SUPREME COURT OF ARIZONA

STATE OF ARIZONA, Appellee, v. WILLIAM MIXTON, Appellant.	No. CR–19–0276 PR Court of Appeals No. 2 CA–CR 17–0217 Pima County Superior Court No. CR20162038–001

AMICUS CURIAE BRIEF OF THE ARIZONA PROSECUTING ATTORNEYS' ADVISORY COUNCIL IN SUPPORT OF APPELLEE STATE OF ARIZONA

ELIZABETH BURTON ORTIZ, #012838
1951 W. Camelback Rd., Suite 202
Phoenix, AZ 85015
602-542-7222
Elizabeth.Ortiz@apaacaz.com
Attorney for Amicus Curiae
Arizona Prosecuting Attorneys' Advisory Council

TABLE OF CONTENTS

TABLE OF CITATIONS

Cases

Rules

INTRODUCTION

The Arizona Prosecuting Attorneys' Advisory Council (APAAC) represents approximately 900 state, county, and municipal prosecutors. APAAC's primary mission is to provide training to Arizona's prosecutors. Additionally, the agency works collaboratively with community and criminal justice stakeholders on a variety of policy and public issues. On occasion, pursuant to Arizona Rules of Civil Appellate Procedure Rule 16(b)(1)(B), APAAC submits amicus curiae briefs on issues of significant concern. This is such an occasion.

Internet crimes have become commonplace and law enforcement must be empowered to effectively investigate crimes committed online. The court of appeals' decision unnecessarily impedes police and prosecutor's ability to effectively investigate internet crimes, such as child pornography, by granting IP addresses and internet subscriber information constitutionally-protected status under Arizona's "private affairs" clause. Only one other state has granted constitutional protection to like information—every other state to be confronted with the question here has declined to apply state constitutional privacy provisions to information that identifies a particular internet user. For these reasons, APAAC joins with Appellee State of Arizona in asking this

Court to grant the petition for review and reverse the decision of the court of appeals.

ARGUMENT

In its Fourth Amendment analysis, the court of appeals was forced to acknowledge that the federal courts have uniformly concluded that an internet user has no Fourth Amendment privacy interest in their identity and that numerous federal courts have found no reasonable expectation of privacy in internet subscriber information. *State v. Mixton*, -- Ariz. ---, 2019 WL 3406661, at *3–4, ¶¶ 11–12 (Ariz. App. July 29, 2019). Yet in assessing article II, § 8 of the Arizona constitution, the court based its conclusion that an IP address and internet subscriber information is a "private affair" in part on decisions from other states declining to adopt the third-party doctrine under their state constitutions. In contrast to the federal courts' Fourth Amendment jurisprudence, those state courts found a reasonable expectation of privacy "in information [citizens] must furnish to companies providing banking, phone, and internet service in order to use those services." *Id.* at *8, ¶ 25 (Ariz. App. July 29, 2019) (collecting cases).

Not one of those cases addressed internet identifying information, the type of information at issue here. But other decisions have. The court of appeals failed to acknowledge other states that have specifically concluded

that there is no reasonable expectation of privacy under their state constitutions in the very information at issue here—IP addresses and internet subscriber information. Thus, rather than "join the several other states that have declined to apply the federal third-party doctrine" under their state constitutions, *id.* at *9, ¶ 27, the court of appeals' decision renders Arizona an outlier by applying the warrant requirement to non-content internet identifying information.

Before the court of appeals did so in this case, six other states have considered whether their constitutions protect internet identifying information. Of those six, all but one concluded that there is no reasonable expectation of privacy in internet subscriber information. *See Rader v. State*, 932 N.E.2d 755, 761–62 (Ind. App. 2010) (no warrant required for internet subscriber information under state constitution; state could obtain that information through grand jury subpoena); *State v. Leblanc*, 137 So.3d 656, 658–62 (La. App. 2014) (although state constitution afforded "greater protections of privacy" than Fourth Amendment, court found "that where an internet subscriber voluntarily discloses routine billing information to an ISP in order to receive service, he has no reasonable expectation of privacy in that information"); *State v. Mello*, 27 A.3d 771, 776–77 (N.H. 2011) ("while individuals may have a reasonable expectation of privacy in the contents of

their communications … they have no such privacy interest in information voluntarily disclosed to an Internet service provider in order to gain access to the Internet"); *State v. Delp*, 178 P.3d 259, 262–64 (Or. App. 2008) (state constitution afforded no "protected privacy interest in subscriber information in the possession of an Internet service provider"); *State v. Simmons*, 27 A.3d 1065, 1069–70 (Vt. 2011) ("Given the necessary and willing exposure of an internet user's access point identification and frequency of use to third party internet service providers, such information cannot reasonably be considered confidential…."); *but see State v. Reid*, 945 A.2d 26, 33–35 (N.J. 2008) (state constitution protects individual's right to privacy in subscriber information given to internet service provider).

The reasoning of these courts persuasively explains why information that simply identifies an internet user should not receive constitutional protection, even under provisions that afford greater privacy protections than the Fourth Amendment. For example, in *State v. Simmons*, the Vermont Supreme Court affirmed the trial court's denial of the defendant's motion to suppress his IP address under that state constitution's search and seizure provision, holding that nothing in its prior decisions "suggest that an internet subscriber address and frequency of use data, unembellished by any personal information, should be treated as private." 27 A.3d at 1069–70. The court

explained that "[g]iven the necessary and willing exposure of an internet user's access point identification and frequency of use to third party internet service providers, such information cannot reasonably be considered confidential, especially when a provider such as MySpace openly declares a policy of disclosure." *Id.* at 1070.

Moreover, the court observed that information at issue "appears no more private than a phone number and the number of calls made, or a street address or post office box and volume of mail, neither of which could plausibly be considered private." *Id.* Consequently, although Vermont's constitution (like Arizona's) "can afford greater protection against warrantless searches than is sometimes accorded by the Fourth Amendment," the court found no compelling reason to depart from the federal case law uniformly holding that such information is not constitutionally protected. *Id.*

Similarly, the Supreme Court of New Hampshire acknowledged "how intertwined and essential computers and the Internet have become to everyday, modern life" given that "[c]itizens routinely access the Internet for a wide range of daily activities, such as gathering information, communicating, shopping, banking, and more." *Mello*, 27 A.3d at 776. Still, the court drew a line between the content of internet communications and information that simply identifies an internet user: "while individuals may

have a reasonable expectation of privacy in the contents of their communications, i.e., the content of e-mails and the specific content viewed over the Internet, they have no such privacy interest in information voluntarily disclosed to an Internet service provider in order to gain access to the Internet." *Id.* at 776–77.

The Louisiana court in *Leblanc* likewise observed that the defendant voluntarily disclosed identifying information to his internet service provider to obtain service and that internet customers "know exactly the type of information they have submitted to their ISPs in order to obtain service." 137 So.3d at 661–62. And in its analysis, the *Delp* court noted the fact that it would not be reasonable for a person to expect privacy in internet subscriber information that an internet provider "independently maintained" "for its own purposes." 178 P.3d at 264.

The common thread running through these decisions is that no one reasonably expects privacy in internet subscriber information that does not reveal the content of a person's internet communications. Though the search-and-seizure provisions of Indiana, Louisiana, New Hampshire, Oregon, and Vermont may be worded differently than Arizona's "private affairs" clause, they apply the same test—whether there is reasonable expectation of privacy. *See State v. Juarez*, 203 Ariz. 441, 445, ¶ 16 (App. 2002) ("Arizona courts

have consistently applied the Fourth Amendment's 'legitimate expectation of privacy' requirement when determining unlawful search or seizure claims made pursuant to Article 2, Section 8"). And those state courts, like the federal courts, are nearly unanimous in determining that it simply is not reasonable for an internet user to expect privacy in their identity. There is no compelling reason to depart from that near-unanimous national consensus.

Though the court of appeals ignored those courts that declined to find a privacy right in the type of information at issue here, it placed substantial weight on the lone decision to the contrary—the New Jersey Supreme Court's decision in *Reid*. *See Mixton*, 2019 WL 3406661, at *9, ¶ 26. The *Reid* court held that under the New Jersey constitution's "search-and-seizure provision, internet users have a reasonable expectation of privacy in their subscriber information, just as they do in their bank records and phone calls." *Id.* (citing *Reid*, 945 A.2d at 26, 28, 32, 28). But with the exception of the court of appeals in this case, no other state has found *Reid*'s conclusion persuasive.

First, as several courts have pointed out—and the court of appeals omitted from its discussion in this case—"[t]he *Reid* court did not go so far as to say that the privacy interest a person holds in his subscriber information required a search warrant for its disclosure." *Leblanc*, 137 So.3d at 661. Rather, the New Jersey court "stated that law enforcement officials could

satisfy the protection of the right to privacy in this instance by serving a grand jury subpoena on an ISP without notice to the subscriber." *Id.* (citing *Reid*, 945 A.2d at 38); *see also Rader*, 932 N.E.2d at 762 ("the court in *Reid* held that law enforcement officials in New Jersey could satisfy that state's constitutional requirements by serving a grand jury subpoena on an ISP"); *Simmons*, 27 A.3d at 1070 n.5 ("[D]espite the privacy retained in internet user identification, the *Reid* court opined that such information was still obtainable by police through properly issued subpoenas, rather than warrants based on probable cause.") (citing *Reid*, 945 A.2d at 36). Moreover, neither probable cause nor notice to the account holder was required for issuance of such subpoenas. 945 A.2d at 35–36.

The opinion below thus makes Arizona the *only* state in the nation to require a warrant for internet subscriber information. Not even New Jersey—the only other state to find a right to privacy in such information—imposes that heightened requirement.

Second, the New Jersey Supreme Court rested its decision on a long history of case law granting state constitutional privacy rights to other matters disclosed to third parties, such as bank and telephone billing records, even though those rights had not been recognized under federal law. *Reid*, 945 A.2d at 32–33; *see also Mixton*, 2019 WL 3406661, at *16, ¶ 52 (Espinosa,

J., dissenting) (*Reid* found ISP subscriber information protected "specifically relying on twenty-five years of expansion of New Jersey privacy rights, rather than out of the blue, as undertaken by the majority here"). Several states without a similar history, however, did not find *Reid* to present a compelling reason for recognizing a privacy right in internet subscriber information. *See Mello*, 27 A.3d at 776 ("our law regarding information voluntarily exposed to third parties is in line with the protection afforded under the Fourth Amendment and diverges significantly from New Jersey law"); *Simmons*, 27 A.3d at 1070 n.5 ("The *Reid* decision was based, in part, on prior recognition of state constitutional privacy rights in matters disclosed to third parties, such as banks and telephone exchanges, whereas no such history precedes the instant case.")

Arizona, like New Hampshire and Vermont, has no such history of granting constitutional privacy protection to information such as bank records and phone information. *See Mixton*, 2019 WL 3406661, at *15, ¶ 50 (Espinosa, J., dissenting) ("It is difficult to understand why such content-lacking information should now be more shielded than, for example, personal telephone numbers and related information, which are not so protected, either federal or, presumably still, in Arizona."). Consequently, the foundation for the *Reid* court's conclusion is absent in Arizona.

The decisions discussed above reveal that the court of appeals' decision here makes Arizona the only state in the nation to apply a warrant requirement to the type of internet-user identifying information at issue in this case. And New Jersey, the only other state to find privacy protection for such information, still allows the government to obtain the information using a grand jury subpoena without probable cause. Moreover, those courts to have considered the question following New Jersey have declined to follow its approach. Given that only a single jurisdiction has found an IP address or ISP subscriber information to be private, it cannot be reasonable to expect privacy in that information. *Cf. Mixton*, 2019 WL 3406661, at *9, ¶ 27 ("[w]e conclude that internet users generally have a reasonable expectation of privacy in their subscriber information"). There is no compelling reason for Arizona to stand alone in applying a privacy right and the warrant requirement to the information at issue in this case.

CONCLUSION

APAAC respectfully urges this Court to grant the State of Arizona's petition for review and reverse the court of appeals' opinion. The opinion below unjustifiably hinders law enforcement's ability to investigate internet crimes by going against the overwhelming national consensus of courts finding that it is not reasonable to expect privacy in non-content internet

identifying information and by making Arizona the only state in the country that imposes the warrant requirement on such information.

RESPECTFULLY SUBMITTED this 5th day of November, 2019.

/s/ *Elizabeth Burton Ortiz*

BY _____

ELIZABETH BURTON ORTIZ
Attorney for *Amicus Curiae*
Arizona Prosecuting Attorneys' Advisory Council