No. _____

IN THE SUPREME COURT OF THE UNITED STATES

WILLIAM MIXTON,

Petitioner,

vs.

STATE OF ARIZONA,

Respondent.

ON PETITION FOR A WRIT OF CERTIORARI
TO THE ARIZONA SUPREME COURT

PETITION FOR WRIT OF CERTIORARI

DAVID J. EUCHNER
Counsel of Record
ABIGAIL JENSEN
Pima County Public Defender's Office
33 N. Stone, 21st Floor
Tucson, Arizona 85701
Telephone: (520) 724-6800
David.Euchner@pima.gov
Abigail.Jensen@pima.gov

Attorneys for Petitioner
William Mixton

QUESTIONS PRESENTED

Police identified William Mixton as the user of an instant-messaging account through the issuance of two administrative subpoenas, both of which involved searches of private information without judicial approval. A slender majority of the Arizona Supreme Court affirmed, determining that the exception to the third-party doctrine in *Carpenter v. United States*, 138 S. Ct. 2206 (2018), was limited to cell site location information and did not create a reasonable expectation of privacy in his IP address or subscriber information.

The questions presented are:

Should this Court overrule the third-party doctrine as stated in *Miller* and *Smith* as being inconsistent with a reasonable expectation of privacy under *Katz v. United States*, 389 U.S. 347 (1967)?

Alternatively, should this Court find that the third-party doctrine is inconsistent with the Fourth Amendment and adopt the Positive Law Model as described in Justice Gorsuch's dissenting opinion in *Carpenter*?

TABLE OF CONTENTS

PAGES

TABLE OF CASES AND AUTHORITIES

UNITED STATES SUPREME COURT CASES PAGES

ARIZONA CASES

OTHER CASES

UNITED STATES CODE

CONSTITUTIONAL PROVISIONS

OTHER AUTHORITIES

PETITION FOR WRIT OF CERTIORARI

William Mixton respectfully petitions for a writ of certiorari to review the Arizona Supreme Court's opinion dated January 11, 2021, which held that the Fourth Amendment affords no protection for the privacy of personal information retained by third parties from government snooping.

In a pair of cases decided in the 1970s, this Court created the "third-party doctrine" which denies any reasonable expectation of privacy in infromation possessed or controlled by third parties. In *United States v. Miller*, 425 U.S. 435 (1976), this Court held that a person has no reasonable expectation of privacy in their bank records. Then, in *Smith v. Maryland*, 442 U.S. 735 (1979), this Court approved the practice of police demanding a telephone company install a pen register to collect all of the telephone numbers dialed by the suspect. Both cases relied on a strained interpretation of what constitutes a reasonable expectation of privacy under *Katz v. United States*, 389 U.S. 347 (1967).

Both *Miller* and *Smith* were widely criticized at the time, and that criticism has only increased with time. Federal courts are constrained by this Court's interpretation of the Fourth Amendment, but many state

courts have rejected the third-party doctrine under their state constitutions. Those state courts that have refused to extend broader protections through their state constitutions have often done so out of deference to this Court, as did the Arizona Supreme Court in this case.

In *Carpenter v. United States*, 585 U.S. __, 138 S. Ct. 2206 (2018), the petitioner neither asked this Court to overrule the third-party doctrine nor asserted an alternative to *Katz* as a basis for finding Fourth Amendment protection. *See id.* at 2272 (Gorsuch, J., dissenting). In addition to relying on *Katz*, this petition raises that alternative basis and presents an ideal opportunity to overrule a doctrine that has run its course. In its place, this Court should adopt the Positive Law Model.

Internet users' willingness to share identifying information with a provider in order to obtain access to the Internet does not equate with an expectation that the government should have access to that information in order to connect anonymous online activity to their identity without judicial review or opportunity to challenge the government's demand. For these reasons, this Court should accept review of this case and overrule the third-party doctrine.

OPINIONS BELOW

The Arizona Court of Appeals' opinion dated July 29, 2019, is reported at 447 P.3d 829 (Ariz. Ct. App. 2019). Exhibit 1. The Arizona Supreme Court's opinion dated January 11, 2021, is reported at 478 P.3d 1227 (Ariz. 2021). Exhibit 2.

STATEMENT OF JURISDICTION

The Arizona Court of Appeals, Division Two, entered its judgment on July 29, 2019. Exhibit 1. The Arizona Supreme Court entered its judgment on January 11, 2021. Exhibit 2. The issues raised herein were raised before the Arizona courts as issues of federal constitutional law. Exhibits 1, 2. This Court has jurisdiction pursuant to 28 U.S.C. § 1257(a).

CONSTITUTIONAL PROVISIONS

The Fourth Amendment to the United States Constitution provides as follows:

> 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.

Section One of the Fourteenth Amendment to the United States Constitution provides as follows:

> All persons born or naturalized in the United States, and subject to the jurisdiction thereof, are citizens of the United States and of the state wherein they reside. No state shall make or enforce any law which shall abridge the privileges or immunities of citizens of the United States; nor shall any state deprive any person of life, liberty, or property, without due process of law; nor deny to any person within its jurisdiction the equal protection of the laws.

STATEMENT OF THE CASE

Petitioner agrees with the statement of facts in the opinion of the Arizona Supreme Court:

> In 2016, an undercover Tucson Police Department detective posted an advertisement on an online forum seeking users interested in child pornography. The detective was contacted by someone with the username "tabooin520," who asked to be added to a group chat on a messaging application called "Kik." Once added, tabooin520 sent images and videos of child pornography to the group chat and to the detective.
>
> Federal agents with Homeland Security Investigations ("HSI"), at the request of the detective, served a federal administrative subpoena authorized under federal law on Kik to obtain tabooin520's IP address. Kik provided the IP address to the detective. The detective, using publicly available databases, determined that Cox Communications ("Cox") was the ISP for the IP address. HSI agents then served another federal administrative subpoena on Cox for the subscriber information associated with the IP address.
>
> Cox complied with the subpoena, disclosing the subscriber information—name, street address, and phone number—of William Mixton. The detective used this information to obtain and execute a search warrant on Mixton's residence. Detectives seized a cell phone, an external hard drive, a laptop, and a desktop computer. A subsequent search of these devices revealed photos and videos of child

> pornography, as well as the messages, photos, and videos that Mixton, under the username "tabooin520," sent to the detective.
>
> Mixton was indicted on twenty counts of sexual exploitation of a minor under fifteen years of age. Mixton moved unsuccessfully to suppress the subscriber information and all evidence seized from his residence on the grounds that the Fourth Amendment to the United States Constitution and article 2, section 8 of the Arizona Constitution require a warrant or court order to obtain his IP address and ISP subscriber information. A jury convicted Mixton on all counts, and he appealed.

State v. Mixton (Mixton II), 478 P.3d 1227, 1230 (Ariz. 2021).

The three-judge panel of the Arizona Court of Appeals reached three different conclusions. Judge Eppich wrote for the court, holding that *Miller* and *Smith* constrained the court's interpretation of the Fourth Amendment and that this Court expressly restrained its holding in *Carpenter* to the facts of that case, but that the state constitution should afford greater privacy protection. *State v. Mixton (Mixton I)*, 447 P.3d 829, 836-44 (Ariz. Ct. App. 2019). Judge Eckerstrom concurred as to the protection afforded by the state constitution but held that the Fourth Amendment would also protect the privacy of this information, *id*. at 845-47 (Eckerstrom, J., concurring in part, dissenting in part), while Judge Espinosa dissented from affording this information any protection at all, *id*. at 847 (Espinosa, J., concurring in part and dissenting in part).

The Arizona Supreme Court split 4-3 in favor of finding no protection afforded by either the Fourth Amendment or state constitution. The majority held that "*Carpenter* expressly preserved the third-party doctrine's existing application to information, such as cell phone and bank records, that is shared with a third party," and that no federal court has yet to extend *Carpenter* to the information at issue in this case. *Mixton II*, 478 P.3d at 1232-34. The majority then rejected Mixton's argument for broader protection under the state constitution. *Id.* at 1234-40. Justice Bolick, joined by Chief Justice Brutinel and Vice Chief Justice Timmer, dissented and held that the state constitution protected this information. *Id.* at 1245 (Bolick, J., dissenting). The dissenters explicitly found it "unnecessary to reach the Fourth Amendment issue" based on its decision on independent state grounds, but in a footnote, they suggested

> that the third-party doctrine may not apply given that Mixton did not provide the information obtained by the government to a single entity. No employee at Kik knew Mixton's identity, only his IP address; and no employee at the ISP could have connected Mixton's IP address to the postings. The police aggregated information, rather than retrieving it from a third party to which Mixton conveyed it in its totality.

Id. at 1253 n.4.

REASONS FOR GRANTING THE WRIT

This Court should grant this petition because there are two reasons for overruling the third-party doctrine.[1] First, there is an intractable split among the states whether, under *Katz*, there is a reasonable expectation of privacy for information provided to banks, telephone companies, and Internet providers, notwithstanding the third-party doctrine as stated in *Miller and Smith*. Second, the *Katz* standard for determining reasonable expectations of privacy has confounded this Court and other state and federal courts, and this Court may take the opportunity to announce a clearer means for protecting Fourth Amendment rights in information shared with third parties: the Positive Law Model. This case offers an ideal vehicle to resolve either or both of these questions.

I. *Miller* and *Smith* should be overruled because they are inconsistent with *Katz*.

In *Katz*, this Court recognized that emerging technology allowed

[1] Although Mixton challenged the searches below on Fourth Amendment grounds, he did not present identical arguments in the Arizona courts as the grounds presented in this petition, because those courts lacked authority to modify or ignore this Court's previous rulings in *Miller* and *Smith*. Regardless, because he challenged those searches under the Fourth Amendment, that issue is fairly presented here. *Yee v. City of Escondido*, 503 U.S. 519, 535 (1992).

government agents to snoop into communications that should be recognized as private but did not involve any trespass. "[T]he Fourth Amendment protects people, not places. What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected." *Katz*, 389 U.S. at 351. With emerging technology comes the ability of law enforcement to find new ways to obtain private information that violate Fourth Amendment rights without committing a trespass. *Id*. at 353. These changes invoke the question of "what limits there are upon this power of technology to shrink the realm of guaranteed privacy." *Kyllo v. United States*, 533 U.S. 27, 34 (2001).

This Court justified the third-party doctrine on the ground that, by voluntarily disclosing information to another, the person assumes the risk that the other person will disclose the information to the government. *Smith*, 442 U.S. at 744 (telephone customer assumes the risk that the phone company will disclose the phone numbers she dials from her home phone to the police); *Miller*, 425 U.S. at 442 (defendant had no expectation of privacy in bank records since they "contain only

information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business."). The Court purported to apply *Katz* to the circumstances of those cases. *Miller*, 425 U.S. at 442; Smith, 442 U.S. at 741-42. Essentially, the logic of the third-party doctrine rests on the false assumption that "[c]onsenting to give a third party access to private papers that remain my property is … the same thing as consenting to a search of those papers by the government." *Carpenter*, 138 S. Ct. at 2263 (Gorsuch, J., dissenting).

From the outset, the third-party doctrine was erected on a rickety foundation. In his dissent in *Miller*, Justice Brennan stated:

> For all practical purposes, the disclosure by individuals or business firms of their financial affairs to a bank is not entirely volitional, since it is impossible to participate in the economic life of contemporary society without maintaining a bank account. In the course of such dealings, a depositor reveals many aspects of his personal affairs, opinions, habits and associations. Indeed, the totality of bank records provides a virtual current biography…. To permit a police officer access to these records merely upon his request, without any judicial control as to relevancy or other traditional requirements of legal process, and to allow the evidence to be used in any subsequent criminal prosecution against a defendant, opens the door to a vast and unlimited range of very real abuses of police power.

Miller, 425 U.S. at 451 (Brennan, J., dissenting) (quoting *Burrows v. Superior Court*, 13 Cal.3d 238, 247 (1974)). Justice Marshall made a

similar point in his *Smith* dissent:

> But even assuming, as I do not, that individuals "typically know" that a phone company monitors calls for internal reasons …, it does not follow that they expect this information to be made available to the public in general or the government in particular. Privacy is not a discrete commodity, possessed absolutely or not at all. Those who disclose certain facts to a bank or phone company for a limited business purpose need not assume that this information will be released to other persons for other purposes.

Smith, 442 U.S. at 749 (Marshall, J., dissenting) (citations omitted).

More recently, Justice Sotomayor expressed her concerns about the applicability of the third-party doctrine in the context of Internet users:

> More fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks. People disclose 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. Perhaps … some people may find the tradeoff of privacy for convenience worthwhile, or come to accept this diminution of privacy as inevitable, and perhaps not. 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. But whatever the societal expectations, they can attain constitutionally protected status only if our Fourth Amendment jurisprudence ceases to treat secrecy as a prerequisite for privacy. I would not assume that all

> information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection.

United States v. Jones, 565 U.S. 400, 417-18 (2012) (Sotomayor, J., concurring) (emphasis added, internal citation and quotation marks omitted). And in *Carpenter*, Justice Gorsuch stated:

> Today we use the Internet to do most everything. Smartphones make it easy to keep a calendar, correspond with friends, make calls, conduct banking, and even watch the game. Countless Internet companies maintain records about us and, increasingly, for us. Even our most private documents—those that, in other eras, we would have locked safely in a desk drawer or destroyed—now reside on third party servers. *Smith* and *Miller* teach that the police can review all of this material, on the theory that no one reasonably expects any of it will be kept private. But no one believes that, if they ever did.

Carpenter, 138 S. Ct. at 2262-63 (Gorsuch, J., dissenting).

Contrary to the notion that people cannot possibly expect information they disclose to third-party service providers, like banks, cellphone companies, internet service providers, websites and online messaging applications, the empirical data shows that people do, in fact, expect their data will be protected, at least from government seizure. Studies show that the vast majority of Americans believe that it is important to maintain privacy and confidentiality in their activities. *See*

Mary Madden & Lee Raine, Americans' Attitudes About Privacy, Security, and Surveillance 4, Pew Research Center (May 20, 2015), https://www.pewresearch.org/internet/wp-content/uploads/sites/9/2015/05/Privacy-and-Security-Attitudes-5.19.15_FINAL.pdf (last visited June 8, 2021). Ninety-three percent of adults said that being in control of who can get information about them is important, and ninety percent said that controlling what information is collected about them is important. *Id*. The same survey also shows that ninety-three percent of adults believe it is essential that they be able to share private information with others in their lives. *Id*. The study thus shows that people believe both that it is essential to protect information and also that disclosing that same information to a trusted individual does not extinguish their privacy interests in that information.

Application of the third-party doctrine also threatens other important constitutional interests. Individuals today conduct the vast majority of their expressive lives through technology. As a result, we entrust the most sensitive information imaginable—about our politics, religion, families, finances, health, and sexual lives—to third parties. *See Riley v. California*, 573 U.S. 373, 396-97 (2014) (describing how mobile

phone applications "can form a revealing montage of the user's life" and store it "in the cloud"). Realities of the digital age provide good reasons to reject the assumptions that underlie the third-party doctrine and to recognize that information retains its private nature even if disclosed to a third party. Even revealing one's name might invade a zone of privacy, depending on context: "One's identity is a gateway to information collected by third persons—some collection occurring even without a person's knowledge; only context can determine whether the disclosure of one's name would be the key that unlocks the door to a protected zone of privacy." *State v. Walton*, 324 P.3d 876, 909 (Haw. 2014).

Nearly every individual interaction with another person or business using modern technology generates a record. These records—created and retained by a wide variety of tools, services, and companies—reveal highly private and intimate details about an individual's life, including political and religious activities. *Riley*, 573 U.S. at 396. The companies and services often collect this sensitive information without a user's knowledge or explicit consent. In fact, platforms, apps, and other online services are often intentionally designed to mislead users into revealing these kinds of highly sensitive information. *See, e.g.*, Shoshana

Zuboff, *The Age of Surveillance Capitalism* 274 (2019). Under these circumstances, it cannot rationally be said that Internet users have voluntarily assumed the risk of government disclosure. Among academic experts and many regulators, it is widely accepted that "[i]n most cases that matter, the assumption that users have actual notice or meaningful choice is an illusion." Neil Richards & Woodrow Hartzog, *Taking Trust Seriously In Privacy Law*, 19 Stan. Tech. L. Rev. 431, 444 (2016).

What this Court recognized in *Carpenter* about cell phones and location data—that opting out is not a realistic option in the modern world—is increasingly true of many kinds of digital information. Employment, access to government services, political and social engagement, and myriad other daily activities are all dependent on nearly constant online access. Connecting to family, friends, and coworkers can require digital-age tools that unavoidably collect data. *See* Stuart A. Thompson & Charlie Warzel, "Twelve Million Phones, One Dataset, Zero Privacy," *New York Times*, Dec. 19, 2019, https://perma.cc/F72N-NBN6.

Digital data—including data in the hands of third parties—implicates the kind of expressive and associational activities that courts

have long endeavored to protect. *See Riley*, 573 U.S. at 395 (contents of cell phones); *United States v. Warshak*, 631 F.3d 266, 286 (6th Cir. 2010) (email). This Court has also recognized that, when significant First Amendment rights are at stake, the warrant requirement must be adhered to with "scrupulous exactitude." *Stanford v. Texas*, 379 U.S. 476, 485 (1965); *Zurcher v. Stanford Daily*, 436 U.S. 547, 564 (1978). A search or seizure that endangers these expressive interests must, at the least, be made pursuant to a warrant supported by probable cause. *Zurcher*, 436 U.S. at 565; *Roaden v. Kentucky*, 413 U.S. 496, 504 (1973).

Finally, amid increasing concerns about inequality in our society, the third-party doctrine threatens to further divide us into those who, out of necessity or otherwise, are willing to sacrifice their personal privacy in order to take advantage of all that digital technology offers in our modern world and those who live in a shadow world without such access because they value their privacy and wish to protect their lives from government intrusion at will. *See Smith*, 442 U.S. at 750 (Marshall, J., dissenting) ("[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."); *see also United States v. Davis*, 785 F.3d 498, 525 (11th

Cir. 2015) (Rosenbaum, J., concurring) ("In our time, unless a person is willing to live 'off the grid,' it is nearly impossible to avoid disclosing the most personal of information to third party service providers on a constant basis, just to navigate daily life.").

The third-party doctrine, while purporting to follow *Katz*, instead turns *Katz*'s reasoning on its head. The time has come for *Miller* and *Smith* to be overruled.

II. State Courts Are Intractably Divided On Whether to Follow the Third-Party Doctrine.

Because the third-party doctrine was settled in this Court's Fourth Amendment jurisprudence nearly a half century ago, there is no split in federal authority on the questions presented in this petition. *See Rodriguez de Quijas v. Shearson/American Express, Inc.*, 490 U.S. 477, 484 (1989) ("If a precedent of this Court has direct application in a case, yet appears to rest on reasons rejected in some other line of decisions, the [lower court] should follow the case which directly controls, leaving to this Court the prerogative of overruling its own decisions.").

The states, however, are free to chart their own course and provide greater protections under state constitutions and state laws, *see City of Mesquite v. Aladdin's Castle, Inc.*, 455 U.S. 283, 293 (1982), and many

states have rejected the third-party doctrine as a matter of state law. Both the *Mixton* majority and dissent "recognized the value in uniformity" between state and federal law. *Mixton II*, 478 P.3d at 1235 (majority), 1245-46 (dissent). This is particularly true when there is a difference between state and federal courts in recognizing privacy interests. By rejecting the third-party doctrine, this Court can assist in returning uniformity to state courts.

At least ten states have followed the third-party doctrine as given in *Miller* and *Smith*: Alabama, Arizona, Georgia, Kansas, Maryland, North Carolina, North Dakota, Oklahoma, South Carolina, and West Virginia. On the other hand, at least a dozen states have rejected the reasoning in *Miller* and *Smith*: California, Colorado, Florida, Hawai'i, Idaho, Illinois, Massachusetts, Montana, New Jersey, Pennsylvania, and Utah.

The New Jersey Supreme Court has consistently rejected *Smith* since its earliest opportunity to forge an independent path. In *State v. Hunt*, 450 A.2d 952, 956 (N.J. 1982), that court observed:

> It is unrealistic to say that the cloak of privacy has been shed because the telephone company and some of its employees are aware of this information. . . . This disclosure has been necessitated because of the nature of the instrumentality, but

> more significantly the disclosure has been made for a limited business purpose and not for release to other persons for other reasons.

More recently, the same court rejected *Miller*, noting that

> although bank customers voluntarily provide information to banks, "they do so with the understanding that it will remain confidential." The disclosure is done to facilitate financial transactions, not to enable banks to broadcast the affairs of their customers.

State v. Reid, 945 A.2d 26, 32-33 (N.J. 2008) (quoting *State v. McAllister*, 875 A.2d 866, 874 (N.J. 2005). Having previously rejected the logic of *Smith* and *Miller*, that court has now extended its state constitutional protections by holding that Internet users have a reasonable expectation of privacy in their IP addresses and subscriber information, even though users expose their IP addresses to the owner of every website they visit, and they disclosed their identities to their internet service providers (ISP's) in order to access the Internet. *Id*. at 398-99. That court has also stated that "cell-phone users have no choice but to reveal certain information to their cellular provider. That is not a voluntary disclosure in a typical sense; it can only be avoided at the price of not using a cell phone." *State v. Earls*, 70 A.3d 630, 641 (N.J. 2013).

The Supreme Court of Hawai'i has recognized the consequences of

continued application of the reasonable-expectation-of privacy test through the third-party doctrine:

> An expectation of privacy, even though extended to matters exposed to third persons, would be viewed as reasonable by society, where such exposure is inevitable and inescapable in the conduct of the necessary affairs of life. The alternative is to countenance the inexorable diminishment of personal privacy and the substantial risk of privacy zones disappearing altogether.

Walton, 324 P.3d at 908. Many other courts have pointed out that the idea that disclosure of information to various service providers in modern society is voluntary is a fiction.

> Simply because the cell phone user knows or should know that his cell phone gives off signals that enable the service provider to detect its location for call routing purposes, and which enable cell phone applications to operate for navigation, weather reporting, and other purposes, does not mean that the user is consenting to use of that location information by third parties for any other unrelated purposes. While a person may voluntarily convey personal information to a business or other entity for personal purposes, such disclosure cannot reasonably be considered to be disclosure for all purposes to third parties not involved in that transaction. . . .

Tracey v. State, 152 So.3d 504. 522 (Fla. 2014). "Requiring a cell phone user to turn off the cell phone just to assure privacy from governmental intrusion that can reveal a detailed and intimate picture of the user's life places an unreasonable burden on the user to forego necessary use of his

cell phone, a device now considered essential by much of the populace." *Id*. at 522-23.

Colorado has interpreted its state constitution to protect individuals' reasonable expectation of privacy in their phone records, *see People v. Timmons*, 690 P.2d 213, 217 (Colo. 1984); *People v. Corr*, 682 P.2d 20, 26-27 (Colo. 1984); bank records, *see People v. Lamb*, 732 P.2d 1216, 1220-21 (Colo. 1987); and tax documents, *see People v. Gutierrez*, 222 P.3d 925, 936 (Colo. 2009). The Idaho Supreme Court has found a reasonable expectation of privacy in numbers dialed, calling numbers, and the accompanying telephone records. *State v. Thompson*, 760 P.2d 1162, 1164-67 (Idaho 1988). *See also People v. Chapman*, 679 P.2d 62 (Cal. 1984); *People v. Jackson*, 452 N.E.2d 85, 88-89 (Ill. App. Ct. 1983); *People v. DeLaire*, 610 N.E.2d 1277, 1282 (Ill. Ct. App. 1993); *Commonwealth v. Melilli*, 555 A.2d 1254, 1258-59 (Pa. 1989); *Commonwealth v. DeJohn*, 403 A.2d 1283, 1291 (Pa. 1979); *State v. Thompson*, 810 P.2d 415, 418 (Utah 1991); *Commonwealth v. Blood*, 507 N.E.2d 1029, 1033 (Mass. 1987); *State v. Nelson*, 941 P.2d 441, 448-50 (Mont. 1997); *State v. Myrick*, 688 P.2d 151, 153-54 (Wash. 1984).

In contrast, those states that, like Arizona, have interpreted their

state constitutions consistently with *Miller* and *Smith* have relied on an assumption that people do not reasonably expect any of their dealings with banks or telephone companies to remain private. The West Virginia Supreme Court collected cases from the aforementioned states in *State v. Clark*, 752 S.E.2d 907, 921 n.13 (W.Va. 2013): *Henderson v. State*, 583 So.2d 276, 292 (Ala. Crim. App. 1990); *Kesler v. State*, 291 S.E.2d 497, 504 (Ga. 1982); *State v. Schultz*, 850 P.2d 818, 823-24 (Kan. 1993); *Smith v. State*, 389 A.2d 858, 868 (Md. 1978); *State v. Melvin*, 357 S.E.2d 379, 382 (N.C. App. 1987); *State v. Lind*, 322 N.W.2d 826, 836-37 (N.D. 1982); *McAlpine v. State*, 634 P.2d 747, 749 (Okla. Crim. App. 1981); *S. Bell Tel. & Tel. Co. v. Hamm*, 409 S.E.2d 775, 779-80 (S.C. 1991).

In Arizona, of the ten appellate judges who considered this issue, five believed that Internet users are entitled to privacy protection, that law enforcement should seek and obtain a search warrant for IP addresses and subscriber information, and that the third-party doctrine is bad policy. Even though *Miller* and *Smith* settled the Fourth Amendment question, the fact that so many state courts refuse to follow the third-party doctrine shows that the time has come for this Court to reconsider and overrule it.

III. This Court Should Adopt the Positive Law Model as an Alternative Means of Protecting Fourth Amendment Rights.

In his *Carpenter* dissent, Justice Gorsuch proposes two paths to undoing the confusion engendered by the third-party doctrine and placing Fourth Amendment law in the digital age on a firmer and more realistic footing. The first proposal is to "retreat[ ] to the root *Katz* question whether there is a 'reasonable expectation of privacy' in data held by third parties." *Carpenter*, 138 S. Ct. at 2264 (Gorsuch, J., dissenting). Mixton offers that proposal because, as shown in the previous section, it is the path that most courts have followed in rejecting the third-party doctrine.

The concern with the test developed in *Katz* is that it has no textual connection to the Fourth Amendment's promise of protections for all "persons, houses, papers, and effects," rather than "some abstract 'expectation of privacy' whose contours are left to the judicial imagination." *Id*. If the *Katz* test is "supposed to pose an empirical question (what privacy expectations do people actually have)," it must be rejected (1) because legislators, rather than judges, are better equipped to answer such questions, and (2) because "judicial judgments often fail to reflect public views." *Id*. at 2265 (citing Christopher Slobogin & Joseph

E. Schumacher, *Reasonable Expectations of Privacy and Autonomy in Fourth Amendment Cases: An Empirical Look at "Understandings Recognized and Permitted by Society,"* 42 Duke L.J. 727, 732, 740-42 (1993)).

If, on the other hand, the reasonable-expectation-of-privacy test presents a normative question, it suffers from the same problem of entrusting unelected judges with the responsibility of deciding what protections the Fourth Amendment should provide to digital data, rather than the legislators who are usually entrusted with such policy questions in our system of government. *Id.* ("When judges abandon legal judgment for political will we … risk decisions where 'reasonable expectations of privacy' come to bear 'an uncanny resemblance to those expectations of privacy' shared by Members of this Court.") (quoting *Minnesota v. Carter*, 525 U.S. 83, 97 (1998) (Scalia, J., concurring)). Justice Gorsuch also highlighted the "often unpredictable—and sometime unbelievable" results of applying the *Katz* test:

> *Smith* and *Miller* are only two examples; there are many others. Take *Florida v. Riley*, 488 U.S. 445 (1989), which says that a police helicopter hovering 400 feet above a person's property invades no reasonable expectation of privacy. Try that one out on your neighbors. Or *California v. Greenwood*, 486 U.S. 35 (1988), which holds that a person has no

> reasonable expectation of privacy in the garbage he puts out for collection. In that case, the Court said that the homeowners forfeited their privacy interests because "[i]t is common knowledge that plastic garbage bags left on or at the side of a public street are readily accessible to animals, children, scavengers, snoops, and other members of the public." *Id.*, at 40 (footnotes omitted). But the habits of raccoons don't prove much about the habits of the country. I doubt, too, that most people spotting a neighbor rummaging through their garbage would think they lacked reasonable grounds to confront the rummager. Making the decision all the stranger, California state law expressly protected a homeowner's property rights in discarded trash. *Id.*, at 43. Yet rather than defer to that as evidence of the people's habits and reasonable expectations of privacy, the Court substituted its own curious judgment.

Id. at 2266 (parallel citations omitted).

Although the *Carpenter* majority "does not 'call into question conventional surveillance techniques and tools, such as security cameras,'" lower courts are still left to wonder "what techniques qualify as 'conventional' and why those techniques would be okay even if they lead to 'permeating police surveillance' or 'arbitrary police power.'" *Id.* at 2267. In the end, "[a]ll we know is that historical cell-site location information (for seven days, anyway) escapes *Smith* and *Miller*'s shorn grasp, while a lifetime of bank or phone records does not. As to any other kind of information, lower courts will have to stay tuned." *Id.* "In the Court's defense, though, we have arrived at this strange place not

because the Court has misunderstood *Katz*. Far from it. We have arrived here because this is where *Katz* inevitably leads." *Id.*

In place of the unworkable "reasonable expectation of privacy test" from *Katz* and as a way out of a thicket of uncertainty, Justice Gorsuch endorsed the Positive Law Model, which entails a return to "the traditional approach" to Fourth Amendment questions applied before *Katz*. *Id.* at 2267-68. While "*Katz* may still supply one way to prove a Fourth Amendment interest," "[n]eglecting more traditional approaches may mean failing to vindicate the full protections of the Fourth Amendment." *Id.* at 2272.

"True to [the Fourth Amendment's] words and their original understanding, the traditional approach asked if a house, paper or effect was *yours* under law. No more was needed to trigger the Fourth Amendment." *Id.* at 2267-68 (emphasis in original). In addition to respecting the language of the Fourth Amendment, this approach "comes with other advantages." *Id.* at 2268. Among other things, it directs courts "to decide cases based on 'democratically legitimate sources of law'—like positive law or analogies to items protected by the enacted Constitution—rather than 'their own biases or personal policy preferences.'" *Id.* (quoting

Todd E. Pettys, *Judicial Discretion in Constitutional Cases*, 26 J.L. & Pol. 123, 127 (2011)). As a consequence, it also "'carves out significant room for legislative participation in the Fourth Amendment context,' … by asking judges to consult what the people's representatives have to say about their rights." *Id.* (quoting William Baude & James Y. Stern, *The Positive Law Model of the Fourth Amendment*, 129 Harv. L. Rev. 1821, 1852 (2016)). Because information or other property can still be "yours," "[u]nder this more traditional approach, Fourth Amendment protections for your papers and effects do not automatically disappear just because you share them with third parties." *Id.* On the contrary, under the positive law, "[e]ntrusting your stuff to others is a bailment," which requires the bailee to protect the bailor's interest in the entrusted property. *Id.*

Additionally, "positive law may help provide detailed guidance on evolving technologies without resort to judicial intuition" as state and federal legislators respond to those changes by enacting legislation defining one's rights to digital data. *Id.* Finally, this model suggests that "positive law cannot be used to defeat" some Fourth Amendment interests, thus providing a floor below which Fourth Amendment

interests may not go and "bar[ring] efforts to circumvent the Fourth Amendment's protection through the use of subpoenas." *Id*. at 2270-71.

This Court should adopt the Positive Law Model—not necessarily in place of the *Katz* test, but as a supplement when the *Katz* test fails to provide clear answers to difficult questions on the scope of Fourth Amendment protections for shared data. Unquestionably, under such a rule, the third-party doctrine must be overruled.

IV. This Case Squarely Presents These Fourth Amendment Issues And Provides An Ideal Vehicle For Deciding Them.

Mixton's case is typical of investigations of Internet-related crimes in that law enforcement could have sought a search warrant from a neutral and detached magistrate, but simply chose not to do so. "The Fourth Amendment demonstrates a 'strong preference for searches conducted pursuant to a warrant.'" *Ornelas v. United States*, 517 U.S. 690, 699 (1996) (quoting *Illinois v. Gates*, 462 U.S. 213, 236 (1983)). For this reason, "[s]earches conducted outside the judicial process, without prior approval by judge or magistrate, are per se unreasonable under the Fourth Amendment—subject only to a few specifically established and well-delineated exceptions." *Arizona v. Gant*, 556 U.S. 332, 338 (2009) (quoting *Katz*, 389 U.S. at 357). In Mixton's case, Arizona has never

attempted to justify its use of the administrative subpoena process by claiming applicability of a warrant exception. Instead, Arizona has asserted that law enforcement would be thwarted by such a requirement. The Arizona Supreme Court majority agreed with the State's position:

> [R]equiring a search warrant to obtain an IP address and subscriber information would essentially limit law enforcement to investigating completed internet-based offenses. For example, what if Mixton had merely queried the undercover detective about trading child pornographic images, but never transferred the photographs? This unworkable approach would invariably stifle proactive investigations of internet-based crimes.

Mixton II, 478 P.3d at 1243. This is a curious statement, as it ignores that law enforcement would have no basis for the search warrant it ultimately obtained had there been no evidence of a crime in the first place.

In any event, courts must not treat the warrant requirement as an impediment to effective law enforcement techniques, but as a protection of the citizenry against government agents "engaged in the often competitive enterprise of ferreting out crime." *Johnson v. United States*, 333 U.S. 10, 13-14 (1948). As this Court recently stated in *Carpenter*, the Fourth Amendment "seeks to secure 'the privacies of life' against 'arbitrary power'" with the purpose of "'plac[ing] obstacles in the way of a too permeating police surveillance.'" *Carpenter*, 138 S. Ct. at 2214

(quoting *Boyd v. United States*, 116 U.S. 616, 630 (1886), and *United States v. Di Re*, 332 U.S. 581, 595 (1948)). *See also Melendez-Diaz v. Massachusetts*, 557 U.S. 305, 325 (2009) ("The Confrontation Clause may make the prosecution of criminals more burdensome, but that is equally true of the right to trial by jury and the privilege against self-incrimination. The Confrontation Clause … is binding, and we may not disregard it at our convenience.").

After *Carpenter*, lower courts cannot know with certainty to what extent that "decision today is a narrow one." *Carpenter*, 138 S. Ct. at 2220. On the one hand, this Court expressly disclaimed it was "disturb[ing] the application of *Smith* and *Miller* or call into question conventional surveillance techniques and tools…" *Id.* On the other hand, the third-party doctrine as stated in *Miller* and *Smith* was an absolute rule, and *Carpenter* has now rejected the core holding that information possessed by third parties is never entitled to the protection of the Fourth Amendment.

Mixton's case reveals the confusion that *Carpenter* has generated. In the Arizona Court of Appeals, of the two judges who held that a warrant should be required to obtain IP addresses and subscriber

information, one held that *Carpenter* changed nothing, while the other held that it changed everything. *Compare Mixton I*, 447 P.3d at 837 n.3 (opinion of Eppich, J.) ("Because the court in *Carpenter* expressly limited its holding to cell phone location tracking, 138 S. Ct. at 2220 (decision is a 'narrow one'), and affirmed the continuing viability of *Miller* and *Smith*, *id*., we decline Judge Eckerstrom's invitation to apply it to the facts here."), with *id*. at 846 (Eckerstrom, J. concurring in part, dissenting in part) ("I can identify no principled basis to distinguish the instant case from the Court's holding in *Carpenter*.").

Because Mixton's case squarely presents these thorny Fourth Amendment issues, this Court should accept review of his petition and overrule the third party doctrine.

CONCLUSION

For these reasons, Petitioner respectfully requests that this Court accept review of the opinion of the Arizona Supreme Court.

Respectfully submitted,

DAVID J. EUCHNER
Counsel of Record
ABIGAIL JENSEN
Pima County Public Defender's Office
33 N. Stone, 21st Floor
Tucson, Arizona 85701
Telephone: (520) 724-6800
David.Euchner@pima.gov
Abigail.Jensen@pima.gov

Attorneys for Petitioner
William Mixton