No. 17-950

In The
Supreme Court of the United States

ROSS WILLIAM ULBRICHT,
Petitioner,

v.

UNITED STATES OF AMERICA,
Respondent.

On Petition For A Writ Of Certiorari To The United States Court Of Appeals For The Second Circuit

BRIEF OF REASON FOUNDATION, CATO INSTITUTE, COMPETITIVE ENTERPRISE INSTITUTE, AND R STREET INSTITUTE AS *AMICI CURIAE* IN SUPPORT OF PETITIONER

MANUEL S. KLAUSNER
LAW OFFICES OF MANUEL S. KLAUSNER
One Bunker Hill Bldg.
601 West Fifth St.
Los Angeles, CA 90071
(213) 617-0414
mklausner@klausnerlaw.us

BRADLEY A. BENBROOK
Counsel of Record
STEPHEN M. DUVERNAY
BENBROOK LAW GROUP, PC
400 Capitol Mall, Ste. 2530
Sacramento, CA 95814
(916) 447-4900
brad@benbrooklawgroup.com

Counsel for Amici Curiae

February 2018

ADDITIONAL COUNSEL FOR *AMICI CURIAE*

ILYA SHAPIRO
TREVOR BURRUS
CATO INSTITUTE
1000 Mass. Ave., N.W.
Washington, D.C. 20001
(202) 842-0200
ishapiro@cato.org

JIM HARPER
COMPETITIVE ENTERPRISE INSTITUTE
1310 L St. NW, 7th Floor
Washington, D.C. 20005
(202) 331-1010
jim.harper@cei.org

CHARLES DUAN
R STREET INSTITUTE
1212 New York Ave. NW, Suite 900
Washington, D.C. 20005
cduan@rstreet.org

QUESTION PRESENTED

Does the Fourth Amendment permit the government to track and monitor citizens' Internet browsing activity without a warrant?

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

INTEREST OF *AMICI CURIAE*[1]

Reason Foundation is a national, nonpartisan, and nonprofit public policy think tank, founded in 1978. Reason's mission is to advance a free society by applying and promoting libertarian principles and policies—including free markets, individual liberty, and the rule of law. Reason supports dynamic market-based public policies that allow and encourage individuals and voluntary institutions to flourish. Reason advances its mission by publishing Reason magazine, as well as commentary on its websites, and by issuing policy research reports. To further Reason's commitment to "Free Minds and Free Markets," Reason selectively participates as *amicus curiae* in cases raising significant constitutional issues.

The Cato Institute was established in 1977 as a nonpartisan public policy research foundation dedicated to advancing the principles of individual liberty, free markets, and limited government. Cato's Robert A. Levy Center for Constitutional Studies was established in 1989 to promote the principles of limited constitutional government that are the foundation of liberty. Toward those ends, Cato publishes books and studies, conducts conferences, produces the annual *Cato Supreme Court Review*, and files *amicus* briefs.

---

[1] Rule 37 statement: All parties were given timely notice and have consented to the filing of this brief. No party's counsel authored this brief in any part. No person other than *amici*, their members, or their counsel made a monetary contribution to its preparation or submission.

The Competitive Enterprise Institute ("CEI") is a non-profit public policy organization dedicated to advancing the principles of limited government, free enterprise, and individual liberty. CEI publishes research and commentary on the intersection of property rights, markets, free enterprise, and liberty.

The R Street Institute is a non-profit, non-partisan public-policy research organization. R Street's mission is to engage in policy research and educational outreach that promotes free markets, as well as limited yet effective government, including properly calibrated legal and regulatory frameworks that support Internet economic growth and individual liberty. R Street's particular focus on Internet law and policy is one of offering research and analysis that show the advantages of a more market-oriented society and of more effective, more efficient laws and regulations that protect freedom of expression and privacy.

This case concerns *amici* because it involves the increasingly common government practice of gathering Internet browsing activity through "pen/trap" devices without first obtaining a warrant. Given the necessity of Internet usage in modern life, *amici* do not agree that American citizens should be deemed to consent to turning over their browsing history to the government as a condition of using the Internet.

INTRODUCTION AND SUMMARY OF ARGUMENT

When the government uses a "pen/trap" device without a warrant to collect the Internet Protocol ("IP") addresses associated with a citizen's Internet browsing over time, it is conducting an unreasonable seizure, so this practice generally violates the Fourth Amendment.[2] This brief aims to demonstrate why various assumptions underlying Fourth Amendment doctrine do not apply to the warrantless seizure of data revealing the IP addresses a citizen visits while using the Internet.

In particular:

1. The Second Circuit's decision, like other recent decisions, applied Fourth Amendment "third party doctrine" to a pen/trap's collection of IP addresses visited during Internet browsing. This doctrine arose from the theory that when one discloses illegal activity to a third party, they "assume the risk" that the third party will disclose that illegal behavior to the government. Along the way, the theory was generalized to say that disclosure of any information,

---

[2] The Court's analysis must be anchored in the Fourth Amendment's text and its original understanding. "[A]t bottom, [the Court] must 'assur[e] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.'" *United States v. Jones*, 565 U.S. 400, 406 (2012) (quoting *Kyllo v. United States*, 533 U.S. 27, 34 (2001)). "Whatever new methods of investigation may be devised, [the Court's] task, *at a minimum*, is to decide whether the action in question would have constituted a 'search' within the original meaning of the Fourth Amendment." *Id.* at 406 n.3. And "[a]s the text makes clear, the ultimate touchstone of the Fourth Amendment is 'reasonableness.'" *Riley v. California*, 134 S. Ct. 2473, 2482 (2014) (internal citation and quotation marks omitted).

legal or illegal, to a third party assumes the risk of a subsequent disclosure to the government.

Inherent in the concept of assumed risk, however, is the notion of *choice*: one must choose whether to disclose the information if they can fairly be said to assume any risk. That assumption is lacking, however, when it comes to whether to use the Internet and thereby disclose your browsing history to an Internet service provider. Using the Internet is a necessity of modern life for any citizen hoping to participate as a functioning member of society. Surely the third party doctrine has been stretched beyond its limit when engaging in such a necessity of life is said to constitute a conscious "choice" to disclose information to a third party, and that such disclosure "assumes the risk" that the government will force the third party to hand it over.

2. The Second Circuit likewise relied on the so-called "content/non-content" distinction underlying Fourth Amendment doctrine in concluding that no search or seizure occurred here. Because, in its view, "routing" information revealed in an IP address does not reveal "content," the Fourth Amendment is not implicated. But this superficial approach ignores reality: an IP address is readily converted to a particular website, which reveals *at least some* of the "content" a citizen is viewing on the Internet. A particular website may have many pages, in which case an IP address alone may not reveal precisely *all* of the content a person viewed at a website, but that does not mean the IP address reveals *zero* content. Yet that appears to be the conclusion reached in the court below.

Finally, we briefly review the statutory scheme authorizing pen/trap seizures to demonstrate that (a) the judicial oversight of government pen/trap applications is ministerial, (b) the statute authorizes essentially any federal or state agency conducting a criminal investigation to obtain such an order, and (c) the scope is incredibly broad both as to subject matter and time. In short, the process is no substitute for a warrant.

Amici agree with Petitioner's suggestion that this case should, at a minimum, be held pending the decision in *Carpenter v. United States*, cert. granted, No. 16-402 (argued Nov. 29, 2017) (historical cell site location data). Yet this case presents its own unique issues and compelling reasons for review.

BRIEF BACKGROUND ON THE RELATIONSHIP BETWEEN IP ADDRESSES AND WEBSITES

When the government engages in pen register and trap-and-trace surveillance, it gathers, among other things, the IP addresses that the monitored citizen visits and the outgoing and incoming Internet routing data for a person's e-mail and other communications. *See United States v. Ulbricht*, 858 F.3d 71, 83 (2d Cir. 2017) ("The [pen/trap] orders authorized law enforcement agents to collect IP address data for Internet traffic to and from Ulbricht's home wireless router and other devices that regularly connected to Ulbricht's home router.").

This brief focuses, in particular, on the government's collection of IP addresses. In many cases, it is a simple matter to convert an IP address into a website. Say, for example, a pen register captures a citizen viewing IP address 141.105.69.239. Government

agents can copy and paste that address into any number of free online databases and learn, instantaneously, that the citizen is looking at the WikiLeaks website, while a person viewing 35.162.89.225 is looking at Reason.org.[3]

To be sure, knowing only an IP address associated with a website does not allow the government to know exactly which web pages within the particular website a citizen visits, each of which has its own Uniform Resource Locator ("URL"). But the government can still learn a substantial amount about a person's web browsing simply from the home pages she visits.

While the government appears to take the position that in extreme cases it can obtain a complete web browsing history, including every page (URL) visited, *see* U.S. Dep't of Justice, U.S. Attorneys' Manual § 9–7.500, multiple courts have acknowledged that government seizure of that data would raise serious Fourth Amendment concerns. *United States v. Forrester*, 512 F.3d 500, 510 n.6 (9th Cir. 2008) ("Surveillance techniques that enable the government to determine not only the IP addresses that a person accesses but also the [URL] of the pages visited might be more constitutionally problematic."); *In re Application of United States for an Order Authorizing Use of a Pen Register & Trap*, 396 F. Supp. 2d 45, 49 (D. Mass. 2005). That sort of seizure would also plainly violate 18 U.S.C. § 3127(3) and (4), which

---

[3] Reverse IP lookup is available at any number of websites. For example, a search using Uwebtools.com's IP Address Search, ip.uwebtools.com, tells you that IP address 160.111.244.22 belongs to the Smithsonian Institution, located in Washington, D.C.

prohibit the government from obtaining the "contents" of any communication gathered in a pen/trap data seizure. *See below*, Section III.

Because the government is doubtless aware that there is no Fourth Amendment justification for the warrantless collection of a *complete* browsing history of every web page a citizen visits, it appears to generally limit its pen/trap data seizure to IP addresses. In other words, the Court is not likely to face a case that raises the issue of warrantless seizure of Internet browsing history in any starker terms than this case.

ARGUMENT

This case asks the Court to once again grapple with how to reconcile the Fourth Amendment's guarantee against unreasonable searches and seizures with advancements in technology. *See, e.g.*, *Kyllo v. United States*, 533 U.S. 27 (2001) (thermal imaging); *United States v. Jones*, 565 U.S. 400 (2012) (GPS tracking); *Riley v. California*, 134 S. Ct. 2473 (2014) (search of digital information on a cell phone). In *Carpenter*, an *amicus* group heavily overlapping with this one argued for application of the Fourth Amendment's text and recognition of property rights in data to resolve the issues in cases like this one. Here, we illustrate how fraught it is to use "reasonable expectation of privacy" doctrine and particularly its derivative, the third-party doctrine.[4]

---

[4] For one view on how to update *Katz*'s reasonable expectation of privacy test for the modern world, *see* Jim Harper, *Escaping Fourth Amendment Doctrine After* Jones*: Physics, Law, and Privacy Protection*, 2011–2012 Cato Sup. Ct. Rev. 219 (2012).

The Court has long recognized that technological advancements shape societal expectations of privacy. "Rapid changes in the dynamics of communication and information transmission are evident not just in the technology itself but in what society accepts as proper behavior." *City of Ontario v. Quon*, 560 U.S. 746, 759 (2010). This dynamic relationship thus shapes both privacy expectations and "the degree to which society will be prepared to recognize those expectations as reasonable." *Id*. at 759–60.

I. Internet Usage Is Literally Essential To Much Of Modern Life, So The "Assumed Risk" Premise Underlying The "Third Party" Doctrine Cannot Be Fairly Applied To It.

When the government monitors, accumulates, and analyzes a citizen's Internet browsing activity—even limited to IP addresses—that is a seizure. The Second Circuit relied on the Fourth Amendment case law's "third party doctrine" to conclude otherwise.

The circuit court analogized the collection of information here to *Smith v. Maryland*, 442 U.S. 735 (1979), which found no Fourth Amendment violation when police executed the warrantless collection through a "pen register" of a list of phone numbers the suspect was dialing. Because collecting IP addresses is supposedly similar, "no reasonable person could maintain a privacy interest" in their Internet traffic information, so therefore no Fourth Amendment interest is implicated. *Ulbricht*, 858 F.3d at 97. In the circuit court's view, Internet users "voluntarily" turn over their browsing information to third parties (Internet service providers) for the purpose of directing and routing their Internet activity, so they

surrender any Fourth Amendment rights they may have regarding that same information. *Id.* at 96.

This is a modern take on the "third party" doctrine, which is a far cry from its original conception.

A. "Assuming Risk" Implies Choice.

The third party doctrine first arose in government-informant cases. Laura K. Donahue, *The Fourth Amendment in a Digital World*, 71 N.Y.U. Ann. Surv. Am. L. 533, 640–46 (2017); Richard M. Thompson II, Congressional Research Service Report For Congress, *The Fourth Amendment Third-Party Doctrine* 7–9 (2014). The notion was that parties "assumed the risk" that, when they disclosed their *criminal* activities to third parties, those third parties would pass that information to the government. *See Lopez v. United States*, 373 U.S. 427, 439 (1963) ("[T]he risk that petitioner took in offering a bribe to Davis fairly included the risk that the offer would be accurately reproduced in court"); *Hoffa v. United States*, 385 U.S. 293, 302 (1966) (observing that "the Fourth Amendment [does not] protect[ ] a wrongdoer's misplaced belief that a person to whom he voluntarily confides his wrongdoing will not reveal it."); *United States v. White*, 401 U.S. 745, 752 (1971) ("[O]ne contemplating illegal activities must realize and risk that his companions may be reporting to the police. If he sufficiently doubts their trustworthiness, the association will very probably end or never materialize. But if he has no doubts, or allays them, or risks what doubt he has, the risk is his."); *Smith*, 442 U.S. at 743–44 ("This Court consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties.").

It is worth noting that these early cases focused on the assumed risk inherent in the disclosure of *illegal* activity to third parties, not simply the passing of *any* information to third parties. But at the risk of sounding quaint, it's also worth noting that the Fourth Amendment exists to protect the innocent among us. *See, e.g.*, *Maryland v. King*, 569 U.S. 435, 482 (2013) (Scalia, J., dissenting) ("[T]he Fourth Amendment's protections ought to be most jealously guarded" for "people who are innocent of the State's accusations."); *Minnesota v. Carter*, 525 U.S. 83, 110 (1998) (Ginsburg, J., dissenting) ("If the illegality of the activity made constitutional an otherwise unconstitutional search, such Fourth Amendment protection, reserved for the innocent only, would have little force in regulating police behavior toward either the innocent or the guilty.").

In any event, given the ultimate task under the text of the Fourth Amendment is determining whether a search or seizure is *reasonable*, the question here is this: Is it reasonable to say that the ordinary citizen "assumes the risk" that their Internet browsing activity will be monitored by the government with a pen/trap device every time they log on to the Internet? The answer is plainly "No."

In his dissent in *Smith*, Justice Marshall questioned the application of the third party doctrine to the collection of a list of phone numbers the suspect called. The majority determined that by "us[ing] his phone," the petitioner "voluntarily conveyed numerical information to the telephone company" and "assumed the risk" that the company would turn over those numbers to the police. 442 U.S. at 744–45. As Justice Marshall pointed out, however, the concept of assuming risk implies "some notion of choice" that,

he believed, wasn't realistically applied to telephone usage:

> [U]nless a person is prepared to forgo use of what for many has become a personal or professional necessity, he cannot help but accept the risk of surveillance. It is idle to speak of "assuming" risks in contexts where, as a practical matter, individuals have no realistic alternative.

442 U.S. at 750 (Marshall, J., dissenting) (citations omitted).

We turn now to whether the third party doctrine's foundational assumption of choice can fairly be applied to Internet usage.

B. Americans Have No Choice Regarding Whether to Use the Internet if They Wish to Be Productive Members of Society.

In a popular television commercial urging customers to change Internet service providers, actor Mark Wahlberg stands in a kitchen and points to a sandwich, a glass of water, and an iPad while explaining: "Food. Water. Internet. We need it to live." AT&T TV & Internet Servs., *AT&T Internet TV Commercial, 'No Extra Fees' Feat. Mark Wahlberg, Anjelica Huston* (2017), online at https://www.ispot.tv/ad/wAt9/at-and-t-internet-no-extra-fees-feat-mark-wahlberg-anjelica-huston. It sounds funny, because it's true.

Using the Internet is central to everyday life–much more so than using the phone when *Smith* was decided in 1979. It simply cannot be said that a per-

son *voluntarily* chooses to surrender privacy by engaging in Internet browsing when there is no alternative. Indeed, looking back at the origins of the third party doctrine, it is bizarre to analogize logging on to the Internet to offering a bribe, *Lopez*, 373 U.S. at 439, or keeping an associate up-to-date on all the crimes one is committing. *Hoffa*, 385 U.S. at 296 n.3.[5]

To be sure, using the Internet is not a necessity because "everyone" is on fun social media networks like Facebook. *But see Packingham v. North Carolina*, 137 S. Ct. 1730, 1735 (2017) (observing that the Internet is "the most important place[ ] (in a spatial sense) for the exchange of views" and citing Facebook's reach). Nor is it a necessity because "everyone" uses text messaging. *Cf. Quon*, 560 U.S. at 760 ("Cell phone and text message communications are so pervasive that some persons may consider them to be essential means or necessary instruments for self-expression, even self-identification.").

Rather, using the Internet is essential to participate as a functioning member of society—there literally is no alternative. Consider one limited example. Imagine a teenager in California who dreams of becoming a lawyer and maybe one day even a judge:

College. If our young student hopes to attend a public university in California, she must use the Internet. The University of California system only processes applications online. University of California, *How to Apply*, online at http://admission.universityofcalifornia.edu/how-to-apply/index.html ("Applications must be submitted online by the last

---

[5] Gone too is the notion of choice in the third party's subsequent disclosure to the government. *See* Section III below.

day of the filing period.").[6] The same goes for the California State University system. The California State University, Press Release, *CSU Launches New Cal State Apply Application Portal* (May 16, 2017), online at https://www2.calstate.edu/csu-system/news/Pages/CSU-Launches-New-Cal-State-Apply-Application-Portal.aspx ("Beginning June 1, 2017, the current portal, CSU Mentor, will be replaced by Cal State Apply, a streamlined user-friendly application for all CSU incoming freshman, transfer, graduate and international students.").[7]

Getting Into Law School. If our ambitious youngster were graduating from college in 2018 and applying for law school, she appears to have no choice but to do so through the Law School Admission Council's website. "Nearly all ABA-approved law schools . . . require the use of LSAC's Credential Assembly Service (CAS) for JD applicants." Law School Admission

---

[6] It appears that even non-citizen applicants living in the United States with no legal status have to use the online application for the University of California system. Univ. of Cal., Undocumented Student Resources, *Applying to UC*, online at http://undoc.universityofcalifornia.edu/applying-to-uc.html ("We don't want the application fee to get in the way of you applying to UC. . . . You can apply for a fee waiver within the online application and be notified immediately whether you have qualified.").

[7] Once at school, our student has no hope of thriving without Internet access. Many schools facilitate classes through an online learning management systems. U.C. Berkeley, for example, uses a platform called bCourses. Professors use the system to distribute course information to students, and students submit assignments through the platform and interact with each other through online learning modules. U.C. Berkeley Educ. Tech. Servs., *bCourses*, online at https://www.ets.berkeley.edu/services-facilities/bcourses.

Council, *So You Want to Go to Law School. What's Next?*, online at https://os.lsac.org/Logon/Access.aspx; *see also* University of California, Berkeley School of Law, *Applying for the J.D. Degree*, online at https://www.law.berkeley.edu/admissions/jd/applying-for-jd-degree/ ("The application process begins when you visit the Law School Admission Council website, where you must establish an account, register for the Law School Admission Test (LSAT), and submit an application . . . . "); Stanford Law School, *JD Application Process, Application Process at a Glance*, online at https://law.stanford.edu/apply/how-to-apply/jd-application-process/ ("You must complete the entire application form and submit it electronically through LSAC.").

Becoming a Lawyer and Practicing Law. In California, law school graduates may only apply to take the bar exam online. The State Bar of California, *Admission Requirements*, online at http://www.calbar.ca.gov/Admissions/Requirements. The same goes for the District of Columbia. The District of Columbia Bar, How to Join, online at https://www.dcbar.org/membership/how-to-join.cfm.[8]

And, of course, more and more courts are requiring online filing of papers in litigation matters. *See, e.g.*, U.S. District Court for the Central District of

---

[8] In order to remain in good standing by paying dues, a California lawyer has to check her online profile in order to know how much to pay. *See* The State Bar of California, *Fee Statement*, online at http://www.calbar.ca.gov/Attorneys/Member-Records/About-Your-State-Bar-Profile/Fees-Payment ("Beginning in 2017, the State Bar launched a new online billing and payment application for annual fees. As a result, paper billing statements are no longer mailed to attorneys. Instead, statements are available online through My State Bar Profile.").

California, Local Rule 5-4.1 ("attorneys are required to file documents electronically" in all civil cases). Indeed, Chief Justice Roberts has hailed the trend of moving litigation online through the case management and electronic case filing ("CM/ECF") system:

> CM/ECF is vitally important to the cause of justice because it can make the courts more accessible, and more affordable, to a diverse body of litigants, drawn from every corner of society, who often enter the courthouse reluctantly, apprehensively, and only as a last resort.

Chief Justice John G. Roberts, 2014 Year-End Report on the Federal Judiciary 5 (Jan. 2015).

* * *

Does this young person really have a choice as to whether she uses the Internet if she wants to participate in society? Of course not. The Fourth Amendment should not be marginalized further by pretending as if she does. The "assumed risk" concept underlying the third party doctrine cannot be fairly applied to Internet browsing.

II. The Second Circuit, Like Other Courts, Inexplicably Concluded That An IP Address Reveals No "Content"—Despite The Link Between The Address And A Particular Website.

The Second Circuit also relied on the so-called "content/non-content" distinction—a theory adopted in many Fourth Amendment cases—to conclude that the government was free to monitor incoming and

outgoing IP address traffic. 858 F.3d at 97–98. The court accepted the government's claim that, like telephone numbers captured by a pen/trap or envelope markings on sealed letters and packages,[9] IP addresses are merely routing data that do not reveal the "content" of what a user is viewing on the Internet—so "no reasonable person could maintain a privacy interest" in them. *Id.* at 97. While the content/non-content distinction has the apparent virtue of simplicity, and its application to pen/trap collection of IP addresses seems simple, the courts are getting it wrong.

The content/non-content distinction is an outgrowth of *Katz v. United States* and *Smith*. In *Katz*, the Court held that the warrantless use of a listening device to record the contents of a conversation inside a telephone booth violated the Fourth Amendment: "No less than an individual in a business office, in a friend's apartment, or in a taxicab, a person in a telephone booth may rely upon the protection of the Fourth Amendment. One who occupies it, shuts the door behind him, and pays the toll that permits him to place a call is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world." *Katz*, 389 U.S. 347, 352 (1967).

---

[9] "[S]ealed packages in the mail cannot be opened without a warrant," and the government's "authority to possess a package is distinct from his authority to examine its contents." *Walter v. United States*, 447 U.S. 649, 654 (1980) (citing *Ex parte Jackson*, 96 U.S. 727 (1877)). *See also United States v. Jacobsen*, 466 U.S. 109, 114 (1984) ("Letters and other sealed packages are in the general class of effects in which the public at large has a legitimate expectation of privacy; warrantless searches of such effects are presumptively unreasonable.").

This distinction was central to the Court's decision in *Smith*, where it rejected the suspect's attempt to align his case with *Katz*: "[A] pen register differs significantly from the listening device employed in *Katz*, for pen registers do not acquire the *contents* of communications." 442 U.S. at 741 (emphasis in original). *See also id.* at 743 ("Although petitioner's conduct may have been calculated to keep the *contents* of his conversation private, his conduct was not and could not have been calculated to preserve the privacy of the number he dialed." (emphasis in original)).

Following these general principles, federal law governing pen registers and trap-and-trace devices nominally requires that they not be used to collect the *contents* of communications. *See, e.g.*, 18 U.S.C § 3127(3) (defining "pen register" as "a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication"); *id.*, subd. (4) (defining "trap and trace device" as "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").[10]

---

[10] "Contents" is defined as "any information concerning the substance, purport, or meaning of that communication." 18 U.S.C. § 2510(8).

The Second Circuit accepted without apparent analysis the government's position that capturing IP address information reveals no "content." 858 F.3d at 84 ("an 'IP address is analogous to a telephone number' because 'it indicates the online identity of the communicating device without revealing the communication's content'" and "[t]he pen/trap orders thus did not permit the government to access the content of Ulbricht's communications"). Assuming that to be true, the court decided that collecting IP address information was "precisely analogous to the capture of telephone numbers" in *Smith*:

> Like telephone companies, Internet service providers require that identifying information be disclosed in order to make communication among electronic devices possible. In light of the *Smith* rule, no reasonable person could maintain a privacy interest in that sort of information.
>
> We therefore join the other circuits that have considered this narrow question and hold that collecting IP address information *devoid of content* is "constitutionally indistinguishable from the use of a pen register."

858 F.3d at 98 (quoting *United States v. Forrester*, 512 F.3d 500, 510 (9th Cir. 2008), and collecting cases) (emphasis added).

Accordingly, the Second and Ninth Circuits have determined that revealing IP addresses of websites that a person visits does not reveal the "content" of

their web browsing.[11] *Id.*; *see Forrester*, 512 F.3d at 510 ("IP addresses constitute addressing information and do not necessarily reveal any more about the underlying contents of communication than do phone numbers.").

These decisions reflect a disturbing inability (or refusal) to recognize that an IP address is so readily converted to home page URLs for a particular Internet site. As such, *of course* an IP address reveals content: It reveals that a person visited a *particular* website, which in itself reveals content.[12]

To be sure, if a citizen being monitored by a pen/trap order clicked through multiple pages at a particular website, the pen/trap would not reveal *all* of that activity. Thus, while knowing an IP address doesn't necessarily reveal all of the content a monitored citizen viewed at a website, it plainly reveals "content." *Some* content does not equal *zero* con-

---

[11] In a similar vein, other circuits have held that Internet users do not have a reasonable expectation of privacy in their IP addresses. *See United States v. Christie*, 624 F.3d 558, 573–74 (3d Cir. 2010); *United States v. Perrine*, 518 F.3d 1196, 1204–05 (10th Cir. 2008).

[12] In some cases, a single IP address is associated with multiple websites. *See, e.g.*, Matthew J. Tokson, *The Content/Envelope Distinction in Internet Law*, 50 Wm. & Mary L. Rev. 2105, 2148–49 (2009) (noting that "personal" and "smaller" websites "are more likely to share an IP address with multiple other sites."); GoDaddy, *What is a dedicated IP?*, online at https://www.godaddy.com/help/what-is-a-dedicated-ip-1053 ("A dedicated [IP] is a unique Internet address dedicated exclusively to a single hosting account. This is in contrast to the normal configuration of several hosting accounts residing on a single server and sharing its IP address.").

tent.[13] (Moreover, some websites consist of *only* a homepage, in which case the IP address reveals *all* of the content associated with it. *See, e.g.*, 107.178.244.221 (DrudgeReport.com)).

Though it seems plain as day that revealing the website a person visits reveals "content" in this manner, the *Forrester* court decided that the failure to reveal all content was equivalent to the failure to reveal any content:

> Surveillance techniques that enable the government to determine not only the IP addresses that a person accesses but also the uniform resource locators ("URL") of the pages visited might be more constitutionally problematic. A URL, unlike an IP address, identifies the *particular document* within a website that a person views and thus reveals *much more information* about the person's Internet activity. For instance, a surveillance technique that captures IP addresses would show only that a person visited the New York Times' website at

---

[13] This Court's website for instance, located at IP address 23.214.57.118, has multiple pages. How can it be said that any of these pages reveals no "content"? On January 30, 2018, for example, the Court's homepage, which may include the least content on the site, explains that "[t]he Supreme Court Building is open to the public from 9 a.m. to 4:30 p.m.," and that "[t]he Court will next convene for a public session in the Courtroom at 10 a.m. on Tuesday, February 20." It also includes a Did-You-Know factoid telling visitors that "Dr. John Rock, a physician, was the first African American to be admitted to the Supreme Court Bar on February 1, 1865, on the motion of Senator Charles Sumner."

> http://www.nytimes.com, whereas a technique that captures URLs would also divulge the particular articles the person viewed.

512 F.3d at 510 n.6 (emphasis added). Surely the *New York Times* would be alarmed by an official statement of the United States judiciary that its website reveals no content.[14]

More broadly, dismissing IP addresses as "non-content" ignores the wealth of information that our Internet browsing activity reveals. By looking at outgoing web traffic, for example, you can learn where someone's allegiances lie: 140.180.223.22 (princeton.edu) or 171.67.215.200 (stanford.edu). An IP address can tell you a person's favorite news source (205.203.132.1, online.WSJ.com), or what they do in their spare time (04.37.111.126, NRA.org).

---

[14] The U.S. Attorney's Manual flaunts the non-distinction between IP addresses and URLs in a policy ostensibly aimed at limiting the collection of data via pen/trap orders to "the non-content information associated with Internet communications." U.S. Dep't of Justice, U.S. Attorneys' Manual § 9–7.500. Because of "privacy and other [that is, Fourth Amendment] concerns relating to the use of pen register orders" "to collect . . . the terms that a person uses to request information on the World Wide Web," investigators are required to consult with the DOJ's computer crime and intellectual property division before applying for a pen register that may collect URLs *directly*. *Id.* Yet the policy "does not apply to applications for pen register orders that would merely authorize collection of Internet Protocol (IP) addresses, *even if such IP addresses can be readily translated into URLs or portions of URLs*." *Id*. In other words, the U.S. Attorney's Manual suggests that IP addresses do not constitute "content" for Fourth Amendment purposes—even if they can be readily and easily converted into URLs, *something the policy prohibits gathering directly*.

A snapshot of someone's browsing activity can reveal political preferences. (You can Make America Great Again at 104.16.34.178, or Feel the Bern at 104.16.42.58.) An IP address can show a person's religious affiliations (154.35.160.5, DalaiLama.com) or lack thereof (104.25.78.100, atheists.org).

And tracking Internet browsing activity *over time* paints a much more intrusive picture. A series of visits can tell a story: 208.93.170.15 (WebMD); 104.16.104.168 (Planned Parenthood); or 129.176.217.220 (The Mayo Clinic). The statutory scheme authorizes pen/traps to collect up to *four months* of activity over two 60-day periods. *See* below. In this extended web history lies the intimate details of our private lives.[15]

The Internet allows every citizen the opportunity to have a virtually unlimited library in their own home. The government's warrantless collection of the IP addresses a citizen visits is analogous to a government agent peering through the window to monitor which books a person pulls from their shelf. While the government actor may not be able to determine exactly which chapters or pages a citizen is reading—just as an IP address may not disclose exactly which pages of a website the citizen visits—the government is plainly learning about the "content" of

---

[15] As Professor Donahue has put it, "[t]echnology . . . is now blurring the doctrinal [content versus non-content] distinction." Donahue, *supra*, 71 N.Y.U. Ann. Surv. Am. L. at 650. "[D]ata traditionally considered to be noncontent, such as pen register and trap and trace data, or envelope information, in light of digital dependence and the growth of social network analytics, generates a tremendous amount of information about individuals' relationships, beliefs, and predilections—precisely the interests that the distinction was meant to protect." *Id.*

the citizen's reading behavior by sitting outside the window and monitoring, day after day, which books the citizen pulls from the shelf. By acquiring the data, the government is conducting a seizure. It is also plainly engaging in a Fourth Amendment search. *See Jones*, 565 U.S. at 406 n.3 ("Whatever new methods of investigation may be devised, our task, *at a minimum*, is to decide whether the action in question would have constituted a 'search' within the original meaning of the Fourth Amendment.").[16]

III. The Statutory Authorization For Pen/Trap Data Seizure Imposes Almost No Limits On Government Attorneys' Discretion.

There should be no impression here that the application process governing the issuance of pen/trap orders operates as any meaningful check on the government's discretion in monitoring Internet usage, let alone that it serves as the functional equivalent of a warrant. Rather, as the Eighth Circuit has accurately observed, "[t]he judicial role in approving use of trap and trace devices is ministerial in nature because, upon a proper application being made under 18 U.S.C. § 3122, 'the court *shall* enter an ex parte order authorizing the installation' of such a device. 18 U.S.C. § 3123(a)." *United States v. Fregoso*, 60

---

[16] "When the Fourth Amendment was adopted, as now, to 'search' meant '[t]o look over or through for the purpose of finding something; to explore; to examine by inspection; as, to *search* the house for a book; to *search* the wood for a thief.'" *Kyllo*, 533 U.S. at 32 n.1 (quoting N. Webster, An American Dictionary of the English Language 66 (1828) (reprint 6th ed.1989)).

F.3d 1314, 1320 (8th Cir. 1995) (additional citations omitted) (emphasis in original).

The statutory standards governing pen/trap applications set an extremely low bar. Aside from disclosing his or her name to the court, the government attorney need only provide a certification that "the information likely to be obtained is *relevant* to an ongoing criminal investigation being conducted by that agency." 18 U.S.C. § 3122(b)(2) (emphasis added). Federal courts have interpreted the "relevance" standard as meriting "extremely limited judicial review," *United States v. Hallmark*, 911 F.2d 399, 402 (10th Cir. 1990), which effectively gives the government a blank check to conduct a dragnet search of Internet activity. And because pen/trap orders collect incoming and outgoing routing information, the government could conceivably make the "relevance" showing as to any known associate of a suspect, no matter how remotely he is connected to the subject of a criminal investigation. *Cf.* Laura K. Donahue, *Bulk Metadata Collection: Statutory and Constitutional Considerations*, 37 Harv. J. L. & Pub. Pol'y 757, 838–42 (2014) (discussing the NSA's bulk collection of data under the Foreign Intelligence Surveillance Act's analogous "relevance" standard).[17]

---

[17] Professor Donahue quotes Judge Walton of the Foreign Intelligence Surveillance Court, who pointed out how the breadth of the "relevance" standard enabled the NSA to amass large amount of data, the "vast majority" of which were not directly tethered to the subject of an investigation:

> [N]early all of the call detail records collected pertain to communications of non-U.S. persons who are *not* the subject of an FBI investigation to obtain foreign intelligence information, [and] are communications of U.S. persons who are *not*

Importantly, the statute is not limited to the United States Department of Justice attorneys; any attorney whose agency is conducting an "ongoing criminal investigation" can apply. 18 U.S.C. § 3122(b)(2). In addition, a "*State* investigative or law enforcement officer may make an application" for a pen/trap order under the statute as well. *Id*., subd. (a)(2). In light of the remarkable growth of state and federal agencies engaging in criminal investigations in recent decades, the list of government lawyers able to use this tool is incredibly long.

The statute further assumes that the standard pen/trap will collect data for up to *four months*. An initial application may seek up to 60 days' worth of data, which can be extended for another 60 days with an updated application making the same minimal showing. 18 U.S.C. § 3123(c)(1) & (2). The subject of the pen register in *Smith*, by contrast, was arrested two days after the device was installed. *Smith*, 442 U.S. at 737. Monitoring a citizen's Internet activity over such a lengthy period allows the government to amass information far more extensive and intrusive than simply collecting the numbers dialed on a rotary phone over the same period of time.

In sum, the statutory scheme increases, rather than mitigates, the potential for Fourth Amendment harm.

> the subject of an FBI investigation to protect against international terrorism or clandestine intelligence activities.

Donahue, *Bulk Metadata Collection*, 37 Harv. J.L. & Pub. Pol'y at 839 (quoting *In re Production of Tangible Things from [Redacted]*, No. BR 08–13, at 11–12, 2009 WL 9150913 (FISA Ct. Mar. 2, 2009)).

CONCLUSION

For these reasons, and those stated by the petitioner, the Court should grant the petition for a writ of certiorari.

Respectfully submitted,

MANUEL S. KLAUSNER
LAW OFFICES OF
MANUEL S. KLAUSNER
One Bunker Hill Bldg.
601 West Fifth St.
Los Angeles, CA 90071
(213) 617-0414
mklausner@klausnerlaw.us

BRADLEY A. BENBROOK
Counsel of Record
STEPHEN M. DUVERNAY
BENBROOK LAW GROUP, PC
400 Capitol Mall, Ste. 2530
Sacramento, CA 95814
(916) 447-4900
brad@benbrooklawgroup.com

ILYA SHAPIRO
TREVOR BURRUS
CATO INSTITUTE
1000 Mass. Ave., N.W.
Washington, D.C. 20001
(202) 842-0200
ishapiro@cato.org

JIM HARPER
COMPETITIVE ENTERPRISE
INSTITUTE
1310 L St. NW, 7th Floor
Washington, D.C. 20005
(202) 331-1010
jim.harper@cei.org

CHARLES DUAN
R STREET INSTITUTE
1212 New York Ave.
NW, Suite 900
Washington, D.C.
20005
cduan@rstreet.org

Counsel for Amici Curiae

February 2018