IN THE ARIZONA SUPREME COURT

STATE OF ARIZONA, Appellee, v. WILLIAM MIXTON, Appellant.	Supreme Court No. CR-19-0276-PR Court of Appeals Case No. 2 CA-CR 2017-0217 Pima County Superior Court Case No. CR2016038001

BRIEF OF *AMICI CURIAE* THE AMERICAN CIVIL LIBERTIES UNION OF ARIZONA, AMERICAN CIVIL LIBERTIES UNION, AND ELECTRONIC FRONTIER FOUNDATION IN SUPPORT OF APPELLANT

Jared G. Keenan
AZ Bar No. 027068
P.O. Box 17148
Phoenix, AZ 85011-0148
(602) 650-1854
jkeenan@acluaz.org

Counsel for Amici Curiae

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Other Authorities

INTRODUCTION

This Court should protect the public's rights under the Arizona Constitution's Private Affairs Clause and reject the proposition that information in the possession of third parties deserves no constitutional privacy protection. The Court has never recognized this "third-party doctrine," and it should not begin to do so now.

From its inception, the third-party doctrine has been in conflict with people's actual expectations of privacy and the realities of life. Some courts have interpreted the doctrine to mean that people waive their Fourth Amendment expectation of privacy in information that they provide to businesses and other third parties, or that these entities generate based on their relationship with their users. However, the U.S. Supreme Court now recognizes that individuals today almost universally rely on third parties—such as email providers, social media companies, and other online services—for critical aspects of their lives, underscoring why the doctrine is highly problematic in the digital age. *See Carpenter v. United States*, 138 S. Ct. 2206, 2217 (2018); *see also United States v. Jones*, 565 U.S. 400, 417 (2012) (Sotomayor, J., concurring).

State courts also recognize that the third-party doctrine is increasingly "untenable in a technological age where in the ordinary course of life, individuals

will of necessity have disclosed a boundless amount of information to third parties." *State v. Walton*, 324 P.3d 876, 901 (Haw. 2014); *see also State v. Hunt*, 450 A.2d 952, 955 (N.J. 1982) ("Technological developments have enlarged our conception of what constitutes the home."). Even before *Carpenter*, state courts had observed that advances in technology "render the third-party doctrine . . . inapposite; the digital age has altered dramatically the societal landscape from the 1970s, when [the seminal third-party doctrine cases] were written." *Commonwealth v. Augustine*, 4 N.E.3d 846, 859 (Mass. 2014).

Arizona should follow suit. Rather than reflexively applying the federal third-party doctrine, this Court should analyze whether particular kinds of information Arizonans provide to third parties constitute a person's "private affairs." Other states have shown that this approach protects individual privacy while creating workable rules for law enforcement. In contrast, the third-party doctrine is both a legal fiction and a blunt instrument that far too often fails to adequately protect personal information reflecting a person's most sensitive, private, and expressive details.

ARGUMENT

I. The federal third-party doctrine was crafted around archaic technology.

The passage of time and advances in technology have shown that the

assumptions underpinning the federal third-party doctrine, derived from the Supreme Court's decisions in *United States v. Miller*, 425 U.S. 435 (1976), and *Smith v. Maryland*, 442 U.S. 735 (1979), are both wrong and acutely problematic in the digital world.

The holdings of both cases were narrow. *Smith*'s holding that individuals have no expectation of privacy in the phone numbers they dial was an outgrowth of an earlier time and a specific technology. As the Court observed, the pen register at issue was "merely the modern counterpart of the operator who, in an earlier day, personally completed calls for the subscriber." *Id.* at 744. Similarly, in *Miller*, the Court held that individuals did not have a reasonable expectation of privacy in deposit slips they hand over to a bank teller. 425 U.S. at 440. These commercial transactions were exposed to bank employees, convincing the Court that "the nature of the particular documents sought" was minimally private. *Id.* at 442–43 (citing cases about words uttered to a government informant).

Thus, the Justices' practical experiences with now-outdated technologies, the human telephone operator and the paper records gathered by a bank teller, were always a shaky foundation for the principle that people enjoy no expectation of privacy in a wide array of information they voluntarily convey to others.

Today, technological changes and a more realistic understanding of social expectations show that the third-party doctrine is ill-founded, out of step with reality, and doomed to imperil individual privacy. Indeed, the U.S. Supreme Court has begun to step away from the third-party doctrine because of its ill fit in cases involving modern technology. *Carpenter*, 138 S. Ct. 2206 (declining to extend the doctrine to permit warrantless collection of cell phone location data). This Court should avoid the pitfalls of the last four decades of federal Fourth Amendment jurisprudence and adopt a more workable and realistic rule.

II. The third-party doctrine is ill-suited to life in the modern world.

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.

A. Digital technologies and services collect vast volumes of personal information—often without people's knowledge, consent, or affirmative choice.

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. *See id.* 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).

We are only just now beginning to understand the ways in which individuals' use of new technologies continually and relentlessly reflects the full tapestry of their personal, financial, social, and professional lives. For example, Facebook proactively collects and aggregates information about its users (and even *non*-users) that is startling in scope. *See* Allen St. John, *How Facebook Tracks You, Even When You're Not on Facebook*, Consumer Reports (April 11, 2018), https://www.consumerreports.org/privacy/how-facebook-tracks-you-even-when-youre-not-on-facebook (describing how Facebook can track people across the

Internet to collect information about their activities and target advertising at them). It is a modern reality that technology companies, advertisers, and third-party data brokers track people "in nearly every corner of today's Internet." Bennett Cyphers and Gennie Gebhart, *Behind the One-Way Mirror: A Deep Dive Into the Technology of Modern Surveillance*, Electronic Frontier Foundation (Dec. 2, 2019), https://www.eff.org/wp/behind-the-one-way-mirror. For example, Internet service providers log user activity (such as the friends whose updates we seek out most frequently, and the physical places from which we do so) and retain the data. *Id*. These records show users' patterns of browsing the web, sending email or text messages, and downloading files. This data, individually and in the aggregate, can comprehensively reveal people's associations, interests, and even thoughts. *Id.*

The generation and collection of this type of revealing information is not limited to one's presence in the virtual world, because our activities online have become inextricably tied to our lives in the physical world as well. Most obviously, people carry cell phones with them essentially at all times. *See Riley*, 573 U.S. at 395. These devices are not just tiny warehouses of digital information, but portals to connections across the globe, and using them has become "'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*, 573 U.S. at 385).

As the U.S. Supreme Court has recognized, they are producing sensitive information not through voluntary sharing but merely "by dint of . . . operation, without any affirmative act on the user's part beyond powering up." *Id.* at 2210. And that means that as people engage in more online activities in more places, they are often unwittingly producing information and interactions that are specifically correlated with real-world locations. This location data, even in limited quantities, reveals highly sensitive social, political, and religious activities.

Location data can reveal activities of an "indisputably private nature," like a visit to the "psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on." *Jones*, 565 U.S. at 415 (Sotomayor, J., concurring) (citation omitted); *see also Carpenter*, 138 S. Ct. at 2217 (location data "provides an intimate window into a person's life, revealing not only his particular movements, but through them his 'familial, political, professional, religious, and sexual associations'"). These records can also be used in the aggregate to identify members of a church, participants in a protest, or patients visiting a doctor's office.

What the Supreme 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*, N.Y. Times, Dec. 19, 2019**,** https://perma.cc/F72N-NBN6**.**

Moreover, companies limit users' freedom of choice in controlling their data and protecting their privacy. Privacy notices are notoriously vague, legalistic, and long. *See* Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 I/S: J. Law & Policy 543, 563 (2008) (finding it would take a consumer approximately 250 hours per year to read the privacy policies of the websites they visit). Even sophisticated users can be unaware of the extent and the purposes for which service providers can access, process, and sell their data. And 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).

B. Neither federal law nor public opinion supports the fiction that information in the hands of third parties is no longer private.

Even before *Carpenter*, the U.S. Supreme Court found that the Fourth

Amendment protects some types of personal information, even when exposed to a third party. In *Ferguson v. City of Charleston*, 532 U.S. 67, 78 (2001), for example, the Court held that a patient has reasonable expectation of privacy in diagnostic test results held by a hospital. In *Bond v. United States*, 529 U.S. 334, 338–39 (2000), a bus passenger retained his expectation of privacy in luggage he placed in the overhead bin, despite the possibility that others might touch or squeeze the bag. In *Stoner v. California*, 376 U.S. 483, 489–90 (1963), the Court held that hotel guests are entitled to Fourth Amendment protection even though hotel guests provide "implied or express permission" for housekeeping and managers to access their rooms. Of course, the contents of letters and phone calls are protected even though exposed to the postal service and the phone company. *Ex parte Jackson*, 96 U.S. 727, 732–33 (1877); *Smith*, 442 U.S. at 741. There never has been a categorical rule that applies to all information accessible to third parties, and no such rule should apply to people's Internet activities. *See Carpenter*, 138 S. Ct. at 2219 ("The Government's position fails to contend with the seismic shifts in digital technology . . . .").[1]

[1] Indeed, in *Carpenter*, every Justice agreed, at least in dicta, that the Fourth Amendment protects the content of emails stored on a third-party service. *See* 138 S. Ct. at 2222 (majority op.); *id.* at 2230 (Kennedy, J., dissenting, joined by Thomas and Alito, JJ.); *id.* at 2262, 2269 (Gorsuch, J., dissenting).

This approach is consistent with the way people conceptualize privacy. Studies show that the vast majority of Americans believe that it is important to maintain privacy and confidentiality in their activities. 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. 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.

III. Arizona should follow other states that have rejected the third-party doctrine and produced workable rules that protect individual privacy.

This Court should make clear that Arizonans need not choose between participating in society or having privacy protections for their most sensitive, intimate, and expressive matters. Indeed, state courts across the country have held that the third-party doctrine is insufficiently protective of people's privacy

interests, and have declined to apply the third-party doctrine under their state constitutions. Courts have looked to state constitutional provisions analogous to the Private Affairs Clause to find privacy interests in bank records, tax documents, telephone records, cell site location information, employment records, medical records, and garbage. These states' experiences show that this Court can and should reject application of the third-party doctrine under the Arizona Constitution.

A. Washington has interpreted the Private Affairs Clause of its state constitution to reject the federal third-party doctrine.

Washington's jurisprudence on the third-party doctrine and its Private Affairs Clause should guide this Court's analysis. *See* Br. of Amicus Curiae Goldwater Institute in Supp. of Pet. for Review at 5–6, 9–13 (citing Timothy Sandefur, *The Arizona "Private Affairs" Clause*, 51 Ariz. St. L.J. 723, 724 (2019)). As this Court explained, "the law announced by [the Washington Supreme Court] is very persuasive" when the issue involves a provision in the Washington Constitution that is "very much like the same provisions" in Arizona's Constitution. *Schultz v. City of Phoenix*, 18 Ariz. 35, 42 (1916); *see also* Goldwater Institute Br. at 5–6 (noting that Arizona derived its Private Affairs Clause from Washington's Constitution).

Rather than applying a reasonable-expectation-of-privacy framework, Washington evaluates whether challenged government conduct constitutes an

intrusion into a defendant's "private affairs." *See State v. Myrick*, 688 P.2d 151, 153–54 (Wash. 1984). "In determining whether a certain interest is a private affair deserving [constitutional] protection, a central consideration is the *nature* of the information sought—that is, whether the information obtained via the governmental trespass reveals intimate or discrete details of a person's life." *State v. Jorden*, 156 P.3d 893, 896, ¶ 8 (Wash. 2007).

Under this framework, Washington considers the unique characteristics of various categories of information and records, even when held by third parties, to determine constitutional protection. *See*, *e.g.*, *State v. Hinton*, 319 P.3d 9, 16–17 (Wash. 2014) (protecting text messages sent to another person); *Jorden*, 156 P.3d at 898 (protecting motel guest registry); *State v. Jackson*, 76 P.3d 217, 224 (Wash. 2003) (protecting location information collected via GPS tracking device on vehicle); *State v. Boland*, 800 P.2d 1112, 1116–17 (Wash. 1990) (protecting garbage); *State v. Butterworth*, 737 P.2d 1297, 1301 (Wash. Ct. App. 1987) (protecting unlisted telephone number); *State v. Gunwall*, 720 P.2d 808, 813 (Wash. 1986) (protecting telephone records).

As the Washington Supreme Court recognizes, "[g]iven the realities of modern life, the mere fact that an individual shares information with another party

and does not control the area from which that information is accessed does not place it outside the realm of [constitutional] protection." *Hinton*, 319 P.3d at 15.

B. Eleven other states also interpret their state constitutions to reject the federal third-party doctrine with respect to at least some categories of information.

Courts in at least eleven other states also hold that some categories of information remain protected even when they are in the hands of third parties. *See generally* Stephen E. Henderson, *Learning from All Fifty States: How to Apply the Fourth Amendment and Its State Analogs to Protect Third Party Information from Unreasonable Search*, 55 Cath. U. L. Rev. 373 (2006).

These states have rejected the "fiction that there is no expectation of privacy in" records merely "because the user voluntarily conveys this information to a third party." *People v. Chapman*, 679 P.2d 62, 67 n.6 (Cal. 1984). Instead, these courts recognize that state constitutional protections apply when people disclose information to third parties "for very limited purposes… [and the] clear expectation is that those limits will be honored." *Id.* at 66. As courts across the country have explained, this protection is essential to avoid "significant dangers to political liberty," *Hunt*, 450 A.2d at 956; to avoid "imped[ing] certain forms of political affiliation and journalistic endeavor that are the hallmark of a truly free society," *State v. Thompson*, 760 P.2d 1162, 1167 (Idaho 1988) (quoting *Smith*,

442 U.S. at 747–48 (Marshall, J., dissenting)); to "stand as a bulwark against the intrusions of [government investigative tools] into our daily life," *Id.* at 1167; and to prevent easy government access to a person's "virtual current biography," *Burrows v. Superior Court*, 529 P.2d 590, 596 (Cal. 1974), and "virtual mosaic of a person's life," *People v. Sporleder*, 666 P.2d 135, 142 (Colo. 1983). A summary of these states' jurisprudence is below.

1. New Jersey: In applying Article I, section 7 of the New Jersey constitution, courts need only find that an expectation of privacy is objectively reasonable. *State v. Hempele*, 576 A.2d 793, 802 (N.J. 1990). Under this framework, New Jerseyans enjoy privacy protections for telephone numbers dialed, *see State v. Mollica*, 554 A.2d 1315, 1322 (N.J. 1989); *Hunt*, 450 A.2d at 955–56; bank records, *see State v. McAllister*, 875 A.2d 866, 875 (N.J. 2005); garbage left for collection, *see Hempele*, 576 A.2d at 810; and internet users' subscriber information, *see State v. Reid*, 945 A.2d 26, 33–34 (N.J. 2008).

2. California: The California Supreme Court has held that "the appropriate test [under the state constitution] is whether a person has exhibited a reasonable expectation of privacy and, if so, whether that expectation has been violated by unreasonable governmental intrusion." *Burrows*, 529 P.2d at 593. Under this framework, California has departed from the federal third-party doctrine regarding

telephone records and bank records, *see People v. Larkin*, 239 Cal. Rptr. 760, 761–62 (Ct. App. 1987); *Chapman*, 679 P.2d 62; *People v. Blair*, 602 P.2d 738, 746 (Cal. 1979); *Burrows*, 529 P.2d at 590; as well as garbage, *see People v. Edwards*, 458 P.2d 713, 718 (Cal. 1969).

3. Colorado: Colorado's constitution "protect[s] an individual's reasonable expectation of privacy from unreasonable governmental intrusion." *Charnes v. DiGiacomo*, 612 P.2d 1117, 1119–20 (Colo. 1980). 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); *Charnes*, 612 P.2d at 1121; and tax documents, *see People v. Gutierrez*, 222 P.3d 925, 936 (Colo. 2009).

4. Hawaii: Hawaii's constitution protects "all information in which individuals have a legitimate expectation of privacy." *Walton*, 324 P.3d at 901. The Hawaii Supreme Court has rejected the proposition that there is no privacy interest in information disclosed to third parties. *Id.* It has held, contrary to *Smith*, 442 U.S. 735, that people do enjoy a reasonable expectation of privacy in their telephone records, *see State v. Rothman*, 779 P.2d 1, 7–8 (Haw. 1989); and business records, *see Walton*, 324 P.3d at 906–907.

5. Idaho: Article I, section 17 of the Idaho constitution protects an individual's reasonable expectation of privacy. *Thompson*, 760 P.2d at 1165. Under this provision, the Idaho Supreme Court has found a reasonable expectation of privacy in numbers dialed, calling numbers, and the accompanying telephone records. *Id.* at 1164–67.

6. Illinois: In contrast to federal law, Illinois courts have recognized a person's reasonable expectation of privacy in bank records, *see People v. Jackson*, 452 N.E.2d 85, 88–89 (Ill. App. Ct. 1983); and telephone records, *see People v. DeLaire*, 610 N.E.2d 1277, 1282 (Ill. Ct. App. 1993).

7. Pennsylvania: The Pennsylvania Supreme Court has deviated from the federal third-party doctrine and found that people have an expectation of privacy in telephone records and bank records. *See Commonwealth v. Melilli*, 555 A.2d 1254, 1258–59 (Pa. 1989); *Commonwealth v. DeJohn*, 403 A.2d 1283, 1291 (Pa. 1979).

8. Utah: The Utah Supreme Court has departed from federal precedent and held that, under the state constitution, people have a reasonable expectation of privacy in the information they supply to a bank. *See State v. Thompson*, 810 P.2d 415, 418 (Utah 1991).

9. Massachusetts: Massachusetts courts consider whether a person has a reasonable expectation of privacy when determining whether article 14 of that state

constitution is applicable. *See Commonwealth v. Blood*, 507 N.E.2d 1029, 1033 (Mass. 1987). Under this reasoning, the court declined to extend the third-party doctrine to cell site location information held by phone companies. *Augustine*, 4 N.E.3d at 866, and text messages obtained from a person's service provider, *Commonwealth v. Fulgiam*, 73 N.E.3d 798, 812–13 (Mass. 2017).

10. Montana: When determining whether an unlawful search has occurred under the state constitution, Montana courts consider "whether there has been government intrusion into an area where privacy is reasonably expected." *See State v. Scheetz*, 950 P.2d 722, 724 (Mont. 1997). Montana has diverged from federal precedent with respect to medical records and employment records. *State v. Nelson*, 941 P.2d 441, 448–50 (Mont. 1997); *Missoulian v. Bd. of Regents of Higher Educ.*, 675 P.2d 962, 970 (Mont. 1984).

11. Florida: Florida's state constitution has an explicit constitutional right of privacy, and the state supreme court has used this provision to recognize and protect a legitimate expectation of privacy in bank and telephone records. *Shaktman v. State*, 553 So. 2d 148, 151–52 (Fla. 1989); *Winfield v. Div. of Pari-Mutuel Wagering*, 477 So. 2d 544, 547–48 (Fla. 1985).

IV. Arizona should follow other states that have rejected the third-party doctrine and produced workable rules that protect individual privacy.

As the experiences of Washington and other states demonstrate, recognizing that individuals retain a privacy interest in information disclosed to third parties is a reasonable and time-honored way to effectuate state constitutional protections. And contrary to the State's protestations, a rule requiring a warrant for such searches will not cause the sky to fall.

Undeniably, finding that Arizonans enjoy a reasonable expectation of privacy in data reflecting their private and/or expressive digital activities and that law enforcement must obtain a warrant to access that information imposes some additional burdens on law enforcement. But the warrant requirement is "an important working part of our machinery of government, not merely an inconvenience to be somehow weighed against the claims of police efficiency." *Riley*, 573 U.S. at 401 (internal citation and quotation omitted). For decades, law enforcement in California has had to obtain a warrant to access phone records, just like police in Washington need a warrant before searching trash that has been left out for collection. *See supra* Section II. There is no evidence that law enforcement investigations in these states (and others that require warrants for certain information held by third parties) have been unduly hindered by the protections

afforded by their states' constitutions.

Moreover, these states' experiences show that the rejection of a reflexive third-party doctrine will not create an unworkable framework for law enforcement in Arizona. As this Court has recognized, bright-line rules—like the third-party doctrine—can run counter to constitutional limits on law enforcement's search and seizure authority. *See State v. Valle*, 196 Ariz. 324, 329–30, ¶ 17 (2000). Interpreting the Private Affairs Clause to require a particularized inquiry, based on the nature and extent of the information sought, is workable and consistent with the contextual analysis this Court and judges in other states repeatedly do.

Rejecting the third-party doctrine does not place digital evidence beyond the law enforcement's reach. Not every type of information request issued to a third party will constitute an invasion of a person's private affairs. Those that do will simply require a warrant. Moreover, police frequently have enough information to obtain a warrant but merely prefer not, or neglect, to do so.[2] This approach merely recognizes that the technology Arizonans use every day—generating data that reveals the very "privacies of life," *Riley*, 573 U.S. at 403 (citation omitted)—does

[2] Indeed, securing a warrant in this very case would have posed no obstacle for investigators. Detectives had probable cause based on their observation that a user of the Kik messaging platform engaged in a crime—posting child pornography.

not *automatically* result in the surrender of their state constitutional rights. Where police seek to invade the "private affairs" of an individual a warrant should be required, even if those private affairs are conducted online.

Moreover, 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 Id.* at 395 (contents of cell phones); *United States v. Warshak*, 631 F.3d 266, 286 (6th Cir. 2010) (email). And the Supreme Court has 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. *See Zurcher*, 436 U.S. at 565; *Roaden v. Kentucky*, 413 U.S. 496, 504 (1973).

CONCLUSION

For the reasons described above, amici respectfully request that the Court reject the third-party doctrine under the Private Affairs Clause of the Arizona Constitution and require law enforcement to obtain a warrant whenever its activities would intrude upon Arizonans' private affairs.

Respectfully submitted, this 20th day of December 2019.

By: /s/ *Jared G. Keenan*
Jared G. Keenan
American Civil Liberties Union Foundation of Arizona

Attorney for Amici Curiae
American Civil Liberties Union of Arizona, American Civil Liberties Union, and Electronic Frontier Foundation