are the unique numbers assigned to every computer or device that is connected to the Internet." *Beginner's Guide to Internet Protocol (IP) Addresses*, Internet Corp. for Assigned Names and Numbers, 2 (2011).[1] Every "web server, smartphone, mail server, or laptop" has an IP address. *Ibid.* When a user "send[s] an email, [or] visit[s] a web site," his computer "sends data packets to the IP address of the other end of the connection and receives packets destined for its own IP address." *Id*. at 4. By monitoring which IP addresses these packets are routed to, a pen register can track the websites a computer is visiting. It can also track the "dates, times, [and] durations" of those visits. JA 30.[2]

No statute requires federal agents to seek a warrant before using a pen register. Although they must obtain a court order,[3] the court must issue the order if a government attorney has certified "that the information likely to be obtained * * * is relevant to an ongoing criminal investigation." 18 U.S.C. § 3123(a)(1).

---

[1] https://perma.cc/7FNM-NPL5.

[2] All subpages of a website have the same IP address. Thus, a pen register that is set up to track only IP addresses but not URLs would not be able to tell the difference between someone visiting, say, www.supremecourt.gov and www.supremecourt.gov/opinions. See *United States* v. *Forrester*, 512 F.3d 500, 504 (9th Cir. 2008).

[3] Except in certain exigencies. See 18 U.S.C. § 3125.

2. During the government's investigation into Silk Road, it learned that the website was operated by someone using the alias "Dread Pirate Roberts" (DPR). JA 6 Because it suspected that Ulbricht was DPR, it obtained orders to install five pen registers to monitor his internet activity. JA 6-7. From this investigation, the government learned that Ulbricht had visited Silk Road. JA 7. It also claims that by comparing the times when Ulbricht visited the website to the times when DPR was active online, it could infer that the two were the same person. *Ibid*. Based in part on the pen register evidence, the government arrested Ulbricht in October 2013. JA 12. After the arrest, the government seized his laptop, which yielded additional evidence linking him to Silk Road. *Ibid*.

B. District court proceedings

1. In 2014, Ulbricht was indicted by a federal grand jury on seven counts stemming from his role in operating Silk Road: (1) narcotics trafficking; (2) distribution of narcotics by means of the internet; (3) narcotics trafficking conspiracy; (4) continuing criminal enterprise; (5) conspiracy to commit and aid and abet computer hacking; (6) conspiracy to traffic in fraudulent identification documents; and (7) money laundering conspiracy. Superseding Indictment 1-14, ECF No. 52.

Before the trial, Ulbricht moved to suppress some of the evidence against him as the fruit of several illegal searches. Among other things, he argued that the government violated the Constitution by using the pen registers without a warrant. JA 29. The district court rejected this argument. It reasoned that investigating the websites Ulbricht visited would be analogous to investigating the phone numbers he called, which would not have required a warrant under *Smith* v. *Maryland*, 442 U.S. 735 (1979). JA 141. As a result of this disposition, the district court has not yet determined which parts of the investigation were fruits of the pen register searches.

2. The trial ran from January 13 through February 4, 2015. JA 13. On February 5, the jury found Ulbricht guilty on all seven counts. Verdict Form, ECF No. 183. Judge Forrest sentenced him on May 29, 2015. JA 26. Under the Federal Sentencing Guidelines ("Guidelines"), counts involving "substantially the same harm" are grouped together. U.S. Sentencing Guidelines Manual § 3D1.2 (U.S. Sentencing Comm'n 2014). Accordingly, the judge divided the counts into three groups during the sentencing hearing. ST 17. The group that ultimately determined Ulbricht's sentence, and the one relevant here, was Group One, which contained Counts Two (distribution of narcotics by means of the internet), Four (continuing criminal enterprise), and Seven (money laundering). *Ibid*.

Under the Guidelines, the base offense level for the Group One counts was 40, ST 18, which carried a recommended sentence of 292 to 365 months, Pet. App. 6a. The sentencing judge then made a series of factual findings that increased the offense level and corresponding sentence range under the Guidelines. She found that Ulbricht commissioned murders, ST 18-19; distributed a controlled substance through mass marketing by means of an interactive computer service, ST 20; maintained premises for the purpose of manufacturing a controlled substance, ST 21; imported methamphetamine, ST 21; and played a leading role in the money laundering conspiracy, ST 22. Although these facts were never submitted to the jury, and were determined only by a "preponderance of the evidence," ST 18, they played a dramatic role in the sentencing. They raised Ulbricht's offense level to 50, ST 24, which carries a recommended sentence of life.[4] ST 64. When deciding whether to follow the recommendation, the judge considered as "relevant to the offense conduct" the fact that several drug-related deaths were connected to Silk Road – another fact that only she found. JA 28; ST 26. Taking into account all the facts that she found,

[4] The sentencing table treats it as a level 43 offense, since the table is capped at that level. ST 24; Pet. App. 6a.

Judge Forrest sentenced Ulbricht to a life term. ST 94. If this sentence stands, Ulbricht will never be eligible for parole and will spend the remainder of his life in prison. *Ibid*.

C. Appellate proceedings

1. Ulbricht appealed to the Second Circuit. He argued, among other things, that the district court should have suppressed the evidence obtained from the pen registers. JA 29. The Court rejected the argument, agreeing with the district court that *Smith* was controlling because "[t]he recording of IP address information" is "analogous to the capture of telephone numbers." JA 33. Although the court noted that "questions have been raised about whether some aspects of modern technology * * * call for a re-evaluation of the * * * doctrine established by *Smith*," it held that it would apply *Smith* until this Court instructs otherwise. *Ibid*.

2. Ulbricht, joined by several amici, also argued that the life sentence was substantively unreasonable. JA 97. He argued that the conduct found by the jury must, standing by itself, justify the sentence. This was so, he claimed, because judicial factfinding "violates a defendant's constitutional right to a jury trial where the factfinding renders reasonable an otherwise substantively unreasonable sentence." JA 106-07 n.72. The court of appeals rejected this argument. *Ibid*. Therefore, while it rejected his claim of substantive unreasonableness, it did so relying heavily on facts found only by the sentencing judge. For example, even though the court admitted that "a life sentence for selling drugs alone would give pause," it noted that in this case, "the district court found by a preponderance of the evidence that Ulbricht commissioned at least five murders." JA 100-01. Thus, although "life sentences are extraordinary and infrequent," it believed that this "case must be considered on its own facts and in light of all the circumstances * * * which, in this case, includes five attempted murders for hire." JA 107. The court therefore affirmed his life sentence.

SUMMARY OF ARGUMENT

I. Americans spend, on average, over six hours a day on the internet. In that time, they may do a remarkably diverse range of things. They may exercise their First Amendment right to speak anonymously. They may research confidential medical conditions. They may explore their sexual orientation, join an advocacy group, or conduct proprietary business research. An internet browsing history is a record of all this activity.

At issue in this case is whether people have a "reasonable expectation of privacy" in that record. *United States* v. *Jones*, 565 U.S. 400, 406 (2012) (quoting *Katz* v. *United States*, 389 U.S. 347, 360 (1967) (Harlan, J., concurring)). If they do, then the government's warrantless investigation of Ulbricht's browsing history was a search within the meaning of the Constitution. Warrantless searches "are per se unreasonable." *Katz*, 389 U.S. at 357. Therefore, if people have a reasonable expectation of privacy in their browsing history, the government's investigation violated the Fourth Amendment.

People have that expectation. A "browsing history" "reveal[s] an individual's private interests or concerns," *Riley* v. *California*, 134 S. Ct. 2473, 2490 (2014), including many details in which people have a recognized privacy interest. For example, among many other intimate details, a browsing history can disclose a record of one's political activity, *McIntyre* v. *Ohio Elections Comm'n*, 514 U.S. 342, 357 (1995); *NAACP* v. *Alabama ex rel. Patterson*, 357 U.S. 449, 461-62 (1958); health issues, *Ferguson* v. *City of Charleston*, 532 U.S. 67, 78 (2001); and home life, *Kyllo* v. *United States*, 533 U.S. 27, 37 (2001). Not surprisingly, Americans have guarded this information jealously. They have forced their internet service providers (ISPs) to promise not to release their browsing records, and they are currently enacting laws to ensure this result.

Plainly, "society is prepared to recognize as 'reasonable'" an expectation of privacy in one's web browsing history. *Katz*, 389 U.S. at 361 (Harlan, J., concurring). The court of appeals erred because it did not directly ask whether that expectation of privacy existed. It instead asked only whether Ulbricht disclosed his browsing data to anyone else. Because Ulbricht (as inevitably one must) disclosed his internet browsing data to his ISP, the court automatically inferred that he lost his privacy interest in that information. That was a mistake for two reasons.

First, the lower court incorrectly applied the Court's case law on third-party disclosure. Although people sometimes waive their privacy interest in information by disclosing it to someone else, that is not true when they have given content to an intermediary. If that were the rule, the government could listen in on telephone conversations or intercept emails with impunity. The browsing history Ulbricht shared with his ISP is akin to a telephone call he might share with his phone company, and is equally protected by the Fourth Amendment.

Second, the court erred by making the categorical assumption that people lose their privacy interest in digital data when they disclose it to an online service. As a majority of the Court has recently recognized, this assumption is "ill suited to the digital age." *Jones*, 565 U.S. at 417 (Sotomayor, J., concurring); see also *id.* at 429 (Alito, J., concurring, joined by Ginsburg, Breyer, and Kagan, JJ.). Today, people export great quantities of data to online services, but still expect that those services will not disseminate the data any further. It would vitiate the protections of the Fourth Amendment to reflexively assume that all that information is unprotected.

Instead, the court of appeals should have analyzed whether the specific information at issue here was protected by the Fourth Amendment. Had it done this, for the reasons discussed above, it would have recognized that the government's warrantless investigation violated the

Constitution and that Ulbricht's conviction rested in part on illegally obtained evidence. The Court should reverse the opinion below so that the district court can determine the remedy in the first instance.

II. Even if Ulbricht's conviction would stand despite the illegally obtained evidence, the Court must reverse for an additional reason. The court below did not review Ulbricht's sentence using the procedure required by the Sixth Amendment, and therefore failed to protect his "right to demand that a jury find him guilty of all the elements of the crime." *United States* v. *Gaudin*, 515 U.S. 506, 511 (1995).

The right to trial by jury was enshrined in the Constitution to protect against "arbitrary punishments upon arbitrary convictions." *United States* v. *Booker*, 543 U.S. 220, 238 (2005) (internal citation omitted); see U.S. Const. amend. VI. For this right to be meaningful, it must apply to any fact that increases an allowable penalty. Thus, it applies to any fact that increases the length of a sentence, *Apprendi* v. *New Jersey*, 530 U.S. 466, 490 (2000); increases the allowable fine, *Southern Union Co.* v. *United States*, 567 U.S. 343, 346 (2012); increases a mandatory minimum sentence, *Alleyne* v. *United States*, 570 U.S. 99, 117 (2013); or is necessary to impose the death penalty, *Ring* v. *Arizona*, 536 U.S. 584, 609 (2002).

Because courts may not impose unreasonable sentences, *United States* v. *Booker*, 543 U.S. 220, 260 (2005), a fact necessary to convert an unreasonable sentence into a reasonable one is a fact that increases the allowable penalty. It "unavoidably follows that any fact necessary to prevent a sentence from being substantively unreasonable * * * is an element that must be either admitted by the defendant or found by the jury." *Jones* v. *United States*, 135 S. Ct. 8, 8 (2014) (Scalia, J., dissenting from denial of certiorari, joined by Thomas and Ginsburg, JJ.). Judges do have discretion to find facts that help them determine an appropriate sentence within the range of

reasonableness. But they have no more discretion to find facts that increase that range than they do to find facts that increase a statutory maximum.

The contrary rule would frustrate the central purpose of the Sixth Amendment. It would allow a defendant to be convicted of one crime by the jury, but punished for another by the judge. Indeed, that happened in this very case. Although the jury convicted Ulbricht of crimes that would rarely merit a life sentence, the district judge found that Ulbricht committed far more serious crimes, and enhanced the sentence. Because there is a serious risk that the life sentence would not be reasonable in light of only the facts found by the jury, the Court should remand so that the Second Circuit can revise its reasonableness analysis.

ARGUMENT

I. The warrantless search of Ulbricht's internet browsing history violated the Fourth Amendment.

Government investigators must obtain a warrant before "violat[ing] a person's 'reasonable expectation of privacy.'" *United States* v. *Jones*, 565 U.S. 400, 406 (2012) (quoting *Katz* v. *United States*, 389 U.S. 347, 360 (1967) (Harlan, J., concurring)).[5] One item carrying such an expectation would be a diary that records, minute to minute, how a person spends most of his day. Since the average American uses the internet for over six hours a day, for him, that diary exists.[6] It is his internet browsing history.

Before the government may access such a sensitive record, it must follow the "time-tested means of effectuating Fourth Amendment rights": getting a warrant. *United States* v. *U.S. Dist. Court for E. Dist. of Mich., S. Div.*, 407 U.S. 297, 318 (1972). Otherwise, a vast range of

[5] Absent certain narrow exceptions not relevant here. See *infra* note 7.
[6] Roxanne Bauer, *Media (R)evolutions: Time Spent Online Continues to Rise*, World Bank (Feb. 10, 2016), https://perma.cc/BVR6-DTRA.

intimate details would be subject to the "arbitrary invasions by governmental officials" that the amendment's "basic purpose" is to prevent. *Camara* v. *Mun. Court of San Francisco*, 387 U.S. 523, 528 (1967). Because the Second Circuit held that the government could access this record without a warrant, JA 35, the Court should reverse.

A. Ulbricht had a reasonable expectation of privacy in the contents of his browsing history.

1. Warrantless searches "are per se unreasonable under the Fourth Amendment * * * subject only to a few specifically established and well-delineated exceptions." *Katz*, 389 U.S. at 357. As none of those exceptions are applicable here, the pen registers violated the Constitution if they were searches within the meaning of the Fourth Amendment.[7] This would be so if Ulbricht had a reasonable expectation of privacy in the content of those investigations, *i.e.*, "an actual (subjective) expectation of privacy" "that society is prepared to recognize as 'reasonable.'" *United States* v. *Knotts*, 460 U.S. 276, 280-81 (1983) (quoting *Katz*, 389 U.S. at 361 (Harlan, J., concurring)). It is undisputed that Ulbricht believed his browsing history was private. At issue here is whether the belief is objectively reasonable.

It is. Society recognizes a reasonable expectation of privacy in the intimate details of one's life. See, *e.g.*, *Ferguson* v. *City of Charleston*, 532 U.S. 67, 78 (2001) (holding that the Fourth Amendment protects the "results of [diagnostic medical] tests"); *Kyllo* v. *United States*, 533 U.S. 27, 38 (2001) ("details of the home"); *Katz*, 389 U.S. at 352 ("private communication[s]"); *Boyd* v. *United States*, 116 U.S. 616, 622 (1886) ("private papers"); *Ex Parte Jackson*, 96 U.S. 727, 733 (1877) (private correspondence). The searches here similarly

[7] The government argued below only that the "good faith exception" should apply. JA 48. "Good faith" is an exception to the Fourth Amendment *remedy* of suppression, not to the *right* against unreasonable searches. See *United States* v. *Leon*, 468 U.S. 897 (1984). Given their dispositions, the lower courts never addressed the remedy, and the issue is not properly before the Court.

violated the Fourth Amendment because a "search and browsing history * * * could reveal an individual's private interests or concerns." *Riley* v. *California*, 134 S. Ct. 2473, 2490 (2014). These interests and concerns include many categories of information that the Court has explicitly recognized as protected.

First, a browsing history search may reveal whether and how someone has exercised his First Amendment freedoms. For example, it can be used to uncover the identity of an anonymous speaker. An investigator can determine that a person published a website by comparing when he visited the website to when it was updated. That is precisely what the government did in this case. While the government's intent here was to catch a criminal, investigators could just as easily use the technique to unmask an anonymous political blogger or whistleblower. Government agents could also use web browsing searches to retaliate against the members of a disfavored advocacy group. For example, if the agent wanted to assemble a list of NRA members, he could track who spent time on nramemberservices.org, a members-only website.

Society does not just recognize the expectation of privacy in one's speech and associational activity as reasonable. It has encoded this expectation into the Constitution. The right to speak anonymously is "an aspect of the freedom of speech protected by the First Amendment." *McIntyre* v. *Ohio Elections Comm'n*, 514 U.S. 342, 357 (1995). The amendment similarly protects "privacy in one's associations" – the abridgement of which is "subject to the closest scrutiny." *NAACP* v. *Alabama ex rel. Patterson*, 357 U.S. 449, 461-62 (1958).

Because browsing history searches reveal activity in which people have a reasonable expectation of privacy backed by the Constitution, they are subject to the Fourth Amendment. As this Court has written, when an investigation may be "an instrument for stifling liberty of expression," the Fourth Amendment denies police the "*unrestricted* power" to investigate.

Marcus v. *Search Warrants*, 367 U.S. 717, 729 (1961) (emphasis added). The amendment also indicates the appropriate restriction: the warrant requirement. *United States* v. *Jeffers*, 342 U.S. 48, 51 (1951). This provides an "orderly procedure," *ibid.*, that lets a "neutral and detached magistrate" decide whether the search has a legitimate investigative purpose or is an attempt at political retaliation, *Johnson* v. *United States*, 333 U.S. 10, 14 (1948). "Anonymity is a shield from the tyranny of the majority," *McIntyre*, 514 U.S. at 357, but unfettered searches of people's internet history would turn the shield into a sieve.

Warrantless searches infringe the liberties of even the people the government is not tracking. The mere concern that "the Government may be watching chills associational and expressive freedoms." *Jones*, 565 U.S. at 416 (Sotomayor J., concurring). Interposing a judge who must issue a warrant between the government and people's sensitive data alleviates this chill. The Court should therefore reaffirm that when a "protected * * * First Amendment" interest is at stake, "the requirements of the Fourth Amendment must be applied with scrupulous exactitude." *Zurcher* v. *Stanford Daily*, 436 U.S. 547, 564 (1978) (internal citation and quotation marks omitted).

Second, browsing history searches are unreasonable because they intrude into the home. "In the home * * * *all* details are intimate details, because the entire area is held safe from prying government eyes." *Kyllo*, 533 U.S. at 37. Therefore, a warrantless search of the home – even one performed without a physical intrusion – may violate the Constitution if it can reveal details like the "hour each night the lady of the house takes her daily sauna and bath." *Id*. at 38.

A browsing history reveals similar household details. "[T]ablets, smartphones, and laptops" are not the only "objects to go online." Stephen Ornes, *The Internet of Things and the Explosion of Interconnectivity*, 113 Proc. Nat. Acad. Sci. 11059, 11059 (2016). Thus, a browsing

history search may reveal when any "smart appliances" in the home have communicated with the internet. For example, a search might reveal how frequently someone visits his internet-connected smart refrigerator or trips on his smart floor. *Ibid.* These facts are no less private than a bathing hour. As "20 billion devices," from thermostats to medicine dispensers, are projected to "be online by 2020," *ibid*., the records of those devices communicating with the internet will give an increasingly comprehensive window into home life. If the government can find out these details without any judicial oversight, people will no longer feel safe "retreat[ing] into [their] own home and there be free from unreasonable governmental intrusion" – the right at "the very core of the Fourth Amendment." *Silverman* v. *United States*, 365 U.S. 505, 511 (1961). "With few exceptions, the question whether a warrantless search of a home is reasonable and hence constitutional must be answered no." *Kyllo*, 533 U.S. at 31. That should be the answer here.

Third, browsing history searches are also unreasonable because they may reveal sensitive medical information. In *Ferguson*, the Court held that people have a "reasonable expectation of privacy" in the results of their "diagnostic tests," and thus government investigators could not get those results from a hospital without a warrant. 532 U.S. at 78. But as *Riley* noted, someone's internet usage pattern can reveal the same information by disclosing a "search for certain symptoms of disease." 134 S. Ct. at 2490. For example, investigators could use a pen register to track someone's frequent visits to viagra.com or aidshealth.org, thereby uncovering the existence of medical conditions the person is entitled to keep private.

2. Browsing histories would be protected by the Fourth Amendment because they violate any one of the constitutionally protected privacy interests discussed above. But they are even more sensitive because they reveal information about not just one topic, but a "broad array of private information" cutting across countless areas. *Riley*, 134 S. Ct. at 2491. The searches thus

implicate the Fourth Amendment's "central concern" with the "unbridled discretion to rummage at will among a person's private effects." *Arizona* v. *Gant*, 556 U.S. 332, 345 (2009).

This concern is heightened by the collection of information in digital form. In *Riley*, the Court unanimously concluded that the police must get a warrant to search an arrestee's smartphone. 134 S.C Ct. at 2492.[8] A smartphone's "immense storage capacity" means that searching it would uncover a broad "range of items." *Id.* at 2489, 2493. This includes the apps someone has on his phone, which "can form a revealing montage of [his] life." *Id.* at 2490. "There are apps for Democratic Party news and Republican Party news; apps for alcohol, drug, and gambling addictions; apps for sharing prayer requests; [and] apps for tracking pregnancy symptoms," among many others. *Ibid.*

For every app, there is a related website. If it violates someone's privacy to know which apps he has installed on his phone of the "over a million" in existence, *ibid.*, then it certainly violates his privacy to know not only which websites he has visited of the over *three hundred million* in existence, Domain Name Industry Brief, Verisign, 2 (Feb. 2018),[9] but also how long and frequent those visits were. Like the apps that someone has downloaded, one's browsing history can reveal private facts including political views (*e.g.*, repeated visits to socialistparty.net, prolife.com, or rnc.org); health, both physical (diabetes.org) and mental (suicideprevention.org, anxiety.org, addiction.org, or thetrevorproject.org [a website for gay youth suffering from depression]); social and relationship difficulties (sextherapy-online.com, intensivecouplestherapy.com, or match.com); religious beliefs or doubts (mormon.org or

[8] *Riley* concerned the question of whether a conceded search should be governed by the normal rule that no warrant is needed for searches incident to an arrest. 134 S. Ct. at 2492. But the underlying inquiry, whether the government needed a warrant to conduct a search, was the same as it is here. If anything, the principles articulated in *Riley* would apply with greater force here, because arrestees have "reduced expectations of privacy." *Id.* at 2488 (quoting *United States* v. *Chadwick*, 433 U.S. 1, 16 n.10 (1977)).

[9] http://perma.cc/9LBE-ZRZL.

athiests.org); financial troubles (debtroundup.com); that he is secretly looking for a new job (monster.com); which news sources he consumes; confidential business information like which firms he is considering investing in or who his clients are; and how much time he spends on vices like watching pornography or playing online poker.

This list could continue indefinitely: our browsing histories are replete with intimate details. Like cellphones, a browsing history "not only contains in digital form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form." *Id.* at 2491. The claim that society does not regard an expectation of privacy in this information as reasonable is risible.

3. In fact, it has been empirically refuted. We know Americans consider their browsing history private because they have said so. Seventy percent of Americans believe that the "[w]ebsites they have visited" is sensitive information. *Public Perceptions of Privacy and Security in the Post-Snowden Era*, Pew Res. Ctr. 7 (2014).[10] They have acted on this belief. Eighty-six percent of internet users have "taken steps online to remove or mask their digital footprints." Lee Rainie et al., *Anonymity, Privacy, and Security Online*, Pew Res. Ctr. (2013).[11] In the marketplace, Americans have demanded that their internet service providers (ISPs) promise "not [to] sell customers' individual internet browsing information." David Shepardson, *Major Internet Providers Say Will Not Sell Customer Browsing Histories*, Reuters (Mar. 31, 2017);[12] see also *Protecting Consumer Privacy Online*, Nat'l Exch. Carrier Assoc. (Jan. 27, 2017) (containing a pledge signed by twenty-two major ISPs, including AT&T, Comcast, Cox and Verizon).[13] And in the political arena, in just the past year, they have convinced legislatures

[10] https://perma.cc/6735-M4Z5.
[11] https://perma.cc/K3P9-C2VZ.
[12] https://perma.cc/ET6X-YQSR.
[13] https://perma.cc/PY8S-NX4R.

in nearly half the states to introduce measures "requiring internet or telecommunications service providers to keep specified information confidential." *Privacy Legislation Related to Internet Service Providers*, Nat'l Conf. State Legislatures (Dec. 29, 2017);[14] see, *e.g.*, Minn. Stat. §§ 324M.01-.09 (forbidding ISPs from "knowingly disclos[ing] personally identifiable information concerning a consumer of the Internet service provider"). In addition, when the federal government recently decided to let ISPs release aggregate browsing data, the chairs of the FCC and FTC made a pointed effort to assure the public that their "individual browsing histor[ies]" would remain private. Ajit Pai & Maureen Ohlhausen, *No, Republicans Didn't Just Strip Away Your Internet Privacy Rights*, Wash. Post. (Apr. 4, 2017).[15]

* * *

This case presents a simple question: is society prepared to recognize as reasonable the expectation that browsing histories are private? The answer is plainly yes. See *Jones*, 565 U.S. at 418 (Sotomayor, J., concurring) ("I for one doubt 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."). "[T]he essential purpose of the Fourth Amendment [is] to shield the citizen from unwarranted intrusions into his privacy." *Payton* v. *New York*, 445 U.S. 573, 588 (1980) (quoting *Jones* v. *United States*, 357 U.S. 493, 497, 498 (1958)). Because browsing history searches are such intrusions, the investigators in this case should have done something "accordingly simple – get a warrant." *Riley*, 134 S. Ct. at 2473.

B. The court of appeals erred by applying the third-party doctrine to this case.

The Second Circuit found that there was no search. It did so without considering what details a browsing history contains or whether society views them as private. JA 29-36. Its

[14] https://perma.cc/TBY2-BR69.
[15] https://perma.cc/8S5W-Q6LX.

conclusion instead hinged on the single argument that Ulbricht waived his privacy interest in his browsing data by disclosing it to his ISP. JA 32-33.

Certainly, someone's expectation of privacy in information may be affected by whether he has disclosed it, and to whom. But it is not the *only* relevant issue. If it were, the Fourth Amendment would often be toothless in the modern world, where "people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks." *United States* v. *Jones*, 565 U.S. 400, 417 (2012) (Sotomayor, J., concurring). But "[n]o single factor determines whether an individual legitimately may claim [protection] under the Fourth Amendment." *Oliver* v. *United States*, 466 U.S. 170, 177 (1984). Under Fourth Amendment, disclosure to a third party is sometimes a waiver of privacy. But other times – including here – it is not.

1. The court of appeals relied primarily on *Smith* v. *Maryland*, 442 U.S. 735 (1979). *Smith* held that the defendant had no expectation of privacy in "information he voluntarily turn[ed] over to" a third party. *Id.* at 743-44. The Court has applied this reasoning, known as the third-party doctrine, to some cases but not to others.

Sometimes, a person loses his privacy interest in information by disclosing it to someone else. For example, in *Smith*, the government did not need a warrant to view which telephone numbers the defendant dialed. He had no expectation of privacy because he "voluntarily conveyed [the] information to the telephone company" by placing the call. *Id.* at 744. Similarly, in *United States* v. *Miller*, the defendant had no "legitimate expectation of privacy" in bank records because he "voluntarily conveyed [them] to the banks." 425 U.S. 435, 442 (1976). And in *United States* v. *White*, the defendant had no "legitimately protected" interest in information he "voluntarily confide[d]" to an undercover informant. 401 U.S. 745, 749 (1971).

But in many other contexts, a person who discloses information to a third party retains a reasonable expectation against further disclosure. For example, in *Ferguson* v. *City of Charleston*, the defendant had a "reasonable expectation" that the results of her medical tests would "not be shared with nonmedical personnel without her consent," despite having voluntarily provided that information to a hospital. 532 U.S. 67, 78 (2001). In *Kyllo* v. *United States*, the defendant had an "expectation of privacy" in the heat emissions from his home that any member of the public could theoretically observe. 533 U.S. 27, 33 (2001). And in *Georgia* v. *Randolph*, the police needed a warrant to search the home of someone who refused consent, even though he shared the space with an occupant who had consented. 547 U.S. 103, 122-23 (2006); see also *Minnesota* v. *Olson*, 495 U.S. 91, 99 (1990) (holding that houseguests "are entitled to a legitimate expectation of privacy" from the police merely because "hosts *will more likely than not* respect the privacy interests of their guests" (emphasis added)). *Ferguson*, *Kyllo*, and *Randolph* were each written over dissents noting that the majority's reasoning ignored the third-party doctrine case law. See *Ferguson*, 532 U.S. at 93-95 (Scalia, J., dissenting); *Kyllo*, 533 U.S. at 44 (Stevens, J., dissenting); *Randolph*, 547 U.S. at 131-33 (Roberts, C.J., dissenting). Thus, for certain categories of investigations, the third-party doctrine is not a per se rule.

2. For two independent reasons, Ulbricht's disclosures to his ISP are also not subject to the third-party doctrine. First, the third-party doctrine does not apply to content given to an intermediary. Second, it does not categorically apply to disclosures of digital data, and should not apply in this particular instance.

a. The third-party doctrine does not apply to communications transferred through an intermediary merely because the intermediary can access them. Otherwise, *Katz* itself would have to be overruled. There, the Court held that warrantless electronic surveillance of a telephone

conversation violated the Fourth Amendment. *Katz* v. *United States*, 389 U.S. 347, 348 (1967). But a "telephone conversation itself must be electronically transmitted by telephone company equipment, and may be recorded or overheard by the use of other company equipment." *Smith*, 442 U.S. at 746 (Stewart, J., dissenting). Yet Katz was "surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world." *Katz*, 389 U.S. at 352.

People who transmit content through other intermediaries are entitled to the same assumption. The Fourth Amendment protects letters placed in the mail, *Ex Parte Jackson*, 96 U.S. 727, 733 (1877), "despite the fact that sealed letters are handed over to perhaps dozens of mail carriers, any one of whom could tear open the thin paper envelopes that separate the private words from the world outside," *United States* v. *Warshak*, 631 F.3d 266, 285 (6th Cir. 2010). "Put another way, trusting a letter to an intermediary does not necessarily defeat a reasonable expectation that the letter will remain private." *Ibid.*

Emails receive the same protection. It "would defy common sense," *id.* at 285, to hold that emails are unprotected, even though services like Gmail collect and "analyze your *content* (*including emails*)." *Privacy Policy*, Google (emphasis added);[16] see also, *e.g.*, *United States* v. *Forrester*, 512 F.3d 500, 511 (9th Cir. 2008) ("The privacy interests in [mail and email] are identical."); *United States* v. *Maxwell*, 45 M.J. 406, 418 (C.A.A.F. 1996) ("[T]he transmitter of an e-mail message enjoys a reasonable expectation that police officials will not intercept the transmission without probable cause."). The Sixth Circuit recognized that the third-party doctrine would suggest a different result, but held that the doctrine did not apply because the ISP that conveyed the defendant's sensitive data "was an *intermediary*." *Warshak*, 631 F.3d at 288.

[16] https://perma.cc/AX92-WU8H. Google promises to share only "non-personally identifiable information" with others. *Ibid*. Ulbricht's ISP, Comcast, makes the same promise. JA 113.

ISPs are intermediaries not just for emails but for all web traffic. The content Ulbricht provided to his ISP is therefore just as protected as the content of his letters, phone conversations, and emails. Like the defendants in *Katz*, *Jackson*, and *Warshak*, people reasonably expect that their ISP will keep private the information it obtains about their life, from their political views to their household activities. Moreover, ISPs promise that they will do so. See *supra* I.A.3. Under *Katz*, Ulbricht was justified in relying on that promise.

b. The court of appeals rejected this reasoning because it mistakenly believed that *Smith* controlled. *Smith* recognized an exception to the intermediary rule for searches that "reveal the existence of connections between communications devices *without disclosing the content of the communications*." JA 33 (emphasis added). But subsequent cases have construed this exception narrowly. For example, although under *Smith* the police do not need a warrant to obtain a list of the numbers a phone has dialed, *Riley* v. *California* suggested that the result would be different if the search revealed even slightly more content, like "identifying information [for those numbers] * * * such as the label 'my house.'" 134 S. Ct. 2473, 2493 (2014).

Riley shows that the information revealed by a dialing history comes close to the constitutional line between non-content covered by the third-party doctrine and content. Browsing history data blows past that line. It reveals not only the device someone was communicating with, but also the *content* of that communication. This is because phones and the internet are structured differently. Unlike a connection between two phones, one end of a computer-website connection is public. Thus, the existence of the connection *is* the content. Once investigators know what website someone visited, they can go to the public website and see for themselves precisely what the person read or posted on that website.

As a result, browsing histories are orders of magnitude more precise than dialing histories. While a dialing history might indicate that an individual spoke anonymously with a reporter about something, a browsing history can reveal the exact text of an anonymous web post. A dialing history may reveal that someone called up a pharmacy to order a drug or a therapist to discuss a mental health concern, but a browsing history may reveal which drug and which concern. And there is no telephonic equivalent to information about how much time someone spends consuming social media or uses his internet-enabled refrigerator. The gulf between the information revealed by dialing and browsing histories continues to increase. The average adult cell phone owner spends over six hours a day on the internet but places or receives just five calls. Amanda Lenhart, *Cell Phones and American Adults*, Pew Res. Ctr. (Sept. 2, 2010).[17]

Given how different they are, analogizing between phone numbers and IP addresses would be the sort of "mechanical interpretation of the Fourth Amendment" that the Court has repeatedly rejected in the face of "advancing technology." *Kyllo* v. *United States*, 533 U.S. 27, 35 (2001). In fact, a more technologically advanced investigation is often a search even if it superficially resembles a less intrusive non-search. For example, using a thermal imager on a house may be a search, even though using a "sensitive thermometer" or "observing snowmelt on the roof" are not. *Id.* at 35 n.2; *id.* at 43 (Stevens, J., dissenting). Similarly, a warrantless cellphone search incident to arrest is unconstitutional even though the police do not need a warrant to view "a highly personal item such as a diary," "photograph," or "bank statement" on an arrestee's person. *Riley*, 134 S. Ct. 2473 at 2490. Because physical items might show up only in "the occasional case," a search of them is "quite different" than a cellphone search. *Id.* at

[17] https://perma.cc/K23C-5BP8.

2493. Similarly, in *Jones*, Justice Alito suggested that although in-person surveillance of a car and a GPS tracker revealed the same information, only the latter was a search because it made "long-term monitoring relatively easy and cheap." 565 U.S. at 429 (Alito, J., concurring, joined by Ginsburg, Breyer, and Kagan, JJ.).

IP addresses are to phone numbers as a heat scanner is to a thermometer, a GPS is to visual tracking of a car, and a cellphone search is to occasionally coming across someone's diary. "Both are ways of getting from point A to point B, but little else justifies lumping them together." *Riley*, 134 S. Ct. at 2488. The websites someone has visited reveal substantially more than the numbers he has called. They are more like the content of the call. Just as it was reasonable for Katz to expect that his phone call would be private, it was reasonable for Ulbricht to expect that his sensitive browsing information would be disseminated no further. Searching it without a warrant violated the Fourth Amendment.

3. Even if this case did not fall under well-established case law exempting disclosure to intermediaries from the third-party doctrine, the doctrine would still not apply here. It is inappropriate to categorically apply the doctrine to disclosures of digital information, and this particular disclosure did not eliminate Ulbricht's expectation of privacy.

"Categorical rules reflect broad generalizations holding true in so many cases that inquiry into whether they apply to the case at hand would be needless and wasteful. However, when the generalizations fail to hold in the run of cases,* * * the justification for the categorical rule disappears." *Ragsdale* v. *Wolverine World Wide, Inc.*, 535 U.S. 81, 82 (2002). Here, a categorical rule would be unjustified. "[T]he ultimate touchstone of the Fourth Amendment is 'reasonableness.'" *Riley*, 134 S.Ct. at 2482 (internal citation and quotation marks omitted). When an unreasonable search would be constitutional according to the third-party doctrine, the doctrine

– not the amendment – must give. Therefore, it is only appropriate to apply the third-party doctrine categorically if it always or almost always accords with society's understanding of privacy.

But when applied to disclosures of digital information, the doctrine frequently leads to the wrong result. One example, as a majority of the Court suggested in *Jones*, is digital location data. In one opinion, four Justices declined to apply the third-party doctrine to such data. 565 U.S. at 418 (Alito, J., concurring, joined by Ginsburg, Breyer, and Kagan, JJ.). This was necessary to their conclusion that using a GPS to track a car on public streets could be a search. Under traditional case law, a car's location was not private because the driver "voluntarily conveyed [it] to anyone who wanted to look." *United States* v. *Knotts*, 460 U.S. 276, 281 (1983). But the Justices believed that digital advances undermined *Knotts*'s rationale. Whereas "[i]n the pre-computer age, the greatest protections of privacy were * * * practical," GPS technology enables "law enforcement agents and others * * * [to] secretly monitor and catalogue every single movement of an individual's car for a very long period." *Jones*, 565 U.S. at 429-30 (Alito, J., concurring). Thus, they concluded, location data should be protected when it is disclosed digitally, even if it is otherwise unprotected. Meanwhile, in another opinion in the same case, Justice Sotomayor addressed the third-party doctrine more broadly, noting that it is "ill suited to the digital age." 565 U.S. at 417 (Sotomayor, J., concurring).

Location data is not the only type of digital information in which society understands there to be a privacy interest even after disclosure. Today, "there is no meaningful choice * * * as to whether or not a digital footprint is created as we go about our daily lives." Laura Donohue, *The Fourth Amendment in a Digital World*, 71 N.Y.U. Ann. Surv. Am. L. 533, 647 (2017). As a result, people must regularly disclose information to online service providers: "the phone

numbers that they dial or text to their cellular providers; the URLs that they visit and the e-mail addresses with which they correspond to their Internet service providers; and the books, groceries, and medications they purchase to online retailers." *Jones*, 565 U.S. at 417 (Sotomayor, J., concurring). Yet a majority of Americans still believe that information like their emails, text messages, web searches, and location should be considered private.[18] "A *per se* rule that it is unreasonable to expect privacy in information voluntarily disclosed to third parties seems unmoored from current understandings of privacy. *United States* v. *Graham*, 824 F.3d 421, 437 (4th Cir. 2016) (en banc).

Because the third-party doctrine suits the digital age poorly, the Court should directly apply the "reasonable expectation of privacy" test to digital disclosures rather than use the doctrine as a proxy. This test can still account for whether the person transmitted the information to a third party, but it will appropriately treat it as one factor among many. Here, for the reasons explained in Part I.A., Ulbricht's disclosure did not terminate his privacy interest in the information.

"While the desire for a bright-line rule is understandable, the Fourth Amendment will not tolerate adoption of an overly broad categorical approach that would dilute the warrant requirement in a context where significant privacy interests are at stake." *Missouri* v. *McNeely*, 569 U.S. 141, 158 (2013) (plurality opinion). The fiction that someone renounces any private interest in a fact once he discloses it to someone else would be "as easy of application as it would be deficient in efficacy and power." *Miranda* v. *Arizona*, 384 U.S. 436, 443 (1966) (quoting *Weems* v. *United States*, 217 U.S. 349, 373 (1910)). It would "allow[] the government to know from YouTube.com what we watch, or Facebook.com what we post or whom we 'friend,' or

[18] Pew, *supra* note 10.

Amazon.com what we buy, or Wikipedia.com what we research, or Match.com whom we date – all without a warrant." *United States* v. *Davis,* 785 F.3d 498, 536 (11th Cir. 2015) (Martin, J., dissenting). This result would leave Americans "at the mercy of advancing technology," *Kyllo*, 533 U.S. at 35, and the Court should reject it.

C. The Court should remand to allow the district court to determine the remedy in the first instance.

"All evidence obtained by an unconstitutional search and seizure [i]s inadmissible in a federal court regardless of its source." *Mapp* v. *Ohio*, 367 U.S. 643, 654 (1961). Once a search is found unlawful, "the trial judge must give opportunity, however closely confined, to the accused to prove that a substantial portion of the case against him was a fruit of the poisonous tree." *Nardone* v. *United States*, 308 U.S. 338, 341 (1939). Because the district court incorrectly determined that there was no search, JA 141, Ulbricht never had that opportunity. The Court should therefore reverse the opinion below so that the district court can determine in the first instance what evidence should have been suppressed from the trial.

II. Under the Sixth Amendment, the sentencing judge was not permitted to find facts necessary to support Ulbricht's otherwise unreasonable sentence.

The Sixth Amendment guarantees defendants the right to have a jury determine "*the truth of every accusation*" against them. *Apprendi* v. *New Jersey*, 530 U.S. 466, 477 (2000) (quoting 4 William Blackstone, Commentaries on the Laws of England 343 (1769)). As this Court has repeatedly affirmed, that right would be meaningless if it extended just to a determination of guilt or innocence. It must also apply to any fact that increases the allowable penalty. *Id*. at 466. Because courts may not impose unreasonable sentences, *Gall* v. *United States*, 552 U.S. 38, 50-

51 (2007), a fact that is necessary to make a sentence reasonable is one that increases the allowable penalty. Such a fact must therefore be found by the jury.

A. The Sixth Amendment guarantees the right to a jury determination of any fact that increases the allowable sentence.

The right to trial by jury was enshrined in the Constitution to protect against "arbitrary punishments upon arbitrary convictions." *Booker*, 543 U.S. at 238 (quoting The Federalist No. 83, at 499 (Charles Rossiter ed. 1961) (Alexander Hamilton)); see U.S. Const. amend. VI. The "jury tradition" has thus been "an indispensable part of our criminal justice system" since the founding. *Apprendi*, 530 U.S. at 497. If "there is any difference" of opinion among attendees of the Constitutional Convention about the value of the jury trial, Alexander Hamilton wrote, some of them "regard it as a valuable safeguard to liberty," while others "represent it as the very palladium of free government." The Federalist No. 83, at 456 (Alexander Hamilton) (Gaunt, Inc. ed., 2003).

Today, the Sixth Amendment right to a jury trial continues to promote "fairness and reliability" in sentencing. *Booker*, 543 U.S. at 244. A jury protects the accused from the "possibility of oppression by the Government," *Baldwin* v. *New York*, 399 U.S. 66, 72 (1970), by standing between the defendant and "unfounded criminal charges," "corrupt or overzealous prosecutor[s]," and "compliant, biased, or eccentric judge[s]." *Duncan* v. *Louisiana*, 391 U.S. 145, 156 (1968). A jury is therefore "the grand bulwark" of liberty that ensures "other liberties * * * remain secure." *Jones* v. *United States*, 526 U.S. 227, 246 (1999) (quoting 4 William Blackstone, Commentaries on the Laws of England 342 (1769)).

For the jury to serve this role effectively, the Sixth Amendment has long "been understood to require that '*the truth of every accusation* * * * should afterwards be confirmed by the unanimous suffrage of twelve of [the defendant's] equals.'" *Apprendi*, 530 U.S. at 477

(quoting 4 William Blackstone, Commentaries on the Laws of England 343 (1769)). Hence, the right extends not just to the guilt or innocence of a defendant, but also to "all the facts and circumstances which constitute the offence." *Id*. at 478 (quoting J. Archbold, Pleading and Evidence in Criminal Cases 44 (15th ed. 1862)). This way, "there may be no doubt as to the judgment which should be given" if he is convicted. *Ibid.* It follows that every criminal defendant has "the right to demand that a jury find him guilty of all the elements of the crime with which he is charged." *United States* v. *Gaudin*, 515 U.S. 506, 511 (1995).

But if that were *all* the right meant, it would be impotent. This is because modern legislatures define both the elements of a crime and additional sentencing factors. A "sentencing factor * * * comes into play only after the defendant has been found guilty of [a crime] beyond a reasonable doubt." *McMillan* v. *Pennsylvania*, 477 U.S. 79, 86 (1986). It is a "fact that was not found by a jury" but that can still "affect the sentence imposed by the judge." *Apprendi,* 530 U.S. at 485. It would be "absurd" if the "jury need only find whatever facts the legislature chooses to label elements of the crime," but "those it labels sentencing factors – no matter how much they may increase the punishment – may be found by the judge." *Blakely* v. *Washington*, 542 U.S. 296, 306 (2004). In such a system, "a judge could sentence a man for committing murder even if the jury convicted him only of illegally possessing the firearm used to commit it – or of making an illegal lane change while fleeing the death scene." *Ibid*.

The Sixth Amendment sees through that ploy. As the Court noted in *Apprendi*, there is a "historic link between verdict and judgment." 530 U.S. at 482. Legislatures may not impose a "scheme that removes the jury from the determination of a fact that, if found, exposes the criminal defendant to a penalty *exceeding* the maximum he could receive if punished according to the facts reflected in the jury verdict alone." *Id*. at 482-83. It makes no difference if the fact is

labeled an "element" or a "sentencing factor" because any fact that authorizes "an increase beyond the maximum authorized statutory sentence" "is the functional equivalent of an element of a greater offense than the one covered by the jury's guilty verdict." *Id*. at 494 n.19. "When a judge's finding based on a mere preponderance of the evidence authorizes an increase in the maximum punishment, it is appropriately characterized as 'a tail which wags the dog of the substantive offense.'" *Id*. at 495 (quoting *McMillan*, 477 U.S. at 88). *Apprendi* thus announced the "bright line rule," *Cunningham* v. *California*, 549 U.S. 270, 288 (2007), that "any fact that increases the penalty for a crime beyond the prescribed statutory maximum must be submitted to a jury." *Apprendi*, 530 U.S. at 490; see also *Cunningham*, 549 U.S. at 274 (invalidating a California law that permitted judges to impose a higher sentence based on facts not "inherent in the jury's verdict").

Apprendi's logic has been extended to facts beyond those that increase the length of prison sentences. For example, the jury must find facts that increase the statutory maximum criminal fine that may be imposed. *Southern Union Co.* v. *United States*, 567 U.S. 343, 346 (2012). And in *Ring* v. *Arizona*, the Court found that "a sentencing judge[] sitting without a jury [may not] find an aggravating circumstance necessary for imposition of the death penalty." 536 U.S. 584, 609 (2002); see also *Hurst* v. *Florida*, 136 S. Ct. 616, 622 (2016) (holding that Florida's capital sentencing scheme violated the Sixth Amendment because it did "not make a defendant eligible for death until findings *by the court* that such person shall be punished by death" (internal quotation marks omitted)). *Ring* rested on the same principle as *Apprendi*: "[i]f a State makes an increase in a defendant's authorized punishment contingent on the finding of a fact, that fact – no matter how the State labels it – must be found by a jury beyond a reasonable

doubt." *Ring*, 536 U.S. at 602. The Court applied *Apprendi* to the Arizona statute even though it required overruling *Walton* v. *Arizona*, 497 U.S. 639 (1990).

The Sixth Amendment right at issue in *Apprendi* applies to mandatory sentencing guidelines just as it applies to statutory maximum penalties. *Blakely*, 542 U.S. at 305. The state sentencing scheme in Washington specified both a "statutory maximum" for a class of felonies and a "standard range" for particular felonies within that class. *Id*. at 303. The law permitted judges to sentence above the standard range, but below the statutory maximum, if they found certain facts. *Ibid*. Washington argued that its rule satisfied *Apprendi*, as the judge did not find facts that put a sentence over the "statutory maximum." *Ibid*. But as the Court explained, simply manipulating what is termed the "statutory maximum" would not be enough to skirt the Sixth Amendment. "[T]he 'statutory maximum' for *Apprendi* purposes is the maximum sentence a judge may impose *solely on the basis of the facts reflected in the jury verdict or admitted by the defendant.*" *Ibid*. Thus, "the relevant 'statutory maximum' is not the maximum sentence a judge may impose after finding additional facts, but the maximum he may impose *without* any additional findings." *Id*. at 303-04.

The next year, the Court overturned a portion of the Federal Sentencing Guidelines for the same reason. At that time, the Guidelines specified a mandatory sentencing range given a certain jury verdict. *United States* v. *Booker*, 543 U.S. 220, 233 (2005). However, the mandatory range could be increased by a judge who found certain facts. *Id*. at 233-34. Thus, there was "no distinction of constitutional significance between the Federal Sentencing Guidelines and the Washington procedures at issue in [*Blakely*]," *id.* at 233, and the guidelines could no longer be mandatory, *id.* at 245. Once again, the Court reiterated *Apprendi*: the Sixth Amendment right "is implicated whenever a judge seeks to impose a sentence that is not solely based on 'facts

reflected in the jury verdict or admitted by the defendant.'" *Id*. at 232 (quoting *Blakely*, 542 U.S. at 303).

The Sixth Amendment right to a jury trial even applies to any fact that increases a mandatory *minimum* sentence. *Alleyne* v. *United States*, 570 U.S. 99, 107 (2013). In *Alleyne*, the Court found that any such fact must go to a jury, as "[e]levating the low-end of a sentencing range heightens the loss of liberty associated with the crime." *Id*. at 113. This is so even if the "defendant could have received the same sentence with or without that fact." *Id*. at 115. Like *Ring*, this decision required overruling a previous opinion, *Harris* v. *United States*, 536 U.S. 545 (2002).

* * *

There are many ways a fact might convert an invalid punishment into a valid punishment, and the Court has consistently reiterated that judges may not find such facts. A judge may not find a fact that increases the allowable maximum penalty, whether it increases the length of a prison term, *Apprendi*, 530 U.S. 466; *Blakely*, 542 U.S. 296; *Cunningham*, 549 U.S. 270, or the size of a fine, *Southern Union Co.*, 567 U.S. 343. He may not find a fact that allows him to impose a new type of penalty. *Ring*, 536 U.S. 584; *Hurst*, 136 S. Ct. 616. He may not even find a fact that removes his discretion to impose a lower penalty. *Alleyne*, 570 U.S. 99. Since *Apprendi*, the Court has not wavered: any fact that increases the permissible penalty must be submitted to a jury.

B. A fact that converts a penalty from reasonable to unreasonable increases the allowable sentence and must therefore be found by a jury.

This case concerns yet another way in which a fact may make a harsher punishment permissible: by turning an unreasonable sentence into a reasonable one.

1. Just as courts may not impose sentences above the statutory maximum penalty, they may not impose unreasonable sentences. *Gall* v. *United States*, 552 U.S. 38, 50-51 (2007). In *United States* v. *Booker*, the Court held that the Sentencing Reform Act implicitly requires sentences to be reasonable, and subjects them to appellate "review for unreasonableness." 543 U.S. 220, 260-61 (2005) (internal quotation marks and citations omitted). A reviewing court must "take into account the totality of the circumstances," *Gall*, 552 U.S. at 51, and if it finds a sentence to be unreasonable, it must "correct such mistakes." *Rita* v. *United States*, 551 U.S. 338, 354 (2007).

The reasonableness inquiry is not a mere formality. Nearly fifteen percent of federal sentences challenged as substantively unreasonable are reversed or remanded. U.S. Sentencing Comm'n, *2015 Sourcebook of Federal Sentencing Guidelines*, Table 59*:* Sentencing Issues Appealed for Reasonableness Issues, Fiscal Year 2015.[19] Examples from the Second Circuit include *United States* v. *Jenkins*, 854 F.3d 181 (2d Cir. 2017) (225-month sentence followed by 25 years of supervised release for the possession and transportation of child pornography); *United States* v. *Singh*, 877 F.3d 107 (2d Cir. 2017) (60-month sentence for illegally reentering the United States after being removed); and *United States* v. *Sawyer*, 672 Fed. App'x 63 (2d Cir. 2016) (30-year sentence for production and receipt of child pornography). Even sentences within the recommended Guidelines range may be substantively unreasonable. See, *e.g.*, *United States* v. *Dorvee*, 616 F.3d 174 (2d Cir. 2010) (240-month sentence for distribution of child pornography).

Since an unreasonable sentence is impermissible, judges should not be permitted to find the facts necessary to support an otherwise unreasonable sentence. "[T]he 'statutory maximum'

[19] https://perma.cc/Q4JQ-DWA8.

for *Apprendi* purposes is the maximum sentence a judge may impose *solely on the basis of the facts reflected in the jury verdict or admitted by the defendant.*" *Blakely* v. *Washington*, 542 U.S. 296, 303 (2004). In other words, the Sixth Amendment "guarantee[s] a jury's finding of any disputed fact essential to increase the ceiling of a potential sentence." *Shepard* v. *United States*, 544 U.S. 13, 25 (2005).

It "unavoidably follows that any fact necessary to prevent a sentence from being substantively unreasonable – thereby exposing the defendant to the longer sentence – is an element that must be either admitted by the defendant or found by the jury. It *may not* be found by a judge." *Jones* v. *United States*, 135 S. Ct. 8, 8 (2014) (Scalia, J., dissenting from denial of certiorari, joined by Thomas and Ginsburg, JJ.). Thus, "for every given crime there is some maximum sentence that will be upheld as reasonable based only on the facts found by the jury or admitted by the defendant. *Every* sentence higher than that is legally authorized only by some judge-found fact[] in violation of the Sixth Amendment." *Rita*, 551 U.S. at 372 (Scalia, J., concurring, joined by Thomas, J.).

2. The contrary rule would reopen the loophole that the Court's post-*Apprendi* cases were written to eliminate. In those cases, the Court recognized that allowing judges to increase the permissible penalty by finding new facts would allow a defendant to be convicted of one crime by the jury, but punished for another by the judge. For instance, in *Apprendi* itself, the defendant was convicted of possession of a firearm, but punished for committing a hate crime based on facts found by the judge. *Apprendi* v. *New Jersey*, 530 U.S. 466, 470-71 (2000).

To guard against this, "[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." *Alleyne v. United States*, 570 U.S. 99, 114-15 (2013) (emphasis added).

But manipulating this rule remains possible if judges are permitted to find the facts necessary to support an otherwise unreasonable sentence:

> For example, the base offense level for robbery under the Guidelines is 20, which [for a first-time offender] corresponds to an advisory range of 33–41 months. If, however, a judge finds that a firearm was discharged, that a victim incurred serious bodily injury, and that more than $5 million was stolen, then the base level jumps by 18, producing an advisory range of 235–293 months. When a judge finds all of those facts to be true and then imposes a within-Guidelines sentence of 293 months, those judge-found facts, or some combination of them, are not merely facts that the judge finds relevant in exercising his discretion; they are the legally essential predicate for his imposition of the 293–month sentence. His failure to find them would render the 293–month sentence unlawful * * * because, were the district judge explicitly to find *none* of those facts true * * * the sentence would surely be reversed as unreasonably excessive.

Rita, 551 U.S. at 371-73 (Scalia, J., concurring) (internal citations omitted). This hypothetical is troubling because the defendant was functionally punished for crimes that he was never convicted of.

The same concern infects this case. Ulbricht's Group One counts included distribution of narcotics by means of the internet, continuing criminal enterprise, and conspiracy to commit money laundering. ST 17. These are not the sort of "egregious violent crimes" for which life sentences are "typically reserved." JA 106. However, the district judge made findings of fact that converted Ulbricht's offenses into far more egregious crimes. She found that Ulbricht commissioned murders, ST 18-19, and that his actions led to several drug-related deaths, ST 26.

But Ulbricht was never convicted of these crimes. And a jury that considered Ulbricht's contentions that "the records associated with the six deaths were substantially incomplete" and that it was "difficult to discern the precise cause of death to a reasonable degree of medical certainty," JA 88-89, may have reached the conclusion that he was not guilty of causing the drug-related deaths. Similarly, "there is no evidence that any of the murders actually occurred," and there is conflicting evidence of whether Ulbricht intended them to be carried out. JA 17, 26.

Ulbricht's life sentence very well may have been for these crimes, found only by a judge. See *infra*, Section II.C. But if the government was unwilling even to charge the commissioned murders, JA 17 n.15, or put "the circumstantial evidence" connecting the drug-related deaths to Silk Road before a jury, JA 90, it should not still reap the benefits of having these crimes considered at the sentencing proceeding. This is the core holding of *Apprendi* and its progeny: a defendant may not be subjected to a system where he "routinely see[s] his maximum potential sentence balloon * * * based not on facts proved to his peers beyond a reasonable doubt," but on facts found by the judge. *Blakely*, 542 U.S. at 311-12. Yet that is what happened here.

A consequence of the government's position is that a defendant may be *acquitted* of a crime, but still have that crime used against him in sentencing – even if that crime is essential for the sentence to be reasonable. This has happened. For example, in *United States* v. *Jones*, 744 F.3d 1362 (D.C. Cir. 2014), the jury had convicted the petitioners of distributing drugs, but acquitted them of conspiring to do so. *Id*. at 1365-66. Despite the acquittal, the sentencing judge found that they had engaged in a conspiracy, and enhanced their sentence on that basis. *Ibid*. Under the government's position, this outcome was permissible "*even if* their sentences would have been substantively unreasonable but for judge-found facts." *Jones*, 135 S. Ct. at 9 (Scalia, J., dissenting from denial of certiorari, joined by Thomas and Ginsburg, JJ.). If the Court sanctions the government's approach, this will continue to happen, and the jury will cease to serve its historical role "as an intermediary between the State and criminal defendants." *Alleyne*, 570 U.S. at 114.

It is true that under *United States* v. *Watts*, a sentencing court may consider acquitted conduct in sentencing. 519 U.S. 148 (1997). But after *Apprendi*, courts may consider acquitted conduct only "[s]o long as the defendant receives a sentence at or below the statutory ceiling set

by the jury's verdict." *United States* v. *White*, 551 F.3d 381, 385 (6th Cir. 2008). Similarly, a court should only be permitted to consider acquitted conduct as long as the sentence it imposes would be reasonable even absent that conduct. If courts treated acquitted conduct necessary to make a sentence reasonable differently than acquitted conduct necessary to increase a statutory maximum, it would imply that an unreasonable sentence is different than a statutorily-barred one. But that is not so. Both are illegal, and allowing the judge to find facts that support either would contravene the Sixth Amendment's command that "the judge's authority to sentence derives wholly from the jury's verdict." *Blakely*, 542 U.S. at 306.

3. Holding that judges may not find facts supporting an otherwise unreasonable sentence would limit their discretion. But it would only do so in the same sense that *Apprendi* and its progeny already have: "to the extent that [it] infringes on the province of the jury." *Blakely*, 542 U.S. at 308. It would remain true that "when a trial judge exercises his discretion to select a specific sentence within a defined range, the defendant has no right to a jury determination of the facts that the judge deems relevant." *Booker*, 543 U.S. at 233. This is because the requirement that a sentence be reasonable, like the requirement that a sentence be below the statutory maximum, defines the range of acceptable punishments. Judges may still find facts to help them determine an appropriate sentence within that range.

Limiting judicial discretion to this degree is essential to vindicating the Sixth Amendment right to a jury trial. Without such a restriction, "the jury would not exercise the control that the Framers intended," *Blakely*, 542 U.S. at 306, and would not be able to play its historical role "as an intermediary between the State and criminal defendants," *Alleyne*, 570 U.S. at 114. Thus, judges would retain their sentencing discretion, as long as that discretion is exercised within the bounds of reasonableness.

C. The Court should remand so the court of appeals can determine whether Ulbricht's sentence was unreasonable in light of the facts found only by the jury.

Based on the jury verdict alone, the Federal Sentencing Guidelines recommend that Ulbricht be sentenced to a prison term of 292 to 365 months. Pet. App. 6a. But the district judge sentenced him to a much harsher term: life imprisonment. "A life sentence is the second most severe penalty that may be imposed in the federal criminal justice system." JA 107. It is "particularly severe because * * * Ulbricht will never be eligible for parole." JA 107 n.73. There will be "no automatic reconsideration of this sentence, or of whether he has reformed," even though as "a young offender, [he] will all but certainly change." *Ibid*. This sentence is even higher than the median Second Circuit sentence for murder: 10.5 years. U.S. Sentencing Comm'n, *Statistical Information Packet, Second Circuit*, Table 7.[20]

Because the Second Circuit rejected the argument that judges cannot find the facts necessary to support an otherwise unreasonable sentence, JA 106-07 n.72, it has not yet decided whether the sentence would have been reasonable in light of only the facts found by the jury. But if it had addressed the issue, it would have likely found the sentence to be unreasonable.

"[E]ven though the Guidelines are advisory rather than mandatory, they are * * * the product of careful study based on extensive empirical evidence derived from the review of thousands of individual sentencing decisions." *Gall* v. *United States*, 552 U.S. 38, 46 (2007); see also *Rita* v. *United States*, 551 U.S. 338, 350 (2007) (noting that the Sentencing Commission "may obtain advice from prosecutors, defenders, law enforcement groups, civil liberties associations, experts in penology, and others" and "revise the Guidelines accordingly"). It is "uncontroversial that a major departure [from the Guidelines range] should be supported by a more significant justification than a minor one." *Gall*, 552 U.S. at 50. A "number of Circuits

[20] https://perma.cc/MU9L-MN9Y.

adhere to the proposition that the strength of the justification needed to sustain an outside-Guidelines sentence varies in proportion to the degree of the variance." *Rita*, 551 U.S. at 355. The Second Circuit is one of them. See *United States* v. *Bowles*, 260 Fed. App'x 367, 368 (2nd Cir. 2008) ("For an 'outside-Guidelines sentence' the district court 'must consider the extent of the deviation and ensure that the justification is sufficiently compelling to support the degree of the variance.'" (quoting *Gall*, 552 U.S. at 38)). Because a life sentence "should be" "extraordinary and infrequent," JA 107, and because the sentence imposed here is far outside the range recommended by the Guidelines for the crimes the jury found, the court of appeals would have required a remarkably persuasive justification for it.

The severity and sheer number of the district judge's findings make it likely that those findings, rather than the facts found by the jury, supplied that justification in this case. Most importantly, the jury did not find Ulbricht guilty of any attempted murders. It was the sentencing judge who alone found this fact by a preponderance of the evidence. ST 18-19. But that was far from all she found. She also found that Ulbricht distributed a controlled substance through mass marketing by means of an interactive computer service, ST 20; maintained premises for the purpose of manufacturing a controlled substance, ST 21; imported methamphetamine, ST 21; played a leading role in the money laundering conspiracy, ST 22; and was responsible for several drug-related deaths, ST 26.

Taking into account these grave and inflammatory charges likely had a large effect on the Second Circuit's reasonableness determination. Its opinion suggests as much. While it mentioned several factors as justifying the sentence's reasonableness, it devoted substantial time to discussing the attempted murder charges. JA 95, 100-102, 104, 107; see also Statement of Facts, *supra*. It even expressly noted that "[c]ommissioning the murders significantly justified the life

sentence." JA 101 n.68; see also JA 107 ("Each case must be considered on its own facts and in light of * * * [the] relevant conduct, which, in this case, includes five attempted murders for hire.").

This Court need not decide the issue in the first instance. Because there is a serious risk that the life sentence would not be reasonable in light of only the facts found by the jury, the Court should remand so that the Second Circuit can address the question. Only this will assure that Ulbricht's "right to demand that a jury find him guilty of all the elements of the crime" is protected. *United States* v. *Gaudin*, 515 U.S. 506, 511 (1995). The district court has the unenviable "power to condemn a young man to die in prison." JA 108. This Court must ensure that this power is exercised in a manner consistent with the Constitution.

CONCLUSION

The judgment of the court of appeals should be reversed on both questions presented.

Respectfully submitted.

ERIC BROOKS
MEGHA RAM

Counsel for Petitioner

APRIL 2018

APPENDIX

The Electronic Communications Privacy Act provides, in relevant part:

18 U.S.C. § 3121

> (a) In general.--Except as provided in this section, no person may install or use a pen register or a trap and trace device without first obtaining a court order under section 3123 of this title or under the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.).
> (b) Exception.--The prohibition of subsection (a) does not apply with respect to the use of a pen register or a trap and trace device by a provider of electronic or wire communication service--
>
> > (1) relating to the operation, maintenance, and testing of a wire or electronic communication service or to the protection of the rights or property of such provider, or to the protection of users of that service from abuse of service or unlawful use of service; or
> > (2) to record the fact that a wire or electronic communication was initiated or completed in order to protect such provider, another provider furnishing service toward the completion of the wire communication, or a user of that service, from fraudulent, unlawful or abusive use of service; or
> > (3) where the consent of the user of that service has been obtained.
>
> (c) Limitation.--A government agency authorized to install and use a pen register or trap and trace device under this chapter or under State law shall use technology reasonably available to it that restricts the recording or decoding of electronic or other impulses to the dialing, routing, addressing, and signaling information utilized in the processing and transmitting of wire or electronic communications so as not to include the contents of any wire or electronic communications.
> (d) Penalty.--Whoever knowingly violates subsection (a) shall be fined under this title or imprisoned not more than one year, or both.

§ 3122

(a) Application.

> (1) An attorney for the Government may make application for an order or an extension of an order under section 3123 of this title authorizing or approving the installation and use of a pen register or a trap and trace device under this chapter, in writing under oath or equivalent affirmation, to a court of competent jurisdiction.
> (2) Unless prohibited by State law, a State investigative or law enforcement officer may make application for an order or an extension of an order under section 3123 of this title authorizing or approving the installation and use of a pen register or a trap and trace device under this chapter, in writing under oath or equivalent affirmation, to a court of competent jurisdiction of such State.

(b) Contents of application.--An application under subsection (a) of this section shall include--

(1) the identity of the attorney for the Government or the State law enforcement or investigative officer making the application and the identity of the law enforcement agency conducting the investigation; and
(2) a certification by the applicant that the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by that agency.

§ 3123

(a) In general.--

(1) Attorney for the Government.--Upon an application made under section 3122(a)(1), the court shall enter an ex parte order authorizing the installation and use of a pen register or trap and trace device anywhere within the United States, if the court finds that the attorney for the Government has certified to the court that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation. The order, upon service of that order, shall apply to any person or entity providing wire or electronic communication service in the United States whose assistance may facilitate the execution of the order. Whenever such an order is served on any person or entity not specifically named in the order, upon request of such person or entity, the attorney for the Government or law enforcement or investigative officer that is serving the order shall provide written or electronic certification that the order applies to the person or entity being served.
(2) State investigative or law enforcement officer.--Upon an application made under section 3122(a)(2), the court shall enter an ex parte order authorizing the installation and use of a pen register or trap and trace device within the jurisdiction of the court, if the court finds that the State law enforcement or investigative officer has certified to the court that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation.
(3)

(A) Where the law enforcement agency implementing an ex parte order under this subsection seeks to do so by installing and using its own pen register or trap and trace device on a packet-switched data network of a provider of electronic communication service to the public, the agency shall ensure that a record will be maintained which will identify--

(i) any officer or officers who installed the device and any officer or officers who accessed the device to obtain information from the network;
(ii) the date and time the device was installed, the date and time the device was uninstalled, and the date, time, and duration of each time the device is accessed to obtain information;
(iii) the configuration of the device at the time of its installation and any subsequent modification thereof; and
(iv) any information which has been collected by the device.

To the extent that the pen register or trap and trace device can be set automatically to record this information electronically, the record shall be maintained electronically throughout the installation and use of such device.

(B) The record maintained under subparagraph (A) shall be provided ex parte and under seal to the court which entered the ex parte order authorizing the installation and use of the device within 30 days after termination of the order (including any extensions thereof).

(b) Contents of order.--An order issued under this section--

(1) shall specify--

(A) the identity, if known, of the person to whom is leased or in whose name is listed the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied;

(B) the identity, if known, of the person who is the subject of the criminal investigation;

(C) the attributes of the communications to which the order applies, including the number or other identifier and, if known, the location of the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied, and, in the case of an order authorizing installation and use of a trap and trace device under subsection (a)(2), the geographic limits of the order; and

(D) a statement of the offense to which the information likely to be obtained by the pen register or trap and trace device relates; and

(2) shall direct, upon the request of the applicant, the furnishing of information, facilities, and technical assistance necessary to accomplish the installation of the pen register or trap and trace device under section 3124 of this title.

(c) Time period and extensions.—

(1) An order issued under this section shall authorize the installation and use of a pen register or a trap and trace device for a period not to exceed sixty days.

(2) Extensions of such an order may be granted, but only upon an application for an order under section 3122 of this title and upon the judicial finding required by subsection (a) of this section. The period of extension shall be for a period not to exceed sixty days.

(d) Nondisclosure of existence of pen register or a trap and trace device.--An order authorizing or approving the installation and use of a pen register or a trap and trace device shall direct that--

(1) the order be sealed until otherwise ordered by the court; and

(2) the person owning or leasing the line or other facility to which the pen register or a trap and trace device is attached or applied, or who is obligated by the order to provide assistance to the applicant, not disclose the existence of the pen register or trap and trace device or the existence of the investigation to the listed subscriber, or to any other person, unless or until otherwise ordered by the court.

* * *

(a) Notwithstanding any other provision of this chapter, any investigative or law enforcement officer, specially designated by the Attorney General, the Deputy Attorney General, the Associate Attorney General, any Assistant Attorney General, any acting Assistant Attorney General, or any Deputy Assistant Attorney General, or by the principal prosecuting attorney of any State or subdivision thereof acting pursuant to a statute of that State, who reasonably determines that--

(1) an emergency situation exists that involves--

(A) immediate danger of death or serious bodily injury to any person;

(B) conspiratorial activities characteristic of organized crime;

(C) an immediate threat to a national security interest; or

(D) an ongoing attack on a protected computer (as defined in section 1030) that constitutes a crime punishable by a term of imprisonment greater than one year;

that requires the installation and use of a pen register or a trap and trace device before an order authorizing such installation and use can, with due diligence, be obtained, and

(2) there are grounds upon which an order could be entered under this chapter to authorize such installation and use; may have installed and use a pen register or trap and trace device if, within forty-eight hours after the installation has occurred, or begins to occur, an order approving the installation or use is issued in accordance with section 3123 of this title.

(b) In the absence of an authorizing order, such use shall immediately terminate when the information sought is obtained, when the application for the order is denied or when forty-eight hours have lapsed since the installation of the pen register or trap and trace device, whichever is earlier.

(c) The knowing installation or use by any investigative or law enforcement officer of a pen register or trap and trace device pursuant to subsection (a) without application for the authorizing order within forty-eight hours of the installation shall constitute a violation of this chapter.

(d) A provider of a wire or electronic service, landlord, custodian, or other person who furnished facilities or technical assistance pursuant to this section shall be reasonably compensated for such reasonable expenses incurred in providing such facilities and assistance.

* * *

§ 3127

As used in this chapter--

(1) the terms “wire communication”, “electronic communication”, “electronic communication service”, and “contents” have the meanings set forth for such terms in section 2510 of this title;

(2) the term “court of competent jurisdiction” means--

(A) any district court of the United States (including a magistrate judge of such a court) or any United States court of appeals that--

(i) has jurisdiction over the offense being investigated;

(ii) is in or for a district in which the provider of a wire or electronic communication service is located;
(iii) is in or for a district in which a landlord, custodian, or other person subject to subsections (a) or (b) of section 3124 of this title is located; or
(iv) is acting on a request for foreign assistance pursuant to section 3512 of this title; or

(B) a court of general criminal jurisdiction of a State authorized by the law of that State to enter orders authorizing the use of a pen register or a trap and trace device;

(3) the term "pen register" means 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, provided, however, that such information shall not include the contents of any communication, but such term does not include any device or process used by a provider or customer of a wire or electronic communication service for billing, or recording as an incident to billing, for communications services provided by such provider or any device or process used by a provider or customer of a wire communication service for cost accounting or other like purposes in the ordinary course of its business;

(4) the term "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, provided, however, that such information shall not include the contents of any communication;

(5) the term "attorney for the Government" has the meaning given such term for the purposes of the Federal Rules of Criminal Procedure; and

(6) the term "State" means a State, the District of Columbia, Puerto Rico, and any other possession or territory of the United States.

Sentencing Table, U.S. Sentencing Guidelines Manual (U.S. Sentencing Comm'n 2014).

SENTENCING TABLE
(in months of imprisonment)

	Offense Level	Criminal History Category (Criminal History Points) I (0 or 1)	II (2 or 3)	III (4, 5, 6)	IV (7, 8, 9)	V (10, 11, 12)	VI (13 or more)
	1	0-6	0-6	0-6	0-6	0-6	0-6
	2	0-6	0-6	0-6	0-6	0-6	1-7
	3	0-6	0-6	0-6	0-6	2-8	3-9
	4	0-6	0-6	0-6	2-8	4-10	6-12
Zone A	5	0-6	0-6	1-7	4-10	6-12	9-15
	6	0-6	1-7	2-8	6-12	9-15	12-18
	7	0-6	2-8	4-10	8-14	12-18	15-21
	8	0-6	4-10	6-12	10-16	15-21	18-24
	9	4-10	6-12	8-14	12-18	18-24	21-27
Zone B	10	6-12	8-14	10-16	15-21	21-27	24-30
	11	8-14	10-16	12-18	18-24	24-30	27-33
	12	10-16	12-18	15-21	21-27	27-33	30-37
Zone C	13	12-18	15-21	18-24	24-30	30-37	33-41
	14	15-21	18-24	21-27	27-33	33-41	37-46
	15	18-24	21-27	24-30	30-37	37-46	41-51
	16	21-27	24-30	27-33	33-41	41-51	46-57
	17	24-30	27-33	30-37	37-46	46-57	51-63
	18	27-33	30-37	33-41	41-51	51-63	57-71
	19	30-37	33-41	37-46	46-57	57-71	63-78
	20	33-41	37-46	41-51	51-63	63-78	70-87
	21	37-46	41-51	46-57	57-71	70-87	77-96
	22	41-51	46-57	51-63	63-78	77-96	84-105
	23	46-57	51-63	57-71	70-87	84-105	92-115
	24	51-63	57-71	63-78	77-96	92-115	100-125
	25	57-71	63-78	70-87	84-105	100-125	110-137
	26	63-78	70-87	78-97	92-115	110-137	120-150
	27	70-87	78-97	87-108	100-125	120-150	130-162
Zone D	28	78-97	87-108	97-121	110-137	130-162	140-175
	29	87-108	97-121	108-135	121-151	140-175	151-188
	30	97-121	108-135	121-151	135-168	151-188	168-210
	31	108-135	121-151	135-168	151-188	168-210	188-235
	32	121-151	135-168	151-188	168-210	188-235	210-262
	33	135-168	151-188	168-210	188-235	210-262	235-293
	34	151-188	168-210	188-235	210-262	235-293	262-327
	35	168-210	188-235	210-262	235-293	262-327	292-365
	36	188-235	210-262	235-293	262-327	292-365	324-405
	37	210-262	235-293	262-327	292-365	324-405	360-life
	38	235-293	262-327	292-365	324-405	360-life	360-life
	39	262-327	292-365	324-405	360-life	360-life	360-life
	40	292-365	324-405	360-life	360-life	360-life	360-life
	41	324-405	360-life	360-life	360-life	360-life	360-life
	42	360-life	360-life	360-life	360-life	360-life	360-life
	43	life	life	life	life	life	life

November 1, 2014