

IN THE
SUPREME COURT OF THE STATE OF ARIZONA

STATE OF ARIZONA,
Appellee,

v.

WILLIAM MIXTON,
Appellant.

No. CR-19-0276-PR
Filed January 11, 2021

Appeal from the Superior Court in Pima County
The Honorable Sean E. Brearcliffe, Judge
No. CR20162038-001

AFFIRMED

Opinion of the Court of Appeals, Division Two
247 Ariz. 212 (2019)

VACATED

COUNSEL:

Mark Brnovich, Arizona Attorney General, Brunn “Beau” W. Roysden III, Solicitor General, Joseph T. Maziarz, Chief Counsel, Criminal Appeals Section, Linley Wilson (argued), Deputy Solicitor General, Phoenix, Attorneys for State of Arizona

Joel Feinman, Pima County Public Defender, Abigail Jensen (argued), David J. Euchner, Deputy Public Defenders, Tucson, Attorneys for William Mixton

Timothy Sandefur, Scharf-Norton Center for Constitutional Litigation at the Goldwater Institute, Phoenix, Attorney for Amicus Curiae Goldwater Institute

Paul V. Avelar, Timothy D. Keller, Keith E. Diggs, Institute for Justice, Tempe, Attorneys for Amicus Curiae Institute for Justice

Elizabeth Burton Ortiz, Arizona Prosecuting Attorneys’ Advisory Council, Phoenix, Attorney for Amicus Curiae Arizona Prosecuting Attorneys’ Advisory Council

STATE v. MIXTON
Opinion of the Court

Jared G. Keenan, American Civil Liberties Union Foundation of Arizona, Phoenix, Attorney for Amici Curiae American Civil Liberties Union of Arizona, American Civil Liberties Union, and Electronic Frontier Foundation

JUSTICE LOPEZ authored the opinion of the Court, in which JUSTICES GOULD, BEENE, and MONTGOMERY joined. JUSTICE BOLICK, joined by CHIEF JUSTICE BRUTINEL and VICE CHIEF JUSTICE TIMMER, dissented.

JUSTICE LOPEZ, opinion of the Court:

¶1 We consider whether the Fourth Amendment to the United States Constitution or article 2, section 8 of the Arizona Constitution requires law enforcement officials to secure a judicially-authorized search warrant or order to obtain either (1) a user’s Internet Protocol (“IP”) address or (2) subscriber information the user voluntarily provides to an Internet Service Provider (“ISP”) as a condition or attribute of service. We hold that neither the federal nor the Arizona Constitution requires a search warrant or court order for such information and that law enforcement officials may obtain IP addresses and ISP subscriber information with a lawful federal administrative subpoena.

BACKGROUND

¶2 An ISP is a company that provides individuals with access to the internet. *United States v. Jean*, 207 F. Supp. 3d 920, 931 (W.D. Ark. 2016), *aff’d* 891 F.3d 712 (8th Cir. 2018). The ISP assigns a string of numbers, called an IP address, to a customer’s modem to facilitate access to the internet. *Id.* at 928. Consequently, a user does not control nor own an IP address. IP addresses are always attached, “like a ‘return address,’ to every ‘envelope’ of information exchanged back and forth by computers that are actively communicating with each other over the internet.” *Id.* at 928–29. When a computer accesses a website, the IP address tells the website where to transmit data. See Frederick Lah, Note, *Are IP Addresses “Personally Identifiable Information”?*, 4 I/S: J.L. & Pol’y for Info. Soc’y 681, 693 (2008). Search engines, such as Google, also log IP addresses of users and use these

STATE v. MIXTON
Opinion of the Court

logs to improve the quality of search results and advertisements for visitors. *Id.* at 693–94.

¶3 An IP address alone does not reveal an internet user’s identity. Rather, it generally reveals only a user’s approximate geographic location, such as a neighborhood, and the user’s ISP. Lincoln Spector, *Your IP address: Who can see it and what you can do about it*, PCWorld (Mar. 17, 2014, 7:15 AM), <https://www.pcworld.com/article/2105405/your-ip-address-who-can-see-it-and-what-you-can-do-about-it.html>. The ISP, however, maintains records and information, such as the name, address, and telephone number associated with an IP address, known as “subscriber information.” See Savanna L. Shuntich & Kenneth A. Vogel, *Doe Hunting: A How-to Guide for Uncovering John Doe Defendants in Anonymous Online Defamation Suits*, Md. B.J. 48, 51 (July/Aug. 2017).

¶4 Here, in 2016, an undercover Tucson Police Department detective posted an advertisement on an online forum seeking users interested in child pornography. The detective was contacted by someone with the username “tabooin520,” who asked to be added to a group chat on a messaging application called “Kik.” Once added, tabooin520 sent images and videos of child pornography to the group chat and to the detective.

¶5 Federal agents with Homeland Security Investigations (“HSI”), at the request of the detective, served a federal administrative subpoena authorized under federal law on Kik to obtain tabooin520’s IP address. Kik provided the IP address to the detective. The detective, using publicly available databases, determined that Cox Communications (“Cox”) was the ISP for the IP address. HSI agents then served another federal administrative subpoena on Cox for the subscriber information associated with the IP address.

¶6 Cox complied with the subpoena, disclosing the subscriber information—name, street address, and phone number—of William Mixton. The detective used this information to obtain and execute a search warrant on Mixton’s residence. Detectives seized a cell phone, an external hard drive, a laptop, and a desktop computer. A subsequent search of these devices revealed photos and videos of child pornography, as well as the messages, photos, and videos that Mixton, under the username “tabooin520,” sent to the detective.

STATE v. MIXTON
Opinion of the Court

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

¶8 In a split decision, the court of appeals affirmed Mixton's convictions and sentences, holding that although Mixton lacked a reasonable expectation of privacy under the Fourth Amendment, *State v. Mixton*, 247 Ariz. 212, 220 ¶ 13 (App. 2019), the Arizona Constitution required a search warrant to obtain his ISP subscriber information, *id.* at 225 ¶ 27, and the federal third-party doctrine did not apply to the Arizona Constitution, *id.* at 227 ¶ 33. The court concluded that, although the State obtained Mixton's ISP subscriber information in violation of the Arizona Constitution, suppression of the information was unnecessary because the good-faith exception to the exclusionary rule applied, as no precedent prohibited the search, controlling law deemed the search reasonable, and law enforcement reasonably relied on existing precedent. *Id.* at 228 ¶ 39.

¶9 On review in this Court, the State argues that article 2, section 8 of the Arizona Constitution does not require a search warrant or court order to obtain IP addresses and ISP subscriber information. Mixton disagrees and further contends that the Fourth Amendment protects IP addresses and ISP subscriber information in light of *Carpenter v. United States*, 138 S. Ct. 2206 (2018).

¶10 We granted review to consider whether the United States or Arizona Constitution requires a search warrant or court order to obtain IP addresses and ISP subscriber information, a recurring issue of statewide importance. We have jurisdiction under article 6, section 5(3) of the Arizona Constitution and A.R.S. § 12-120.24.

DISCUSSION

¶11 Whether the United States or Arizona Constitution requires a search warrant or court order to obtain an IP address and ISP subscriber information involves the interpretation of constitutional provisions, a matter we review de novo. *See State v. Hegyi*, 242 Ariz. 415, 416 ¶ 7 (2017).

STATE v. MIXTON
Opinion of the Court

I.

¶12 We consider first whether, in light of *Carpenter*, the United States Constitution requires a search warrant or court order to obtain an IP address and ISP subscriber information.

A.

¶13 The Fourth Amendment protects “[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures.” The Fourth Amendment was designed to protect individuals against “arbitrary invasions by governmental officials.” *Carpenter*, 138 S. Ct. at 2213 (quoting *Camara v. San Francisco*, 387 U.S. 523, 528 (1967)). Traditionally, the Supreme Court viewed search and seizure under the Fourth Amendment through a lens of “common-law trespass.” *See United States v. Jones*, 565 U.S. 400, 405 (2012). However, the Court has recognized that the Fourth Amendment protects people, not just places, when an individual “seeks to preserve something as private” and that expectation is “one that society is prepared to recognize as reasonable.” *Carpenter*, 138 S. Ct. at 2213 (quoting *Smith v. Maryland*, 442 U.S. 735, 740 (1979)). “A ‘search’ occurs when an expectation of privacy that society is prepared to consider reasonable is infringed.” *United States v. Jacobsen*, 466 U.S. 109, 113 (1984).

B.

¶14 Federal appellate courts held uniformly, before *Carpenter*, that the Fourth Amendment does not protect IP addresses and ISP subscriber information because such information falls within the exception created by the “third-party doctrine.” *See, e.g., United States v. Bynum*, 604 F.3d 161, 164 (4th Cir. 2010) (noting that every federal court considering this issue has held that subscriber information provided to an internet provider is not protected by the Fourth Amendment); *United States v. Perrine*, 518 F.3d 1196, 1204–05 (10th Cir. 2008) (collecting cases that hold the Fourth Amendment’s privacy expectation does not apply to IP addresses and ISP subscriber information); *United States v. Forrester*, 512 F.3d 500, 510 (9th Cir. 2008) (holding that IP addresses and ISP subscriber information are not protected by the Fourth Amendment). The third-party doctrine is premised on the concept of privacy. Specifically, the doctrine is an analytical construct used to differentiate between information a person seeks to preserve as private, and information that, because he shares it with others, is not treated as

STATE v. MIXTON
Opinion of the Court

private. Using this construct, a person has no expectation of privacy in information he voluntarily discloses to third parties, even if there is an assumption it will be used only for a limited purpose. *Carpenter*, 138 S. Ct. at 2216. And, because it is no longer private, the government may obtain such information from a third party without triggering the Fourth Amendment's protections. *Id.*

¶15 The third-party doctrine traces its roots to *United States v. Miller*, 425 U.S. 435 (1976), and *Smith v. Maryland*, 442 U.S. 735 (1979). In *Miller*, the government subpoenaed a defendant's bank for records, including the defendant's checks, deposit slips, and statements. 425 U.S. at 437–38. The Supreme Court held that those documents were business records of the bank; thus, the defendant had no privacy interest in them. *Id.* at 440.

¶16 In *Smith*, the Supreme Court held that a defendant did not have “a legitimate expectation of privacy regarding the numbers he dialed on his phone.” 442 U.S. at 742 (internal quotation marks omitted). The Court emphasized that customers knew they were conveying phone numbers to the telephone company and that the company could keep records of those phone calls. *Id.* It also reasoned that recording the numbers a customer dials does not convey the *contents* of the communication, thus distinguishing *Katz v. United States*, 389 U.S. 347 (1967), which held that the warrantless monitoring of telephone conversations from a public telephone booth violated the Fourth Amendment. *Smith*, 442 U.S. at 741.

¶17 Thus, “*Smith* and *Miller* . . . did not rely solely on the act of sharing [information]. Instead, they considered ‘the nature of the particular documents sought’ to determine whether ‘there is a legitimate “expectation of privacy” concerning their contents.’” *Carpenter*, 138 S. Ct. at 2219 (quoting *Miller*, 425 U.S. at 442). The Ninth Circuit has aptly described the de minimis privacy interests implicated in the non-content information generated by an IP address:

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

STATE v. MIXTON
Opinion of the Court

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. Like IP addresses, certain phone numbers may strongly indicate the underlying contents of the communication; for example, the government would know that a person who dialed the phone number of a chemicals company or a gun shop was likely seeking information about chemicals or firearms. Further, when an individual dials a pre-recorded information or subject-specific line, such as sports scores, lottery results or phone sex lines, the phone number may even show that the caller had access to specific content information. Nonetheless, the Court in *Smith* and *Katz* drew a clear line between unprotected addressing information and protected content information that the government did not cross here.

Forrester, 512 F.3d at 510.

¶18 As with bank records and dialed telephone numbers, an internet user voluntarily provides subscriber information and IP addresses to third-party ISPs and servers. Subscriber information and IP addresses also do not reveal the substance or content of the internet user's communication any more than the information affixed to the exterior of a mailed item. *See* Shuntich & Vogel, *supra* ¶ 3, at 51 (noting that 18 U.S.C. § 2701 et seq. prohibits companies from disclosing “contents of a communication,” but they may turn over non-content information like IP addresses, phone numbers, and physical addresses in response to a subpoena); *cf. Forrester*, 512 F.3d at 511 (“In a line of cases dating back to the nineteenth century, the Supreme Court has held that the government cannot engage in a warrantless search of the contents of sealed mail, but can observe whatever information people put on the outside of mail, because that information is voluntarily transmitted to third parties.”).

C.

¶19 In *Carpenter*, decided nearly 40 years after *Smith*, officers accessed cellphone data, commonly known as cell-site location information (“CSLI”), to reveal a suspect's movements over the course of 127 days. 138 S. Ct. at 2217. CSLI is generated by a cellphone whenever it receives a text,

STATE v. MIXTON
Opinion of the Court

email, call, or when an app seeks to refresh data. *Id.* at 2220. As a result, CSLI is generated continuously without a user’s affirmative act. The Court described CSLI evidence as “detailed, encyclopedic, and effortlessly compiled,” *id.* at 2216, and noted that it “tracks nearly exactly the movements of its owner,” allowing the government to achieve “near perfect surveillance, as if it had attached an ankle monitor to the phone’s user,” *id.* at 2218. Concerned that CSLI could be used to continuously and effortlessly surveil cell phone users, the Court created a “narrow” exception to the third-party doctrine, requiring the government to obtain a search warrant for CSLI. *Id.* at 2220. The Court emphasized that a “detailed chronicle of a person’s physical presence compiled every day, every moment, over several years” implicated privacy concerns far exceeding those in *Smith and Miller*. *Id.*

¶20 Following *Carpenter*, every federal appellate court addressing the issue has affirmed that the Fourth Amendment’s warrant requirement does not reach IP addresses and ISP subscriber information. *See, e.g., United States v. Hood*, 920 F.3d 87, 92 (1st Cir. 2019) (holding that IP addresses are subject to the third-party doctrine and fall outside the scope of *Carpenter*); *United States v. Contreras*, 905 F.3d 853, 857 (5th Cir. 2018) (ruling that, post-*Carpenter*, ISP subscriber information “falls comfortably within the scope of the third-party doctrine”); *see also United States v. Wellbeloved-Stone*, 777 F. App’x 605, 607 (4th Cir. 2019) (declining to revisit *Bynum*’s holding that subscriber information was not protected by the Fourth Amendment in light of *Carpenter*); *United States v. VanDyck*, 776 F. App’x 495, 496 (9th Cir. 2019) (declining to revisit *Forrester*’s holding that IP addresses and ISP subscriber information are not protected by the Fourth Amendment in light of *Carpenter*).

¶21 Although this Court is not bound by federal appellate courts’ interpretations of federal constitutional provisions, *see State v. Montano*, 206 Ariz. 296, 297 ¶1 n.1 (2003), we may embrace them to “further predictability and stability of the law.” *See Weatherford ex rel. Michael L. v. State*, 206 Ariz. 529, 533 ¶ 9 (2003). Here, because the federal appellate courts’ jurisprudence is uniform and sound, we decline to depart from it.

D.

¶22 Despite federal appellate courts’ refusal to extend *Carpenter*’s exception to the third-party doctrine to IP addresses and ISP subscriber

STATE v. MIXTON
Opinion of the Court

information, the court of appeals' dissent and Mixton argue that this information *should* fall within *Carpenter's* exception. *Mixton*, 247 Ariz. at 228–29 ¶¶ 42–43 (Eckerstrom, J., dissenting in part). We disagree. Both stretch *Carpenter* beyond its jurisprudential reach.

¶23 First, *Carpenter* expressly preserved the third-party doctrine's existing application to information, such as cell phone and bank records, that is shared with a third party. See 138 S. Ct. at 2216–17, 2220 (“We do not disturb the application of *Smith* and *Miller*.”). It is beyond contention that IP addresses and ISP subscriber information fit this description. Second, the nature of an IP address and ISP subscriber information is fundamentally different from CSLI's perpetual surveillance attributes. “IP addresses . . . are widely and voluntarily disseminated in the course of normal use of networked devices,” *United States v. Weast*, 811 F.3d 743, 748 (5th Cir. 2016), reveal only the approximate geographical location of a subscriber, *supra* ¶ 3, and do not divulge the content of a user's communication, *supra* ¶¶ 17–18. ISP subscriber information includes only data the subscriber voluntarily provides the ISP—typically the subscriber's name, address, and phone number. Third, although internet activity may be akin to cell phone use in its centrality to participation in a modern society, CSLI is generated without an affirmative act by cell phone users and can be avoided only by ceasing cell phone use entirely, whereas internet users retain a measure of autonomy in masking their online activities. For example, users can anonymously access the internet via public and private services, such as public libraries and public WiFi networks at private businesses, or mask their online movements through proxy services like virtual private networks (“VPN”). See Shuntich & Vogel, *supra* ¶ 3, at 51. Thus, the IP address may not trace back to the user if he uses a third-party network. See *Hood*, 920 F.3d at 89 (describing a suspect's use of a hotel's Wi-Fi network to access a messaging app).

¶24 We also reject Mixton's request that we recognize a novel Fourth Amendment protection to avert the government's theoretical derivative use of IP addresses to trace internet users' browsing history. Mixton's sole source for this claim is a 2013 report by the Office of the Privacy Commissioner of Canada, which asserts that an IP address's internet history can be discovered by using the address as a search term in Google and other public search engines. Off. of the Priv. Comm'r of Can., *What an IP Address Can Reveal About You* (May 2013),

STATE v. MIXTON
Opinion of the Court

https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2013/ip_201305/.

¶25 Mixton’s claim is a thin reed upon which to rest a radical departure from unanimous federal Fourth Amendment jurisprudence concerning the lack of a privacy interest in an IP address. First, the study appears premised on the unproven assumption that an IP address search accurately and exhaustively identifies websites visited by a user. Second, it is not apparent that the report’s results have been replicated, and we are unaware of any other authority that supports the report’s claim that an IP address’s exhaustive search history is publicly accessible. See *Product Privacy Notice – VPN Products*, Pango, <https://www.pango.co/privacy/vpn-products/#:~:text=Our%20VPN%20products%20do%20not%20log%20or%20otherwise%20record%20IP,accessed%20through%20a%20VPN%20connection> (last visited Jan. 05, 2020) (explaining that an IP address only reveals a user’s ISP and geographical identifiers). In fact, during argument, counsel for Mixton conceded that, with respect to such Google searches, she did not “know specifically how much information [IP addresses] reveal.” Third, even if an IP address could be used to peruse a user’s search history with a public search engine, any assertion of privacy is even more attenuated because a website would have to deliberately publicize its visitors’ IP addresses to reveal a user’s browser history. See Joshua J. McIntyre, *Balancing Expectations of Online Privacy: Why Internet Protocol (IP) Addresses Should Be Protected As Personally Identifiable Information*, 60 DePaul L. Rev. 895, 896 (2011) (explaining that IP addresses are logged by a visited website); Ron A. Dolin, J.D., Ph.D., *Search Query Privacy: The Problem of Anonymization*, 2 Hastings Sci. & Tech. L.J. 137, 160–61 (2010) (asserting that IP addresses disclosed to a search engine may become the intellectual property of the search engine); Wikipedia, *Welcome unregistered editing*, https://en.wikipedia.org/wiki/Wikipedia:Welcome_unregistered_editing (last visited Jan. 05, 2020) (explaining that Wikipedia records and publicizes the IP addresses of users who edit a page without logging into an account); Zach Lerner, *A Warrant to Hack: An Analysis of the Proposed Amendments to Rule 41 of the Federal Rules of Criminal Procedure*, 18 Yale J.L. & Tech. 26, 64 (2016) (“The collection of a user’s IP address is less harmful to that user than the collection of his or her browsing history, email content, or other, more personal information.”). Finally, there is no allegation in this case that the State made derivative use of Mixton’s IP address. Instead, the sole issue before us is the constitutionality of the

STATE v. MIXTON
Opinion of the Court

State's use of a federal administrative subpoena to obtain an IP address and ISP subscriber information, which is the only relevant authority the federal statute confers.

¶26 In sum, *Carpenter* expressly preserves existing applications of *Smith* and *Miller* and its logic does not extend its exception to the third-party doctrine for CSLI information to IP addresses and ISP subscriber information. Such information does not implicate the privacy interests embodied in the de facto omnipresent surveillance generated by "detailed, encyclopedic" CSLI information. *Carpenter*, 138 S. Ct. at 2217. Therefore, we hold that—just as every federal court has held—the Fourth Amendment does not, in light of *Carpenter*, require a search warrant to obtain IP addresses and ISP subscriber information.

II.

¶27 We turn next to Mixton's contention that the Arizona Constitution, article 2, section 8, requires the State to obtain a warrant or court order to acquire his IP address or ISP subscriber information.

A.

¶28 Our primary purpose when interpreting the Arizona Constitution is to "effectuate the intent of those who framed the provision." *Jett v. City of Tucson*, 180 Ariz. 115, 119 (1994). "When the language of a provision is clear and unambiguous, we apply it without resorting to other means of constitutional construction." *Heath v. Kiger*, 217 Ariz. 492, 494 ¶ 6 (2008). We may examine its history, if necessary, to determine the framers' intent. *Boswell v. Phx. Newspapers, Inc.*, 152 Ariz. 9, 12 (1986).

¶29 The Arizona Constitution provides that "[n]o person shall be disturbed in his private affairs, or his home invaded, without authority of law." Ariz. Const. art. 2, § 8. This section, entitled "Right to Privacy" and often referred to as the "Private Affairs Clause," was adopted verbatim from the Washington State Constitution. See Wash. Const. art. 1, § 7. Passage of Arizona's Private Affairs Clause preceded the Fourteenth Amendment's incorporation of the Fourth Amendment, see John Leshy, *The Making of the Arizona Constitution*, 20 Ariz. St. L.J. 1, 81 (1988), but it "is of the same general effect and purpose as the Fourth Amendment to the Constitution of the United States." *Turley v. State*, 48 Ariz. 61, 70 (1936).

STATE v. MIXTON
Opinion of the Court

¶30 As an analytical starting point, we compare the texts of Arizona’s Constitution and the relevant federal amendments to determine whether Arizona’s Constitution provides greater protections than its federal counterpart. *See, e.g., Brush & Nib Studio, LC v. City of Phoenix*, 247 Ariz. 269, 281 ¶ 45 (2019) (comparing the language in the First Amendment and article 2, section 6 of the Arizona Constitution). We have observed that “[t]he Arizona Constitution is even more explicit than its federal counterpart in safeguarding the fundamental liberty of Arizona citizens.” *State v. Ault*, 150 Ariz. 459, 463 (1986). The Fourth Amendment protects a finite index of enumerated items — “persons, houses, papers, and effects” — whereas the Private Affairs Clause, by its terms, encompasses the seemingly more expansive realm of “private affairs.” *Compare* U.S. Const. amend. IV *with* Ariz. Const. art. 2, § 8.

¶31 We have noted since statehood that “[s]ection 8, article 2, of the state Constitution . . . , although different in its language, 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). *See also State v. Pelosi*, 68 Ariz. 51, 57 (1948) (noting that the Private Affairs Clause “was adopted for the purpose of preserving the rights which the Fourth Amendment to the Federal Constitution was intended to protect”), *overruled on other grounds by State v. Pina*, 94 Ariz. 243 (1963). “We have the right, however, to give such construction to 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*, 48 Ariz. at 70-71.

¶32 Indeed, we have recognized that the Private Affairs Clause provides broader protections to the home than the Fourth Amendment. *Ault*, 150 Ariz. at 463. But we have also recognized the value in uniformity with federal law when interpreting and applying the Arizona Constitution. *See State v. Casey*, 205 Ariz. 359, 362 ¶ 11 (2003) (superseded by statute, A.R.S. § 13-205(A)) (“Although 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.”). To that end, we have held that the exclusionary rule, for example, as a matter of state law is “no broader than the federal rule.” *State v. Bolt*, 142 Ariz. 260, 269 (1984) (“It is poor judicial policy for rules

STATE v. MIXTON
Opinion of the Court

governing the suppression of evidence to differ depending upon whether the defendant is arrested by federal or state officers.”). Notably, we have yet to expand the Private Affairs Clause’s protections beyond the Fourth Amendment’s reach, except in cases involving warrantless home entries. *State v. Peltz*, 242 Ariz. 23, 30 ¶ 24 n.3 (App. 2017).

B.

¶33 “Private affairs” is not defined in the Arizona Constitution. When the Arizona Constitution does not define its terms, we “look to their ‘natural, obvious, and ordinary meaning,’” *Kotterman v. Killian*, 193 Ariz. 273, 284 ¶ 33 (1999) (quoting *Cnty. of Apache v. Sw. Lumber Mills, Inc.*, 92 Ariz. 323, 327 (1962)), and our focus is on their meaning at the time the Constitution was adopted. See Antonin Scalia & Bryan A. Garner, *Reading Law: The Interpretation of Legal Texts* 78 (2012) (“Words must be given the meaning they had when the text was adopted.”). “Private” is defined as “affecting or belonging to private individuals, as distinct from the public generally.” *Private*, Black’s Law Dictionary (2d. ed. 1910); see also *Private*, New Websterian Dictionary (1912) (“peculiar to one’s self; personal; alone; secret; not public; secluded; unofficial”). “Affairs” is defined as “a person’s concerns in trade or property; business.” *Affairs*, Black’s Law Dictionary (2d. ed. 1910). Thus, because “private affairs” is an ambiguous concept that eludes precise demarcation, it is subject to differing interpretations. Therefore, to discern its meaning, we may consider the context of the provision, “the language used, the subject matter, its historical background, its effects and consequences, and its spirit and purpose.” *Wyatt v. Wehmuller*, 167 Ariz. 281, 284 (1991).

¶34 To discern the meaning of the Private Affairs Clause, we consider the history of its passage. *Boswell*, 152 Ariz. at 12–13. “Arizona’s right to privacy 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 Inc.*, 190 Ariz. 272, 277 (App. 1997) (considering the Arizona constitutional convention record in holding that article 2, section 8 does not restrict a private individual’s actions). The most consequential reference to article 2, section 8, arose in the context of a discussion of article 14, section 16, which requires the “records, books and files” of most types of public corporations to be subject to the “full visitorial and inquisitorial powers of the state.” See *Leshy*, *supra* ¶ 29, at 86–87. Delegates argued in favor of article 14, section 16, because “corporations

STATE v. MIXTON
Opinion of the Court

were ‘persons’ and thus protected by the privacy provisions of the Declaration of Rights in article II,” and the provision was necessary to facilitate regulatory oversight of corporations. *Id.* at 87. To the extent this reference may implicitly support the proposition that the Private Affairs Clause shields a corporation from the state’s sweeping legislative authority to examine all of its records for regulatory purposes as envisioned under article 14, section 16, it does not illuminate whether a federal administrative subpoena seeking non-content information from a third-party corporation to advance a criminal investigation of a subscriber runs afoul of the Arizona Constitution. And although the constitutional convention record is silent on the intent of the Private Affairs Clause, it details several delegates’ objections to extending state constitutional protections in other contexts beyond those recognized under the federal Constitution at the time. *See, e.g., id.* at 84–85 (discussing an amendment which would have suppressed evidence obtained from prisoners “under the ‘third degree’” or by torture, and the convention’s rejection of a proposal to ban the death penalty).

¶35 Mixton and Amici argue that the Arizona constitutional convention’s deliberations support the view that the Private Affairs Clause protects IP addresses and ISP subscriber information. Amicus Goldwater Institute and the dissent advance the argument that Arizona adopted the provision to shield businesses and individuals from growing government demands to investigate their financial dealings. *See* Timothy Sandefur, *The Arizona “Private Affairs” Clause*, 51 *Ariz. St. L.J.* 723, 731 (2019) (highlighting historical editorial complaints from the *Arizona Republican* against legislative investigations); *infra* ¶ 108. But, as noted, the constitutional convention record is devoid of affirmative evidence of this sentiment. Further, the dissent’s reliance on contemporaneous editorial comments made to the *Arizona Republican* sheds no light on this issue, because those complaints centered on the dangers of sweeping *legislative* investigations involving unfettered state access to a corporation’s business records for political or nefarious purposes. *Id.* In short, notably absent from the records of the constitutional convention is any objection to state use of a subpoena to obtain a business record to facilitate a legitimate criminal investigation of a corporate customer.

¶36 Having failed to identify relevant support for its position in the Arizona constitutional convention archives or contemporaneous writings from the local paper of record, the dissent asserts the federal third-party doctrine and its underlying logic are irreconcilable with the Arizona

STATE v. MIXTON
Opinion of the Court

Constitution because “‘private affairs’ were understood in the early Twentieth Century to broadly encompass both personal and business matters, even if transmitted through third parties.” *Infra* ¶¶ 100, 107. But the dissent’s examples – telegraphs, census data, tax returns, and the like – concern the propriety of public disclosure of the content of communications or sensitive information gathered by the government. *Infra* ¶ 106. The legal protections afforded the contents of telegraphs or detailed personal census or tax information collected by the government do not inform whether non-content IP address or ISP information is a “private affair” under the Arizona Constitution.

¶37 The dissent also cites to *Boyd v. United States*, 116 U.S. 616 (1886), and *Ex parte Jackson*, 96 U.S. 727 (1877), in support of its claim that, at the time of Arizona statehood, the Private Affairs Clause was widely understood to include business transactions “even within Fourth Amendment jurisprudence at the turn of the century.” *Infra* ¶ 109. But *Boyd* is distinguishable because it merely held that the Fourth and Fifth Amendments foreclose the government from compelling a defendant business owner in a criminal and forfeiture case, without a warrant, to produce at trial self-incriminating business records. 116 U.S. at 620–22. And *Jackson* simply establishes the unremarkable proposition that opening and reading the contents of sealed mail requires a warrant. 96 U.S. at 733. *Boyd* and *Jackson* fail to illuminate what convention delegates may have thought about an entirely different constitutional proposition – the propriety of the state’s use of an administrative subpoena for corporate records to advance a criminal investigation against a customer who does not own or control the records.

¶38 Significantly, even assuming the Private Affairs Clause protects private information unrelated to business dealings, nothing in the record supports the proposition that the Arizona Constitution prohibits the state from obtaining an IP address and ISP information from a third-party provider, via federal subpoena, to advance a criminal investigation. If anything, the text of article 14, section 16, and the discussion preceding its passage, militate in favor of state access to certain corporate records held by third parties to aid criminal investigations. Accordingly, Arizona’s constitutional convention record does not support the conclusion that the Private Affairs Clause protects such information and, thus, forecloses the State’s warrantless access to it.

STATE v. MIXTON
Opinion of the Court

C.

¶39 We next address the applicability of the “reasonable expectation of privacy” analysis to our delineation of the scope of the Private Affairs Clause’s protections.

¶40 The dissent urges that we avoid any inquiry of the reasonableness of our citizens’ expectation of privacy in discerning the meaning of “private affairs.” *Infra* ¶127. But the very concept of “privacy” is difficult to reconcile with persons who transmit information to third parties, such as corporate entities, who are free to collect, maintain, and make collateral commercial use of it. Consequently, any definition of “privacy” must logically entail consideration of the nature of the information, and whether and how it is shared with others. Additionally, it must necessarily include an assessment of the reasonableness of an asserted privacy interest to determine whether it is, in fact, private.

¶41 Our consideration of the reasonable expectation of privacy analysis, or at least its inherent logic in defining the scope of the Private Affairs Clause, is not novel, and the dissent ignores or discounts our long-standing approach to article 2, section 8. We do not discern the scope of the Private Affairs Clause in a vacuum, but rather we apply the “reasonable expectation of privacy test” to determine its protections. *See, e.g., Mazen v. Seidel*, 189 Ariz. 195, 198–200 (1997) (holding that a homeowner forfeits any reasonable expectation of privacy once firefighters enter his house); *Ault*, 150 Ariz. at 463 (“It is clear that the Fourth Amendment . . . and article 2, section 8 of the Arizona Constitution proscribe unreasonable search and seizure by the state.”); *State v. Juarez*, 203 Ariz. 441, 445 ¶ 16 (App. 2002) (“Arizona courts have consistently applied the Fourth Amendment’s ‘legitimate expectation of privacy’ requirement when determining unlawful search or seizure claims made pursuant to Article 2, Section 8.”). Thus, the Private Affairs Clause protects a privacy interest in an IP address and ISP subscriber information only if society is prepared to accept such an expectation of privacy as reasonable, *see Mazen*, 189 Ariz. at 198–200; *Juarez*, 203 Ariz. at 445 ¶ 16, or, stated differently, if the nature and use of the information is consistent with what is reasonably conceived as being private.

¶42 Mixton and the court of appeals contend that internet users are entitled to a reasonable expectation of privacy in all internet activity.

STATE v. MIXTON
Opinion of the Court

But the technological reality belies this claim. Indeed, the websites themselves are public, and are locatable through public search engines. Moreover, third parties often engage in pervasive and prolific derivative disclosure and sharing of internet users' online activity. For example, "[i]nternet activity tracking is used frequently by online advertising networks to create target[ed] advertisements based on users' individual preferences by tracking the user in a variety of ways." Alicia Shelton, *A Reasonable Expectation of Privacy Online "Do Not Track" Legislation*, 45 U. Balt. L.F. 35, 41 (2014). In fact, third-party advertisement networks often share browsing information from multiple websites to build profiles on users. See *id.* ("Suddenly the ad network knows not just technical details of a browser, but potentially very personal information about its user."). An investigation of third-party collection and use of internet users' activity revealed that numerous companies track online activity through the top 100 visited websites. Andrew Coats, *Top 100 Websites: How They Track Your Every Move Online*, Digital Trends (Aug. 30, 2012), <http://www.digitaltrends.com/web/top-100-websites-how-are-they-tracking-you/>.

¶43 Website operators also collect data on, and analyze, internet users' activities. For example, websites can use "browser fingerprinting" programs to gather "innocuous bits of information, such as a browser's version number, plug-ins, operating system, and language, [so that] websites can uniquely identify ('fingerprint') a browser and, by proxy, its user." Omer Tene & Jules Polonetsky, *To Track or "Do Not Track": Advancing Transparency and Individual Control in Online Behavioral Advertising*, 13 Minn. J.L. Sci. & Tech. 281, 294-95 (2012); see also DuckDuckGo, *Privacy Mythbusting #4: I can't be identified just by browsing a website. (If only!)* (July 11, 2017), <https://spreadprivacy.com/browser-fingerprinting/>. Apps and other programs on mobile devices can also be used to "track users across websites." See Tene & Polonetsky, *supra*, at 296; Thomas Brewster, *Exclusive: Warning Over Chinese Mobile Giant Xiaomi Recording Millions of People's 'Private' Web and Phone Use*, Forbes (Apr. 30, 2020, 09:25 AM), <https://www.forbes.com/sites/thomasbrewster/2020/04/30/exclusive-warning-over-chinese-mobile-giant-xiaomi-recording-millions-of-peoples-private-web-and-phone-use/#75527f831b2a>. Websites also often employ "cookies" that allow them to track internet users' browsing habits. *In re Nickelodeon Consumer Privacy Litig.*, 827 F.3d 262, 268 (3d Cir. 2016).

STATE v. MIXTON
Opinion of the Court

¶44 In sum, in this age of information sharing and inter-connectivity, “[m]ost of us understand that what we do on the [i]nternet is not completely private.” *Id.* at 266 (noting that our personal data “feed[s] an entire system of trackers, cookies, and algorithms designed to capture and monetize the information we generate”). Our “ubiquitous and pervasive internet use” that is “internet-connected, cloud-dependent, and app-reliant for personal communications, all manner of commercial transactions, 24-7 entertainment, and universal positional tracking,” makes it hard to believe that anyone still retains “this largely antiquated notion” of “anonymity in their internet use.” *Mixton*, 247 Ariz. at 230 ¶ 49 (Espinosa, J., dissenting in part). Whether internet users are troubled with this degree of data collection and sharing is beyond the purview of our authority. It is the legislature’s prerogative to proscribe or curtail use of such data. However, given third-parties’ widespread and pervasive collection, analysis, and sharing of detailed internet activity, including website visitation, we are unpersuaded that Mixton held a reasonable expectation of privacy in his IP address and ISP subscriber information. Consequently, as here, when a person discloses non-content information to a third party, even under the earnest but misguided belief that the third-party will safeguard the information, such information sharing is fundamentally inconsistent with any notion of privacy and he forfeits a reasonable expectation of privacy in that information. *See Carpenter*, 138 S. Ct. at 2216.

¶45 The dissent asserts that the reasonable expectation inquiry provides an “amorphous standard” that is absent in our constitutional text. Specifically, the dissent claims that this framework “replaces an objective state constitutional command with a subjective standard whose meaning changes over time to reflect an evolving societal consensus.” In so claiming, the dissent dismisses the relevance of court decisions to the inquiry. *Infra* ¶ 111.

¶46 The dissent overlooks the obvious. The text of the Private Affairs Clause does not define the meaning of “private affairs,” nor does the history of its passage delineate the scope of its application. Thus, its text does not command, objectively or otherwise, the standard by which we determine its reach. We merely follow this Court’s longstanding approach in applying the reasonable expectation analysis to determine how to apply the Private Affairs Clause, and the central inquiry remains whether an asserted interest is private. *See supra* ¶ 41. The dissent’s invocation of “an

STATE v. MIXTON
Opinion of the Court

objective state constitutional command” does nothing to inform the inquiry.

¶47 The unanimous federal court authority, *supra* ¶ 20, and the clear consensus of state courts, *infra* ¶ 64, finding no privacy interest in IP addresses and ISP subscriber information, have affirmed their respective jurisdiction’s popular consensus on this point as reflected in their laws permitting access to this information without court authorization. Federal and state laws—like the one that authorized the federal administrative subpoenas in this case—reflect a consensus view of our citizens’ privacy interests in IP addresses and ISP subscriber information. *Furman v. Georgia*, 408 U.S. 238, 383 (1972) (Burger, CJ., dissenting) (“[I]n a democratic society legislatures, not courts, are constituted to respond to the will and consequently the moral values of the people.”). Here, the Arizona legislature also expressed the will of our citizens by authorizing law enforcement officials to obtain such information with subpoenas. *See* A.R.S. § 13-3018(A), (C).

¶48 The dissent urges that in lieu of assessing what reasonable expectation of privacy society is prepared to accept, we should adopt an analytical framework wherein we ask two questions: “(1) whether the search encompasses intimate details of a person’s life, and (2) whether the disclosure of information was made for a limited purpose and not for release to other persons for other reasons. If those two criteria are met, the information is a private affair and the government may obtain it only with authority of law.” *Infra* ¶ 127. The dissent then concludes that both criteria are met here. We disagree.

¶49 First, IP addresses and ISP information do *not* reveal intimate details of a person’s life. *Supra* ¶¶ 3, 25. Second, as discussed, an IP address is akin to a return address on an envelope deposited in the mail, and an internet user’s online activities are routinely “released to other persons for other reasons.” *Supra* ¶¶ 2, 40–41. Third, IP addresses and ISP records belong to the third-party provider, not the subscriber. *Supra* ¶ 25. Moreover, despite the dissent’s assertion that sharing information with individuals in an ostensible position of trust does not render the information public, *infra* ¶ 130, providing information to a third-party ISP that may disseminate the information for commercial purposes stretches the notion of privacy too far. Thus, we conclude that IP addresses and ISP

STATE v. MIXTON
Opinion of the Court

information are not a “private affair” even under the dissent’s alternative analytical approach.

¶50 Essentially, the dissent contends that the textual differences between the Fourth Amendment and the Private Affairs Clause necessarily lead to different protections for IP addresses and subscriber information. *Infra* ¶¶ 78, 86–89, 99. We disagree. Although we agree that the textual variations signal broader protections under the Private Affairs Clause, we reject the dissent’s implication that the term “private affairs” forecloses consideration of conduct – such as sharing information with a third party – that is inconsistent with the notion of privacy when defining the provision’s scope, or that its different terms necessarily provide broader protections than the Fourth Amendment in every circumstance.

¶51 Thus, we conclude that an IP address and subscriber information are not “private affairs” under the Private Affairs Clause because the nature of the information is inconsistent with privacy: an internet user’s expectation of privacy in such non-content information is unreasonable in light of the nature of the information; it is voluntarily shared with third parties; and such third parties own, and often engage in pervasive legal derivative use of, it.

D.

¶52 The court of appeals asserts that the state’s possession of an IP address and ISP subscriber information 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.” *Mixton*, 247 Ariz. at 225 ¶ 27. We disagree. As discussed, *supra* ¶ 25, an IP address does not provide the state with an illicit view into an internet user’s private affairs because, absent a warrant, the state is prohibited from examining the substance or content of a user’s communications. In fact, the only information the state theoretically could acquire about an internet user’s online activities through an IP address is the information a user discloses to a website and which the website subsequently chooses to publicize. *See, e.g., Kelly Weill, Edits to Wikipedia pages on Bell, Garner, Diallo traced to 1 Police Plaza*, Politico (Mar. 13, 2015, 05:28 AM), <https://www.politico.com/states/new-york/city-hall/story/2015/03/edits-to-wikipedia-pages-on-bell-garner-diallo-traced-to-1-police-plaza-087652> (explaining that

STATE v. MIXTON
Opinion of the Court

reporters determined internet users at New York Police Department headquarters edited Wikipedia pages because Wikipedia published the IP addresses of unregistered editors).

¶53 The sole issue before us is whether the State may obtain an IP address and ISP subscriber information with a valid federal administrative subpoena. Although we hold that internet users, by virtue of voluntarily providing this non-content information to third-party providers, do not have a reasonable expectation of privacy in this discrete class of information under the federal or Arizona Constitutions, we need not consider the constitutionality of the State’s theoretical derivative use of this non-content information to discover what some websites may publicize about a user’s internet search history. We underscore, however, that the third-party doctrine applies only to non-content information, *see supra* ¶¶ 14–20; 18 U.S.C. § 2702(a) (protecting the “contents of a communication”), as does our holding under the Arizona Constitution.

E.

¶54 Mixton and the court of appeals rely on cases from other jurisdictions that have rejected applications of the third-party doctrine, or the doctrine’s inherent logic, on state constitutional grounds. The court of appeals claims that these states have rejected this approach under their state constitutions because they have concluded that “people . . . have a reasonable expectation of privacy in information they must furnish to companies providing banking, phone, and internet services in order to use those services.” *See Mixton*, 247 Ariz. at 224 ¶ 25 (collecting cases from states that have rejected the third-party doctrine on state constitutional grounds). But, save one of these cases, *infra* ¶ 62, these courts have not recognized a reasonable expectation of privacy in an IP address or ISP subscriber information.

¶55 In any event, numerous state courts have applied the third-party doctrine or similar reasoning under their respective constitutions. *See State v. Clark*, 752 S.E.2d 907, 921 n.13 (W. Va. 2013) (noting that Alabama, Georgia, Kansas, Maryland, North Carolina, North Dakota, Oklahoma, and South Carolina have adopted the third-party doctrine pursuant to *Smith and Miller*). At best, Mixton correctly notes a split in state court authority on the applicability of the third-party doctrine or similar reasoning to state constitutions.

STATE v. MIXTON
Opinion of the Court

¶56 Mixton places particular emphasis on Washington state court decisions, namely *State v. Gunwall*, 720 P.2d 808, 812 (Wash. 1986), and *State v. Miles*, 156 P.3d 864, 868 ¶ 14 (Wash. 2007), for the proposition that the third-party doctrine or its reasoning is inconsistent with Arizona’s Private Affairs Clause. Mixton contends that Washington has rejected *Miller* and *Smith* and, thus, the third-party doctrine, and urges us to do the same. We are unpersuaded. Washington has not categorically rejected the third-party doctrine or its logic, but rather examines the scope of its state constitution’s protections on a case-by-case basis, and it has not considered whether its constitution requires a warrant or court order to obtain an IP address and ISP subscriber information.

¶57 Washington courts employ a non-exclusive, six-part test to determine whether the state constitution affords broader protections than the federal Constitution. *Gunwall*, 720 P.2d at 812–13 (enumerating factors such as the textual language of the state constitution, significant textual differences between the state and federal constitutions, state constitutional and common law history, preexisting state law, structural variance between the state and federal constitutions, and matters of state interest or local concern). In interpreting the Washington Constitution, “the relevant inquiry for determining when a search has occurred is whether the State unreasonably intruded into the defendant’s ‘private affairs.’” *Id.* at 814. Thus, Washington courts consider “the type of information those records revealed” and “what kind of protection has historically been afforded to the interest asserted” when deciding whether a search violates the state constitution. *Miles*, 156 P.3d at 868 ¶ 12–13.

¶58 In *Gunwall*, the Washington Supreme Court held that a warrantless pen register violated the Washington Constitution. The court emphasized that state statutes protecting communications were “broad, detailed and extend[ed] considerably greater protections to [Washington] citizens in this regard than . . . comparable federal statutes and rulings.” 720 P.2d at 815. It also reasoned that a pen register, which records all of a defendant’s outgoing calls, “may affect other persons and can involve multiple invasions of privacy as distinguished from obtaining documents in a single routine search using a conventional search warrant.” *Id.* at 816. As such, *Gunwall* relied on Washington’s statutes and the nature of pen register information to inform its analysis of the scope of Washington’s constitutional privacy protections.

STATE v. MIXTON
Opinion of the Court

¶59 In *Miles*, the Washington Supreme Court held that the state’s use of an administrative subpoena to search a person’s banking records violated the state constitution. 156 P.3d at 866 ¶ 1. The court’s analysis centered on its precedents and the nature of the seized information to determine whether it was protected by the state constitution. *Id.* at 868 ¶ 14 (noting that court’s prior holding that garbage placed at the curb is protected by the state constitution because it may contain sensitive personal information). The court emphasized that banking records reveal “what political, recreational, and religious organizations a citizen supports. They potentially disclose where the citizen travels, their affiliations, reading materials, television viewing habits, financial condition, and more.” *Id.* at 869 ¶ 17. The *Miles* Court also noted, as in *Gunwall*, that state statutes protect a customer’s banking information and govern third-party disclosures. *Id.* at 869 ¶ 16. The court reasoned that the sensitive nature of a customer’s banking records required a warrant or subpoena issued by a neutral magistrate for its seizure. *Id.* at 869–70 ¶¶ 19–22.

¶60 We find *Gunwall* and *Miles* distinguishable. First, unlike Washington, Arizona statutes and court decisions do not provide greater protections concerning pen registers or banking records than do federal statutes and rulings. *See, e.g.*, A.R.S. § 13-1812 (authorizing county attorneys to issue a subpoena duces tecum for financial institution account records). In fact, contrary to Washington’s expansive legislative privacy protections which animate its courts’ constitutional decisions in this area, *see State v. Roden*, 321 P.3d 1183, 1185–86 (Wash. 2014), the Arizona legislature has authorized the state to issue administrative subpoenas for subscriber information and other non-content service provider records based on a showing that “the information likely to be obtained is relevant to an ongoing criminal investigation.” *See* § 13-3018(A), (C). Second, an IP address or ISP subscriber information does not implicate the privacy interests addressed in those cases. *See supra* ¶¶ 24–25.

¶61 The dissent’s reliance on *State v. Hinton* is similarly misplaced. There, the Washington Supreme Court held that police may not inspect text messages on a defendant’s cell phone without a search warrant because they are a “private affair” under the state constitution. 319 P.3d 9, 11 ¶ 1 (Wash. 2014). But a text message, unlike an IP address or subscriber information, is considered “content” and, thus, is also subject to the Fourth

STATE v. MIXTON
Opinion of the Court

Amendment's warrant requirement. *See Riley v. California*, 573 U.S. 373, 403 (2014). *Hinton* is inapposite to the issue before us.

¶62 We also note that the Washington Supreme Court considers the interests of national uniformity when determining whether to extend its state constitutional provisions beyond the federal constitutional protections. *Gunwall*, 720 P.2d at 813. We recognize the utility in uniform state and federal criminal rules, procedures, and standards. *See, e.g., Bolt*, 142 Ariz. at 269. The nature of cybercrime squarely implicates these interests and militates in favor of uniform federal and state search and seizure standards. *See, e.g., Megan McGlynn, Competing Exclusionary Rules in Multistate Investigations: Resolving Conflicts of State Search-And-Seizure Law*, 127 Yale L.J. 406, 411 (2017) (noting that multi-jurisdictional search and seizure issues are proliferating as a consequence of advancing technologies).

¶63 Thus, we conclude that, even applying the Washington courts' approach, Arizona's Private Affairs Clause does not require a warrant or court order to obtain an IP address or subscriber information.

F.

¶64 State courts may be split on the applicability of the third-party doctrine or similar approaches to state constitutions, but a clear consensus now exists concerning whether such constitutions protect an IP address and ISP subscriber information. Of the six states that have considered the issue, all but one have determined that their citizens hold no reasonable expectation of privacy in such information. *See Rader v. State*, 932 N.E.2d 755, 761–62 (Ind. Ct. App. 2010) (holding that the state constitution does not require a warrant for internet subscriber information); *State v. Leblanc*, 137 So. 3d 656, 658–62 (La. Ct. App. 2014) (“Even if we were to assume that defendant or his wife had an actual or subjective expectation of privacy in the subscriber information provided to Cox, we would still find that this expectation of privacy would not be recognized by society as reasonable.”); *State v. Mello*, 27 A.3d 771, 776–77 (N.H. 2011) (“[W]hile individuals may have a reasonable expectation of privacy in the contents of their communications, *i.e.*, the content of e-mails and the specific content viewed over the Internet, they have no such privacy interest in information voluntarily disclosed to an Internet service provider in order to gain access to the Internet.”); *State v. Delp*, 178 P.3d 259, 262–65 (Or. Ct. App. 2008) (“[D]efendant has not directed us to any source of law that establishes that

STATE v. MIXTON
Opinion of the Court

he has some interest in keeping private the noncontent information that is held by a third party regarding his Internet usage. Nor are we aware of any principle that would prevent AOL from responding to a proper government subpoena concerning his subscriber information.”); *State v. Simmons*, 27 A.3d 1065, 1069–70 (Vt. 2011) (“Nothing in our [state constitutional] rulings suggest that an internet subscriber address and frequency of use data, unembellished by any personal information, should be treated as private.”).

¶65 Apart from the court of appeals and dissent here, the only court to recognize a state constitutional right to privacy in subscriber information provided to an ISP did not require the state to procure a search warrant for such information, but rather permitted disclosure of the information with a grand jury subpoena and without notice to the subscriber. *State v. Reid*, 945 A.2d 26, 33–37 (N.J. 2008). The dissent’s search warrant requirement for non-content IP address and ISP subscriber information calls into question the viability of other long-standing law enforcement compulsory process investigative tools, including those that require a court order to collect private information but permit disclosure under a lower standard than probable cause. *See, e.g.*, A.R.S. § 13-3017 (authorizing law enforcement officials to obtain a judicial ex parte order to install and use a pen register or trap and trace device based upon the likelihood that the information “to be obtained is relevant to an ongoing criminal investigation”); A.R.S. § 13-1812 (authorizing a county attorney to issue “a subpoena duces tecum to a financial institution to obtain account records” in an investigation or prosecution of enumerated offenses).

¶66 The dissent contends that “it should not be difficult” for the state to obtain a search warrant “in the circumstances of this case.” *Infra* ¶ 131. But requiring a search warrant to obtain an IP address and subscriber information would essentially limit law enforcement to investigating completed internet-based offenses. For example, what if Mixton had merely queried the undercover detective about trading child pornographic images, but never transferred the photographs? This unworkable approach would invariably stifle proactive investigations of internet-based crimes.

G.

STATE v. MIXTON
Opinion of the Court

¶67 The court of appeals and Mixton warn that the logic underlying the third-party doctrine may lead to eradication of anonymous speech and that internet users would have to engage in “some unidentified Herculean effort to maintain anonymity” to partake in internet activities free from government intrusion. *Mixton*, 247 Ariz. at 226 ¶ 31. Not true.

¶68 First, Mixton’s assertion of a right to speak anonymously does not extend to anonymous distribution of illicit material without legal consequence. *See New York v. Ferber*, 458 U.S. 747, 763 (1982) (noting “child pornography as a category of material outside the protection of the First Amendment”); *Mobilisa, Inc. v. Doe*, 217 Ariz. 103, 108 ¶ 12 (App. 2007) (“The right to speak anonymously, however, is not absolute . . . [and] an anonymous speaker, like a known one, has no First Amendment right to engage in obscenity.”). Neither the federal administrative subpoena here, nor any provision under Arizona law, would permit the state to acquire an IP address or subscriber information for a reason unrelated to a criminal investigation, and no federal or Arizona constitutional provision protects the anonymous distribution of child pornography.

¶69 Second, anonymous speech is not implicated in this case because Mixton did not plausibly endeavor to elude identification. Although he used a pseudonym as his personal identifier on his Kik account, he conveyed data files to others using his actual IP address. As noted, *supra* ¶ 2, an IP address functions as a return address for any internet-based computer activity. Essentially, Mixton’s internet use of a pseudonym is analogous to his mailing a letter under a pseudonym but scrawling his actual return address on the outside of the envelope. Unsurprisingly, a letter sender is afforded no constitutional protections to the information on the outside of an envelope. *See Forrester*, 512 F.3d at 511. Although we embrace the principle of anonymous speech and recognize its inestimable contribution to our liberty, authoring an essay under the pseudonym “Publius” does little to preserve the author’s anonymity if the exterior of the envelope containing the essay reads “From the Office of Alexander Hamilton.”

¶70 Third, the court of appeals and Mixton exaggerate the lengths necessary to maintain anonymity over the internet. An internet user’s “Herculean effort to maintain anonymity” entails no more than using publicly available computers, publicly available WiFi networks, or VPNs to mask his IP address. Shuntich & Vogel, *supra* ¶ 3, at 51; *supra* ¶ 23.

STATE v. MIXTON
Opinion of the Court

¶71 Finally, Mixton and the court of appeals' remonstrance on the demise of anonymous speech is curious in light of its persistence in the wake of more than a decade of uniform federal jurisprudence affirming the constitutionality of law enforcement subpoena access to IP address and ISP subscriber information. *Supra* ¶¶ 14–20.

H.

¶72 The court of appeals and Mixton raise the specter of official misuse of the non-content fruits of the federal administrative subpoena. This reasoning is highly speculative and beyond the facts before us. We decline the invitation to center our constitutional analysis on such speculation about potential abuse of government authority. *See Golden v. Zwickler*, 394 U.S. 103, 108 (1969) (noting that “‘concrete legal issues, presented in actual cases, not abstractions’ are requisite” to adjudicating constitutional issues (quoting *United Pub. Workers of Amer. (C.I.O.) v. Mitchell*, 330 U.S. 75, 89 (1947))).

¶73 First, in this case, the scope of the federal administrative subpoena is not subject to abuse on its terms because, as relevant here, it only allows an agency district director or special agent to obtain IP address and ISP subscriber information based upon an articulable belief that the information is relevant to investigation of a child-exploitation crime. 19 U.S.C. § 1509(a)(1) (“In any investigation . . . conducted for the purpose of . . . insuring compliance with the laws of the United States administered by the United States Customs Service, the Secretary (but no delegate of the Secretary below the rank of district director or special agent in charge) may – examine . . . any record . . . which may be relevant to such investigation.”). The subpoena did not permit the government to obtain content-based information, which remains subject to a warrant requirement. *Supra* ¶¶ 14–20. Any concern that the government *may* misuse the non-content IP address and ISP subscriber information, once lawfully obtained, is not before us.

¶74 Second, it is illogical to condition the constitutionality of an otherwise lawful compulsory process based on speculation that the process may be abused or its fruits may be put to illegal use. Instead, an aggrieved party may seek recourse from the courts to rectify an unlawful search or seizure. *See, e.g., State v. Buccini*, 167 Ariz. 550, 558 (1991) (suppressing

STATE v. MIXTON
Opinion of the Court

evidence when a police officer “has deliberately or recklessly made material misstatements and omissions in the original affidavit” and a redrafted affidavit would otherwise lack probable cause). Here, the state obtained Mixton’s IP address and ISP subscriber information with a valid federal administrative subpoena, and could similarly have done so under Arizona law (§ 13-3018(A), (C)), which ensures that a record is generated to justify its issuance and to afford a remedy. *See United States v. Barnes*, No. CR18-5141 BHS, 2019 WL 2515317, at *7 (W.D. Wash. June 18, 2019) (noting that, although 19 U.S.C. § 1509(a)(1) provides no suppression remedy, evidence seized based upon a statutory violation may be suppressed if “the excluded evidence arose directly out of statutory violations that implicated important Fourth and Fifth Amendment interests” (quoting *Sanchez-Llamas v. Oregon*, 548 U.S. 331, 348 (2006))).

CONCLUSION

¶75 We hold that neither the Fourth Amendment to the United States Constitution nor article 2, section 8 of the Arizona Constitution requires law enforcement officials to secure a search warrant or court order to obtain IP addresses or subscriber information voluntarily provided to ISPs as a condition or attribute of service. The Fourth Amendment does not apply to IP addresses or subscriber information under the third-party doctrine, and this information is not a “private affair” under the Private Affairs Clause. Thus, the state lawfully obtained this information with a valid federal administrative subpoena.

¶76 Because we hold that IP address and ISP subscriber information does not qualify for protection as a “private affair” under article 2, section 8, and that the state lawfully obtained this information with a federal administrative subpoena, we need not address whether the Arizona Constitution’s “lawful authority” requirement is necessarily limited to a search warrant, nor do we consider the state’s good-faith exception argument.

¶77 We affirm Mixton’s convictions and vacate the court of appeals’ opinion.

STATE v. MIXTON
JUSTICE BOLICK, joined by CHIEF JUSTICE BRUTINEL and VICE CHIEF
JUSTICE TIMMER, Dissenting

BOLICK, J., joined by BRUTINEL, C.J. and TIMMER, V.C.J., dissenting.

¶78 We are now in the second century of Arizona statehood, yet this is the first time the Court has given more than cursory consideration to the meaning of the private affairs clause of article 2, section 8 of the Arizona Constitution. That provision has no analogue in the federal constitution and was clearly intended to provide additional and forceful protections to Arizonans against government intrusions into their private affairs. Because the majority interprets the private affairs clause in lockstep with the less-protective Fourth Amendment as construed by the United States Supreme Court, thereby draining the meaning expressed in the clause and intended by its architects, we respectfully dissent.

I.

¶79 As Arizona was the forty-eighth state, its framers “had the opportunity to ponder more than 100 years of United States history before penning their own constitution, allowing them to adopt or adjust provisions employed by the federal government or other states to meet Arizona’s needs.” Rebecca White Berch et al., *Celebrating the Centennial: A Century of Arizona Supreme Court Constitutional Interpretation*, 44 Ariz. St. L.J. 461, 468 (2012) [hereinafter “Berch”]. In some instances, the framers concluded they could not improve upon the federal constitutional framers’ handiwork; in others, they sought to add greater protections of individual rights and constraints on government power.

¶80 In particular, as this Court has recognized, our constitution’s Declaration of Rights is the “main formulation of rights and privileges conferred on Arizonans.” *Mountain States Tel. & Tel. Co. v. Ariz. Corp. Comm’n*, 160 Ariz. 350, 356 (1989). Thus, it is our duty to “first consult our constitution” whenever a right it “guarantees is in question.” *Id.* As former Chief Justice Rebecca Berch observed, “[h]ad the framers merely intended to mirror the guarantees found in the Federal Bill of Rights, they could have simply adopted the first eight amendments of the U.S. Constitution. But records of Arizona’s convention clearly show that the framers did not always agree with the language or implementation of the Federal Bill of Rights.” Berch, *supra* ¶ 79, at 469.

STATE v. MIXTON
JUSTICE BOLICK, joined by CHIEF JUSTICE BRUTINEL and VICE CHIEF
JUSTICE TIMMER, Dissenting

¶81 The federal constitution is the baseline for the protection of individual rights, below which the states cannot go; but in our system of federalism, states are free to provide greater protections. *City of Mesquite v. Aladdin's Castle, Inc.*, 455 U.S. 283, 293 (1982); *see also Prune Yard Shopping Ctr. v. Robins*, 447 U.S. 74, 81 (1980). Our constitution's framers repeatedly did so in the Declaration of Rights, and especially in the private affairs clause. Whereas the vast majority of state constitutions have provisions that roughly parallel the language of the Fourth Amendment, only two—ours and Washington State's, whose provisions are identical—deliberately chose to depart from the Fourth Amendment's language in favor of a distinct provision encompassing a protection for private affairs. Timothy Sandefur, *The Arizona "Private Affairs" Clause*, 51 *Ariz. St. L.J.* 723, 724 (2019).

¶82 Rather than accord independent vitality to a protection of individual rights in our constitution, the majority urges that we should extol "the value in uniformity with federal law when interpreting and applying the Arizona Constitution." *Supra* ¶ 32. Uniformity is certainly a value, and when all other things are equal, uniformity may be preferable to divergence. But where the Constitution's framers made deliberate effort to distinguish our state constitutional protections from the narrower confines of the federal constitution, our failure to credit and enforce our constitution's language and intent inevitably means that those protections will not have their intended effect. *See Berch, supra* ¶ 79, at 473 ("[I]t is not always appropriate to assume that state and federal provisions should be construed identically, given the unique legislative history, purpose, and text of the Arizona provision."); *see also Ruth V. McGregor, Recent Developments in Arizona State Constitutional Law*, 35 *Ariz. St. L.J.* 265, 276 (2003) ("None of the opinions from our court provide any in-depth analysis of the reasons we have so often opted for a goal of uniformity.").

¶83 Indeed, the Supreme Court has recognized that an "interest in uniformity . . . does not outweigh the general principle that States are independent sovereigns with plenary authority to make and enforce their own laws as long as they do not infringe on federal constitutional guarantees." *Danforth v. Minnesota*, 552 U.S. 264, 280 (2008). The states' authority to make distinct rules of criminal procedure, the Court remarked, "is not otherwise limited by any general, undefined federal interest in

STATE v. MIXTON
JUSTICE BOLICK, joined by CHIEF JUSTICE BRUTINEL and VICE CHIEF
JUSTICE TIMMER, Dissenting

uniformity. Nonuniformity is, in fact, an unavoidable reality in a federalist system of government." *Id.*

¶84 This Court has consistently recognized "that a Constitution should be construed so as to ascertain and give effect to the intent and purpose of the framers and the people who adopted it." *State ex rel. Morrison v. Nabours*, 79 Ariz. 240, 245 (1955); *accord Rumery v. Baier*, 231 Ariz. 275, 278 (2013). Arizona's framers did not leave us guessing what they had in mind in crafting the Declaration of Rights, emphasizing in the first two sections "the security of individual rights" and that the purpose of government is "to protect and maintain individual rights." Ariz. Const. art. 2, §§ 1-2.

¶85 Constitutional text should be interpreted according to its ordinary public meaning, that is, by reference to the meaning of the language generally understood when it was adopted. *See, e.g., District of Columbia v. Heller*, 554 U.S. 570, 577 (2008). Thus, this Court has emphasized that "effect be [especially] given to the purpose indicated, by a fair interpretation of the language used, and unless the context suggests otherwise words are to be given their natural, obvious and ordinary meaning." *Morrison*, 79 Ariz. at 245; *accord State ex rel. Brnovich v. City of Phoenix*, 468 P.3d 1200, 1205 ¶ 21 (2020) (explaining that, in interpreting state constitutional provisions, "we give the words their ordinary meaning, unless the context suggests a different one").

¶86 A comparison of the words of the Fourth Amendment and those chosen by the framers of article 2, section 8 underscore the stark differences:

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

U.S. Const. amend. IV.

STATE v. MIXTON
JUSTICE BOLICK, joined by CHIEF JUSTICE BRUTINEL and VICE CHIEF
JUSTICE TIMMER, Dissenting

No person shall be disturbed in his private affairs, or his home
invaded, without authority of law.

Ariz. Const. art. 2, § 8.

¶87 Most obvious and pertinent here, the protection of “private affairs” is nowhere found in the Fourth Amendment. Indeed, a right to privacy—based not on express constitutional text but on “penumbras, formed by emanations” — would not be found in the federal constitution for another 53 years. *See Griswold v. Connecticut*, 381 U.S. 479, 484 (1965). Its express inclusion in a 1912 state constitution strongly suggests that the framers had a significant protection in mind, one whose omission in the federal constitution they found wanting.

¶88 Moreover, by its terms, the Fourth Amendment is limited to “persons, houses, papers, and effects,” which are protected only against “unreasonable searches and seizures.” By contrast, the scope of “private affairs” under article 2, section 8 is broader on its face, and the protection is categorical. *See State v. Simpson*, 622 P.2d 1199, 1205 (Wash. 1980) (construing identical language that “clearly recognizes an individual’s right to privacy with no express limitations”).

¶89 And our constitutional language was not chosen randomly. The delegates to the constitutional convention considered language parallel to the Fourth Amendment, but instead adopted language containing the private affairs clause from the Washington Constitution. *See Goff, Records of the Arizona Constitutional Convention* 507–08 (1991). In other words, the language of article 2, section 8 was *deliberately chosen as an alternative* to the language of the Fourth Amendment. *Cf. State v. Gunwall*, 720 P.2d 808, 814–15 (Wash. 1986) (noting that delegates to the Washington State constitutional convention specifically rejected Fourth Amendment language, which “lends support to reading [the private affairs clause] independently of federal law”).

¶90 Indeed, in rejecting language echoing the Fourth Amendment, Arizona’s constitutional framers changed *existing* Arizona law. The Arizona territory was governed by the Howell Code, which contained a provision nearly identical to the Fourth Amendment. Howell

STATE v. MIXTON
JUSTICE BOLICK, joined by CHIEF JUSTICE BRUTINEL and VICE CHIEF
JUSTICE TIMMER, Dissenting

Code art. VII (1864). Once statehood was achieved, the new constitution’s architects abandoned that approach in favor of the broader, express privacy provision of article 2, section 8. And when a legislature amends a provision by making a significant change in language, we presume it intended a different meaning. Antonin Scalia & Bryan A. Garner, *Reading Law: The Interpretation of Legal Texts* 256 (2012).

¶91 All of which invites the question: if the framers wanted to craft language that would be enforced on its own terms, how could they have better done so than to reject one set of words and deliberately adopt another? Under such circumstances, we should be loath to interpret the language the framers chose in lockstep with language the framers consciously rejected, and indeed, not only as it was interpreted in 1912 but as the Supreme Court has construed it many years later. *See Sandefur, supra* ¶ 81, at 750 (“Even if the wording of both constitutions is identical, there is no constitutional justification for following federal precedent that only originates *after* the people of a state ratify their state constitution.”).

¶92 That the framers meant our constitutional language to have independent vitality necessarily follows from the fact that when our constitution was adopted, the Fourth Amendment was not yet applicable to the states through incorporation under the Fourteenth Amendment. *See Wolf v. Colorado*, 338 U.S. 25, 33 (1949) (declining to apply exclusionary rule against the states); *see also Twining v. New Jersey*, 211 U.S. 78, 108–14 (1908) (discussing history of incorporation and collecting cases). Thus, our Declaration of Rights was meant to provide the solitary protection for individual liberty against the state. Berch, *supra* ¶ 79, at 468. As former Chief Justice Ruth McGregor has observed, because the Bill of Rights did not yet apply to the states, “the drafters of our state constitution could not have operated under the assumption that interpretations of the federal constitution would control the rights guaranteed citizens under the state constitution.” McGregor, *supra* ¶ 82, at 275.

¶93 And the dominant school of state constitutional interpretation at the time was originalism, so the framers likely expected their handiwork to be interpreted on its own terms rather than through federal court interpretations of a different constitution. *See* Jeremy M. Christiansen, *Originalism: The Primary Canon of State Constitutional Interpretation*, 15 Geo.

STATE v. MIXTON
JUSTICE BOLICK, joined by CHIEF JUSTICE BRUTINEL and VICE CHIEF
JUSTICE TIMMER, Dissenting

J.L. & Pub. Pol’y 341, 351 (2017); *id.* at 368–69 (recounting Arizona cases to that effect). Our early cases specified that the purpose of rules of interpretation is to arrive at the intent of the framers. *See, e.g., State v. Osborne*, 14 Ariz. 185, 204 (1912) (stating that the rule of constitutional construction that each clause should be given meaning exists “so that intent of the framers may be ascertained and carried out”).

¶94 This Court frequently has interpreted provisions of our state constitution more broadly than their federal counterparts, and sensibly, we have done so especially where the language is different. Thus, we have repeatedly held that our speech protection is broader than that accorded by the First Amendment. *See, e.g., Brush & Nib Studios, LC v. City of Phoenix*, 247 Ariz. 269, 281–82 ¶ 45 (2019); *Mountain States*, 160 Ariz. at 354–56. Likewise, our courts have construed the broader language of article 2, section 17 of the Arizona Constitution to provide greater protection against eminent domain than does the Fifth Amendment’s takings clause as construed by the Supreme Court. *See, e.g., Inspiration Consol. Copper Co. v. New Keystone Copper Co.*, 16 Ariz. 257, 259–60 (1914) (stating that court decisions construing takings provisions in the federal and other state constitutions “are not controlling in this state, and, indeed, lend us but little aid” in interpreting art. 2, § 17); *Bailey v. Myers*, 206 Ariz. 224, 229 ¶ 20 (App. 2003) (“The federal constitution provides considerably less protection against eminent domain than our Constitution provides.”). By contrast, where the state constitutional language parallels that of the Bill of Rights, we have tended to construe it in tandem with Supreme Court interpretations of the federal constitutional provision. *See, e.g., State v. Carter*, 469 P.3d 449, 449 ¶ 1 n.2 (2020) (“The analysis under both the federal and state constitutions is the same because the language is virtually identical . . .”).

¶95 Before today, this Court’s analysis of the private affairs clause has been scant. Indeed, the Court’s initial analysis of the interplay between article 2, section 8 and the Fourth Amendment comprised fewer than fifty words. *Malmin v. State*, 30 Ariz. 258, 261 (1926) (cited *supra* § 31) (stating that the two provisions “are of the same general effect and purpose”). Shortly thereafter, the Court emphasized that despite *Malmin*, “[w]e have the right . . . to give such construction to our own constitutional provisions as we think logical and proper, notwithstanding their analogy to the

STATE v. MIXTON
JUSTICE BOLICK, joined by CHIEF JUSTICE BRUTINEL and VICE CHIEF
JUSTICE TIMMER, Dissenting

Federal Constitution and the federal decisions based on that Constitution.”
Turley v. State, 48 Ariz. 61, 70–71 (1936).

¶96 By contrast, as the majority acknowledges, this Court has construed the second provision of article 2, section 8—the home invasion clause—more broadly than the Fourth Amendment. *Supra* ¶ 32. See *State v. Ault*, 150 Ariz. 459, 464–65 (1986) (rejecting the federal inevitable discovery doctrine); *State v. Bolt*, 142 Ariz. 260, 264–65 (1984) (holding that warrantless home entry is per se unlawful absent exigent circumstances). In *Bolt*, the Court was “cognizant of the need for uniformity in interpretation,” but recognized that “[o]ur constitutional provisions were intended to give our citizens a sense of security in their homes and personal possessions.” *Id.* at 264–65. Thus, it rendered its decision “based upon our own constitutional provision, its specific wording, and our own cases, independent of federal authority.” *Id.* at 265. Likewise, in *Ault*, the Court noted that “[u]nlawful entry of homes was the chief evil which the Fourth Amendment was designed to prevent,” 150 Ariz. at 463, and that “our constitutional provisions were generally intended to incorporate federal protections . . . [but] they are more specific in preserving the sanctity of homes and in creating a right of privacy.” *Id.* at 466 (emphasis added) (citation omitted).

¶97 These cases, juxtaposed against the Court’s decision today, leave us in a curious and perplexing place. On the one hand, this Court has construed the home invasion provision of article 2, section 8 more broadly than the Fourth Amendment and has rejected Supreme Court doctrines inconsistent with that clause, even though both provisions protect homes. By contrast, the majority here subsumes the private affairs clause within the Supreme Court’s interpretation of the Fourth Amendment, even though the Fourth Amendment does *not* on its face protect against government intrusions into private affairs. By what principle does it do so? We are left to ponder not only that, but by what standard we will determine when to give independent meaning to our state constitutional language in other contexts. By our lights, we should at least do so where the language is conspicuously different, and certainly where (as here) no analogous provision exists in the federal constitution. Otherwise, the necessary consequence is to diminish constitutional protections.

STATE v. MIXTON
JUSTICE BOLICK, joined by CHIEF JUSTICE BRUTINEL and VICE CHIEF
JUSTICE TIMMER, Dissenting

¶98 It is especially hazardous to hitch the meaning of our constitution to the Supreme Court’s Fourth Amendment jurisprudence, which the majority charitably depicts as “uniform and sound,” *supra* ¶ 21, but is in fact characterized by confusion and constant change. The opacity of this jurisprudence is visible in our recent decision in *State v. Jean*, in which we attempted to determine whether the Supreme Court’s Fourth Amendment precedent requires a warrant for police to install a GPS device on a commercial vehicle under the facts of the case. 243 Ariz. 331 (2018). The case generated five separate opinions, including a majority opinion with different parts written by two different justices who disagreed with the parts of the opinion they did not write. Indeed, even the lodestars invoked by the majority here—*Smith v. Maryland*, 442 U.S. 735 (1979), and *United States v. Miller*, 425 U.S. 435 (1976)—are called into question, to an unknown extent, by *Carpenter v. United States*, 138 S. Ct. 2206 (2018).

¶99 We should not follow that long and winding road of Fourth Amendment jurisprudence to its uncharted destination. See *State v. Ingram*, 914 N.W.2d 794, 797–98 (Iowa 2018) (holding that “we encourage stability and finality in law by decoupling Iowa law from the winding and often surprising decisions of the United States Supreme Court,” and “take the opportunity to stake out higher constitutional ground”). When the constitutions converge, it makes sense to take Supreme Court decisions into account and place value on uniform application. But where the language of the two constitutions differs—and especially where our provision does not appear in the federal constitution in any manner—relying on the Supreme Court to determine our constitutional meaning deprives our citizens of the precious freedoms their forebears proclaimed when they embraced a wider conception of liberty than the federal constitution. After all, Supreme Court justices do not take an oath to uphold the Arizona Constitution. But we do.

II.

¶100 This is the first case to attach the Supreme Court’s Fourth Amendment third-party doctrine to the Arizona Constitution. A fair

STATE v. MIXTON
JUSTICE BOLICK, joined by CHIEF JUSTICE BRUTINEL and VICE CHIEF
JUSTICE TIMMER, Dissenting

independent reading of the text and intent of article 2, section 8 shows the protection of private affairs is incompatible with that doctrine.

¶101 While the Fourth Amendment specifies that “persons, houses, papers, and effects” are protected, article 2, section 8 more broadly protects “private affairs.” And while the Fourth Amendment prohibits “unreasonable” searches and seizures, article 2, section 8 categorically prohibits any disturbance “without authority of law.” By the provision’s clear terms, then, if the state wishes to invade a person’s private affairs, it may do so only with authority of law, which makes the definition of “private affairs” determinative.

¶102 This Court gives provisions in law “their ordinary meaning unless it appears from the context or otherwise that a different meaning is intended.” *Arizona ex rel. Brnovich v. Maricopa Cnty. Cmty. Coll. Dist. Bd.*, 243 Ariz. 539, 541 ¶ 7 (2018). The dictionary definition of “private,” both now and at the time of Arizona’s constitutional adoption, includes anything concerning an individual or group that is not “intended to be known publicly.” *Private*, Merriam-Webster, <https://www.merriam-webster.com/dictionary/private> (last visited Jan. 16, 2020); *see also* Harry Thurston Peck, *New Websterian 1912 Dictionary Illustrated* 649 (defining private as “not public” and “peculiar to one’s self.”). Likewise, “affairs” means “personal business.” *Affairs*, Merriam-Webster; *accord* Peck at 17.

¶103 The majority similarly defines “private” as “affecting or belonging to private individuals, as distinct from the public generally”; and “affairs” as “a person’s concerns in trade or property; business.” *Supra* ¶ 33. That is the first and only time the majority grapples with the original meaning of “private affairs,” and it ultimately disposes of the term as “ambiguous,” *id.*, never to be raised again.

¶104 True, “private affairs” is not unambiguous. But this Court does not throw up its hands in the face of ambiguity: if “a constitutional provision is not clear on its face, we can use extrinsic evidence to show the intent of the framers and the electorate that adopted it.” *Heath v. Kiger*, 217 Ariz. 492, 495 ¶ 9 (2008). And significant, uncontroverted evidence suggests we should read article 2, section 8 in a way that gives effect to its text.

STATE v. MIXTON
JUSTICE BOLICK, joined by CHIEF JUSTICE BRUTINEL and VICE CHIEF
JUSTICE TIMMER, Dissenting

¶105 “Private affairs” was a commonly used term during the period preceding our constitution’s adoption, and the protection of private affairs was a major preoccupation of contemporary legislatures, courts, and scholars. See, e.g., Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193 (1890). A review of these efforts concludes that “[m]ind your own business’ was an eleventh commandment in nineteenth century America.” *The Right to Privacy in Nineteenth Century America*, 94 Harv. L. Rev. 1892, 1904 (1981).

¶106 In particular, Americans in the twilight of the Nineteenth and dawn of the Twentieth Centuries sought to keep what was private from becoming public. A major concern was preventing the disclosure of private information when third parties, such as telegraph operators, were entrusted with transmission or delivery and the “messages were necessarily read by the operators who sent and received them.” *Id.* at 1901–02. Similarly, Congressman James Garfield championed legislation against disclosure of census information, so that an individual’s “private affairs, the secrets of his family and his business,” would not be revealed. *Id.* at 1905. The shielding of tax returns, in the words of the newspaper *The Nation*, protected “the ‘natural and inalienable right’ of everybody to keep his affairs to himself.” *Id.* at 1906. Courts likewise protected the confidentiality of certain public records to prevent making “public men’s private affairs.” *Id.* at 1907 (quoting *Buck & Spencer v. Collins*, 51 Ga. 391, 397 (1874)).

¶107 These examples illustrate that “private affairs” were understood in the early Twentieth Century to broadly encompass both personal and business matters, even if transmitted through third parties, thus making Arizona’s constitutional provision irreconcilable with the later-emerging federal “third-party” doctrine allowing any information divulged to a third party to be obtained by the government without a warrant.

¶108 The protection of private affairs was also reflected in local concerns. In 1912, the year our constitution was adopted, the *Arizona Republican* editorialized against a proposal to disclose the names of their subscribers, condemning it as a “perniciously inquisitorial” effort to gain access to “private business affairs and financial affairs.” Sandefur, *supra*

STATE v. MIXTON
JUSTICE BOLICK, joined by CHIEF JUSTICE BRUTINEL and VICE CHIEF
JUSTICE TIMMER, Dissenting

¶ 81, at 731 n.47. That same year, the newspaper warned against congressional investigations of alleged monopolies because “attacks upon corporate credit and private affairs . . . ought to be deprecated.” *Id.* at 731. It appears clear that the common meaning of “private affairs” in statehood-era Arizona encompassed the type of business transactions that would be swept up by the third-party doctrine many decades later.

¶109 Indeed, this meaning of private affairs and its inclusion within our constitutional protections is manifested even within Fourth Amendment jurisprudence at the turn of the century. In *Boyd v. United States*, the Court invalidated, under the Fourth and Fifth Amendments, federal laws pursuant to which business invoices were obtained without a warrant. 116 U.S. 616 (1886). The Court held that the principles animating those amendments “apply to all invasions on the part of the government and its employe[e]s of the sanctity of a man’s home and the privacies of life,” holding that obtaining the business records “is the invasion of his indefeasible right of personal security, personal liberty, and private property.” *Id.* at 630. Seemingly anticipating a decision like today’s, the Court urged “that constitutional provisions for the security of person and property should be liberally construed. A close and literal construction deprives them of half their efficacy, and leads to gradual depreciation of the right, as if it consisted more in sound than in substance.” *Id.* at 635; *see also Ex parte Jackson*, 96 U.S. 727, 733 (1877) (holding that sealed mail cannot be opened without a warrant).

¶110 Given that the framers of article 2, section 8 intended to incorporate the protections of the Fourth Amendment, *see Ault*, 150 Ariz. at 463, these decisions form at minimum the baseline for the rights protected. That our framers understood that private affairs meant one’s business, including transactions with others, is uncontested. Surely it would surprise the framers to know that the protections they embraced would be subject to severe diminution through Supreme Court interpretations of different provisions in the federal constitution many decades later.

¶111 Yet the majority asserts that the private affairs clause “protects a privacy interest . . . only if society is prepared to accept such an expectation of privacy as reasonable.” *Supra* ¶ 41. That amorphous

STATE v. MIXTON
JUSTICE BOLICK, joined by CHIEF JUSTICE BRUTINEL and VICE CHIEF
JUSTICE TIMMER, Dissenting

standard derives not from our constitutional text, but from a concurring opinion in a Supreme Court decision applying the Fourth Amendment, *Katz v. United States*. 389 U.S. 347, 361 (1967) (Harlan, J., concurring).¹ In so doing, the majority replaces an objective state constitutional command with a subjective standard whose meaning changes over time to reflect an evolving societal consensus.²

¶112 That standard has no textual or historical foundation in article 2, section 6. The framers of that provision informed us what society was prepared to recognize when our constitution was adopted: that any invasion of private affairs requires authority of law. And for us, then, the proper inquiry is whether a particular matter constitutes a private affair.

¹ In contrast to the majority here, however, Justice Harlan repeatedly expressed an “aversion to national uniformity,” which he rejected as inconsistent with our system of federalism that protects pluralism and individual rights. See J. Harvie Wilkinson III, *Justice John M. Harlan and the Values of Federalism*, 57 Va. L. Rev. 1185, 1196 (1971) (citing, *inter alia*, *Duncan v. Louisiana*, 391 U.S. 145, 182 n.21 (1968) (Harlan, J., dissenting) (disdaining “the needless pursuit of uniformity”) and *Ker v. California*, 374 U.S. 23, 45 (1963) (Harlan, J., concurring) (expressing concern over a “constitutional straitjacket”)).

² Even at the federal level, the *Katz* formulation has been subjected to substantial criticism. See, e.g., *Carpenter*, 138 S. Ct. at 2244 (Kennedy, Thomas, and Alito, JJ., dissenting) (“That the *Katz* test departs so far from the text of the Fourth Amendment is reason enough to reject it. But the *Katz* test also has proved unworkable in practice.”); *United States v. Jones*, 565 U.S. 400, 407 (2012) (stating that courts must, at minimum, preserve the degree of privacy that existed when the Fourth Amendment was adopted, and that *Katz* does not provide the exclusive means to determine that protection). Remarking on the *Katz* test’s inherent subjectivity, Justice Scalia observed that it “bear[s] an uncanny resemblance to those expectations of privacy that this Court considers reasonable,” and “has no plausible foundation in the text of the Fourth Amendment.” *Minnesota v. Carter*, 525 U.S. 83, 97 (1998) (Scalia, J., concurring).

STATE v. MIXTON
JUSTICE BOLICK, joined by CHIEF JUSTICE BRUTINEL and VICE CHIEF
JUSTICE TIMMER, Dissenting

¶113 The third-party doctrine is the progeny of *Katz*. The majority explains it aptly:

[A] person has no expectation of privacy in information he voluntarily discloses to third parties, even if there is an assumption it will be used only for a limited purpose And, because it is no longer private, the government may obtain such information from a third party without triggering the Fourth Amendment’s protections.

Supra ¶ 14.

¶114 Whatever the continuing vitality of this doctrine following *Carpenter* in the Fourth Amendment context, we should reject it here, just as this Court rejected Supreme Court doctrines that did not reflect the text and intent of article 2, section 8’s home invasion clause in *Ault* and *Bolt*. Whereas the Fourth Amendment warrant protection applies only where a reasonable expectation of privacy exists, our protection applies to all private affairs. As reflected by the types of business transactions that animated article 2, section 8’s framers, affairs can still be considered private even if they are shared by two or more people in a position of trust.

¶115 For that reason, the Washington Supreme Court, whose private affairs provision is both identical to and the source of ours,³ has rejected the Fourth Amendment “reasonable expectation of privacy” construct in interpreting its provision. “While we may turn to the Supreme Court’s interpretation of the United States Constitution for guidance in establishing a hierarchy of values and principles under the Washington Constitution, we rely, in the final analysis, upon our own legal foundations in determining its scope and effect.” *State v. Myrick*, 688 P.2d 151, 153 (Wash. 1984). Whereas under Fourth Amendment jurisprudence “the

³ We have often looked for guidance to the Washington Supreme Court’s decisions when interpreting similar provisions in our constitutions. *See, e.g., Mountain States*, 160 Ariz. at 355 (“[O]ur recognition of the broad protection for speech in Arizona conforms with the Washington Supreme Court’s reading of Washington Constitution art. 1, § 5, the model for Arizona’s art. 2, § 6.”).

STATE v. MIXTON
JUSTICE BOLICK, joined by CHIEF JUSTICE BRUTINEL and VICE CHIEF
JUSTICE TIMMER, Dissenting

inquiry is whether the defendant possessed ‘a reasonable expectation of privacy,’” *id.* (quoting *Katz*, 389 U.S. at 357), “under the Washington Constitution the relevant inquiry for determining when a search has occurred is whether the state unreasonably intruded into the defendant’s ‘private affairs.’” *Id.* at 153–54.

¶116 Nonetheless, several other states have rejected the third-party doctrine in construing their own constitutions even when they parallel the Fourth Amendment. *See, e.g., State v. Walton*, 324 P.3d 876, 906 (Haw. 2014); *State v. Thompson*, 810 P.2d 415, 418 (Utah 1991); *Shaktman v. State*, 553 So. 2d 148, 151 (Fla. 1989); *State v. Thompson*, 760 P.2d 1162, 1165 (Idaho 1988); *People v. Sporleder*, 666 P.2d 135, 141–42 (Colo. 1983); *Commonwealth v. DeJohn*, 403 A.2d 1283, 1289 (Pa. 1979). Notably, all those decisions interpret constitutions that do *not* contain a private affairs provision.

¶117 Indeed, the Supreme Court itself has questioned the foundations of the third-party doctrine in the information technology era. In declining to extend *Smith* and *Miller* to certain cell phone records under control of a third party, the Court noted the “seismic shifts in digital technology” that have made cell phones and the data they contain and transmit “‘such a pervasive and insistent part of daily life’ that carrying one is indispensable to participating in modern society.” *Carpenter*, 138 S. Ct. at 2220 (quoting *Riley v. California*, 573 U.S. 373, 385 (2014)). As with Internet Protocol (“IP”) addresses, “there is no way to avoid leaving behind a trail of location data. As a result, in no meaningful sense does the user voluntarily ‘assume[] the risk’” of having the data turned over to government officials. *Id.* (quoting *Smith*, 442 U.S. at 745).

¶118 Justice Gorsuch made the point even more directly:

Even our most private documents – those that, in other eras, we would have locked safely in a desk drawer or destroyed – now reside on third-party servers. *Smith* and *Miller* teach that the police can review all of this material, on the theory that no one reasonably expects any of it will be kept private. But no one believes that, if they ever did.

STATE v. MIXTON
JUSTICE BOLICK, joined by CHIEF JUSTICE BRUTINEL and VICE CHIEF
JUSTICE TIMMER, Dissenting

Id. at 2262 (Gorsuch, J., dissenting). Justice Gorsuch added that “I do not agree with the Court’s decision to keep *Smith* and *Miller* on life support and supplement them with a new and multilayered inquiry that seems to be only *Katz*-squared.” *Id.* at 2272.

¶119 Whatever the scope and persistence of the third-party doctrine after *Carpenter*, or the implications of that case for the facts here, the *Carpenter* dissenters aptly remark that the decision “destabilizes long-established Fourth Amendment doctrine,” *id.* at 2247 (Alito, J., dissenting) and will “keep defendants and judges guessing for years to come” *id.* at 2234 (Kennedy, J., dissenting) (citation omitted); *see also id.* at 2213–14 (main opinion) (“[N]o single rubric definitively resolves which expectations of privacy are entitled to protection.”).

¶120 The majority here prizes national uniformity even where Arizonans have chosen a markedly different approach in their organic law. That priority is misplaced given that in our federalist system, “state constitutions are our basic charters of state governance.” *Simpson v. Miller*, 241 Ariz. 341, 345 ¶ 8 (2017); *accord State v. Wein*, 244 Ariz. 22, 32 ¶ 39 (2018) (Bolick, Gould, and Lopez, JJ., dissenting); *see also* Jeffrey S. Sutton, *51 Imperfect Solutions: State Constitutions and the Development of American Constitutional Law* 42–83 (2018) (highlighting greater state constitutional protections for the rights of criminal defendants). We do Arizonans a disservice by elevating the value of discordant national uniformity over enforcement of our own constitution and the greater clarity and protection it affords.

III.

¶121 The majority asserts that a “clear consensus” of state courts hold that their state constitutions do not protect IP addresses or ISP subscriber information. *Supra* ¶ 47. Unfortunately, those decisions do little to aid us, for none of the constitutions at issue contains a private affairs clause. Applying the language and intent of our state constitutional provision, rather than decisions more than a half-century later applying markedly different constitutional language, we conclude that the data here

STATE v. MIXTON
JUSTICE BOLICK, joined by CHIEF JUSTICE BRUTINEL and VICE CHIEF
JUSTICE TIMMER, Dissenting

is protected by article 2, section 8's private affairs clause and may be obtained by the government only with authority of law.⁴

¶122 We entrust private information to third parties every day: every time we use a credit card, provide our Social Security number, use a security card reader, mail a saliva sample to a genetics lab, make a bank deposit or withdrawal, use a password to enter a website, or even send an email. Even under a reasonable expectation of privacy analysis, “[p]eople often *do* reasonably expect that information they entrust to third parties, especially information subject to confidentiality agreements, will be kept private.” *Carpenter*, 138 S. Ct. at 2263 (Gorsuch, J., dissenting). Indeed, sharing such information often is a precondition to engaging in commerce. The majority points to the widespread third-party data collection on the internet, *supra* ¶¶ 42-44, but that observation is simply irrelevant as the private affairs clause restricts government action. The notion that anything one must share for purposes of voluntary transactions is thereby subject to government inspection would eviscerate any meaningful notion of privacy.

¶123 The private affairs clause “encompasses those legitimate privacy expectations protected by the Fourth Amendment; but is not confined to the subjective privacy expectations of modern citizens who, due to well publicized advances in surveillance technology, are learning to expect diminished privacy in many aspects of their lives.” *Myrick*, 688 P.2d at 154. “In determining whether a certain interest is a private affair . . . a central consideration is the *nature* of the information sought—that is, whether the information obtained via the governmental trespass reveals

⁴ Because we would decide the case on independent and adequate state grounds, it is unnecessary to reach the Fourth Amendment issue. *Ault*, 150 Ariz. at 466. We note, however, that the third-party doctrine may not apply given that Mixton did not provide the information obtained by the government to a single entity. No employee at Kik knew Mixton's identity, only his IP address; and no employee at the ISP could have connected Mixton's IP address to the postings. The police aggregated information, rather than retrieving it from a third party to which Mixton conveyed it in its totality. *Cf. Bond v. United States*, 529 U.S. 334, 338-39 (2000) (holding that physical manipulation of luggage was a search, even though the luggage itself was exposed to the public in the storage rack of a bus).

STATE v. MIXTON
JUSTICE BOLICK, joined by CHIEF JUSTICE BRUTINEL and VICE CHIEF
JUSTICE TIMMER, Dissenting

intimate or discrete details of a person's life." *State v. Jordan*, 156 P.3d 893, 896 ¶ 8 (Wash. 2007). When the search "involves the gathering of personal information by the government, this court has also considered the purpose for which the information sought is kept, and by whom it is kept." *Id.* at ¶ 9.

¶124 Thus, courts that have rejected the Supreme Court's reasonable expectation of privacy analysis have focused not on societal or subjective expectations of privacy, but instead have made an objective determination about whether the information obtained reveals intimate or discrete details of a person's life. *See, e.g., Myrick*, 688 P.2d at 153-54. This is in keeping with the meaning of private affairs and the provision's historical intent and context. Moreover, limited disclosure of personal information to a private third party, as opposed to the public generally, does not give the government *carte blanche* access to that information. *See, e.g., Gunwall*, 720 P.2d at 816 (citing *State v. Hunt*, 450 A.2d 952, 956 (N.J. 1982)) (holding that telephone records are a private affair because, among other things, telephones are a necessary component of public life and the disclosure of information to the telephone company was made for a limited purpose and not for release to other persons for other reasons); *People v. Chapman*, 679 P.2d 62, 67 (Cal. 1984) (holding that a telephone company "customer's expectation of privacy in information gathered by the company during the regular course of its business must be honored as a reasonable one. That expectation cannot be deemed to have been abandoned because the customer is required to disclose" such information).

¶125 The Washington Supreme Court has construed the identical language of its constitution that way. "Given the realities of modern life, the mere fact that an individual shares information with another party and does not control the area from which that information was accessed does not place it outside the realm" of the private affairs clause. *State v. Hinton*, 319 P.3d 9, 15 ¶ 17 (Wash. 2014). In *Hinton*, the Washington Supreme Court ruled that police need a warrant to inspect text messages. The Court acknowledged that those who share personal information assume the risk that it will be disclosed by a third party, "[b]ut that risk should not be transposed into an assumed risk of intrusion by the government." *Id.*

STATE v. MIXTON
JUSTICE BOLICK, joined by CHIEF JUSTICE BRUTINEL and VICE CHIEF
JUSTICE TIMMER, Dissenting

¶126 Washington State courts have applied those principles under the private affairs provision to forbid warrantless inspections in a broad variety of contexts, even garbage. *State v. Boland*, 800 P.2d 1112, 1116 (Wash. 1990) (holding that although someone placing garbage can expect scavengers to snoop through it, “[p]eople reasonably believe that police will not indiscriminately rummage through their trash bags to discover their personal effects” (quoting *State v. Tanaka*, 701 P.2d 1274, 1275 (Haw. 1985)); see also *State v. Jorden*, 156 P.3d 893 (Wash. 2007) (motel registry); *State v. Miles*, 156 P.3d 864, 869 (Wash. 2007) (bank records, as they “potentially reveal[] sensitive information”); *State v. Butterworth*, 737 P.2d 1297 (Wash. Ct. App. 1987) (unpublished telephone listing). None of these likely would be shielded from police inspection under the pre-*Carpenter* third-party doctrine, but all were deemed private affairs under Washington State’s private affairs clause. These cases hold that where private information is disclosed to limited persons for limited purposes, it retains its private character for purposes of constitutional protection against searches without authority of law.

¶127 Adopting this framework for interpreting the identical language of our private affairs clause would provide greater clarity, consistency, and predictability than the evolving and uncertain post-*Carpenter* Fourth Amendment framework. It adheres to both the text of the private affairs clause and the intent of its framers to include business transactions within its protection. Applying this framework, we would not have to—as the majority has undertaken to do conscientiously yet unnecessarily—forecast what privacy interests society is prepared to accept, assess whether a person has a reasonable expectation of privacy with an anvil on the scale if the person has conveyed that information to a third party in any fashion, or delve into a fact-based determination of the nature of the technology or precisely what information it contains or emits. Rather, in this context, we would ask (1) whether the search encompasses intimate details of a person’s life, and (2) whether the disclosure of information was made for a limited purpose and not for release to other persons for other reasons. If those two criteria are met, the information is a private affair and the government may obtain it only with authority of law.

¶128 Here, both criteria are plainly met. The IP address and ISP information at issue, standing alone, do not disclose intimate personal

STATE v. MIXTON
JUSTICE BOLICK, joined by CHIEF JUSTICE BRUTINEL and VICE CHIEF
JUSTICE TIMMER, Dissenting

information. But when combined (in this case through two different subpoenas), they allow the police to determine which websites a person has visited. That information was not made available to the public (indeed, in combination it was not made available to anyone). Rather, the information shared through an IP address and with an ISP is necessary to obtain access to the internet. It is furnished for a limited purpose with the expectation it will not be shared with others, and certainly not with the government. IP addresses and ISP location data are not normally held out to the public but, like a credit card, disclosed to the provider to consummate the transaction. See Joshua J. McIntyre, *Balancing Expectations of Online Privacy: Why Internet Protocol (IP) Addresses Should be Protected as Personally Identifiable Information*, 60 DePaul L. Rev. 895, 900 (2011) (noting that, unlike a physical letter, which can be mailed without a return address, internet browsing requires leaving sender data).

¶129 In this regard, the New Jersey Supreme Court’s opinion in *State v. Reid* is especially instructive. 945 A.2d 26 (N.J. 2008). The court recognized that “it is hard to overstate how important computers and the Internet have become to everyday, modern life. Citizens routinely access the Web for all manner of daily activities: to gather information, explore ideas, read, study, shop, and more.” *Id.* at 33. As they do so, they transmit a numerical IP address to the websites they visit. Only an ISP, however, can translate an IP address into a user’s name (or, in this case, a street address). Having that combined information, “one can track a person’s Internet usage. ‘The government can learn the names of stores at which a person shops, the political organizations a person finds interesting, a person’s . . . fantasies, her health concerns, and so on.’” *Id.* (quoting Daniel Solove, *The Future of Internet Surveillance Law*, 72 Geo. Wash. L. Rev. 1264, 1287 (2004)). But key for our purposes is the court’s recognition that “the nature of the technology requires individuals to obtain an IP address to access the Web. Users make disclosures to ISPs for the limited goal of using that technology and not to promote the release of personal information to others.” *Id.* Construing the New Jersey Constitution, whose provision mirrors the Fourth Amendment, the court held that “users are entitled to expect confidentiality under these circumstances.” *Id.* Even though New Jersey’s constitution has no private affairs clause, this analysis dovetails with our constitutional text and intent.

STATE v. MIXTON
JUSTICE BOLICK, joined by CHIEF JUSTICE BRUTINEL and VICE CHIEF
JUSTICE TIMMER, Dissenting

¶130 The majority suggests that even if such information is a private affair, the person sharing it must take extraordinary precautions, such as encryption, or it loses its private character. We have expressly rejected that argument in the Fourth Amendment context. *State v. Peoples*, 240 Ariz. 244, 248–49 (2016) (rejecting the arguments that leaving a cellphone in plain view, or failing to password-protect it, allowed police to inspect its contents). Rather, we would adhere to the view that when police seek information about the intimate details of a person’s life by obtaining information that was shared in limited fashion with persons in a position of trust, rather than with the public at large, the private nature of the transaction is maintained to prevent police inspection without a warrant.

¶131 The majority does not reach the question of what constitutes “authority of law” under these circumstances, so neither do we. But assuming that a warrant would be necessary, it should not be difficult to obtain one in this case. *Cf. Riley*, 573 U.S. at 401 (noting that technology has made “the process of obtaining a warrant itself more efficient”). As Judge Eckerstrom noted, “[t]he warrant requirement would have posed no impediment to the investigation of the instant case. Mixton’s . . . 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.” *State v. Mixton*, 247 Ariz. 212, 230 ¶ 47 n.15 (Eckerstrom, J., concurring in part and dissenting in part); *accord id.* at 226 ¶ 32 (majority opinion). Regardless of the burden the government might face in securing such permission, the protection of having a neutral judge determine the propriety and scope of a search is essential. That protection becomes more crucial, not less, as information technology and our dependence upon it grows.

¶132 Our constitution’s framers aimed, as plainly as they could, to protect our private affairs from unsupervised government scrutiny. The majority’s non-textual opinion drains meaning from this essential constitutional protection. For these reasons, and with great respect to our colleagues, we dissent.