IN THE

ARIZONA COURT OF APPEALS

DIVISION TWO

THE STATE OF ARIZONA,
Appellee,

v.

WILLIAM MIXTON,
Appellant.

No. 2 CA-CR 2017-0217
Filed July 29, 2019

Appeal from the Superior Court in Pima County
No. CR20162038001
The Honorable Sean E. Brearcliffe, Judge

AFFIRMED

COUNSEL

Mark Brnovich, Arizona Attorney General
Joseph T. Maziarz, Chief Counsel
By Linley Wilson, Assistant Attorney General, Phoenix
Counsel for Appellee

Joel Feinman, Pima County Public Defender
By Abigail Jensen, Assistant Public Defender, Tucson
Counsel for Appellant

OPINION

Presiding Judge Eppich authored the opinion of the Court, in which Judge Eckerstrom concurred in part and dissented in part and Judge Espinosa concurred in part and dissented in part.

E P P I C H, Presiding Judge:

¶1 William Mixton appeals his convictions for twenty counts of sexual exploitation of a minor under fifteen years of age, arguing police violated his federal and state constitutional rights by obtaining, without a warrant, information from two service providers identifying him as the sender of certain incriminating internet messages. He contends the trial court erred in failing to suppress evidence obtained as a result of that warrantless acquisition of information. We conclude that, although the information was obtained in violation of article II, § 8 of the Arizona Constitution, the good-faith exception to the exclusionary rule applies. Accordingly, we affirm Mixton's convictions and sentences.

Factual and Procedural Background

¶2 In March 2016, an undercover detective investigating child exploitation placed an ad on a popular internet advertising forum targeting offenders interested in child pornography and incest, inviting those interested to contact him to join a group chat on a messaging application known for minimal verification of its users' identities. Several people responded to the ad, including one who provided his messaging application screen name "tabooin520" and asked to be added to the group chat. In the days after the detective added this user to the group, the user posted several images and videos depicting child pornography. When the detective sent a person-to-person message to the user thanking him for the pictures, the user responded by sending the detective additional images of child pornography in personal messages.

¶3 At the detective's request, federal agents participating in the investigation served a federal administrative subpoena on the messaging application provider to obtain the user's IP address.[1] Once the provider furnished the IP address, the detective was able to determine the user's internet service provider (ISP) by using publicly available information. Again, federal agents served a subpoena, and as a result, the ISP supplied

[1] "An IP address is a number assigned to each device that is connected to the Internet. Although most devices do not have their own, permanent ('static') addresses, in general an IP address for a device connected to the Internet is unique in the sense that no two devices have the same IP address at the same time." *United States v. Vosburgh*, 602 F.3d 512, 518 (3d Cir. 2010).

the street address of the user to whom the IP address was assigned. Based on this information, the detective obtained a search warrant for that address.

¶4 Mixton lived in a room at that address. During execution of the search warrant, police seized from Mixton's room a cell phone, an external hard drive, a laptop computer, and a desktop computer, each of which contained numerous images and videos containing child pornography. In some of the folders containing these images and videos, police also found images of Mixton, and images the detective had sent to the user via the messaging application.

¶5 Based on images found on the devices in Mixton's room, a grand jury indicted Mixton on charges including twenty counts of sexual exploitation of a minor under fifteen years of age. The trial court severed counts for other offenses, and after a four-day trial for sexual exploitation, a jury convicted Mixton on all twenty counts. For each count, the court imposed a seventeen-year sentence, all to be served consecutively. We have jurisdiction over Mixton's appeal pursuant to A.R.S. §§ 13-4031 and 13-4033(A)(1).

Motion to Suppress

¶6 Before trial, Mixton moved to suppress both the subscriber information obtained via the administrative subpoenas and all evidence collected as a result of that information including the evidence obtained during the search of his home. He argued that both the Fourth Amendment and article II, § 8 of the Arizona Constitution protected his reasonable expectation of privacy in the subscriber information, prohibiting law enforcement from obtaining that information without a warrant or other court order. After brief oral argument, the trial court denied the motion, ruling that Mixton had no recognized privacy interest in the subscriber information.[2]

[2] The trial court ruled that the information obtained was not protected under the Fourth Amendment but did not separately address Mixton's claim under article II, § 8. Given that the court referred to article II, § 8, we assume it concluded that article II, § 8's protections coextend with the Fourth Amendment under the facts of this case. *Cf. State v. Bolt*, 142 Ariz. 260, 269 (1984) ("We . . . do not propose to make a separate exclusionary rule analysis as a matter of state law in each search and seizure case.").

¶7 On appeal, Mixton reasserts his contention that both the Fourth Amendment and article II, § 8 protect the identifying information he transmitted to the service providers. We review de novo constitutional issues raised in a motion to suppress, considering only the evidence presented at the suppression hearing and viewing that evidence in the light most favorable to upholding the trial court's ruling. *State v. Blakley*, 226 Ariz. 25, ¶ 5 (App. 2010). Here, the parties did not present evidence at the motion hearing, however, arguing the motion on their filings. The relevant facts appear to be undisputed; we view them in the light most favorable to upholding the ruling. *Cf. State v. Navarro*, 241 Ariz. 19, n.1 (App. 2016) (considering undisputed facts to decide suppression motion where no hearing held).

¶8 As a preliminary matter, Mixton urges us to address the issue under article II, § 8 before we address it under the Fourth Amendment in order to "honor[] the intent of the [state constitution's] framers to provide an independent and primary organic law, and . . . ensure[] that the rights of Arizonans will not erode even when federal constitutional rights do." Clint Bolick, *Vindicating the Arizona Constitution's Promise of Freedom*, 44 Ariz. St. L.J. 505, 509 (2012). Our supreme court has held, however, that "decisions of the United States Supreme Court have great weight in interpreting those provisions of the state constitution which correspond to the federal provisions." *Pool v. Superior Court*, 139 Ariz. 98, 108 (1984). While worded differently, article II, § 8 corresponds to the Fourth Amendment; both exist to protect against unreasonable searches and seizures. *See State v. Ault*, 150 Ariz. 459, 463 (1986). Moreover, article II, § 8 "is of the same general effect and purpose as the Fourth Amendment, and, for that reason, decisions on the right of search under the latter are well in point on section 8." *Malmin v. State*, 30 Ariz. 258, 261 (1926). Very recently, our supreme court stated that "[t]he Arizona Constitution's protections under article 2, section 8 are generally coextensive with Fourth Amendment analysis." *State v. Hernandez*, 244 Ariz. 1, ¶ 23 (2018). Indeed, its interpretations of article II, § 8 have rarely departed from Fourth Amendment precedent, and never in a case that does not involve physical invasion of the home. *See State v. Peltz*, 242 Ariz. 23, n.3 (App. 2017). Therefore, while "we cannot and should not follow federal precedent blindly" in interpreting our state constitution, *Pool*, 139 Ariz. at 108, neither can we turn a blind eye to it. On the other hand, our independent interpretation of article II, § 8 would be of little assistance in analyzing the Fourth Amendment, an area of law in which decisions of our federal Supreme Court bind us.

¶9 For this reason, and because Mixton has also challenged his convictions under the Fourth Amendment, we analyze the issues here first under the Fourth Amendment. In doing so we follow the lead of our supreme court, which has taken this approach in deciding article II, § 8 challenges. *See, e.g.*, *Hernandez*, 244 Ariz. 1, ¶¶ 11-23; *State v. Bolt*, 142 Ariz. 260, 263-65 (1984). We recognize our duty to independently interpret and give effect to our state constitution, however. *See Pool*, 139 Ariz. at 108. To the extent we find rights in article II, § 8 beyond those that have been found under the Fourth Amendment, we may always exert our state sovereignty and avoid federal review through a "clear and express statement that [our] decision rests on adequate and independent state grounds." *Michigan v. Long*, 463 U.S. 1032, 1042 n.7 (1983); *see also Ault*, 150 Ariz. at 466 ("We decide this case on independent state grounds."); *Bolt*, 142 Ariz. at 265 (similar).

Fourth Amendment

¶10 The Fourth Amendment provides that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated." "A 'search' under the Fourth Amendment occurs 'when an expectation of privacy that society is prepared to consider reasonable is infringed.'" *State v. Welch*, 236 Ariz. 308, ¶ 8 (App. 2014) (quoting *United States v. Jacobsen*, 466 U.S. 109, 113 (1984)). Before police conduct a search that infringes upon a person's subjective and objectively reasonable expectation of privacy, police generally must obtain a warrant supported by probable cause. *Carpenter v. United States*, ___ U.S. ___, ___, 138 S. Ct. 2206, 2213 (2018). Evidence obtained in violation of this requirement may be subject to suppression, *see Bolt*, 142 Ariz. at 265-69, but only the person whose rights were violated may claim the violation, *see State v. Jeffers*, 135 Ariz. 404, 413 (1983); *State v. Juarez*, 203 Ariz. 441, ¶ 12 (App. 2002) (citing *Rakas v. Illinois*, 439 U.S. 128, 143 (1978)).

¶11 In 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." *United States v. Miller*, 425 U.S. 435, 443 (1976) (government's warrantless acquisition of customer's bank records held by bank did not violate Fourth Amendment); *see also Smith v. Maryland*, 442 U.S. 735, 744-45 (1979) (warrantless collection of subscriber's phone calls via "pen register" did not violate Fourth Amendment). Federal 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. *See, e.g.*, *United States v. Weast*, 811 F.3d 743, 747-48 (5th Cir. 2016), *cert. denied*, ___ U.S. ___, 137 S. Ct. 126 (2016); *United States v. Christie*, 624 F.3d 558, 573-74 (3d Cir. 2010) ("Federal courts have uniformly held that 'subscriber information provided to an internet provider is not protected by the Fourth Amendment's privacy expectation.'" (quoting *United States v. Perrine*, 518 F.3d 1196, 1204 (10th Cir. 2008))), *cert. denied*, 562 U.S. 1236 (2011); *Perrine*, 518 F.3d at 1204. Thus, an internet user has no recognized Fourth Amendment privacy interest in his IP address or the personally identifying information he or she submitted to his or her ISP to subscribe to its service. The third-party doctrine does not allow the government to obtain the contents of communications from a third-party communication technology provider, however. *See Katz v. United States*, 389 U.S. 347, 348, 359 (1967) (striking down conviction based on warrantless surveillance of defendant's phone calls via electronic listening device); *Smith*, 442 U.S. at 741 ("[A] pen register differs significantly from the listening device employed in *Katz,* for pen registers do not acquire the *contents* of communications."). Recently, the United States Supreme Court declined to extend the third-party doctrine established by *Miller* and *Smith* to "detailed, encyclopedic, and effortlessly compiled" cell-site location records, but characterized its decision as a "narrow one" and expressly left existing application of *Miller* and *Smith* undisturbed. *Carpenter*, 138 S. Ct. at 2216-17, 2220.

¶12 Mixton nonetheless contends that he had a reasonable expectation of privacy in his identity because his conduct shows a calculated effort to maintain anonymity: He used a messaging application known for collecting little information from its users and communicated in that application using a pseudonym. But while a person must have a subjective expectation of privacy in order to invoke Fourth Amendment protection, it must also be "one that society is prepared to recognize as 'reasonable'" for the Fourth Amendment to apply. *Smith*, 442 U.S. at 740 (quoting *Katz*, 389 U.S. at 361 (Harlan, J., concurring)). As explained above, *Smith* and the federal circuit cases following it have established that an internet user has no recognized Fourth Amendment privacy interest in his or her identity. And while Mixton points out that he only shared his subscriber information with the service providers, this presumably was also true in the many federal cases that have found no reasonable expectation in such subscriber information. *See, e.g.*, *Weast*, 811 F.3d at 747-48; *Christie*, 624 F.3d at 573-74; *Perrine*, 518 F.3d at 1204. No reasonable expectation of privacy exists under the Fourth Amendment by virtue of this fact: The federal third-party doctrine has been applied even when

information is shared with only one third party. *See United States v. Caira*, 833 F.3d 803, 806 (7th Cir. 2016). While Mixton notes that investigators obtained his IP address in addition to his identity, federal courts have not recognized a protected privacy interest in an IP address. *See, e.g.*, *Caira*, 833 F.3d at 806-07; *Weast*, 811 F.3d at 747-48; *Perrine*, 518 F.3d at 1204-05. Finally, Mixton reminds us we are not bound to follow the federal circuit cases, *see State v. Montano*, 206 Ariz. 296, n.1 (2003), but we are bound by *Smith*, which dictated the result in those cases.[3]

¶13 Because 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. The trial court did not err in denying Mixton's Fourth Amendment claim.

Article II, § 8 of the Arizona Constitution

¶14 Article II, § 8 of the Arizona Constitution provides that "[n]o person shall be disturbed in his private affairs, or his home invaded, without authority of law." Although article II, § 8 "is of the same general effect and purpose as the Fourth Amendment to the Constitution of the United States," "[w]e have the right [to interpret] our own constitutional provisions as we think logical and proper, notwithstanding their analogy to the Federal Constitution and the federal decisions based on that Constitution." *Turley v. State*, 48 Ariz. 61, 70-71 (1936). Pursuant to article II, § 8's explicit mention of the home, Arizona courts have, on occasion, found protections from warrantless physical intrusions into a home not recognized in Fourth Amendment jurisprudence. *See Ault*, 150 Ariz. at 466 (declining "to extend the inevitable discovery doctrine into defendant's home . . . regardless of the position the United States Supreme Court would take on this issue"); *Bolt*, 142 Ariz. at 263-65 (declining to follow United States Supreme Court case involving warrantless entry of home to "secure" it until search warrant obtained).

¶15 While Arizona's appellate courts have never extended article II, § 8 beyond the Fourth Amendment outside the context of the home, *see Peltz*, 242 Ariz. 23, n.3, our supreme court "has never expressly held, based on considered analysis, that [article II, § 8's protections of "private

[3]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.

affairs" are] coextensive with the United States Supreme Court's interpretation of Fourth Amendment protections," *Hernandez*, 244 Ariz. 1, ¶ 30 (Bolick, J., concurring). Consistent with our prerogative to independently interpret our constitution, *see Pool*, 139 Ariz. at 108, our supreme court has left open the possibility that article II, § 8 rights extend beyond those that have been found in the Fourth Amendment in circumstances other than warrantless physical intrusion into the home, *see Hernandez*, 244 Ariz. 1, ¶ 23 ("We are not persuaded that the scope of the Arizona Constitution's protections exceeds the Fourth Amendment's reach *under the circumstances of this case*." (emphasis added)).

¶16 No published opinions address the third-party doctrine under Arizona's Constitution.[4] We review de novo a matter of first impression regarding whether a particular expectation of privacy should be recognized under constitutional law. *State v. Huerta*, 223 Ariz. 424, ¶ 4 (App. 2010).

¶17 Mixton argues that because article II, § 8 explicitly grants protection to "private affairs" in addition to homes, its protection of private affairs must extend beyond the protections offered by the Fourth Amendment, as it does for homes. He urges us to follow Justice Bolick's view that article II, § 8's protection of "private affairs" must differ from the protection afforded by the Fourth Amendment because the language is different. *See Hernandez*, 244 Ariz. 1, ¶ 29 (Bolick, J., concurring) ("It is axiomatic, as a matter of constitutional or statutory interpretation, that where different language is used in different provisions, we must infer that a different meaning was intended." (citing *Rochlin v. State*, 112 Ariz. 171, 176 (1975))).

¶18 To determine whether a private affair has been disturbed, Mixton contends that we should focus on "the nature of the government's actions" rather than applying a reasonable-expectation-of-privacy test akin to that in Fourth Amendment jurisprudence. *See State v. Campbell*, 759 P.2d 1040, 1044 (Or. 1988) (rejecting reasonable-expectation-of-privacy test under Oregon Constitution's search-and-seizure provision). But as Mixton

[4]In *State v. Welch*, 236 Ariz. 308, n.1 (App. 2014), this court summarily concluded any expectation of confidentiality from an internet provider would be unreasonable. However, insofar as Welch had not asserted such an expectation of privacy, either below or on appeal, the court's observation was clearly dicta, which, for the reasons explained below, we decline to follow.

acknowledges, 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. *See Juarez*, 203 Ariz. 441, ¶ 16 (Arizona courts have "consistently" applied reasonable-expectation-of-privacy test in article II, § 8 challenges since 1980). That test is consistent with the term "*private* affairs," which we conclude refers to those affairs in which a person has a reasonable expectation of privacy. *See also Webster's Third New Int'l Dictionary* 35 (1971) (defining "affairs" as "commercial, professional, or personal business"). We therefore apply a reasonable-expectation-of-privacy test in analyzing the issue here under article II, § 8.[5]

¶19 Mixton next argues that internet users have a reasonable expectation of privacy in their identity when communicating using a pseudonym on the internet. Noting growing public concern about government's ability to collect information from technologies such as the internet that are an indispensable part of modern life, he urges us to join "[a] growing number of states [that] have declined to import the third-party doctrine into their state constitutional search-and-seizure provisions." *Zanders v. State*, 73 N.E.3d 178, 186 (Ind. 2017), *cert. granted, judgment vacated on federal grounds*, ___ U.S. ___, 138 S. Ct. 2702 (2018).

¶20 As mentioned above in our discussion of the Fourth Amendment, the federal third-party doctrine generally holds that a person has no reasonable expectation of privacy in information revealed to a third

[5]Even though article II, § 8 derives from identical language in article I, § 7 of the Washington Constitution, we have not adopted Washington's interpretations of that provision. *See Juarez*, 203 Ariz. 441, ¶¶ 21-22, n.10 (notwithstanding wording similarities, "Arizona's interpretation and application of our right to privacy provision has not paralleled that of Washington's"). Washington courts have interpreted "private affairs" to mean "those privacy interests which citizens of this state have held, and should be entitled to hold, safe from governmental trespass." *State v. Athan*, 158 P.3d 27, 33 (Wash. 2007) (quoting *State v. Myrick*, 688 P.2d 151, 154 (Wash. 1984)). Washington has expressly rejected the reasonable-expectation-of-privacy test in analyzing whether a privacy interest is protected. *See Myrick*, 688 P.2d at 153-54. Instead, Washington courts examine "the historical treatment of the interest being asserted, analogous case law, and statutes and laws supporting the interest asserted." *Athan*, 158 P.3d at 33. While these considerations may inform the application of the reasonable-expectation test in a given case, we decline to adopt these formulations in lieu of that test.

party, even "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." *Miller*, 425 U.S. at 443. The doctrine has its roots in a line of cases in which the Court ruled that defendants had no protected Fourth Amendment interest in their conversations with a false friend (either a government informant or agent), even when the false friend records the conversation or allows others to listen in without the defendant's consent. *See id.* (citing *United States v. White*, 401 U.S. 745, 751-52 (1971) (incriminating statements made in person to government informer, overheard by government agents informer allowed to eavesdrop in person and through electronic surveillance); *Hoffa v. United States*, 385 U.S. 293, 302 (1966) (incriminating statements made in person to government informer); and *Lopez v. United States*, 373 U.S. 427 (1963) (recording of defendant's conversation by person to whom defendant spoke)). In *Miller*, the Court ruled that a person had no reasonable expectation of privacy in their bank records held by their bank. *Id.* at 442. The Court found that what the government obtained, including the defendant's financial records and bank slips, were "not confidential communications," as the records "contain[ed] only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business." *Id.* The Court concluded that a bank customer, like a person whose confidence is betrayed by a false friend, "takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government." *Id.* at 443 (citing *White*, 401 U.S. at 751-52).

¶21 In *Smith*, the Court concluded that the suspect had no reasonable expectation of privacy in the phone numbers he dialed. 442 U.S. at 745-46. There, police, without obtaining a warrant, requested the phone company to install a "pen register" to record the phone numbers dialed on a suspect's phone. *Id.* at 737. The Court questioned whether phone users had even a subjective expectation of privacy in the phone numbers they dial:

> [W]e doubt that people in general entertain any actual expectation of privacy in the numbers they dial. All telephone users realize that they must "convey" phone numbers to the telephone company, since it is through telephone company switching equipment that their calls are completed. All subscribers realize, moreover, that the phone company has facilities for making permanent records of the numbers they dial, for they see a list of their long-distance (toll) calls on their monthly bills. In fact, pen

> registers and similar devices are routinely used by telephone companies "for the purposes of checking billing operations, detecting fraud and preventing violations of law." . . . Telephone users, in sum, typically know that they must convey numerical information to the phone company; that the phone company has facilities for recording this information; and that the phone company does in fact record this information for a variety of legitimate business purposes. Although subjective expectations cannot be scientifically gauged, it is too much to believe that telephone subscribers, under these circumstances, harbor any general expectation that the numbers they dial will remain secret.

Id. at 742-43 (quoting *United States v. New York Tel. Co.*, 434 U.S. 159, 174-75 (1977)). Therefore, according to the Court, even if a person takes steps calculated to keep the contents of the call confidential, such as calling from the privacy of their home, that conduct does not preserve any subjective expectation of privacy in the phone numbers dialed, which are necessarily shared with the phone company to complete the call regardless of the other circumstances of the call. *Id.* Further, *Smith* also found no expectation of privacy in the phone calls that society was prepared to accept as reasonable. *Id.* at 743-44. Like in *Miller*, the Court reasoned that the defendant had voluntarily shared the information with a third party and assumed the risk the third party would share it with the government:

> When he used his phone, petitioner voluntarily conveyed numerical information to the telephone company and "exposed" that information to its equipment in the ordinary course of business. In so doing, petitioner assumed the risk that the company would reveal to police the numbers he dialed.

Id. at 744.

¶22 Federal courts have uniformly applied the third-party doctrine in *Smith* to information held by ISPs such as the subscriber information of a particular user, logs showing the user's internet activity through the IP addresses of websites a user has visited, and the email addresses of those who send and receive emails to and from the user.

See, e.g., *Caira*, 833 F.3d at 806-07 (IP address used to access email account and subscriber information associated with that IP address); *Weast*, 811 F.3d at 747-48 (subscriber information associated with particular IP address used to access the internet); *Christie*, 624 F.3d at 573-74 (same); *Perrine*, 518 F.3d at 1204-05 (same); *United States v. Forrester*, 512 F.3d 500, 509-10, n.4 (9th Cir. 2008) (to/from addresses of email messages sent and received and IP addresses of websites visited). In *Forrester*, for example, the Ninth Circuit explained that the reasoning in *Smith* applies directly to newer technologies:

> [E]-mail and Internet users have no expectation of privacy in the to/from addresses of their messages or the IP addresses of the websites they visit because they should know that this information is provided to and used by Internet service providers for the specific purpose of directing the routing of information. Like telephone numbers, which provide instructions to the "switching equipment that processed those numbers," e-mail to/from addresses and IP addresses are not merely passively conveyed through third party equipment, but rather are voluntarily turned over in order to direct the third party's servers.
>
> Second, e-mail to/from addresses and IP addresses constitute addressing information and do not necessarily reveal any more about the underlying contents of communication than do phone numbers. When the government obtains the to/from addresses of a person's e-mails or the IP addresses of websites visited, it does not find out the contents of the messages or know the particular pages on the websites the person viewed. At best, the government may make educated guesses about what was said in the messages or viewed on the websites based on its knowledge of the e-mail to/from addresses and IP addresses—but this is no different from speculation about the contents of a phone conversation on the basis of the identity of the person or entity that was dialed.

Forrester, 512 F.3d at 510 (citation omitted) (quoting *Smith*, 442 U.S. at 744).

¶23 The concerns Mixton raises regarding the third-party doctrine are not new: Justices Stewart and Marshall, both joined by Justice Brennan, raised the same general concerns in dissents in *Smith*.[6] Justice Stewart noted the essential role of the telephone in private communications, and concluded that phone users were entitled to assume that the numbers they dialed were private just like the conversations. *Smith*, 442 U.S. at 746-48 (Stewart, J., dissenting). Stewart rejected the notion that phone numbers did not have content, concluding that because that information "could reveal the identities of the persons and the places called," it could "reveal the most intimate details of a person's life." *Id.* at 748. Stewart also noted that the information collected from a private phone call often "emanates from private conduct within a person's home or office"—places entitled to protection. *Id.* at 747.[7] For these reasons, Stewart believed phone users had a legitimate expectation of privacy in the phone numbers they dialed, notwithstanding the necessary involvement of the telephone company in transmitting calls and its ability by virtue of its position to record the numbers called. *Id.* at 746-48. Justice Marshall attacked the opinion's assumption-of-risk rationale, remarking that "unless 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. It is idle to speak of 'assuming' risks in contexts where, as a practical matter, individuals have no realistic alternative." *Id.* at 750 (Marshall, J., dissenting) (citation omitted). He warned that allowing the government to discover where a person had placed phone calls without first showing probable cause risked more than just general harm to people's sense of security: For example, it could allow the government to discover the author of anonymous political speech or a journalist's confidential sources. *See id.* at 751.

¶24 Many legal scholars have lodged similar criticisms and concerns. For example, one remarked:

> Privacy of information normally means the selective disclosure of personal information rather than total secrecy. . . . A bank customer

[6]Justices Brennan and Marshall also dissented in *Miller*. 425 U.S. at 447-56.

[7]Of course, *Smith* was decided long before the widespread use of mobile phone technology.

> may not care that the employees of the bank know a lot about his financial affairs, but it does not follow that he is indifferent to having those affairs broadcast to the world or disclosed to the government.

Richard Posner, *The Economics of Justice* 342 (1981); *see also* Wayne R. LaFave, 1 Search & Seizure § 2.7(c) (5th ed. 2018) ("The result reached in *Miller* is dead wrong, and the Court's woefully inadequate reasoning does great violence to the theory of Fourth Amendment protection the Court had developed in *Katz*."); Avidan Y. Cover, *Corporate Avatars and the Erosion of the Populist Fourth Amendment*, 100 Iowa L. Rev. 1441 (2015) ("[T]he third-party doctrine proves unsupportable in the big data surveillance era, in which communicating and sharing information through third parties' technology is a necessary condition of existence, and non-content data, such as Internet subscriber information . . . , provides an intimate portrait of a person's activities and beliefs.").

¶25 Many 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. *See, e.g.*, *People v. Chapman*, 679 P.2d 62, 67 n.6 (Cal. 1984) (rejecting the "fiction" in *Miller* and *Smith* that a person has no reasonable expectation of privacy in bank or phone call records); *People v. Sporleder*, 666 P.2d 135, 141-42 (Colo. 1983) (rejecting *Smith* and finding reasonable expectation of privacy in phone numbers dialed); *Charnes v. DiGiacomo*, 612 P.2d 1117, 1120-21 (Colo. 1980) (rejecting *Miller* in construing state constitution's search-and-seizure provision); *Shaktman v. State*, 553 So. 2d 148, 151 (Fla. 1989) (person has reasonable expectation of privacy in phone number dialed); *State v. Walton*, 324 P.3d 876, 906 (Haw. 2014) (*Miller* and *Smith* "incorrectly rely on the principle that individuals who convey information to a third party have assumed the risk of that party disclosing the information to the government. In our times individuals may have no reasonable alternative."); *State v. Thompson*, 760 P.2d 1162, 1165 (Idaho 1988) ("[I]n Idaho there is a legitimate and reasonable expectation of privacy in the phone numbers that are dialed."); *People v. DeLaire*, 610 N.E.2d 1277, 1282 (Ill. App. 1993) ("We believe that citizens have a legitimate expectation that their telephone records will not be disclosed."); *Commonwealth v. DeJohn*, 403 A.2d 1283, 1289 (Pa. 1979) ("As we believe that *Miller* establishes a dangerous precedent, with great potential for abuse, we decline to follow that case when construing the state constitutional protection against unreasonable searches and seizures.");

State v. Thompson, 810 P.2d 415, 418 (Utah 1991) (rejecting *Miller*). *But see State v. Clark*, 752 S.E.2d 907, 921 n.13 (W. Va. 2013) (declining to depart from *Smith* and citing cases in eight states that follow *Miller* and *Smith*).

¶26 For example, in *State v. Reid*, the New Jersey Supreme Court affirmed the trial court's suppression of an internet user's subscriber information, holding that under that state 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. 945 A.2d 26, 28, 32, 38 (N.J. 2008). The court observed that internet use, like banking and phone use, is an essential part of modern life that necessarily involves a third-party service provider. *Id.* at 33. Despite the involvement of an ISP, however, the court in *Reid* found that internet users generally enjoy—and expect—anonymity in their internet use. *Id.* at 29, 33. The court noted that during typical internet use, an IP address, which is assigned to the user by their ISP and allows them to connect to websites, email, and other services, is ordinarily insufficient to identify the user; an IP address usually only identifies the ISP to which it is assigned, and only that ISP can match their customer's identity to an IP address. *Id.* at 29. When the government obtains the user's identity through his or her subscriber information, the government can learn intimate details of the subscriber's life, including the "stores at which a person shops, the political organizations a person finds interesting, a person's . . . fantasies, her health concerns, and so on." *Id.* at 33 (alteration in original) (quoting Daniel Solove, *Reconstructing Electronic Surveillance Law*, 72 Geo. Wash. L. Rev. 1264, 1287 (2004)). The court concluded that internet users are "entitled to expect confidentiality" in this information, and the fact that they have disclosed their identities to third-party internet service providers "does not upend the privacy interest at stake." *Id.*

¶27 For similar reasons, we conclude that internet users generally have a reasonable expectation of privacy in their subscriber information.[8] We therefore join the several other states that have declined to apply the federal third-party doctrine established in *Miller* and *Smith* under their state constitutions in circumstances analogous to those before us. In the internet era, the electronic storage capacity of third parties has in many cases

[8]The record in this case is devoid of evidence of the terms of any contract between the ISP and Mixton or any privacy policy the provider may have disclosed to him. We therefore have no occasion to consider the impact, if any, such terms may have on the reasonableness of a particular subscriber's expectation of privacy in a given case.

replaced the personal desk drawer as the repository of sensitive personal and business information—information that would unquestionably be protected from warrantless government searches if on paper in a desk at a home or office. The third-party doctrine allows the government a peek at this information in a way that is the twenty-first-century equivalent of a trip through a home to see what books and magazines the residents read, who they correspond with or call, and who they transact with and the nature of those transactions. *Cf. Riley v. California*, 573 U.S. 373, 393-95 (2014) (discussing how mass transition from paper data storage to digital data storage has increased privacy interests in cell phones). We doubt the framers of our state constitution intended the government to have such power to snoop in our private affairs without obtaining a search warrant.

¶28 The state rests its argument in favor of the third-party doctrine on the rationales from *Smith*: It argues the information at issue here was "non-content" information that Mixton voluntarily submitted to the third-party service providers. But information that has been deemed as "non-content," such as a person's bank records, who a person calls or emails, what websites a person visits, or, as here, the identity behind anonymous communications, is part and parcel of a person's private affairs; access to it affords the government significant insight into a person's private activities and beliefs. Warrantless government collection of this information from an internet service provider or similar source thus constitutes a significant and unwarranted intrusion into a person's private affairs—an intrusion our constitution unambiguously prohibits. And we are not persuaded that a person gives up any reasonable expectation of privacy in this information because he or she "voluntarily" reveals his or her identity to an ISP to get service. The user provides the information for the limited purpose of obtaining service. It is entirely reasonable for the user to expect the provider not to exceed that purpose by revealing the user's identity to authorities in a way that connects it to his or her activities on the internet. Therefore, when the government compels the provider to release the internet user's identity in that way, and without a warrant, it invades the user's reasonable expectation of privacy.

¶29 We are especially troubled that the third-party doctrine grants the government unfettered ability to learn the identity behind anonymous speech, even without any showing or even suspicion of unlawful activity. An author's decision to remain anonymous, whether "motivated by fear of economic or official retaliation, by concern about social ostracism, or merely by a desire to preserve as much of one's privacy as possible," "is an aspect of the freedom of speech protected by the First Amendment." *McIntyre v. Ohio Elections Comm'n*, 514 U.S. 334, 341-42, 357

(1995) (striking down state statute outlawing anonymous political leaflets). Even in benign exercise, the government's ability to identify anonymous speakers, if not meaningfully limited, intrudes on the speaker's desire to remain anonymous and may discourage valuable speech. At worst, the power may be wielded to silence dissent.

¶30 Even if the government obtains nothing more without a warrant than basic identifying information connected to specific internet activity, other cherished rights are endangered. The right of free association, for example, is hollow when the government can identify an association's members through subscriber information matched with particular internet activity. The importance of privacy in one's associations is illustrated by *NAACP v. Alabama*, in which the Court ruled that the state could not compel the NAACP to produce the names and addresses of its members even with a court order, ruling that the compelled disclosure violated the members' freedom of association. 357 U.S. 449, 453, 466 (1958). The decision illustrates "the vital relationship between freedom to associate and privacy in one's associations":

> It is hardly a novel perception that compelled disclosure of affiliation with groups engaged in advocacy may constitute . . . effective . . . restraint on freedom of association. . . . This Court has recognized the vital relationship between freedom to associate and privacy in one's associations. . . .
>
> We think that the production order, in the respects here drawn in question, must be regarded as entailing the likelihood of a substantial restraint upon the exercise by [the NAACP's] members of their right to freedom of association. [The NAACP] has made an uncontroverted showing that on past occasions revelation of the identity of its rank-and-file members has exposed these members to economic reprisal, loss of employment, threat of physical coercion, and other manifestations of public hostility. Under these circumstances, we think it apparent that compelled disclosure of [the NAACP's] Alabama membership is likely to affect adversely the ability of petitioner and its members to pursue their collective effort to

> foster beliefs which they admittedly have the right to advocate, in that it may induce members to withdraw from the Association and dissuade others from joining it because of fear of exposure of their beliefs shown through their associations and of the consequences of this exposure.

Id. at 462-63. To allow the government to obtain without a warrant information showing who a person communicates with and what websites he or she visits may reveal a person's associations and therefore intrude on a person's right to privacy in those associations.

¶31 In his partial dissent, Judge Espinosa allows that suppression of evidence of such First Amendment-protected activity obtained through government investigation of an IP address may be warranted. But were we to adopt his conclusion that, absent some unidentified Herculean effort to maintain anonymity, citizens abandon any claim to privacy in their internet activities, we would be hard-pressed to find a reasoned basis upon which to do so. Moreover, the privacy protections afforded by our constitutions are not limited to the exclusion of evidence in criminal proceedings; rather, they prohibit abusive governmental intrusions in the first place.

¶32 As to the concern that our reasoning would unduly impair legitimate law enforcement investigation of crimes like Mixton's, as noted in Judge Eckerstrom's dissent, police could have easily obtained a search warrant in this case.[9] Our courts have long recognized that such minimal burdens on law enforcement are justified in service of constitutional protections. *See, e.g., Riley*, 573 U.S. at 401 (impact of warrant requirement on ability to combat crime the cost of privacy). We see no reason to forgo the warrant requirement merely because one's private affairs are conducted online.[10]

---

[9]Judge Espinosa posits that there can be no expectation of privacy in circumstances such as these because of the ease with which one's identity can be ascertained from an IP address. But if such identification is so easy, why did police need to resort to subpoenas to identify Mixton? The record contains no evidence that he could be identified other than through his ISP.

[10]Nor are we persuaded the risk of ISP security breaches renders an expectation of privacy from government intrusion any less reasonable than do the prospects of burglary in the context of the home.

¶33 We are mindful our supreme court has expressed a reluctance to depart from Fourth Amendment precedent in analyzing suppression issues under article II, § 8. *See Bolt*, 142 Ariz. at 269 ("[E]ven though on occasion we may not agree with the parameters of the exclusionary rule as defined by the United States Supreme Court, we propose, so long as possible, to keep the Arizona exclusionary rule uniform with the federal."). But the federal third-party doctrine, at least as applied to obtain Mixton's identity here, is unsupportable in our view. We therefore decline to apply it on independent state law grounds. *See Long*, 463 U.S. at 1042 n.7. Because the search warrant in this case was issued based upon identifying information obtained in violation of Mixton's rights under article II, § 8, we turn to the issue of whether the evidence recovered in execution of the warrant should have been suppressed.

Good-Faith Exception

¶34 The purpose of the exclusionary rule is to deter unlawful police conduct. *See Illinois v. Krull*, 480 U.S. 340, 347 (1987). However, when law enforcement officers act with an objectively reasonable belief that their conduct was lawful, deterrence is unnecessary and the exclusionary rule does not apply. *State v. Valenzuela*, 239 Ariz. 299, ¶ 31 (2016). The good-faith exception to the exclusionary rule applies to violations of article II, § 8 as it does to violations of the Fourth Amendment. *See State v. Coats*, 165 Ariz. 154, 158 (App. 1990) (citing *Bolt*, 142 Ariz. at 269).

¶35 Although the identifying information in this case was obtained by an administrative subpoena rather than a search warrant, we agree with the state's contention that the good-faith exception set forth in *United States v. Leon*, 468 U.S. 897 (1984), applies here because the incriminating evidence obtained from Mixton's residence was ultimately obtained through execution of the warrant. And although Mixton argues the warrant was premised upon unlawfully obtained information, none of the exceptions recognized in *Leon* apply.[11] *See id.* at 923.

[11]As noted by the state, four situations preclude the application of the good-faith exception under *Leon*: (1) when a magistrate is misled by information the affiant knew was false or would have known was false but for reckless disregard for the truth; (2) when the magistrate wholly abandons his or her judicial role; (3) when the warrant affidavit is so lacking in indicia of probable cause to render belief in its existence entirely unreasonable; and (4) when a warrant is so facially deficient that executing officers cannot reasonably presume it to be valid. 468 U.S. at 923.

¶36 Other factors support our conclusion that the detective's reliance on the warrant issued by a neutral magistrate was objectively reasonable. First, the detective was aware federal agents obtained the identifying information using subpoena authority recognized by federal law. Second, every federal circuit court that has considered the issue has concluded, based upon United States Supreme Court precedent, that there is no expectation of privacy in one's identifying information given to an internet service provider.[12] And third, as noted above, no Arizona state appellate court has previously found such an expectation of privacy. Indeed, other than in situations involving physical intrusion into the home, *see Ault*, 150 Ariz. 459; *Bolt*, 142 Ariz. 260, the provisions of article II, § 8 have never expressly been held to afford greater protection than that afforded under the Fourth Amendment, *see State v. Jean*, 243 Ariz. 331, ¶ 45 (2018) (exception to exclusionary rule based upon objectively reasonable reliance on binding precedent under *Davis v. United States*, 564 U.S. 229 (2011), "requires good faith and reasonableness, not a crystal ball").

¶37 While no binding appellate precedent specifically authorized the warrantless search here under article II, § 8, a significant body of appellate law, some of it binding, supported the practice as a reasonable search. In the circumstances here, it was objectively reasonable for police to rely on that precedent. *See State v. Weakland*, 246 Ariz. 67, ¶ 9 (2019) (good-faith exception does not require that binding appellate precedent specifically authorize police practice at issue; objectively reasonable reliance on binding precedent suffices). This is simply not a situation in which there appear to be ongoing violations of defendants' privacy rights as a result of recurring or systemic negligence by police that could render the good-faith exception inapplicable. *See State v. Havatone*, 241 Ariz. 506, ¶ 21 (2017).

¶38 Finally, Arizona's statutory exceptions to the exclusionary rule weigh in favor of a finding of good faith. *See* A.R.S § 13-3925(B) (in suppression proceeding, "the proponent of the evidence may urge that the peace officer's conduct was taken in a reasonable, good faith belief that the conduct was proper" and the evidence should be admitted), (C) ("The trial court shall not suppress evidence that is otherwise admissible in a criminal

[12]The warrant in this case was issued before the Supreme Court decided *Carpenter*. And in any event, its narrow holding does not sufficiently call into question the continuing vitality of the lower federal court cases discussed above so as to render reliance on them unreasonable. *Carpenter*, 138 S. Ct. at 2220.

proceeding if the court determines that the evidence was seized by a peace officer as a result of a good faith mistake or technical violation.").

Disposition

¶39 Although the evidence used to convict Mixton was obtained in violation of his right to be free from government interference in his private affairs under article II, § 8 of the Arizona Constitution, the good-faith exception to the exclusionary rule applies. We therefore affirm his convictions and sentences.

E C K E R S T R O M, Judge, concurring in part, dissenting in part:

¶40 The majority opinion comprehensively explains why article II, § 8 of the Arizona Constitution requires the state to secure a warrant under the circumstances here. That opinion observes correctly that a person's actions on the internet may expose "intimate details of the subscriber's life," over which a person would have a reasonable, societally recognized expectation of privacy. The opinion aptly identifies the analytical limitations of the third-party doctrine in describing the boundaries of reasonable expectations of privacy in this contemporary context. Were we to find no violation of article II, § 8 under these facts, we would render the specific guarantee of the Arizona Constitution—that "[n]o person shall be disturbed in his private affairs . . . without authority of law"—an empty promise. I join fully in that section of the opinion. I write separately because I would hold that the Fourth Amendment to the United States Constitution provides the same protection.

¶41 As the majority observes, lower federal courts have consistently held that persons have no expectation of privacy in identifying information voluntarily conveyed to internet service providers. *See Weast*, 811 F.3d at 747-48; *Christie*, 624 F.3d at 573-74; *Perrine*, 518 F.3d at 1204. But my colleagues overlook that those cases pre-date, and have been overtaken by, the United States Supreme Court's reasoning in *Carpenter*, 138 S. Ct. 2206.

¶42 In *Carpenter,* the Court addressed whether the government may, without a warrant, track a person's movements by use of cell-site location information (CSLI). *Id.* at 2220. There, as here, the government argued that, because the defendant/subscriber had knowingly exposed that information to the cellular service provider, he retained no reasonable expectation of privacy in it. *Id.* at 2219. Chief Justice Roberts, writing for the majority, declined to apply the third-party doctrine when the government secures "a detailed and comprehensive record of the person's

movements" by capitalizing on that person's use of a technology that "is indispensable to participation in modern society." *Id.* at 2217, 2220. Although the majority specifically recognized that each new privacy domain created by evolving technology would require a discrete Fourth Amendment calculus, it lucidly articulated its criteria for weighing a defendant's privacy interests in those contexts. The Court's reasoning demonstrated that it would reject the third-party doctrine (1) when the societally recognized privacy interest is acute and (2) when the privacy domain cannot be accessed without the incidental disclosure of some private information to a third party. *Id*. at 2216-21.

¶43 That reasoning should be dispositive here. The privacy interest at stake is no less substantial. As the majority opinion explains, our actions on the internet expose our worries, fantasies, and political views at least as comprehensively as the sequence of our physical locations. Internet access has likewise become an integral part of participation in contemporary culture: it is a place we shop, converse with friends and romantic partners, seek information about medical conditions, and debate the issues of the day. And, as with cell-phone use, one cannot secure such access without exposing some private information to a vendor. *See Carpenter*, 138 S. Ct. at 2220 (questioning whether persons voluntarily "assume[] the risk" of exposing private actions under such circumstances (alteration in *Carpenter*) (quoting *Smith*, 442 U.S. at 745)).

¶44 In fact, our expectation of privacy in internet use is arguably greater than any similar expectation we hold for our physical movements in public. A visit to an internet site is presumptively anonymous unless we choose to make it otherwise;[13] our movements on public streets are presumptively visible to all we encounter. For this reason, the Court has required a warrant for the locational tracking of criminal suspects only

[13] As my dissenting colleague correctly observes, many people choose to use the internet for public activities, such as social media, wherein they consciously relinquish any expectation of privacy. But, as Judge Posner has explained, an expectation of privacy is not an expectation of total secrecy. Posner, *supra* ¶ 24, at 342. Rather, it is an expectation that a person has the power to selectively determine who may have access to a presumptively private domain. We do not waive our right of privacy in our homes simply because we occasionally choose to invite relatives, friends, or housekeepers to enter it. Similarly, we do not waive our right of privacy in all our internet activities simply because we choose to make some part of it public.

when that tracking is sufficiently protracted to reveal private features of their lives. *See, e.g.*, *id.* at 2220; *United States v. Jones,* 565 U.S. 400, 430 (2012). By contrast, each discrete internet visit may expose an acutely private thought process and may do so in a context where the visitor has taken every precaution to retain his anonymity. Surely, if the government is required to obtain a warrant to track, through technology, a suspect's public physical movements, it should likewise need a warrant to expose a suspect's private digital behavior.

¶45 For these reasons, I can identify no principled basis to distinguish the instant case from the Court's holding in *Carpenter*. The United States Supreme Court's precedents are binding on this court as to federal constitutional matters. I would therefore follow *Carpenter* and hold that the Fourth Amendment required the state to secure a warrant to acquire Mixton's identifying information from his internet provider.[14]

¶46 As Justice Roberts emphasized, the Court's application of the Fourth Amendment to evolving technologies involves no novel guiding principles. To the contrary, "it is informed by historical understandings" of "the privacies of life" in the founding era. *Carpenter*, 138 S. Ct. at 2214. As "technology has enhanced the Government's capacity to encroach upon areas normally guarded from inquisitive eyes," the Court has sought to protect those same privacies. *Id.*

¶47 Nothing about our opinion—which the majority bases exclusively on our state constitution and I would base on the Fourth

---

[14]I concur that the state's violation of Mixton's rights occurred in good faith. The Court did not issue *Carpenter* until June 2018, long after the search in question occurred. As the majority opinion correctly observes, all previous federal case law had applied the third-party doctrine to similar searches, finding no constitutional violation. Furthermore, until our opinion today, outside of the context of home searches, no previous Arizona court had held article II, § 8 of the Arizona Constitution to provide greater privacy rights than those enforced by the United States Constitution. *See State v. Hernandez*, 244 Ariz. 1, ¶ 23 (2018) ("Arizona Constitution's protections under article 2, section 8 are generally coextensive with Fourth Amendment analysis" except in context of law enforcement's warrantless physical entry into a home); *State v. Peltz*, 242 Ariz. 23, n.3 (App. 2017) ("[T]he right of privacy under article II, § 8 has not been expanded beyond that provided by the Fourth Amendment, except in cases involving unlawful, warrantless home entries.").

Amendment as well—should prevent our law enforcement agencies from enforcing the rule of law. Indeed, as new technologies become primary conduits of human behavior, our police have no choice but to effectively conduct law enforcement activities in those realms. We merely hold here that our officers need appropriate legal cause, confirmed by a neutral magistrate, to invade traditional privacies that persons now exercise in new domains.[15]

E S P I N O S A, Judge, concurring in part and dissenting in part:

¶48 I fully agree that no Fourth Amendment violation occurred on the facts of this case, and even if there had been, such would have been cured under both the federal and Arizona good-faith doctrines. I write separately, however, because I respectfully disagree with the majority's novel discovery of constitutional protection for internet subscriber information under the Arizona Constitution, particularly in this day and age of constant personal internet connection and dependency, where little, absent extraordinary measures, can confidently be deemed private and shielded.

¶49 In concluding that utilizing otherwise properly obtained third-party ISP subscriber information through a federally authorized subpoena now violates a societal expectation of privacy under article II, § 8 of the Arizona Constitution, my colleagues assert that "internet users generally enjoy—and expect—anonymity in their internet use," citing a 2008 New Jersey case, *Reid*, 945 A.2d 26. But I am not sure who on Earth, at least anyplace with the ubiquitous and pervasive internet use we enjoy in 2019, would still agree with this largely antiquated notion when so much of modern society is now internet-connected, cloud-dependent, and app-reliant for personal communications, all manner of commercial transactions, 24-7 entertainment, and universal positional tracking. Everyone utilizing cell phones, electronic tablets, laptop computers, smartwatches, and even modern automobiles, not to mention a host of other, less-mobile devices,[16] is subject to pervasive tracking "cookies,"

---

[15]The warrant requirement would have posed no impediment to the investigation of the instant case. Mixton's e-mail correspondence with the undercover officer, together with the attachment of child pornography to that correspondence, provided ample basis to secure a warrant for Mixton's personal identifying information.

[16]The popularity of the Internet of Things (IoT) is growing by leaps and bounds, with all manner of household devices and appliances utilizing

unseen meta-data in copiously shared photos and files, and constant geo-location. *See In re Nickelodeon Consumer Privacy Litig.*, 827 F.3d 262, 266, 269 (3d Cir. 2016) ("We browse the Internet, and the data-collecting infrastructure of the digital world hums along quietly in the background."); *see also Carpenter*, 138 S. Ct. at 2217 (cell phones create a "detailed and comprehensive record of [a] person's movements"). Much of the resulting information is, and should be, constitutionally protected, *see, e.g.*, *Carpenter*, 138 S. Ct. at 2217 (cell phone location data warrants constitutional protection),[17] but basic identifying information in the hands of third parties has never been deemed so under the U.S. Constitution, and for similar reasons should not be broadly shielded in Arizona, *see United States v. D'Andrea*, 497 F. Supp. 2d 117, 120 (D. Mass. 2007) ("[F]ederal courts [have] uniformly conclude[d] that internet users have no reasonable expectation of privacy in their subscriber information . . . and other noncontent data to which service providers must have access.").

¶50 While specific subscriber IP addresses are primarily in the possession of ISPs,[18] the underlying data is received by visited servers and

---

the same type of Internet Protocol (IP) addresses and subscriber information as involved in this case. *See* Swaroop Poudel, Note, *Internet of Things: Underlying Technologies, Interoperability, and Threats to Privacy and Security*, 31 Berkeley Tech. L. J. 997, 997, 1000, 1005, 1008 (2016) (providing definitions of IoT).

[17]Contrary to Judge Eckerstrom's concerns, it is important to keep in mind that only basic identifying information is at issue here. Police obtained neither Mixton's "public physical movements" as in *Carpenter*, nor his "internet visit[s]," but only the source and "street address" of the illicit material after obtaining the poster's IP address from a single internet site. Access 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.

[18] ISPs, however, like countless other repositories of individual consumer data, suffer breaches that result in the wholesale theft of private and confidential information, unlike the typical home burglary, with resulting dissemination (or sale) of that information. *See, e.g.*, Robert Hackett, *Verizon's Data Breach Fighter Gets Hit With, Well, a Data Breach*, Fortune (Mar. 24, 2016), http://fortune.com/2016/03/24/verizon-enterprise-data-breach/ (contact information of some 1.5 million Verizon customers stolen in data breach); Paige Leskin, *The 21 Scariest Data Breaches of 2018*, Bus. Insider (Dec. 30, 2018), https://www.businessinsider.com/data-hacks-breaches-biggest-of-

can be matched with identity information by many other third parties.[19] S*ee Weast*, 811 F.3d at 748 (IP addresses "widely and voluntarily disseminated in the course of normal use of networked devices"). Such third-party content-neutral information has been found not to warrant constitutional protection by every federal court that has considered the issue. *See Caira*, 833 F.3d at 806-07 (listing and summarizing numerous federal cases); *Perrine*, 518 F.3d at 1204-05 (same). This court too, in *Welch*, noted that IP addresses, universally assigned by third-party ISPs, are not subject to a reasonable expectation of privacy, in a salient comment the majority discounts as "dicta":

> Welch has provided no authority for the proposition that internet usage conducted through identifying markers—such as the user's unique IP address—preserve one's expectation of privacy. As Detective Barry testified, "every device that connects to the Internet is assigned an Internet protocol address" that internet providers—such as Cox Communications or Comcast—assign to their customers in order to identify them and verify their status as paying customers. Welch did not argue—either below or on appeal—that he had any expectation of confidentiality from such a provider, and we conclude that any alleged expectation of privacy would be unreasonable.

236 Ariz. 308, n.1. It is difficult to understand why such content-lacking identifying information should now be more shielded than, for example, personal telephone numbers and related information, which are not so protected, either federally or, presumably still, in Arizona. *See Forrester*, 512 F.3d at 510, 512 (computer surveillance can be "constitutionally

---

2018-2018-12; David McCandless et al., *World's Biggest Data Breaches & Hacks*, Information is Beautiful, https://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/ (last updated Apr. 1, 2019).

[19]Saul Hansell, *Google Says I.P. Addresses Aren't Personal*, N.Y. Times: Bits (Feb. 22, 2008), https://bits.blogs.nytimes.com/2008/02/22/google-says-ip-addresses-arent-personal/ (IP addresses alone not "personal information," but once user registers for any online service, IP address can be associated with user's identity and everything else the user does online).

indistinguishable" from the use of a telephone pen register that captures and records numbers dialed from individual phone lines); *see also State v. Ring*, 200 Ariz. 267, ¶ 18 (2001), *rev'd on other grounds*, 536 U.S. 584 (2002) (pen registers employed to gather evidence against defendant, but their effectiveness "limited, as they simply established that contacts were made without revealing the content of the communications").

¶51 In support of their holding, my colleagues refer 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. Indeed, such governmental prying might well warrant constitutional protection and suppression of any such evidence gained through investigating an IP address.[20] But these are red herrings; 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. The majority also cites cases relying on the First Amendment to the United States Constitution for its protection of freedom of speech. The criminally perverted "speech" in this case, however, clearly enjoys no such protection. *See New York v. Ferber*, 458 U.S. 747, 763 (1982) (child pornography "a category of material outside the protection of the First Amendment").

¶52 It is notable that, despite my colleagues' suggestion of a growing trend, today's decision joins what appears to be only one state court in the entire country that has found ISP subscriber information protected under its state constitution. That court did so, however, 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. *See Reid*, 945 A.2d at 32. The unprecedented and unnecessary impact in

[20] To fortify its conclusion, the majority miscasts my position as requiring citizens to "abandon any claim to privacy in their internet activities" to avoid "abusive governmental intrusions." But, as already noted, that dire specter invokes a far different factual scenario and issue, well beyond what occurred in this case. *See Velasco v. Mallory*, 5 Ariz. App. 406, 410-11 (1967) (opinions rendered should deal with specific facts at issue and not anticipate "troubles which do not exist" and imagined scenarios that "may never exist" in the future); *see also Golden v. Zwickler*, 394 U.S. 103, 108 (1969) (in adjudicating constitutional questions, "'concrete legal issues, presented in actual cases, not abstractions' are requisite" (quoting *United Pub. Workers of Am. (C.I.O.) v. Mitchell*, 330 U.S. 75, 89 (1947))).

Arizona, should this decision endure, may be a significant diminution of law enforcement's ability to efficiently and legitimately investigate serious crimes such as identity theft, cyberattacks, online espionage, theft of intellectual property, fraud, unlawful sale of drugs, human trafficking, and, of course, sexual exploitation of children, through the measured use of federally authorized third-party subpoenas. *See* 19 U.S.C. § 1509; *see also* 18 U.S.C. § 2703(c), (d).[21]

¶53 But there is another, equally important reason I refrain from joining the majority's novel interpretation of the Arizona Constitution. It is entirely unnecessary for the resolution of this appeal. As our supreme court has observed, "[W]e should resolve cases on non-constitutional grounds in all cases where it is possible and prudent to do so." *State v. Korzuch*, 186 Ariz. 190, 195 (1996); *see Fragoso v. Fell*, 210 Ariz. 427, ¶ 6 (App. 2005) (same); *see also Progressive Specialty Ins. Co. v. Farmers Ins. Co.*, 143 Ariz. 547, 548 (App. 1985) (appellate courts should not give advisory opinions or decide questions unnecessary to disposition of appeal). If ever there was an archetypical example of good-faith conduct by law enforcement officers, this one is it. I fully agree with my colleagues that there was no reason for the officers involved here to believe that their investigation was anything but proper, and no cause to anticipate that an unprecedented legal interpretation of article II, § 8 would find a routine and long accepted

[21] My colleagues posit that "police could have easily obtained a search warrant in this case." But that sidesteps the question of whether law enforcement should have to resort to such formal and burdensome means in the first place, particularly during the preliminary stages of an investigation. *See Fernandez v. California*, 571 U.S. 292, 306-07 (2014) ("Even with modern technological advances, the warrant procedure imposes burdens on the officers who wish to search [and] the magistrate who must review the warrant application."); *California v. Acevedo*, 500 U.S. 565, 586-87 (1991) (White, J., dissenting) ("Our decisions have always acknowledged that the warrant requirement imposes a burden on law enforcement."). Moreover, it is not necessarily a given that a neutral magistrate will always find sufficient probable cause to issue a search warrant based chiefly on the capture of an IP address. And that Mixton might have been identified through other means, while illustrating the very minimal privacy interest at hand, should not be a reason for undercutting prudent and well-established police procedures that do not infringe on constitutional rights. *Cf. Kyllo v. United States*, 533 U.S. 27, 35 n.2 (2001) (that police might have obtained evidence through other means not a factor in Fourth Amendment analysis).

investigative tool to be unlawful. The good-faith doctrine being dispositive, there is no reason to explore uncharted and unlikely territory within Arizona's state constitution.

¶54 In sum, the third-party identifying information at issue in this appeal is far too widely accessible to support a reasonable expectation of privacy. And even were it indeed time to expand the reach of article II, § 8 in this technological direction, the case at hand is not the one for it. Accordingly, I respectfully dissent from the majority's constitutional analysis in paragraphs 14-33, but join in the other sections of the opinion and its disposition of Mixton's appeal.