No. _____

IN THE
SUPREME COURT OF THE UNITED STATES

RYAN GALAL VANDYCK
Petitioner,

vs.

UNITED STATES OF AMERICA
Respondent.

ON PETITION FOR WRIT OF CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE NINTH CIRCUIT

PETITION FOR WRIT OF CERTIORARI

JON M. SANDS
Federal Public Defender
District of Arizona

*M. EDITH CUNNINGHAM
Assistant Federal Public Defender
407 W. Congress, Suite 501
Tucson, AZ 85701
Telephone: (520) 879-7500
Facsimile: (520) 879-7600
edie_cunningham@fd.org

**Counsel of Record*

QUESTIONS PRESENTED

1. Once it is linked to a particular subscriber, an Internet Protocol address is capable of revealing a wealth of private information about that subscriber's online activities. Does the Fourth Amendment therefore require a warrant supported by probable cause for the government to obtain the subscriber information associated with an Internet Protocol address?

2. Should this Court abandon the third-party doctrine in favor of case-by-case consideration of whether an interest falls within the scope of the Fourth Amendment's protections?

PARTIES AND PROCEEDINGS

All parties to the proceedings are listed in the caption. The petitioner is not a corporation.

This case arises from the following proceedings in the United States District Court for the District of Arizona and the United States Court of Appeals for the Ninth Circuit: *United States v. VanDyck*, No. 4:15-cr-00742-TUC-CKJ (D. Ariz. Dec. 5, 2016) and *United States v. VanDyck*, Ninth Cir. No. 16-10524 (9th Cir. 2019).

Undersigned counsel is not aware of any other proceedings in state or federal trial or appellate courts, or in this Court, that are directly related to this case.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes

U.S. Constitution

Other Authorities

INTRODUCTION

Using a subpoena that required no showing of cause or suspicion, the police ascertained the identity of the Comcast subscriber associated with the Internet Protocol (IP) address used to transmit an image of child pornography via email. The rationale of *Carpenter v. United States*, 138 S. Ct. 2206 (2018), compels the conclusion that such acquisition of the subscriber information linked to an IP address requires a warrant.

In *Carpenter*, this Court held that the government must obtain a warrant to acquire cell-site location information, even if held by a third party, because such a search can reveal intimate details about a person's life. Especially given the ability to use an IP address to monitor internet usage, acquiring—without a warrant—the subscriber associated with an IP address similarly gives the government unwarranted access to *the content* of users' private online activities.

It also eviscerates the right to anonymous speech. The Fourth Amendment's protection of internet privacy in this context is therefore essential to safeguarding First Amendment rights in today's society.

Under the facts here, although they did not do so, the police could have established probable cause to support acquisition of the name and address of the subscriber associated with the IP address that was used to transmit child pornography. But, under current law, the police could have just as easily obtained via subpoena the identifying information of the subscriber linked to *any* IP address, without establishing even reasonable suspicion of criminal wrongdoing. For

example, the police could have detected that the user of a certain IP address had anonymously posted views online that were critical of certain government policies. The police could have then used a subpoena to ascertain the identity of the internet service subscriber assigned to that IP address, and then monitored the online and offline activities of that household and targeted individuals for prosecution based on their political views. The Fourth Amendment cannot abide the potential for such abuse in the digital age.

The courts of appeal to have recently addressed this recurring issue—whether a warrant is needed to obtain subscriber information linked to an IP address—have declined to reevaluate the propriety of applying the third-party doctrine in light of *Carpenter*. *See United States v. Morel*, 922 F.3d 1, 8-10 (1st Cir. 2019); *United States v. Wellbeloved-Stone*, 777 F. App'x 605, 607 (4th Cir. 2019) (unpublished); *United States v. VanDyck,* 776 F. App'x 495, 496 (9th Cir. 2019) (unpublished). An Arizona state court jurist, however, concluded that, under *Carpenter*'s reasoning, the Fourth Amendment requires a warrant to obtain this information. *State v. Mixton*, 447 P.3d 829, 846 (Ariz. Ct. App. 2019) (Eckerstom, J., dissenting in part), *review granted* (Nov. 19, 2019).

This Court should grant the writ to settle this important question of federal law. It should also abandon the widely criticized third-party doctrine in favor of case-by-case consideration of whether an interest falls within the ambit of the Fourth Amendment's protections.

OPINION BELOW

The court of appeals' decision (Appendix A) is unpublished, *VanDyck*, 776 F. App'x at 496.

JURISDICTION

The judgment of the United States Court of Appeals for the Ninth Circuit was entered on August 28, 2019. Appendix A. The Court of Appeals denied Mr. VanDyck's petition for rehearing and rehearing en banc on January 3, 2020. Appendix B. The Honorable Justice Kagan extended the time for filing the petition for 47 days, from April 2 to May 19, 2020. Appendix C. The Court automatically granted an extension for another 13 days, from May 19 to June 1, 2020, due to the COVID-19 crisis. Appendix D. The jurisdiction of this Court is invoked under 28 U.S.C. § 1254(1).

CONSTITUTIONAL PROVISION

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.

STATEMENT OF THE CASE

A. Material Facts

The opening brief includes a detailed recitation of the facts, with record citations. *See* Opening Brief of Appellant, *United States v. VanDyck*, Ninth Cir. No.

16-10524, DktEntry 37, 2018 WL 4561816, at *3-*8 (OB).

In March 2014, America Online submitted a tip to the National Center for Missing and Exploited Children (NCMEC), which included an image that contained child pornography. The image, sent from IP address 69.244.63.8, was attached to an email originating from doudykid@aim.com with the subject line "Re: please trade." NCMEC conducted an automated review, which determined that the IP address was located in Tucson and associated with Comcast, an internet service provider (ISP). The IP address at issue here is the address of the router provided by Comcast, which is shared every time the user of the address accesses the internet, such as by sending an email or visiting a website.[1]

NCMEC forwarded this information to Arizona law enforcement officials, who sought and obtained the issuance of a grand jury subpoena compelling Comcast to provide the name, address, and phone number of the subscriber assigned to that IP address at the relevant time. The subpoena process did not require prior judicial or grand jury authorization. Comcast responded the next day that the IP address was associated with a business called Premier Landscaping Services. The detectives determined that this business was owned by Mr. VanDyck, who lived in a home located at the address identified by Comcast.

Based on the above information and additional information ascertained by

[1] *See* Cale Guthrie Weissman*, What is an IP address and what can it reveal about you?,* BUSINESS INSIDER (May 18, 2015), available at https://www.businessinsider.com/ip-address-what-they-can-reveal-about-you-2015-5 (last visited May 21, 2020); *SEC v. PlexCorps*, No. 17-CV-7007-CBA-RML, 2018 WL 4299983, at *3 n.2 (E.D.N.Y. Aug. 9, 2018) (unpublished).

investigating Mr. VanDyck's prior law enforcement contacts, the Arizona detectives obtained a warrant to search Mr. VanDyck's home. The fruits of the state warrant led to Mr. VanDyck's federal indictment in this case.

B. District Court Proceedings

Mr. VanDyck moved under the Fourth Amendment to suppress the warrant and all evidence obtained as a result. He argued, *inter alia*, that an individual possesses a reasonable expectation of privacy in the subscriber information linked to an IP address and that the state detectives had unlawfully obtained his subscriber information by means of an illegal, purported state grand jury subpoena in violation of both state and federal law and the Fourth Amendment. The district court denied the motion to suppress. Mr. VanDyck was convicted of conspiracy to produce child pornography and possession of child pornography. *See* OB at *7-*8 (citing record).

C. Ninth Circuit Proceedings

On appeal, Mr. VanDyck argued, *inter alia*, that the Fourth Amendment requires a warrant supported by probable cause to obtain the subscriber information associated with an IP address, because individuals enjoy both a reasonable expectation of privacy and a proprietary interest in the linkage of that information. OB at *20-*36; Reply Brief of Appellant, *United States v. VanDyck*, Ninth Cir. No. 16-10524, DktEntry 69, 2019 WL 2290385, at *10-*17 (RB). He argued that, although 18 U.S.C. § 2703(c)(2) requires an ISP to disclose subscriber information to a government entity that uses a state grand jury subpoena, the good

faith exception to the exclusionary rule should not apply because Arizona law enforcement officials violated multiple state and federal laws in issuing the purported subpoena used to obtain his subscriber information from Comcast. OB at *36-*41; RB at *17-*20.

The Ninth Circuit concluded that the holding of *United States v. Forrester*, 512 F.3d 500, 510 (9th Cir. 2008)—that "internet users have no expectation of privacy in the IP addresses of the websites they visit" under the third-party doctrine—foreclosed Mr. VanDyck's argument and that it was "bound by . . . *Forrester* as it is not clearly irreconcilable with *Carpenter*." *VanDyck*, 776 F. App'x at 496. The en banc court denied review. Appendix B.

REASONS FOR GRANTING THE WRIT

I. A warrant is required to ascertain the identity of the subscriber associated with an IP address because of the wealth of private information that such an address, once linked to a particular subscriber, can reveal about that individual.

A. The Fourth Amendment requires a warrant for invasive searches that implicate the arbitrary exercise of government power, even if the government seeks information held by a third party.

The Fourth Amendment prohibits unreasonable searches and seizures. *Carpenter*, 138 S. Ct. at 2213, 2221. The "basic purpose of this Amendment . . . is to safeguard the privacy and security of individuals against arbitrary invasions by governmental officials." *Id.* at 2213 (citation omitted). "[W]arrantless searches are typically unreasonable where 'a search is undertaken by law enforcement officials to discover evidence of criminal wrongdoing.'" *Id.* at 2221 (citation omitted). Thus, "[i]n

the absence of a warrant, a search is reasonable only if it falls within a specific exception to the warrant requirement." *Id.* (citation omitted).

In *Carpenter*, this Court held that the government's "acquisition of [] cell-site [location] records was a search within the meaning of the Fourth Amendment." *Id.* at 2220. These records are generated every time a cell phone connects to the closest cell site to find the best signal. *Id.* at 2211. Wireless carrier companies collect and save this information for business purposes. *Id.* at 2212. Prosecutors sought and obtained court orders under the Stored Communications Act, 18 U.S.C. § 2703(d), for cell-site location records of the defendant, who was suspected of participating in a string of robberies. That statute merely requires a showing of "reasonable grounds to believe" that the records sought "are relevant and material to an ongoing investigation." *Carpenter*, 138 S. Ct. at 2212. The Court held that this showing was insufficient, because the Fourth Amendment requires a warrant supported by probable cause to gain access to seven days or more of cell-site location information; it declined to decide whether the government may gain access to such records for a more limited period without Fourth Amendment scrutiny. *Id.* at 2217, n.3, 2221.

In so holding, this Court declined to apply the third-party doctrine, under which the Court had previously held that an individual possesses no reasonable expectation of privacy—and hence no Fourth Amendment protection—in information voluntarily turned over to a third party. *Id.* at 2216-17 (citing *Smith v. Maryland*, 442 U.S. 735, 743-44 (1979) (telephone numbers dialed), and *United States v. Miller*, 425 U.S. 435, 443 (1976) (bank records)).

In declining to apply the third-party doctrine to cell-site location records, the *Carpenter* majority emphasized that "what [one] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected." *Id.* at 2217 (citing *Katz v. United States*, 389 U.S. 347, 351 (1967)). The Court recognized that, in the digital age, records held by third parties can "implicate[] basic Fourth Amendment concerns about arbitrary government power much more directly than corporate tax or payroll ledgers." *Id.* at 2222. The Court concluded that individuals enjoy a reasonable expectation of privacy in cell-site location information—which allows tracking of an individual's location over a period of time—despite the fact that a third-party wireless carrier possesses that information and uses it for business purposes. *Id.* at 2219-20, 2222. *See also United States v. Jones*, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring) (a warrant is needed for GPS monitoring because it provides "a wealth of detail about [a person's] familial, political, professional, religious, and sexual associations"); *id.* at 430 (Alito, J., concurring in the judgment) (society reasonably expects that law enforcement agents cannot "secretly monitor and catalogue" an individual's movements for a very long period).

The Court also observed that such information is not "voluntarily" "shared" as those terms are normally understood, because "cell phones and the services they provide are 'such a pervasive and insistent part of daily life' that carrying one is indispensable to participation in modern society." *Carpenter*, 138 S. Ct. at 2220 (quoting *Riley v. California*, 573 U.S. 373, 385 (2014)). People take their phones everywhere, including "into private residences, doctor's offices, political

headquarters, and other potentially revealing locales." *Id.* at 2218. Cell-site information can therefore be used not only to monitor a person's movements, but also to reconstruct a person's past movements. *Id.* The Court further noted that an individual's cell-site records are generated automatically whenever a phone is turned on and often involve no affirmative act on the user's part, such as with incoming calls, texts, or emails. *Id.* at 2220. *Carpenter*, therefore, compels courts to consider the propriety of the third-party doctrine in light of the unique circumstances and concerns implicated by the government's acquisition of information related to people's digital and online lives.

B. Under the rationale of *Carpenter* and other recent cases, the Fourth Amendment requires a warrant supported by probable cause to obtain the subscriber information associated with an IP address, because individuals enjoy a reasonable expectation of privacy-by-anonymity to connect to the internet in a home through an anonymous public IP address.

In *Forrester*, which preceded *Carpenter* and upon which the panel relied in this case, the Ninth Circuit held that the defendant had no reasonable expectation of privacy in the to/from addresses of email messages, the IP addresses of websites visited, and the total amount of data transmitted to or from an account. 512 F.3d at 510. The investigators in the *Forrester* case—who were aware of the defendant's identity—suspected the defendant's involvement in illegal drug activity and obtained a pen register analogue to monitor the above information. *Id.* at 505-06, 509-10. In rejecting the defendant's Fourth Amendment claim, the court relied on the third-party doctrine, and in particular on *Smith*, 442 U.S. 735, in which this

Court held that the use of a pen register that records numbers dialed from a phone line does not constitute a search for Fourth Amendment purposes. Other circuits have held, for similar reasons, that internet subscriber information is not protected by the Fourth Amendment. *See*, *e.g.*, *United States v. Perrine*, 518 F.3d 1196, 1204 (10th Cir. 2008) (citing cases). These conclusions must be reconsidered in light of *Carpenter*'s holding that application of the third-party doctrine depends upon whether people reasonably enjoy an expectation of privacy despite sharing information with a third-party service provider in order to obtain a service essential to modern life.

In explaining its rationale, the Ninth Circuit emphasized in *Forrester* that "a website typically only has one IP address even though it may contain hundreds of thousands of pages," and therefore the IP address of the website alone typically does not reveal much about the content reviewed. 512 F.3d at 510 & n.5. But the court acknowledged that constitutional problems may arise if government agents were able to ascertain the actual content reviewed by someone accessing a website. *Id.* at 510 & n.6. As explained below, agents *can* ascertain the *content* of internet activity engaged in by the user of a router's IP address.

In any event, under the logic of *Carpenter*, *Jones*, and *Riley*, a person has a reasonable expectation of privacy in the websites they visit, even if an agent is unable to ascertain content that a person has contributed or searched for within a site. Although some websites (like the New York Times) are vast, such that a person's visit to the site reveals little about their private beliefs or concerns, others

are highly specific and can provide particularized information about a person's familial, political, professional, religious, and sexual associations. In the internet era, personal and business information is often stored on a third-party's server instead of in a file cabinet. The third-party doctrine now allows the government access to exponentially more private information than was the case in the 1970s when *Smith* and *Miller* were decided. *See Riley*, 573 U.S. at 393-94 (discussing how mass transition from paper to digital storage heightened privacy interests in cell phones); *Jones*, 565 U.S. at 418 (Sotomayor, J., concurring) (noting significant privacy concerns implicated by "the warrantless disclosure to the Government of a list of every Web site [people] had visited in the last week, or month, or year").

1. The Constitution protects the right to speak and associate anonymously.

Ascertaining what society understands as a reasonable expectation of privacy requires consideration of "source[s] outside of the Fourth Amendment." *Rakas v. Illinois*, 439 U.S. 128, 143 n.12 (1978). The First Amendment is such a source. As emphasized in *Carpenter*, the Fourth Amendment must guard against infringements upon a person's "familial, political, professional, religious, and sexual associations." 138 S. Ct. at 2217. Freedom of association is also protected by the First Amendment. *Janus v. Am. Fed'n of State, Cty., & Mun. Employees, Council 31*, 138 S. Ct. 2448, 2463 (2018). The degree to which the Fourth Amendment protects internet privacy therefore must be viewed through the lens of the First Amendment.

A well-established component of the First Amendment is the right to speak and associate with anonymity. *See, e.g.*, *Buckley v. American Constitutional Law*

Found., 525 U.S. 182, 200 (1999) (invalidating, on First Amendment grounds, a Colorado statute that required initiative petition circulators to wear identification badges); *McIntyre v. Ohio Elections Comm'n*, 514 U.S. 334, 357 (1995) (overturning an Ohio law that prohibited the distribution of campaign literature that did not contain the name and address of the person issuing the literature; holding that "[u]nder our Constitution, anonymous pamphleteering is not a pernicious, fraudulent practice, but an honorable tradition of advocacy and dissent."); *Talley v. California*, 362 U.S. 60, 65 (1960) (invalidating a California statute prohibiting the distribution of "any handbill in any place under any circumstances" that did not contain the name and address of the person who prepared it; holding that "identification and fear of reprisal might deter perfectly peaceful discussions of public matters of importance").

"Anonymity is a shield from the tyranny of the majority . . . . It thus exemplifies the purpose behind the Bill of Rights . . . ." *McIntyre*, 514 U.S. at 357 (citing J. Mill, ON LIBERTY AND CONSIDERATIONS ON REPRESENTATIVE GOVERNMENT 1, 3-4 (R. McCallum ed. 1947)). Today, internet usage is integral to the exercise of First Amendment rights. *Packingham v. North Carolina*, 137 S. Ct. 1730, 1735 (2017) ("While in the past there may have been difficulty in identifying the most important places (in a spatial sense) for the exchange of views, today the answer is clear. It is cyberspace—the 'vast democratic forums of the Internet'"). The Fourth Amendment's protection of internet privacy is therefore essential to

protecting First Amendment rights in contemporary society.

Here, law enforcement used a subpoena to get the subscriber information linked to the IP address used to send the email that precipitated the investigation in this case. That subscriber information revealed the physical address of Mr. VanDyck's home office, and thus revealed the location of his residence. When, as here, a person uses an email address that does not reveal his identity, he reasonably expects that the email will not reveal his identity or the physical location of his home. Allowing law enforcement to ascertain a person's identity and physical location based on an anonymous email also contravenes a person's constitutionally protected right to anonymous speech.

2. Unmasking the identity of the subscriber associated with an IP address provides access to a detailed picture of the household's private online activities and contravenes the right to anonymity.

As the Supreme Court of Canada recently observed, subscriber information associated with an anonymous public IP address assigned to a router inside a home allows unfettered access to a detailed picture of the private online activities of the household. *R. v. Spencer*, 2 S.C.R. 212, 2014 SCC 43, ¶¶ 32, 46 (Can. 2014).[2]

A government agent can use the IP address as an internet search term. WHAT AN IP ADDRESS CAN REVEAL ABOUT YOU: A REPORT PREPARED BY THE TECHNOLOGY ANALYSIS BRANCH OF THE OFFICE OF THE PRIVACY COMMISSIONER OF CANADA (May

[2] available at https://www.canlii.org/en/ca/scc/doc/2014/2014scc43/2014scc43.html (last visited May 21, 2020).

2013) at 4 ("Canadian Privacy Commissioner Report").[3] These searches can reveal that IP address's file-sharing activities, records in web server log files, and web activities (as specifically as the *content* of edits to a particular Wikipedia page made by the user of an IP address and the *content* of the user's online searches). *Id.* at 4-7.[4] The information can also be used to ascertain where the user of an IP address has been physically. *Id.* at 7. Additionally, search engines may record users' search terms, and "cookies" can track consumer habits and reveal information about the options selected within a website, the websites visited previously and subsequently, and any personal information provided. *Spencer*, 2014 SCC 43, ¶ 46 (citing Nathaniel Gleicher, *Neither a Customer Nor a Subscriber Be: Regulating the Release of User Information on the World Wide Web*, 118 YALE L.J. 1945, 1948-49 (2009)). *See also United States v. Falso*, 544 F.3d 110, 124 n.20 (2d Cir. 2008) (noting that government can monitor the traffic on websites). Technological advances continue to make it even easier for the government to monitor the internet activity associated with an IP address. *See*, *e.g.*, *United States v. Thomas*, 788 F.3d 345, 347-48, 351 (2d Cir. 2015) (describing software program enabling government to monitor internet traffic from an IP address).

This internet data can reveal sensitive information regarding an individual's

[3] available at https://www.priv.gc.ca/media/1767/ip_201305_e.pdf (last visited May 21, 2020).

[4] For example, the analysts involved in this investigation were able to ascertain—using just an IP address—that the user of the address made certain extensive, detailed revisions to Wikipedia pages about certain television shows and history topics. *Id.* at 5. They were also able to ascertain that the user of the IP address "participated in a discussion board about a television channel" and "[v]isited a site devoted to sexual preferences following an online search for a specific type of person." *Id.* at 6.

political inclinations, health, religion, and sexuality. *Spencer*, 2014 SCC 43 at ¶ 46; Canadian Privacy Commissioner Report at 4-5; *State v. Reid*, 945 A.2d 26, 33 (N.J. 2008) (citing Daniel Solove, *Reconstructing Electronic Surveillance Law*, 72 GEO. WASH. L. REV. 1264, 1287 (2004)) (noting that, with the combination of subscriber information and an IP address, the government "can track a person's internet usage" and "learn the names of stores at which a person shops, the political organizations a person finds interesting, a person's . . . fantasies, her health concerns, and so on").

3. A warrant requirement is necessary to protect online privacy and anonymity.

For these reasons, the Supreme Court of Canada recently held that individuals enjoy a reasonable expectation of privacy when police attempt to obtain subscriber information matching an IP address. *Spencer*, 2014 SCC 43 at ¶ 66. The court concluded that such a law enforcement request is a search, which presumptively requires a warrant in the absence of exigent circumstances. *Id.* at ¶¶ 68-74.

In *Spencer*, the police identified an IP address used to access child pornography through a file-sharing program. *Id.* at ¶¶ 7-8. Then, without judicial authorization, police requested that the ISP reveal the name, address, and telephone number of the subscriber associated with the IP address. *Id.* at ¶¶ 11-12. The subscriber was identified as the defendant's sister, and police obtained a

warrant to search her home; they seized the defendant's computer and found child pornography images and videos. *Id.* at ¶¶ 11-14.

In holding that the defendant enjoyed a reasonable expectation of privacy under these circumstances, the *Spencer* court stressed that it must consider "not only the nature of the precise information sought, but also the nature of the information that it reveals." *Id.* at ¶ 26. Thus, "[t]he subject matter of the search was not simply a name and address of someone in a contractual relationship with [the ISP]. Rather, it was the identity of an Internet subscriber which corresponded to a particular internet usage." *Id.* at ¶ 32. The court emphasized "the significance of an IP address and what such an address, once identified with a particular individual, is capable of revealing about that individual, including the individual's online activity in the home." *Id.* (citation omitted).

The *Spencer C*ourt also explained that the issue was not whether the defendant had a "legitimate privacy interest in concealing his use of the Internet [to access] child pornography, but whether people generally have a privacy interest" when they use computers in their home, and outside their homes on portable devices. *Id.* at ¶¶ 36-37. In short, the court concluded that internet users reasonably expect to maintain online anonymity when using their devices in the home or elsewhere. *Id.* at ¶ 37. The defendant enjoyed this expectation, even though his sister was the subscriber, because he had his sister's permission to use the internet and lived in her home. *Id.* at ¶ 19.

Consistent with this Court's decisions in *Carpenter* and *Jones*, the *Spencer* court emphasized that "[t]he mere fact that someone leaves the privacy of their home and enters a public space does not mean that the person abandons all of his or her privacy rights." *Id.* at ¶ 44 (citations omitted). Although "we may expect to be casually observed" in some public contexts, we "may justifiably be outraged by intensive scrutiny" and surveillance when we expect to "merge into the situational landscape." *Id.* (citation omitted).

The *Spencer* court analogized prolonged, extensive surveillance in physical spaces to the prolonged, extensive surveillance of an individual's internet usage that is possible when police obtain subscriber information associated with an IP address. *Id.* at ¶¶ 46-47. Armed with that information, police can monitor an individual's virtual travels on the internet in a way that reveals "the privacies of life," including a person's "familial, political, professional, religious, and sexual associations." *Carpenter*, 138 S. Ct. at 2217 (quoting *Jones*, 565 U.S. at 415 (Sotomayor, J., concurring) and *Riley*, 573 U.S. at 402-03). This Court has already ruled that individuals enjoy a reasonable expectation of privacy against such intrusions.

Moreover, consistent with our First Amendment freedom to speak and associate anonymously, the *Spencer* court emphasized the importance of an individual's right to "present ideas publically" without being "identified as their author." *Spencer*, 2014 SCC 43 at ¶ 45 (citing A.F. Westin, PRIVACY AND FREEDOM 32 (1970)). "[A]nonymity," the court observed, is an aspect of "informational privacy"

that is "particularly important in the context of Internet usage." *Id.* The internet allows people to communicate regarding matters of public importance in a way that is "accessible to millions of people but is not identified with [the] author" of the communication. *Id.*

Even if the unmasking of the subscriber assigned to an IP address only links the subscriber to one discrete internet activity, "each discrete internet visit may expose an acutely private thought process and may do so in a context where the visitor has taken every precaution to retain his anonymity." *Mixton*, 447 P.3d at 846 (Eckerstom, J., dissenting in part). "Surely, if the government is required to obtain a warrant to track, through technology, a suspect's public physical movements, it should likewise need a warrant to expose a suspect's private digital behavior." *Id.* at 846. In *Mixton*, the majority held that a warrant is required under the Arizona Constitution to obtain the identity of a subscriber associated with an IP address. *Id.* at 837-44. Judge Eckerstom dissented in part because he would hold that, in light of *Carpenter*, the Fourth Amendment "provides the same protection." *Id.* at 845-47. The Arizona Supreme Court granted review of both the state constitutional and Fourth Amendment claims, but it has not yet ruled. *See* Arizona Supreme Court Oral Argument Case Summary, *State v. Mixton*, CR 19-0276-PR.[5]

Like cell-phone use, internet use is not truly voluntary in today's society. It is pervasive and integral to day-to-day life. Internet users have "no [] choice" but to

[5] available at https://www.azcourts.gov/clerkofcourt/AgendasandCasesbeforetheCourt.aspx (last visited May 21, 2020).

"have an IP address to access a website." *Reid*, 945 A.2d at 33 (holding that New Jersey Constitution protects an individual's privacy interest in the subscriber information provided to an ISP). To get an IP address, individuals must subscribe to an internet service provider. *Id.* Only that provider "can translate an IP address into a user's name." *Id.* Thus, the third-party doctrine should not apply in this situation.

Therefore, as explained above, protecting the right to speak and search anonymously on the internet is, today, essential to protecting the ideals embodied in the Bill of Rights. Identifying, without a warrant, the subscriber associated with an IP address used for internet communication eviscerates the right to anonymous speech. As the Supreme Court of Canada held in *Spencer*, obtaining such information should require a warrant supported by probable cause. That conclusion is compelled here by this Court's First Amendment precedent and recent opinions, including *Carpenter*, addressing the Fourth Amendment's protection of privacy in the digital age.

C. An individual also has a property interest in the subscriber information linked to an IP address that warrants Fourth Amendment protection.

Fourth Amendment protection of the subscriber information linked to an IP address is also warranted by the subscriber's proprietary interest in that information. *See Carpenter*, 138 S. Ct. at 2272 (Gorsuch, J., dissenting). Common law and current positive law aid in determining whether information belongs to an individual or entity, such that the government should need a warrant supported by

probable cause to access it. *See id.* at 2268.

Our laws and traditions recognize the right to informational privacy—"the claim of individuals . . . to determine for themselves when, how and to what extent information about themselves is communicated to others." *U.S. Dep't of Justice v. Reporters Comm. for Freedom of the Press*, 489 U.S. 749, 764 n.16 (1989) (quoting A. WESTIN, PRIVACY AND FREEDOM 7 (1967)). This Court has assumed without deciding that the Constitution protects this right. *See* Scott Skinner-Thompson, *Outing Privacy*, 110 NW. U. L. REV. 159, 163 & n.10 (2015) (citing *NASA v. Nelson*, 562 U.S. 134, 138 (2011); *Nixon v. Adm'r of Gen. Servs.*, 433 U.S. 425, 457 (1977); *Whalen v. Roe*, 429 U.S. 589, 605-06 (1977)).

The right to informational privacy was protected at common law. *Reporters Comm. for Freedom of the Press*, 489 U.S. at 763 & n.15 (citing Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 198 (1890); RESTATEMENT (SECOND) OF TORTS § 652D, pp. 385-386 (1977)). Laws such as the Privacy Act of 1974 (5 U.S.C. § 552a), the Health Insurance Portability and Accountability Act of 1996 and 2013 (42 U.S.C. § 1320d-6), and the Driver's Privacy Protection Act of 1994 (18 U.S.C. § 2721) effectuate the right to informational privacy.

This right logically includes the information that can be revealed by the disclosure of subscriber information associated with an IP address. Indeed, federal and state laws protect against disclosure of this kind of information.

Arizona law prohibits the procurement of communication service records,

including subscriber information, without the consent of the customer or by false or deceptive means. ARIZ. REV. STAT. §§ 44-1376(1), 44-1376.01(A)(1) & (C).

Federal law likewise prohibits cable service providers such as Comcast, which provided Mr. VanDyck's internet service, from disclosing subscriber information without customer consent. 47 U.S.C. § 551(c). That statute further prohibits disclosure to a government entity except upon a showing by clear and convincing evidence that the subject of the information is suspected of engaging in criminal activity, and the subject has the opportunity to appear and contest the claim. § 551(h). Subscriber information can also be disclosed as authorized under chapters 119, 121, or 206 of Title 18 (which includes the use of state grand jury subpoenas under 18 U.S.C. § 2703(c)(2)), except that such disclosure shall not include records revealing cable subscriber selection of video programming. 47 U.S.C, § 551(c)(2)(D). As explained above, providing the subscriber information linked to an IP address allows the government a window into an individual's life that is at least as revealing as the video programming a person selects.

The federal Telecommunications Act also generally prohibits telecommunications carriers from disclosing, without customer consent,[6] customer proprietary network information, including information regarding the type and amount of use of a customer's telecommunications service and information contained in the customer's bills (except for subscriber list information for the

[6] Exception are made for collection of bills, protecting the rights and property of the carrier, rendering services desired by the customer, and emergency situations. 47 U.S.C. § 222(d).

purpose of publishing telephone directories). 47 U.S.C. § 222. The rationale for this protection of telecommunications privacy logically applies to the subscriber information linked to an IP address.

Americans overwhelmingly consider their internet browsing habits to be private. PEW RESEARCH CENTER, PUBLIC PERCEPTIONS OF PRIVACY AND SECURITY IN THE POST-SNOWDEN ERA (November 12, 2014) (70% of adults consider the websites they have visited to be "very sensitive" or "somewhat sensitive" information).[7] The traditions and laws discussed above reflect society's conception that a person has the right to control the linkage of personally identifiable information with internet usage. This proprietary interest further supports a warrant requirement for government acquisition of the subscriber information linked to an IP address.

II. The Court should abandon the third-party doctrine in favor of a case-by-case determination of whether an interest falls within the scope of the Fourth Amendment's protections.

Miller, 425 U.S. 435, and *Smith*, 442 U.S. 735, were based on the faulty premise that it is unreasonable for individuals to expect any privacy when they provide information to third parties. *See People v. Chapman*, 679 P.2d 62, 67 & n.6 (Cal. 1984) (individuals, who must use a telephone to participate in modern life, enjoy a reasonable expectation of privacy in telephone numbers of calls they make or receive). In the digital age, it is all but impossible to perform everyday tasks—such as using one's cell phone, conducting an internet search, or sending an email—

[7] available at http://www.pewinternet.org/2014/11/12/public-privacy-perceptions (last visited May 21, 2020).

without revealing personal information to third-party service providers. It is entirely reasonable for individuals to expect the government to get a warrant before obtaining certain information held by such providers, such as "a list of every Web site they had visited in the last week, or month, or year." *Jones*, 565 U.S. at 418 (Sotomayor, J., concurring).

It is simply untenable to conclude that, in all circumstances, individuals "assume the risk" that a third party will disclose information to the government. The assumption-of-risk doctrine is a creature of tort law, which requires that an individual expressly or impliedly agree to accept a risk of harm. *Carpenter*, 138 S. Ct. at 2263 (Gorsuch, J., dissenting). People, however, do not agree to accept such a risk when they disclose information on the understanding that it will not be shared with others and will be used only for a specific purpose, *id.,* as they do when they entrust financial records to a bank or when they dial a telephone number on a landline phone.

Thus, the assumption-of-risk justification "made little sense [even] when it appeared in the 1970s." David. A. Harris, *Riley v. California and the Beginning of the End for the Third-Party Search Doctrine*, 18 U. PA. J. CONST. L. 895, 898-99 (2016). Many states have already rejected the third-party doctrine on state constitutional grounds. *See*, *e.g*, *State v. Walton*, 324 P.3d 876, 906 (Haw. 2014); *State v. Thompson*, 810 P.2d 415, 418 (Utah 1991); *Reid*, 945 A.2d at 31-34; *Shaktman v. State*, 553 So. 2d 148, 151 (Fla. 1989); *State v. Thompson*, 760 P.2d 1162, 1163 (Idaho 1988); *Chapman*, 679 P.2d at 67 & n.6; *People v. Sporleder*, 666

P.2d 135, 141-42 (Colo. 1983); *Commonwealth v. DeJohn*, 403 A.2d 1283, 1289 (Pa. 1979); *People v. DeLaire*, 610 N.E.2d 1277, 1282 (Ill. Ct. App. 1993).

The realities of the digital age bring the third-party doctrine's flaws into sharp focus. Under that doctrine, individuals who undergo genetic testing with a third party to learn more about their ancestry risk warrantless disclosure of their DNA profiles to law enforcement. Claire Abrahamson, *Guilt by Genetic Association: The Fourth Amendment and the Search of Private Genetic Databases by Law Enforcement*, 87 FORDHAM L. REV. 2539, 2564 (2019). The third-party doctrine likewise leaves users of the internet "cloud" vulnerable to the warrantless acquisition of information contained in personal emails, documents, and photographs, even if users take reasonable precautions to ensure security. *See Riley*, 573 U.S. at 397 ("Cell phone users often may not know whether particular information is stored on the device or in the cloud, and it generally makes little difference."). Today, therefore, under the third-party doctrine's flawed logic, the government can obtain, at will, an individual's "virtual current biography," *Chapman*, 679 P.2d at 68, without running afoul of the Fourth Amendment, something the founders of our nation could not have fathomed and surely would not have condoned.

The Court should abandon the third-party doctrine in favor of case-by-case consideration of whether an interest falls within the ambit of the Fourth Amendment's protection. Positive law provides a logical floor for determining which interests are protected. *See Carpenter*, 138 S. Ct. at 2267-71 (Gorsuch, J.,

dissenting). "[I]f it's objectionable for a private party to encroach on privacy or security in a certain way, then it's at least as objectionable—and probably much more objectionable—for the government to do the same." Richard M. Re, *The Positive Law Floor*, 129 HARV. L. REV. FORUM 313, 333 (2016). Thus, courts should presume that the Fourth Amendment requires the government to get a warrant to invade an individual's privacy if it would be unlawful for a nongovernment actor to similarly invade privacy. William Baude & James Y. Stern, *The Positive Law Model of the Fourth Amendment*, 129 HARV. L. REV. 1821, 1823, 1831 (2016).

Positive law, however, cannot be the only basis for defining Fourth Amendment protections. Regardless of positive law, the Court "must assur[e] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted," *Jones,* 565 U.S. at 406 (quoting *Kyllo v. United States*, 533 U.S. 27, 34 (2001)), and extend that protection to "modern analogues" of the rights protected at the founding. *Carpenter*, 138 S. Ct. at 2271 (Gorsuch, J., dissenting).

The *Katz* reasonable-expectation-of-privacy test—*sans* the third-party doctrine—must also remain to fill in gaps and account for democratic distortions. *See* Re, *supra*, at 329 (discussing instances in which democratic lawmaking will not adequately protect Fourth Amendment interests). *See also Carpenter*, 138 S. Ct. at 2265-66 (Gorsuch, J., dissenting) (acknowledging that *Katz* "is capable of principled application"). For example, Fourth Amendment protection must not depend on the whim of tyrannical majorities who want to make it easier for the government to

investigate certain "politically disempowered" individuals or groups based on improper motives. Re, *supra*, at 326, 329. Nor can it be manipulated by powerful lobbyists "with focused concerns," including "data brokers [with] an interest in the sale of personal data." *Id.* at 329.

CONCLUSION

For the reasons set forth above, the Court should grant the writ of certiorari.

Respectfully submitted this 28th day of May, 2020.

JON M. SANDS
Federal Public Defender
District of Arizona

s/M. Edith Cunningham
*M. Edith Cunningham
Assistant Federal Public Defender
407 W. Congress Street, Suite 501
Tucson, Arizona 85701
Telephone: (520) 879-7500
Facsimile: (520) 879-7600
edie_cunningham@fd.org
**Counsel of Record*