ARIZONA SUPREME COURT

STATE OF ARIZONA, Appellee, v. WILLIAM MIXTON, Appellant.	CR– Court of Appeals No. 2 CA–CR 2017–0217 Pima County Superior Court No. CR–2016–2038–001

THE STATE OF ARIZONA'S PETITION FOR REVIEW

Mark Brnovich
Attorney General
(Firm State Bar No. 14000)

Joseph T. Maziarz
Chief Counsel

Linley Wilson
Assistant Attorney General
Criminal Appeals Section
2005 N. Central Ave.
Phoenix, Arizona 85004–1508
Telephone: (602) 542–4686
cadocket@azag.gov
(State Bar Number 027040)
Attorneys for Appellee

I. ISSUE PRESENTED FOR REVIEW.

> Did the two-judge majority of the court of appeals err when it declared that article II, § 8 of the Arizona Constitution protects a right to privacy in an internet protocol ("IP") address and internet subscriber information, and held that federal agents investigating the electronic transmission of child pornography violated this novel constitutional right when they acquired this information—which revealed only Mixton's identity—through federally-authorized subpoenas?

II. MATERIAL FACTS.

A Pima County Grand Jury indicted Appellant, William Mixton, on 20 counts of sexual exploitation of a minor under the age of 15. (R.O.A. 1.) Prior to trial, Mixton filed a motion to suppress "subscriber information" that Homeland Security Investigations ("HSI") agents acquired by issuing two federal administrative subpoenas to Kik Interactive Inc. ("Kik"), a smartphone messaging application, and Cox Communications ("Cox"), Mixton's internet service provider ("ISP"). (R.O.A. 41.) The State filed a response. (R.O.A. 46.) Mixton did not file a reply and neither party requested an evidentiary hearing. (*Id.*; R.O.A. 41; R.T. 2/21/17, at 3.) The parties' briefs established the following undisputed facts.

In March 2016, HSI and the Tucson Police Department ("TPD") began a joint investigation to find individuals transmitting child pornography online. (R.O.A. 41.) TPD Detective Barry worked undercover to initiate contact with prospective offenders by placing ads on Craigslist. (*Id.*) Using the name "UC," Detective Barry started a group chat on Kik. (*Id.*; R.O.A. 46.)

On March 15, Mixton responded to one of Detective Barry's Craigslist ads using the name "Monda Monda." (R.O.A. 46.) "Monda Monda" informed Detective Barry that his Kik name was "tabooin520." (*Id.*) Detective Barry invited "tabooin520" to join his group chat. (R.O.A. 41.) Between March 21 and March 25, "tabooin520" posted images and videos of child pornography to the group chat and to a private chat with Detective Barry. (R.O.A. 46.)

On March 23, an HSI agent's supervisor issued an administrative subpoena to Kik in accordance with 19 U.S.C. § 1509.[1] (*Id.*) Kik complied with the subpoena and provided the following information for the account established by "tabooin520": (1) the user's IP address was 68.110.82;[2] (2) the user's email address was billnunyain520@gmail.com; and (3) the user's name was "Bill Nunya." (*Id.*)

---

[1] This statute authorizes subpoenas for records "which may be relevant to [an] investigation" "for insuring compliance with the laws of the United States administered by the United States Customs Service." 19 U.S.C. § 1509(a)(1). Importation of child pornography is prohibited by federal law. 18 U.S.C. § 2252(a); *see also United States v. Cray*, 673 F. Supp. 2d 1368, 1377 & n.10 (S.D. Ga. 2009) (approving use of § 1509 summonses to investigate "the likely importation of child pornography images" and noting "ICE has regularly used its summons authority to obtain subscriber information on Internet accounts").

[2] An IP address is "a string of numbers associated with a device that had, at one time, accessed a wireless network"; it "does not itself convey any location information." *United States v. Hood*, 920 F.3d 87, 92 (1st Cir. 2019). An IP address can be static (set for a specific user) or dynamic (randomly assigned to internet users and changing frequently). *See Call of the Wild Movie, LLC v. Does 1-1*, 770 F. Supp. 2d 332, 356 (D.D.C. 2011).

Using publicly-available information, HSI agents learned that the IP address belonged to Cox. (*Id*.) Another HSI agent issued an administrative subpoena requesting Cox to "provide subscriber information related to the IP address 68.110.1.82, used on the dates and times that 'tabooin520' posted in the Kik group and private chat." (*Id*.) Cox responded to the subpoena, providing Mixton's name, address, and phone number. (*Id*.) A detective obtained a search warrant for that address (where Mixton lived); execution of the search warrant led to the discovery of child pornography on electronic devices in Mixton's room. (R.O.A. 41.)

In his suppression motion, Mixton argued, in relevant part, that he had a privacy interest in the IP address and his subscriber information under article II, § 8 of the Arizona Constitution and that the HSI agents violated this right to privacy. (R.O.A. 41, at 4–7.) The trial court denied Mixton's motion, emphasizing "the only information the government gained" from Kik and Cox was internet subscriber information, which is not protected by the Fourth Amendment. (R.O.A. 50.) The court did not expressly address Mixton's state-constitutional claim.

On appeal, Mixton maintained that the officers' acquisition of the IP address and subscriber information without a warrant violated article II, § 8. (Opening Brief, at 9–36.) He also claimed the evidence should have been suppressed under the Fourth Amendment. (*Id*. at 37–41.) The State argued, *inter alia*: (1) under the third-party doctrine established in *Smith v. Maryland*, 442 U.S. 735 (1979), and

United States v. Miller, 425 U.S. 435 (1976), Mixton does not have a reasonable expectation of privacy in his IP address or subscriber information; and (2) article II, § 8 does not provide broader protection than the Fourth Amendment in this context. (Answering Brief, at 6–30.)

The court of appeals issued a fractured opinion. *State v. Mixton*, 2019 WL 3406661 (Ariz. App. July 29, 2019) (attached). The court first analyzed Mixton's Fourth Amendment claim, consistent with this Court's precedent. *Mixton*, ¶ 9. The court recognized that "[i]n general, the Fourth Amendment does not protect information that a person reveals to a third party who then reveals it to the state, 'even if the information is revealed [to the third party] on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.'" *Mixton*, ¶ 11 (quoting *Miller* and citing *Smith*). The court of appeals observed that "[f]ederal courts applying this principle have consistently found internet users to have no reasonable expectation of privacy in their IP addresses or in their subscriber information (name, street address, etc.) voluntarily conveyed to third-party service providers." *Mixton*, ¶ 11 (collecting cases).

Accordingly, Judges Eppich and Espinosa held that "[b]ecause Mixton had no federally recognized privacy interest in his subscriber information or IP address, law enforcement did not need a warrant under the Fourth Amendment to obtain that information from Mixton's service providers." *Id.*, ¶ 13; *see also id.*, ¶ 48

(Espinosa, J., agreeing that "no Fourth Amendment violation occurred"). Judge Eckerstrom dissented from this conclusion, stating he could not distinguish this case from the Supreme Court's holding in *Carpenter v. United States*, 138 S. Ct. 2206 (2018). *Mixton*, ¶ 45 (Eckerstrom, J., dissenting in part). But as the other two judges pointed out, the *Carpenter* holding was limited to cell phone location tracking and "affirmed the continuing viability of *Miller* and *Smith*[.]" *Id.*, n.3.

Judges Eppich and Eckerstrom nonetheless held that "the federal third-party doctrine, at least as applied to obtain Mixton's identity here, is unsupportable," and concluded the agents' acquisition of Mixton's "identifying information" violated article II, § 8 of the Arizona Constitution. *Mixton*, ¶ 33; *see also id.*, ¶ 40 (Eckerstrom, J., "join[ing] fully" in the article II, § 8 analysis). In so holding, the two-judge majority did not explicitly hold that an IP address or internet subscriber information is a "private affair" under the state constitution. Instead, the majority decided that "the identity behind anonymous communications [] is part and parcel of a person's private affairs" and "access to it affords the government significant insight into a person's private activities and beliefs." *Mixton*, ¶ 28.

Judge Espinosa dissented, disagreeing with "the majority's novel discovery of constitutional protection for internet subscriber information under the Arizona Constitution[.]" *Id.*, ¶ 48 (Espinosa, J., dissenting in part). He emphasized that "only basic identifying information is at issue here" and that "[a]ccess to any of

Mixton's 'public activities' or 'private domain,' at least on this record, only came about through the execution of a duly issued search warrant." *Id.* n.17. Judge Espinosa noted that the majority "refer[s] to a parade of potential horribles that could flow from the disclosure of an internet user's identity, including where they shop, organizations they belong to, medical information, and other details of a person's life." *Id.*, ¶ 51. Yet these concerns are "red herrings" because "nothing of the sort is involved here, where only subscriber identity information was legitimately sought by law enforcement for the sole purpose of revealing the source of suspected child pornography distribution." *Id.*

The court unanimously agreed that the officers acquired the information in good faith and declined to apply the exclusionary rule. *Id.*, ¶¶ 34–39, 54.

III. REASONS THIS COURT SHOULD GRANT REVIEW.

The majority below correctly noted that "[n]o published opinions address the third-party doctrine under Arizona's Constitution." *Id.*, ¶ 16. In its interpretation of article II, § 8, however, the majority committed several critical errors in concluding that the state constitution offers broader protection than the Fourth Amendment in this context. As discussed below: (1) neither the constitution's text, nor Arizona case law construing article II, § 8, supports the majority's implicit conclusion that the agents "disturbed [Mixton] in his private affairs" when they acquired an IP address and subscriber information for the sole purpose of learning

his identity; (2) given Arizona's historical reliance on federal law in interpreting article II, § 8, the majority erred in its outright rejection of the third-party doctrine in this context, where uniformity with federal law is highly desirable; and (3) the majority purported to rely on a growing trend among states, but failed to recognize that *no* other state in the country requires law enforcement to obtain a search warrant for an IP address or internet subscriber information. The majority's holding also conflicts with the court of appeals' earlier decision in *State v. Welch*, 236 Ariz. 308, 311–12, ¶¶ 4–11 & n.1 (App. 2014). Accordingly, it is imperative that this Court grant review.[3] *See* Ariz. R. Crim. P. 31.21(d)(1)(C).

A. *Neither the text of article II, § 8 nor Arizona case law supports the majority's conclusion that an IP address or internet subscriber information is a "private affair," let alone that the agents unconstitutionally disturbed Mixton in his private affairs.*

Article II, § 8, entitled, "Right to privacy," provides that "[n]o person shall be disturbed in his private affairs, or his home invaded, without authority of law." This provision "was taken verbatim from the Washington constitution, and the records of the Arizona constitutional convention contain no material addressing its intent." *Hart v. Seven Resorts*, 190 Ariz. 272, 277 (App. 1997). When the Arizona Constitution does not further define a term, courts "look to their 'natural, obvious,

[3] Although the Arizona Constitution does not provide more protection than the Fourth Amendment in this context, this is not to say that it never provides more protection than the Fourth Amendment, and it may in other contexts.

and ordinary meaning.'" *Kotterman v. Killian*, 193 Ariz. 273, 284, ¶ 33 (1999). The ordinary meaning of "affairs" means "commercial, professional, or personal business." *Mixton*, ¶ 18 (citing *Webster's Third New Int'l Dictionary* 35 (1971)).

The Arizona Constitution's protections under article II, § 8 "are generally coextensive with Fourth Amendment analysis[,]" except that "this Court has recognized more expansive protections under the Arizona Constitution concerning officers' warrantless physical entry into a home." *State v. Hernandez*, 244 Ariz. 1, 6, ¶ 23 (2018) (collecting cases). Although the text of the state constitution "is different and arguably broader than the Fourth Amendment, particularly as it pertains to a person's 'private affairs' and 'home,' its proscription applies to intrusions undertaken 'without authority of law.'" *State v. Adair*, 241 Ariz. 58, 64, ¶ 24 (2016). Accordingly, this Court has held that a search "does not violate Arizona's constitutional privacy clause, as long as the search is reasonable under the totality of circumstances." *Id*.

This Court has also explained—consistent with Fourth Amendment principles—that the "rights [under article II, §8] are personal and can be invoked only by a defendant with a 'legitimate expectation of privacy in the invaded place.'" *State v. Peoples*, 240 Ariz. 244, 247, ¶ 8 (2016) (quoting *Rakas v. Illinois*, 439 U.S. 128, 143 (1978)); *see also Oliver v. United States*, 466 U.S. 170, 182–83 (1984) ("The test of legitimacy is not whether the individual chooses to conceal

assertedly 'private' activity," but instead "whether the government[al] intrusion infringes upon the personal and societal values protected by the Fourth Amendment."). "A defendant's subjective expectation of privacy is 'legitimate' if it is 'one that society is prepared to recognize as reasonable.'" *Peoples*, 240 Ariz. at 247, ¶ 8 (citation omitted).

Here, the textual difference between the Fourth Amendment and article II, §8 does not support the majority's conclusion that an IP address or internet subscriber information is a "private affair" protected by the state constitution. *See Welch*, 236 Ariz. at 317 n.1 (observing that ISPs assign IP addresses to their customers "in order to identify them and verify their status as paying customers" and concluding "any expectation of privacy [from an ISP] would be unreasonable"); *see also Mixton*, ¶ 50 (Espinosa, J., stating, "[t]his court too, in *Welch*, noted that IP addresses, universally assigned by third-party ISPs, are not subject to a reasonable expectation of privacy" and questioning the majority's characterization of *Welch*'s "salient comment" as dicta). As noted above, the "private affairs" clause was taken verbatim from the Washington constitution. *Hart*, 190 Ariz. at 277. The Washington Supreme Court, in interpreting this language, has reasoned that "[i]n 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).

An IP address is merely a string of numbers that does not even identify a person or a location, let alone reveal any details about a person's life. *See supra*, n.2; *see generally* Internet Assigned Numbers Authority Overview, *available at www.iana.org/numbers* (describing two types of IP addresses in active use that ISPs assign to users) (last visited August 27, 2019). As Mixton himself noted in his suppression motion, it is "unlikely" that an IP address will reveal a defendant's "true identity" because "[m]ost, if not all, of the IP addresses will actually reflect a wireless router or networking device, meaning that while the ISPs will provide the name of its subscriber, the alleged infringer could be the subscriber, a member of his or her family, an employee, invitee, neighbor or interloper." (R.O.A. 41, at 6 [quoting *In re BitTorrent*, 296 F.R.D. 80 (D.C.N.Y. 2012)].)

And internet subscriber information—name, address, and phone number—can hardly be characterized as "intimate or discrete details of a person's life." *See Thomas v. Industrial Comm'n*, 126 Ariz. 406, 408–09 (App. 1980) (holding a procedural rule requiring petitioner to disclose his residential address to receive workmen's compensation is not a disturbance of his "private affairs" under article II, § 8). *Cf. Whalen v. Roe*, 429 U.S. 589, 591–606 (1977) (upholding, against Fourteenth Amendment challenge, state law requiring centralized recording of

names and addresses of all persons who have obtained, pursuant to a doctor's prescription, certain drugs for which there is both a lawful and unlawful market). Instead, subscriber information is general in nature and has historically been accessible to law enforcement for broad investigative purposes. *See State v. McKinney*, 60 P.3d 46, 49–52 (Wash. 2002) (holding information in driver's license records is not protected by "private affairs" clause where police only accessed "names and addresses of the registered owners associated with license plate numbers, physical descriptions, and license status," reasoning "it is unlikely that a citizen would expect this information is not available for law enforcement purposes").

As Judge Espinosa emphasized, the majority conflates an IP address and internet subscriber information with an individual's theoretical online "affairs." *Compare Mixton*, ¶ 28 (reasoning "the identity behind anonymous communications [] is part and parcel of a person's private affairs" and "access to it affords the government significant insight into a person's private activities and beliefs"), *with id.* n.17 (Espinosa, J., noting, "it is important to keep in mind that only basic identifying information is at issue here," police did not obtain Mixton's internet visits or public physical movements, "but only the source and 'street address' of the illicit material after obtaining the poster's IP address from a single internet site"). Simply put, no violation of article II, § 8 occurred because Mixton cannot

show, as a threshold matter, that he has a "legitimate expectation of privacy in the invaded place." *See Peoples*, 240 Ariz. at 247, ¶ 8.

Moreover, the federal agents obtained this limited information by issuing federally-authorized subpoenas to Kik and Cox. Their conduct was authorized by law, *see* 19 U.S.C. § 1509, and reasonable under the totality of the circumstances. *See Adair*, 241 Ariz. at 64, ¶ 24. For these reasons, Mixton was not unconstitutionally "disturbed in his private affairs" when the agents acquired this information for the *sole* purpose of learning his identity. *Cf. State v. Surge*, 156 P.3d 208, 215, ¶ 23 (Wash. 2007) (upholding statute authorizing collection of convicted felons' DNA against challenge under state constitution's "private affairs" clause, noting statute does not permit "any use other than for identity purposes" and "there is no basis to conclude that samples contained in these cases have been used for any improper purpose").

B. *Because Arizona courts have historically given great weight to federal law in interpreting article II, § 8, the majority erred by rejecting the third party doctrine in this context, where uniformity is paramount.*

Article II, § 8, "although different in its language, is of the same general effect and purpose as the Fourth Amendment[.]" *Malmin v. State*, 30 Ariz. 258, 262 (1926). And "[a]lthough this Court, when interpreting a state constitutional provision, is not bound by the Supreme Court's interpretation of a federal constitutional clause, those interpretations have 'great weight' in accomplishing the

desired uniformity between the clauses." *State v. Casey*, 205 Ariz. 359, 362, ¶ 11 (2003) (citation omitted). The majority correctly observed that "Arizona courts have long applied the reasonable-expectation-of-privacy test in analyzing the protections provided by both the Fourth Amendment and article II, § 8." *Mixton*, ¶ 18; *see State v. Juarez*, 203 Ariz. 441, 445, ¶¶ 15–16 (App. 2002) (stating article II, § 8 "has historically been construed as imposing limits on search and seizure consistent with the prohibitions of the Fourth Amendment") (collecting cases). Yet inexplicably, the majority criticized the third-party doctrine for its *potential* application to other types of cases that *might* implicate First Amendment rights, instead of applying the doctrine to the lawfulness of the federal agents' acquisition of the IP address and subscriber information. *See id.*, ¶¶ 23–33; *see also id.*, ¶ 51 and n.20 (Espinosa, J., explaining the majority's concerns about "governmental prying" into details of a person's life and citation to "cases relying on the First Amendment" have no application to the facts of this case).

The Supreme Court "consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." *Smith*, 442 U.S. at 743; *see also Miller*, 425 U.S. at 443. In *Smith*, for example, the Court held that the installation and use of a "pen register"—i.e., a device that tracked the phone numbers dialed from the defendant's phone—did not violate the Fourth Amendment because, *inter alia*, it did not reveal "any communication

between the caller and the recipient of the call, their identities, nor whether the call was even completed[.]" 442 U.S. at 741 (citation omitted). Likewise, in *Miller*, the Court held that the defendant did not have a reasonable expectation of privacy in his banking records, noting the records did not contain "confidential communications." 425 U.S. at 442.

Consequently, federal courts "have uniformly held that subscriber information provided to an internet provider is not protected by the Fourth Amendment's privacy expectation … ." *United States v. Christie*, 624 F.3d 558, 573 (3d Cir. 2010) (internal quotation marks omitted, collecting cases); *see also United States v. Hood*, 920 F.3d 87, 92 (1st Cir. 2019) (the conclusion that defendant "did not have a reasonable expectation of privacy in the [IP address] that the government acquired from Kik without a warrant ... is in accord [] with the rulings of all the circuits that had addressed this issue before *Carpenter* had been decided" and with the Fifth Circuit's post-*Carpenter* ruling) (collecting cases).

The Supreme Court's holdings in *Smith* and *Miller* should be given significant weight in this factually-analogous context. As discussed above, the agents' use of administrative subpoenas in this case did not reveal *any* communications; instead, Kik provided an IP number and Cox disclosed basic identifying information that Mixton voluntarily provided. *See United States v. Caira*, 833 F.3d 803, 806–09 (7th Cir. 2016) (applying *Smith*'s and *Miller*'s third-

party doctrine in rejecting defendant's claim that he had a reasonable expectation of privacy in his IP address) (collecting cases). In fact, the information acquired via the administrative subpoenas divulged *less* personal information than that at issue in *Smith* and *Miller*. Even in *Carpenter*, the Supreme Court anticipated the government "will be able to use subpoenas to acquire records in the overwhelming majority of investigations" and it would be a "rare case where the suspect has a legitimate privacy interest in records held by a third party." 138 S. Ct. at 2222.

Federal law overwhelmingly establishes that Mixton has no cognizable privacy interest in an IP address or internet subscriber information. The majority failed to appreciate Arizona's historical preference to give "great weight" to federal law to achieve uniformity, *see Casey*, 205 Ariz. at 362, ¶ 11, and uniformity is highly desirable here. Consistent search-and-seizure standards in this context are necessary, given the unlimited geographic reach of the internet, the legitimate law enforcement interests at stake, and the lack of any textual reason to construe the Arizona Constitution more broadly. *See State v. Bolt*, 142 Ariz. 260, 268 (1984) ("[O]ne of the few things worse than a single exclusionary rule is two different exclusionary rules."). Here, when the federal agents acquired the IP address from Kik, this limited information did not reveal Mixton's identity or location. It only revealed that Cox was associated with that particular IP address, and it was not until Cox released Mixton's subscriber information that the agents learned

Mixton's name and physical location in Arizona. This Court should correct the majority's unjustified departure from federal law.

C. *The majority erred when it purported to join a growing trend among states and failed to recognize that no state has gone this far.*

Finally, Judge Espinosa correctly pointed out that "despite [his] colleagues suggestion of a growing trend, [the majority's] decision joins what appears to be only one state court in the entire country [New Jersey] that has found ISP subscriber information protected under its state constitution." *Mixton*, ¶ 52 (Espinosa, J., dissenting). This statement responded to the majority's assertion that "[m]any states have refused to adopt the third-party doctrine established in *Miller* and *Smith* under their state constitutions, concluding that people do have a reasonable expectation of privacy in information they must furnish to companies providing banking, phone, and internet service in order to use those services." *Mixton*, ¶ 25. In support of this sweeping pronouncement, the majority cited cases from nine states—California, Colorado, Florida, Hawaii, Idaho, Illinois, New Jersey, Pennsylvania, and Utah. *Id.*, ¶¶ 25–26.

As discussed above, the majority improperly considered theoretical scenarios, facts, and constitutional rights that are not implicated in this case. *Id.* n.20 (Espinosa, J., dissenting). Additionally, *none* of the cases cited by the majority addressed an IP address or internet subscriber information, let alone held that their state constitutions protect this information. *See People v. Chapman*, 679

P.2d 62, 67 n.6 (Cal. 1984) (telephone records); *People v. Sporleder*, 666 P.2d 135, 141–42 (Colo. 1983) (phone numbers dialed); *Charnes v. DiGiacomo*, 612 P.2d 1117, 1120–21 (Colo. 1980) (bank records); *Shaktman v. State*, 553 So.2d 148, 151 (Fla. 1989) (pen register records); *State v. Walton*, 324 P.3d 876, 906 (Haw. 2014) (defendant's membership card located in a backpack found at crime scene); *State v. Thompson*, 760 P.2d 1162, 1165 (Idaho 1988) (installation of pen register); *People v. DeLaire*, 610 N.E.2d 1277, 1282 (Ill. 1993) (telephone "message unit detail" records); *Commonwealth v. DeJohn*, 403 A.2d 1283, 1289 (Pa. 1979) (bank records); *State v. Thompson*, 810 P.2d 415, 418 (Utah 1991) (bank records).[4] Pennsylvania, in fact, has expressly *rejected* a claim that a person "had a right of privacy in the mere name and address information disclosed by his bank," holding its state constitution jurisprudence "should not be expanded to encompass such a circumstance[.]" *Comm. v. Duncan*, 817 A.2d 455, 459 (Pa. 2003).

And even in New Jersey where internet users have "confidentiality" in their subscriber information, *see Mixton*, ¶ 26 (citing *State v. Reid*, 945 A.2d 26 (N.J.

---

[4] The Utah Supreme Court later emphasized that *Thompson* simply "stands for the unremarkable proposition that there is no violation of [the Utah Constitution] when the state obtains bank records through a reasonable search and seizure," noting that "whatever 'right to privacy' individuals may have in their bank records, the Utah Constitution permits the state to intrude upon it 'pursuant to a subpoena' that is 'lawfully issued' to a bank." *Schroeder v. Utah Attorney General's Office*, 358 P.3d 1075, 1081–82, ¶ 24 (Utah 2015) (citing *Thompson*, 810 P.2d at 418).

2008)), law enforcement officials satisfy this state constitutional right to privacy by serving a "proper grand jury subpoena" based "upon a showing of relevance." *Reid*, 945 A.2d at 36–38; *see also State v. Simmons*, 27 A.3d 1065, 1070 n.5 (Vt. 2011) ("[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.").[5]

Ultimately, decisions from other jurisdictions interpreting their own constitutions that contain different wording than article II, § 8 "are of little value" in interpreting the Arizona Constitution. *Juarez*, 203 Ariz. at 446, ¶ 20. The majority's reliance on factually-distinguishable cases evaluated under dissimilar provisions of other states' constitutions presents this Court with an opportunity to reinforce the legal framework for evaluating a claim asserted under Arizona's right to privacy clause. State constitutional rights should not emerge "out of the blue," *see Mixton*, ¶ 52 (Espinosa, J., dissenting), particularly in cases like this one, where

---

[5] Notably, New Jersey declines to apply the exclusionary rule to suppress evidence acquired by federal actors in violation of the state constitution, reasoning that "application of the state constitution to the officers of another jurisdiction would disserve the principles of federalism and comity, without properly advancing legitimate state interests." *State v. Mollica*, 554 A.2d 1315, 1327 (N.J. 1989). In the event Mixton seeks review of the court of appeals' application of the good-faith exception to the exclusionary rule, or if this Court reaches the question whether the exclusionary rule should apply, the State preserves the argument that violations of the state constitution do not apply to federal actors. *See id*.

courts are confronted with questions involving technology, electronic information, and privacy rights. *See Carpenter*, 138 S. Ct. at 2220 ("We do not express a view on matters not before us ... As Justice Frankfurter noted when considering new innovations in airplanes and radios, the Court must tread carefully in such cases, to ensure that we do not 'embarrass the future.'") (quoting *Northwest Airlines, Inc. v. Minnesota*, 322 U.S. 292, 300 (1944)).

IV. CONCLUSION.

For all the foregoing reasons, this Court must grant review.

RESPECTFULLY SUBMITTED this 28th day of August, 2019.

Mark Brnovich
Attorney General

Joseph T. Maziarz
Chief Counsel

/s/
Linley Wilson
Assistant Attorney General
Attorneys for Appellee

8092806